FortiGate

VM on OCB Flex Engine Installation and Deployment Guide

24th September 2021

Version 4.0

document control

date	version no.	author	change/addition
6th December 2018	1.0	Ahmad Samak	Creation
1st February 2020	2.0	Ahmad Samak	Update the installation process of FortiGate VM on OCB FE.
20th September 2021	3.0	Ahmad Samak	Adding the initial network interfaces configuration steps of fortigate ECS, static Mode configuration as a work around to fixe the DHCP issue on OCB FE
24th September 2021	4.0	David Bignell	Add section 6 Solution Configuration copied from separate FortiGate on OCB FE Configuration Guide v2 from 1st Feb 2020

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-install50.pdf#M8.9.51917.Chapter.Title.FortiGate.VM.Deployment
[2]	Fortigate System administration Guide	https://docs.fortinet.com/uploaded/files/1052/fortigate-system-admin-40-mr3.pdf

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.

Guide Scope

This document describes how to deploy a FortiGate virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance. This document assumes:

- you have already successfully installed the virtualization server on the physical machine,
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started.

3 FortiGate VM Overview

Organizations generally move to the public cloud with the goals of increasing scale and reducing time to deployment. Achieving these goals requires application architectures built specifically for the public cloud. Before you can architect for the public cloud, you must understand how it is different from traditional on-premises environments.

3.1 ForiGate VM models and Licensing

Fortinet offers the FortiGate VM in five virtual appliance models determined by license. When configuring your FortiGate VM, be sure to configure hardware settings within the ranges outlined in Table 1. Contact your Fortinet Authorized Reseller for more information.

Table 1: FortiGate VM model information

Technical Specification	FG-VM00	FG-VM01	FG-VM02	FG-VM04	FG-VM08
Virtual CPUs (min/max)	1/1	1/1	1/2	1/4	1/8
Virtual Network Interfaces (min/max)	2 / 10				
Virtual Memory (min/max)	1 GB / 1 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB	1 GB / 12 GB
Virtual Storage (min/max)	30 GB / 2 TB				
Managed Wireless Access Points (tunnel mode / global)	32 / 32	32 / 64	256 / 512	256 / 512	1024 / 4096
Virtual Domains (default / max)	1 / 1	10 / 10	10 / 25	10 / 50	10 / 250

After placing an order for FortiGate VM, a license registration code is sent to the email address used on the order form. Use the registration number provided to register the FortiGate VM with Customer Service & Support and then download the license file. Once the license file is uploaded to the FortiGate VM and validated, your FortiGate VM appliance is fully functional.

3.2 Register FortiGate VM with Customer Service and Support

To obtain the FortiGate VM license file you must first register your FortiGate VM with Customer Service & Support.To register your FortiGate VM:

1.Log in to the Customer Service & Support portal using an existing support account or select Sign Up to create a new account.

2.In the main page, under Asset, select Register/Renew.The Registration page opens.

3.Enter the registration code that was emailed to you and select Register. A registration form will display.

4.After completing the form, a registration acknowledgement page will appear.

5.Select the License File Download link.

6.You will be prompted to save the license file (.lic) to your local computer.

3.3 Deployment package contents

KVM

The FORTINET.out.kvm.zip contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

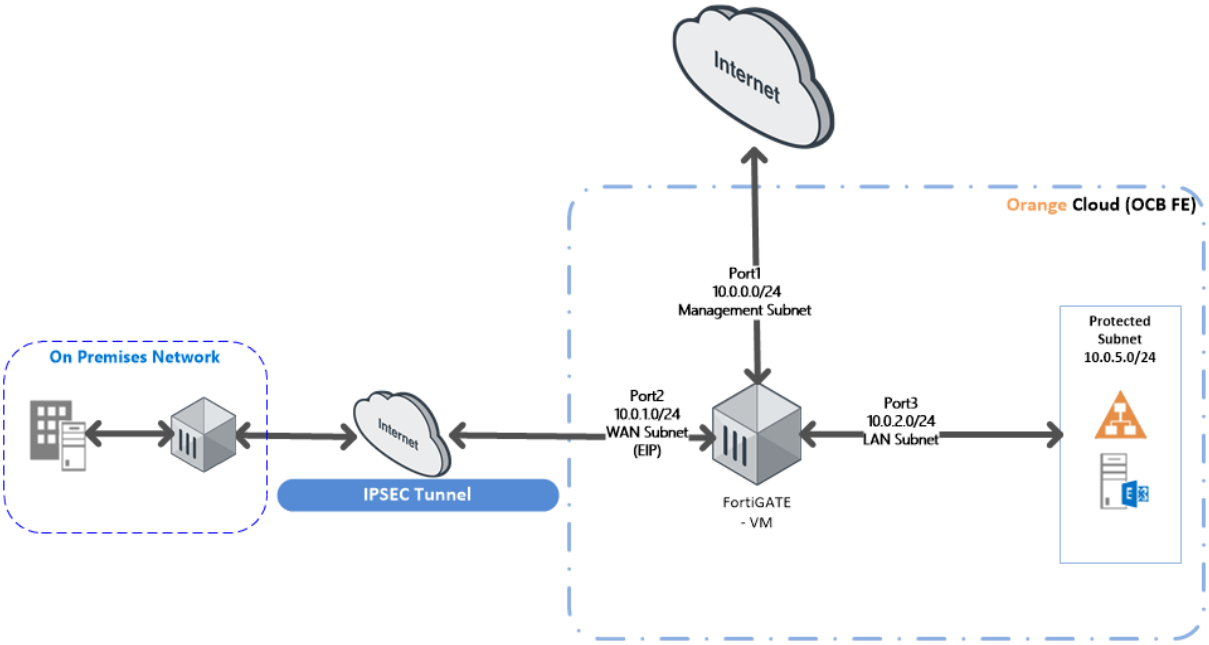
- create a 30GB log disk
- specify the virtual hardware settings

4 Deployment Methods

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

4.1 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.



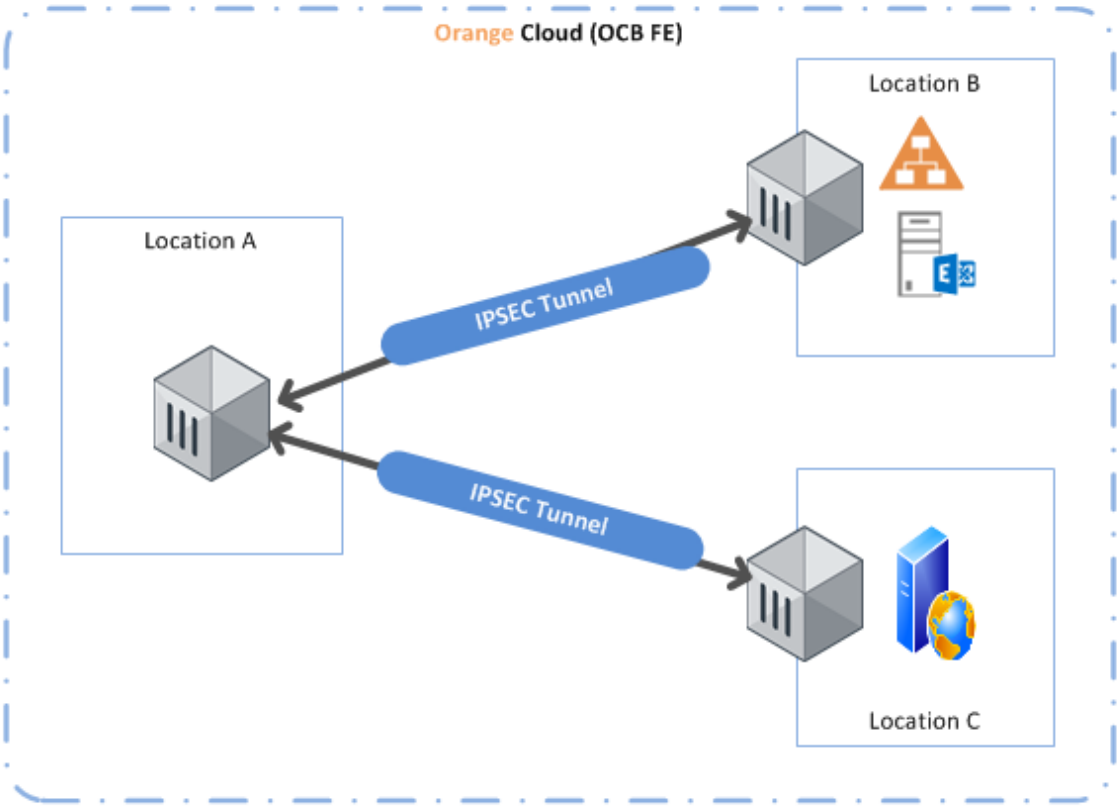
• Inter-Subnet —The Fortigate firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.

• Gateway—The Fortigate 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.

4.2 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.

5 Deploy the VM-Series Firewall on Orange Flex Engine

In our scenarios we have 3 VPC's

- FG VPC that will host FortiGate VM Firewall
- Business VPC hosting active directory and exchange servers
- Web VPC hosting a webserver.

5.1 Create VPC

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

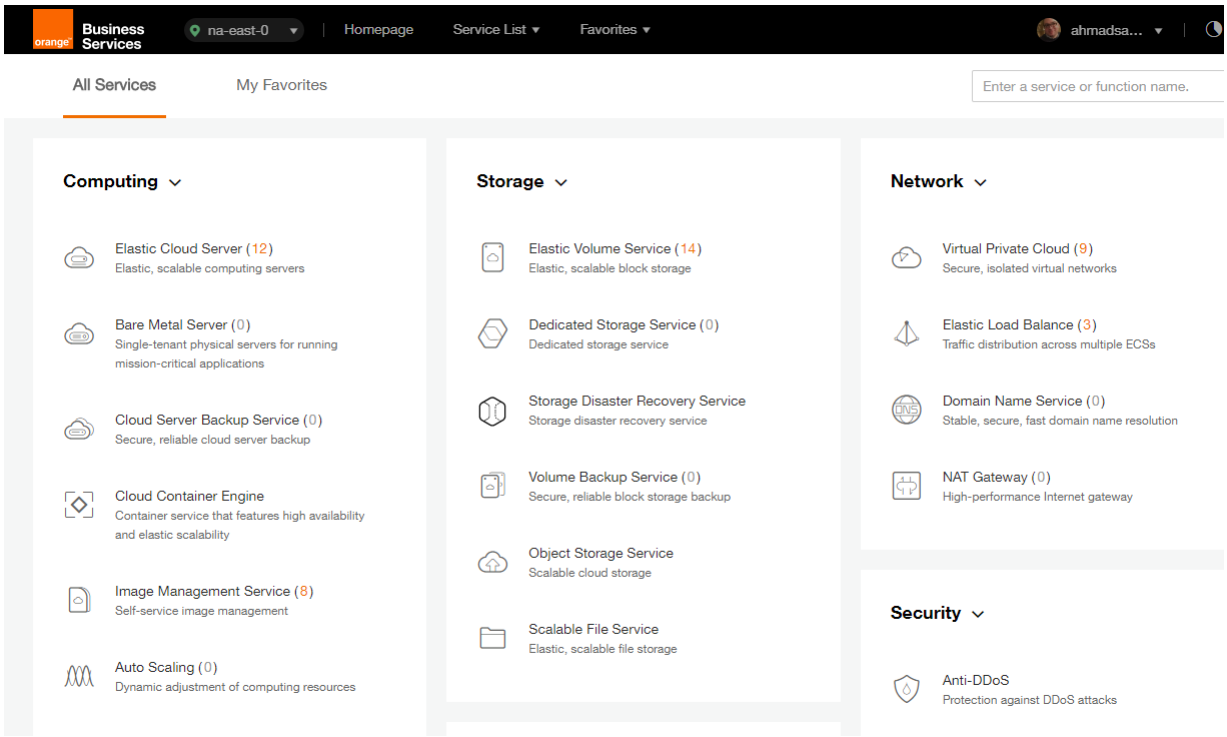
To use a VPC, first create it by following the procedure provided in this section. Then, create subnets, security groups, and VPNs, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

In our solution . You will have to create 1 VPC containing 3 or more Subnets.

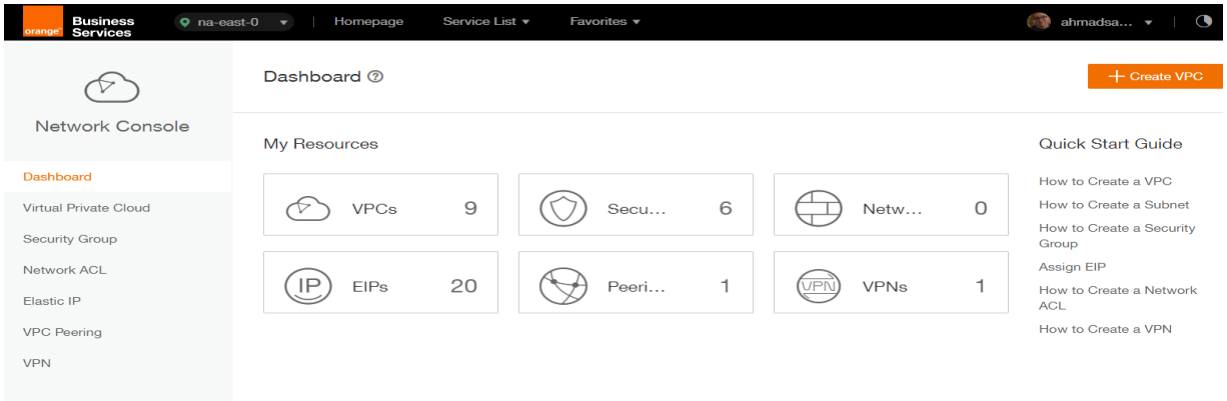
- Management Subnet
- Internet Facing Subnet
- LAN Subnet
- Protected Subnet

Procedure

1. Log in to the management console.
2. On the console homepage, under Network, click Virtual Private Cloud.



3. On the **Dashboard** page, click **Create VPC**.



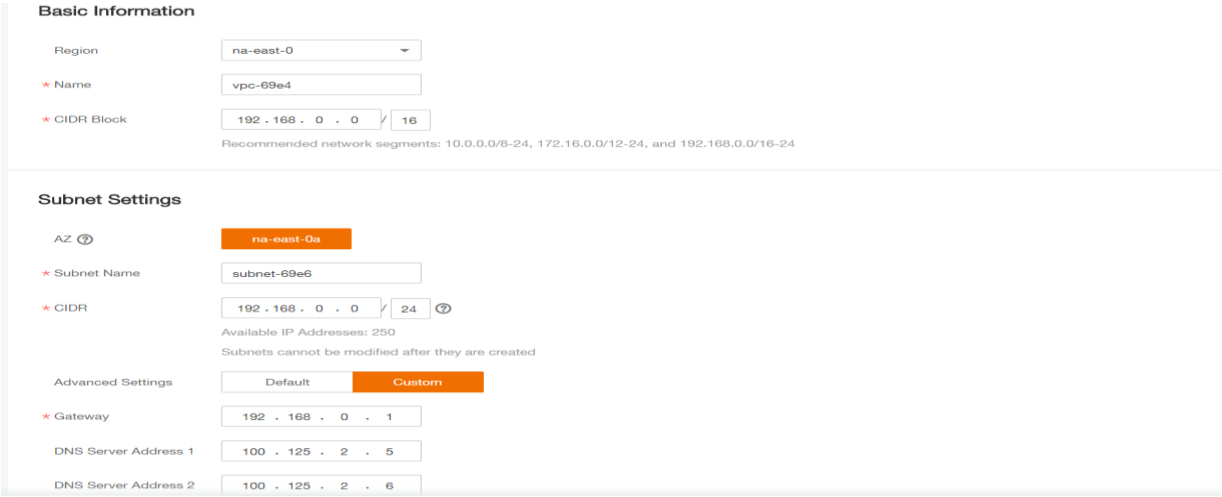
On the displayed **Apply for VPC** page, set the parameters as prompted.

Table 1 Parameter description

Parameter	Description	Example Value
Name	Specifies the VPC name.	VPC-001
VPC CIDR	Specifies the Classless Inter-Domain Routing (CIDR) block for the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset (for multiple subnets in the VPC).	192.168.0.0/16

Table 1 Parameter description

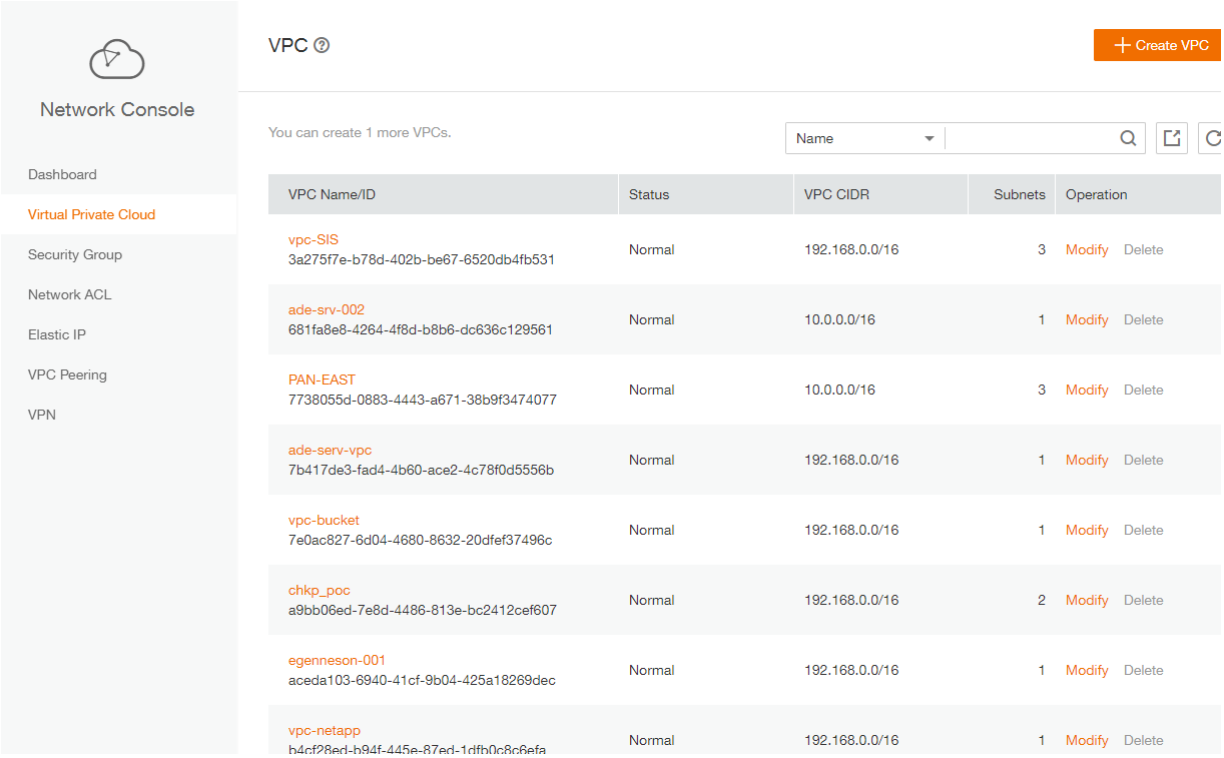
Parameter	Description	Example Value
	The following CIDR blocks are supported: 10.0.0.0/8–24 172.16.0.0/12–24 192.168.0.0/16–24	
Name	Specifies the subnet name.	Subnet-001
CIDR	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.	192.168.0.0/24
Gateway	Specifies the gateway address of the subnet.	192.168.0.1



4. The external DNS server address is used by default. If you need to change the DNS server address, click **Show Advanced Settings** and configure the DNS server addresses. You must ensure that the configured DNS server addresses are available.

5. Click **Create Now**.

   The created VPC will be shown in the VPC List

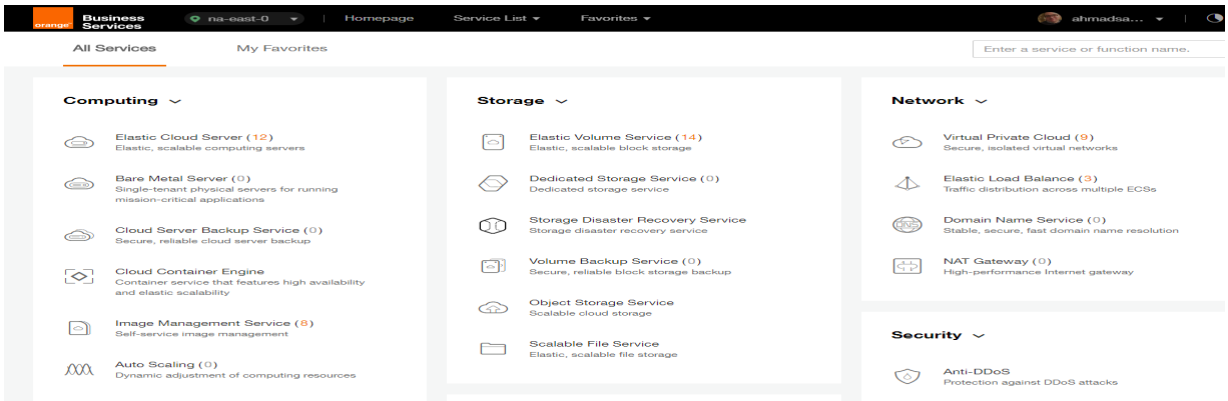


5.2 Install FortiGate VM on the VPC

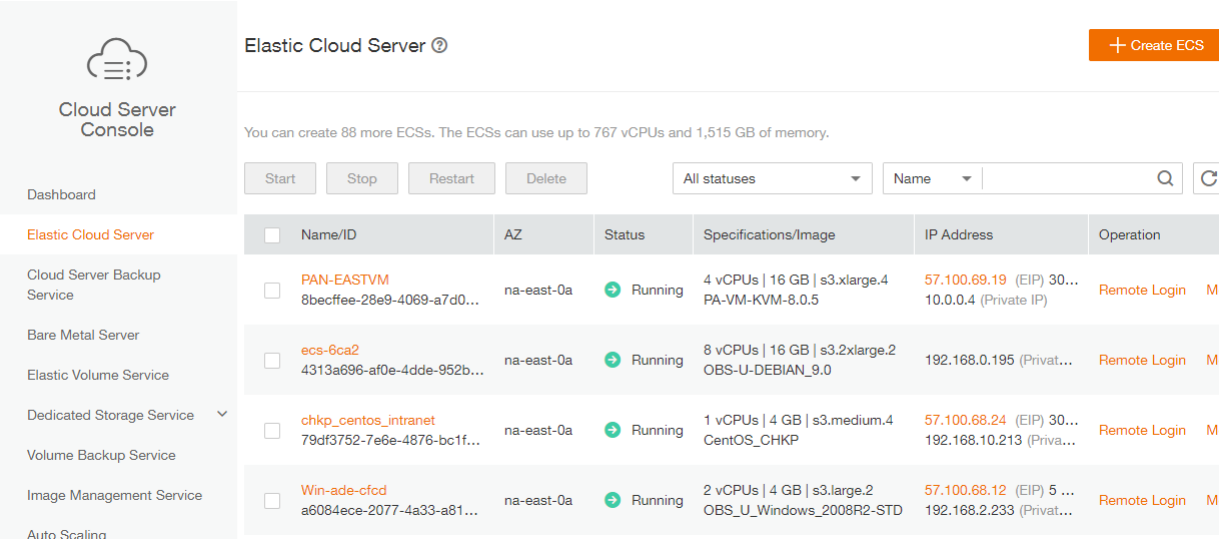
ECSs are more cost-effective than physical servers. Within minutes, you can obtain ECS resources from the public cloud. ECS resources are flexible and on-demand. This section describes how to create an ECS.

1. Log in to the management console.

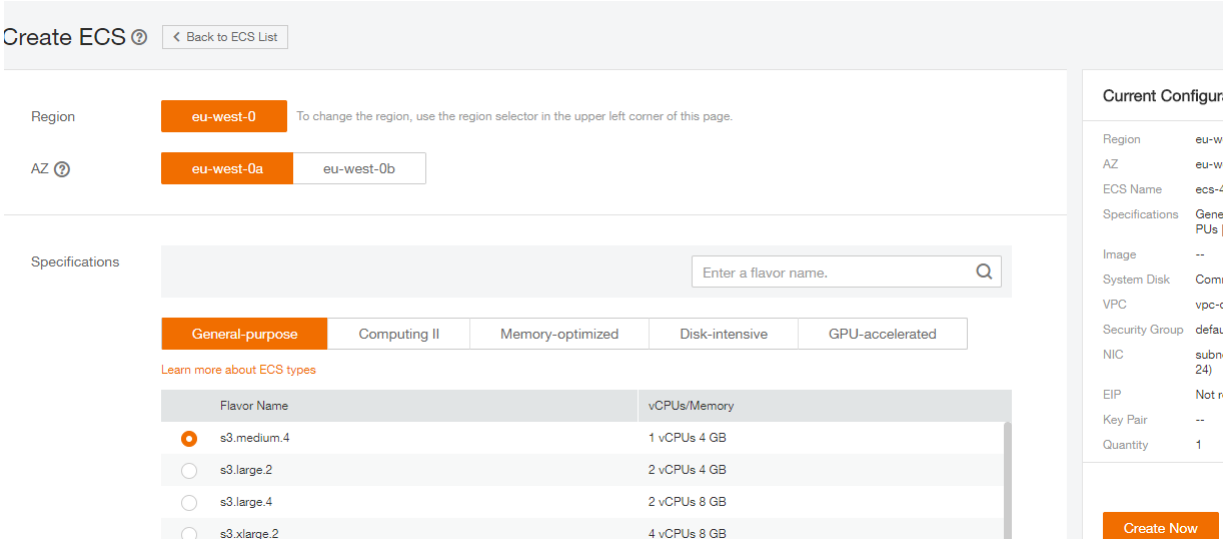
2. Under **Computing**, click **Elastic Cloud Server**.



3. Click **Create ECS**.



The ECS creation page is displayed.



4. Confirm the region.

If the region is incorrect, click  in the upper left corner of the page for correction.

5. Select an AZ.

An AZ is a physical region where power and networks are physically isolated. AZs in the same region can communicate with each other over an intranet.

1. To enhance application availability, create ECSs in different AZs.
2. To shorten network latency, create ECSs in the same AZ.

6. Click  to open the **Select Specifications** page. On the page, select an ECS type.

7. Set **Local-Disk**.

   This parameter is optional and is automatically displayed when you use a local disk.

   A local disk specifies the local storage for the physical host where the ECS is deployed. Only hard disk drives (HDDs) are supported. If you select the disk-intensive ECS type, the system automatically attaches local disks to the ECS.

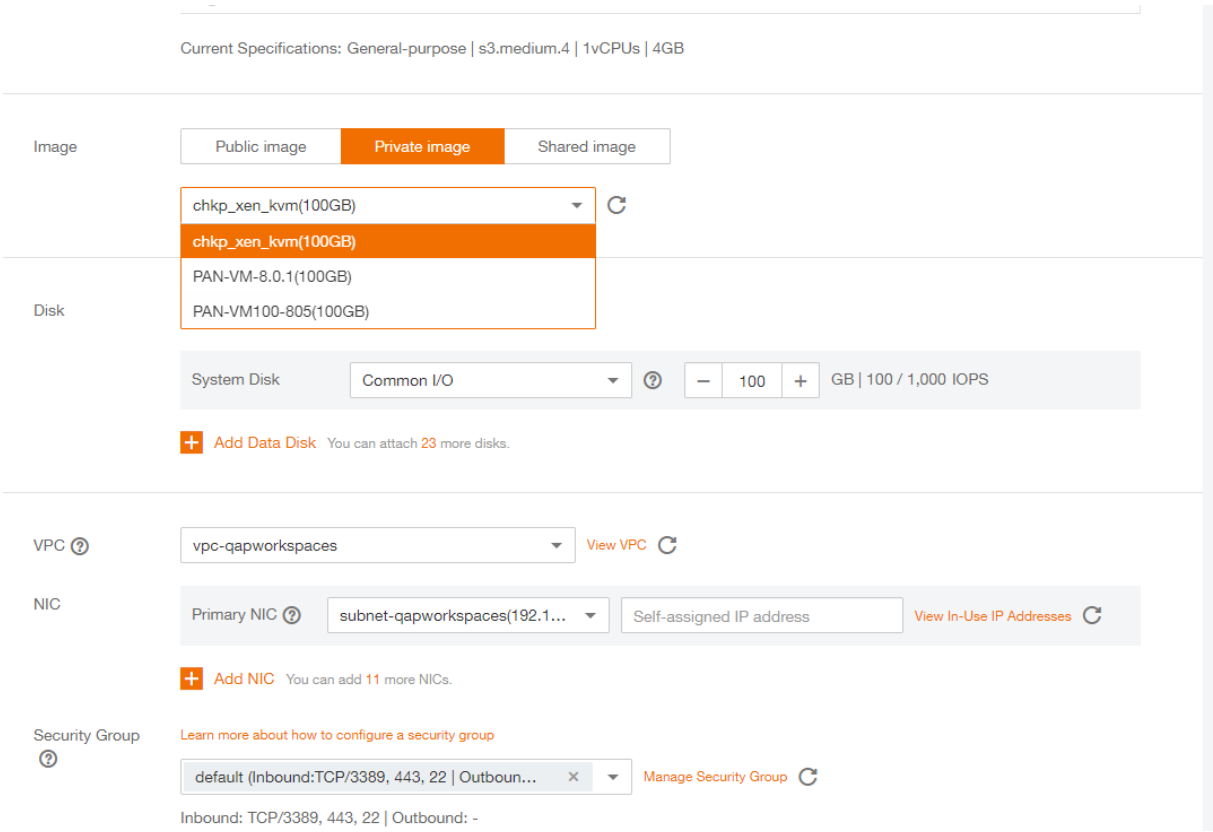
   For example, if the Local Disk value is 3 x 1800 GB, three HDDs are attached to the ECS and the capacity of each HDD is 1800 GB.

8. Click **Image**.

   Private Image

   A private image is an image available only to the user who creates it. It contains an OS, preinstalled public applications, and the user's private applications. Using a private image to create ECSs removes the need to configure multiple ECSs repeatedly.

   In our installation we previuosly uploaded a KVM image for Fortigate VM . to check how to upload a private image to certain region please check the URL: https://docs.prod-cloud-ocb.orange-business.com/en-us/usermanual/ims/en-us_topic_0030713190.html



9. Set **Disk**.

A disk can be a system disk or a data disk. You can create multiple data disks for an ECS and customize their disk sizes.

10. Set network parameters, including VPC, Security Group, and NIC.

When you use VPC for the first time, the system automatically creates a VPC for you, including the security group and NIC.

Table 2 Parameter descriptions

Parameter	Description
VPC	Provides a network, including subnet and security group, for an ECS. You can select an existing VPC, or click **View VPC** and create a desired one. For more information about VPC, see *Virtual Private Cloud User Guide*. **NOTE:** DHCP must be enabled in the VPC to which the ECS belongs.
Security Group	Controls instance access within or between security groups by defining access rules. This enhances instance security. When creating an ECS, you can select multiple (recommended not more than five) security groups. In such a case, the access rules of all the selected security groups apply on the ECS. **NOTE:** Before initializing an ECS, ensure that the security group rule in the outbound direction meets the following requirements: • **Protocol**: **TCP** • **Port Range**: **80** • **Remote End**: **169.254.0.0/16** If you use the default security group rule in the outbound direction, the preceding requirements are met, and the ECS can be initialized. The default security group rule in the outbound direction is as follows: • **Protocol**: **ANY** • **Port Range**: **ANY** • **Remote End**: **0.0.0.0/16**
NIC	Consists of a primary NIC and one or more extension NICs. **MTU Settings**: optional If your ECS is of M2, large-memory, H1, or D1 type, you can click **MTU Settings** to configure the maximum transmission unit (MTU) for a to-be-added extension NIC for improving network performance. An MTU can only be a number, ranging from 1280 to 8888.
EIP	A static public IP address bound to an ECS in a VPC. Using the EIP, the ECS provides services externally. The following options are provided:

Table 2 Parameter descriptions

Parameter	Description
	• **Do not use** Without an EIP, the ECS cannot access the Internet and is used only in the private network or cluster. • **Automatically assign** The system automatically assigns an EIP for the ECS. The EIP provides exclusive bandwidth that is configurable. • **Specify** An existing EIP is assigned for the ECS. When using an existing EIP, you cannot create ECSs in batches. ** In our scenario: We assigned 2 EIP's one for the management NIC and the other for the Internet Facing NIC.

11. Set ECS Name.

    If you want to create multiple ECSs at a time, the system automatically sequences these ECSs.

12. Configure the number of ECSs to be created.

    After the configuration, click Price Calculator to view the ECS configuration fee.

13. Click Create Now.

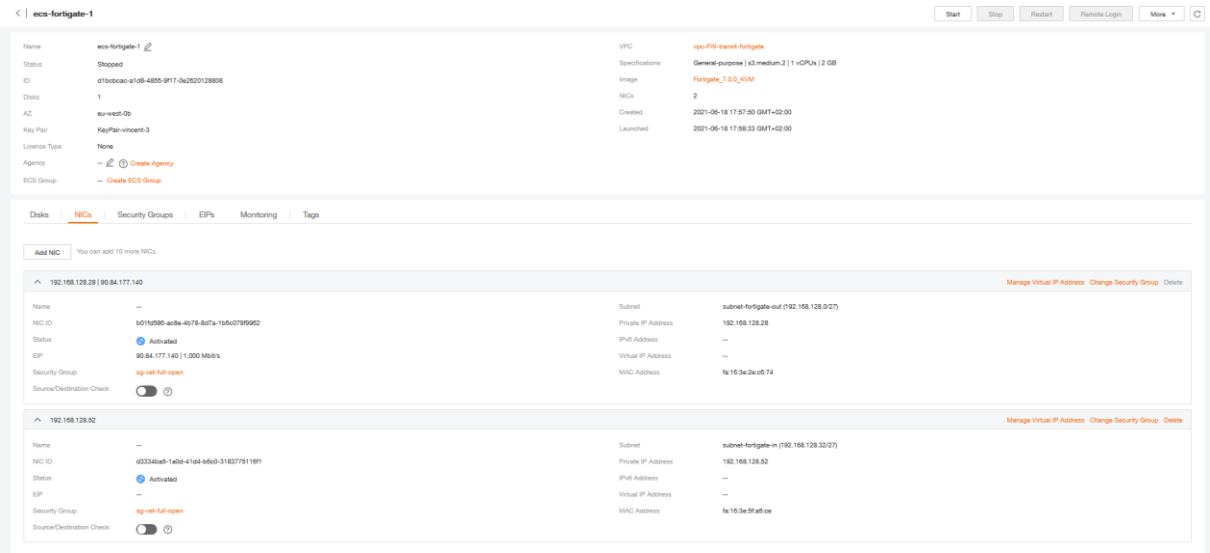
14. On the ECS specification confirmation page, confirm the ECS specifications and click Submit.

    After the ECS is created, you can view information about it on the Elastic Cloud Server page.

15. After creating the Fortigate VM you can access it through Https using the EIP of the Management NIC. (username: admin / no password)

5.3 Configure Network Interfaces manually

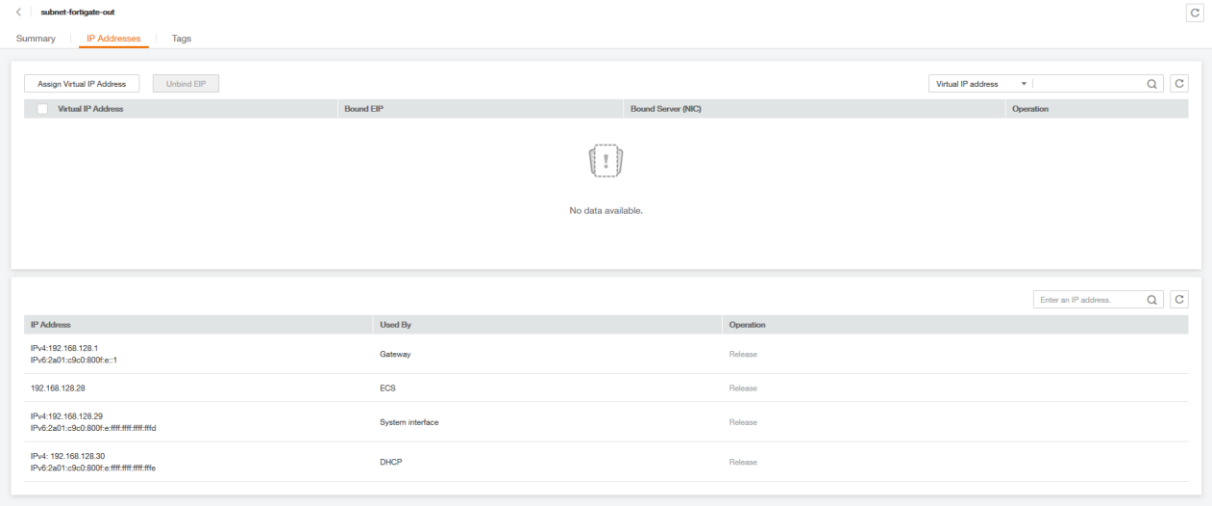
Fortigate DHCP client is currently not compatible with FE DHCP service.
To configure network interfaces (NIC) of a Fortigate ECS, static mode configuration is required.
IP addresses associated with Fortigate ECS NIC in FE console must be used for this manual configuration.
Those IP addresses can be retrieved on the Cloud Server Console page, in Fortigate ECS description (NIC tab) :



In this example, IP address of main NIC is 192.168.128.28 in subnet 192.168.128.0/27(255.255.255.224) and IP address of extension NIC is 192.168.128.52 in subnet 192.168.128.32/27(255.255.255.224).

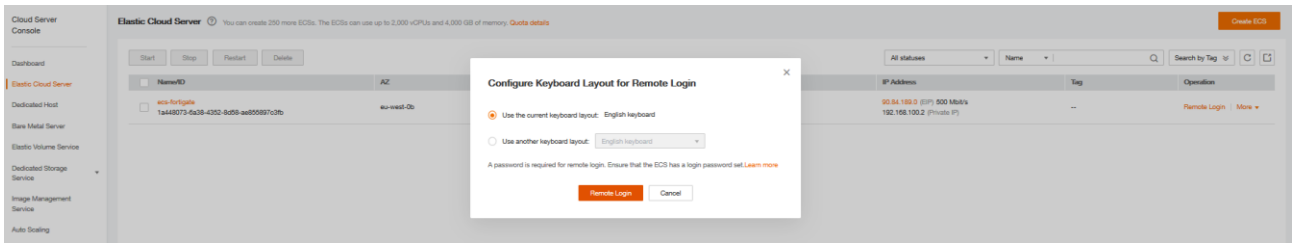
Note that “Source/Destination Check” option must disactivated on all Fortigate ECS NIC.

The address of the main NIC subnet gateway can be retrieved on the Network Console, in the main NIC subnet description:

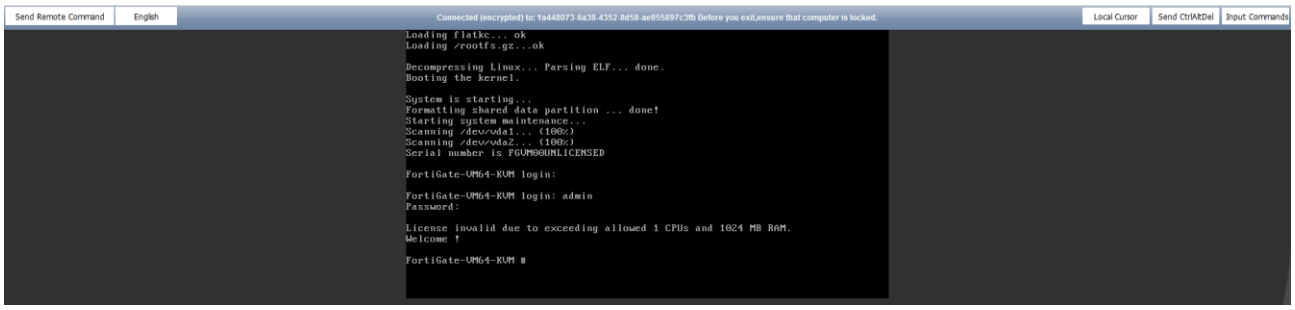


In this example, the subnet gateway address is 192.168.128.1.

To configure Fortigate ECS NIC in static mode, connect to ECS using “Remote Login” on Cloud Server Console:



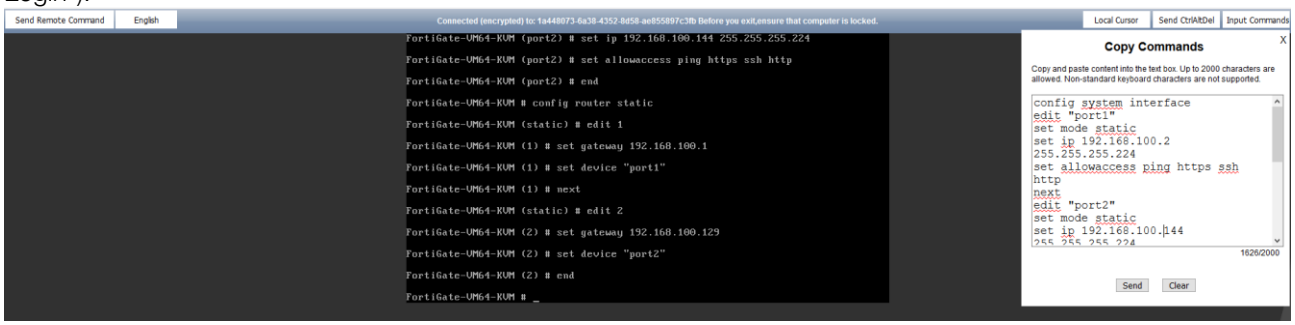
In “Remote Login” console, log in to Fortigate instance using login “admin” and empty password:



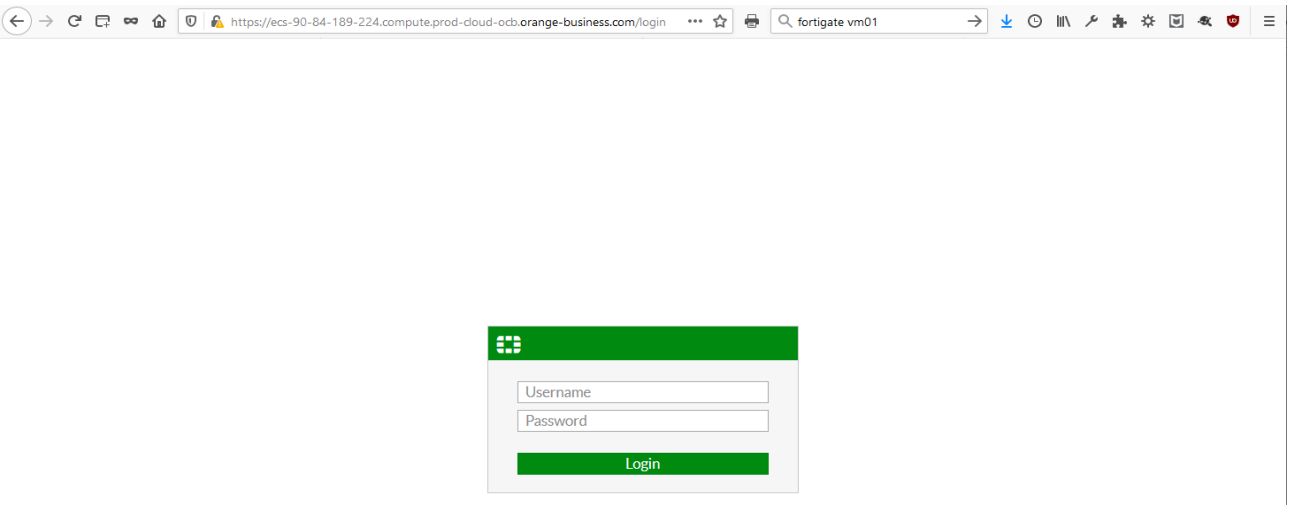
Once logged in, type in the following commands to configure Fortigate ECS NIC with addresses captured previously:

config system interface
edit "port1"
set mode static
set ip 192.168.128.28 255.255.255.224
set allowaccess ping https ssh http
next
edit "port2"
set mode static
set ip 192.168.128.52 255.255.255.224
set allowaccess ping https ssh http
end
config router static
edit 1
set gateway 192.168.128.1
set device "port1"
end

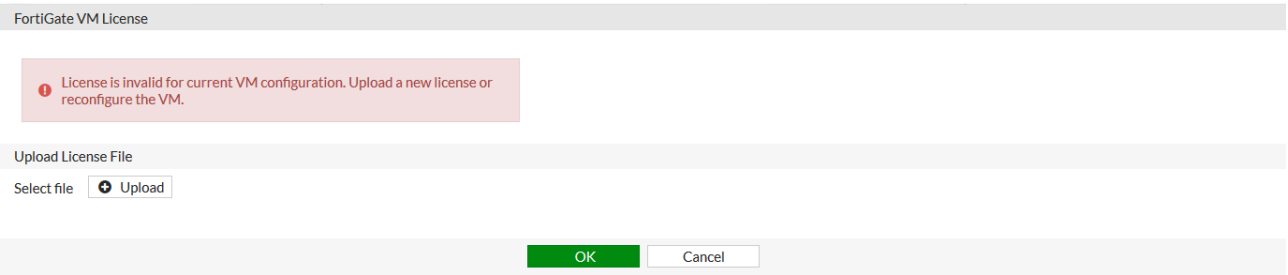
To ease this, use “Input Commands” button (available if you select “English keyboard” layout for “Remote Login”):



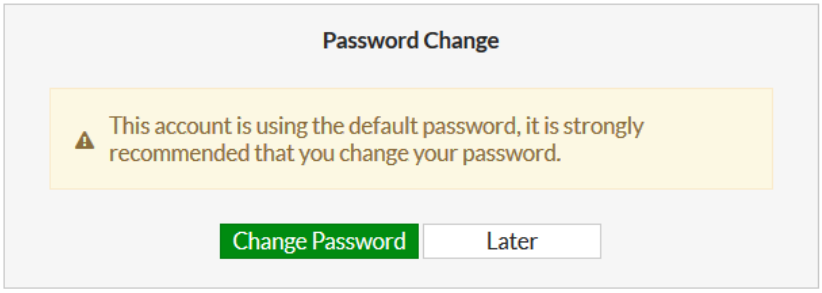
Once NIC configuration done, you can connect to Fortigate Web Console, using reverse DNS name of EIP associated with ECS main NIC (example: EIP=90.84.189.224 => reverse DNS=ecs-90-84-189-224.compute.prod-cloud-ocb.orange-business.com) :



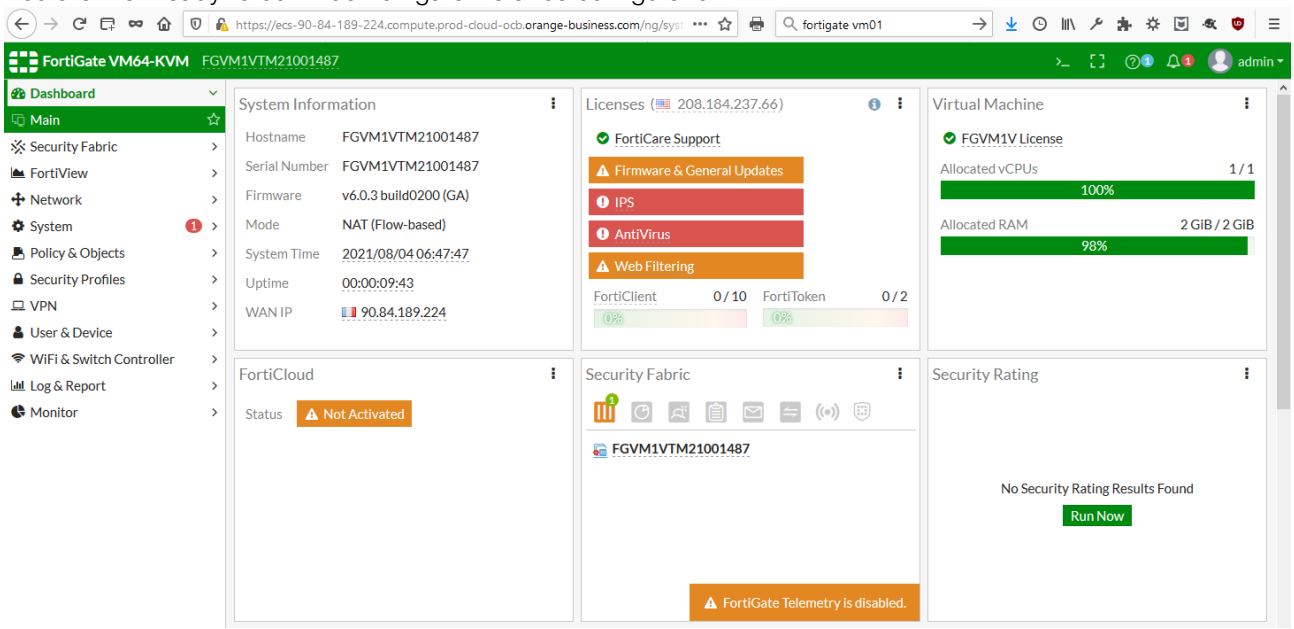
In Fortigate Web console, log in using userame “admin” and empty password:
Then upload your Fortigate licence:



Once license is installed, the Fortigate instance reboots and after login, you will need to change admin password:

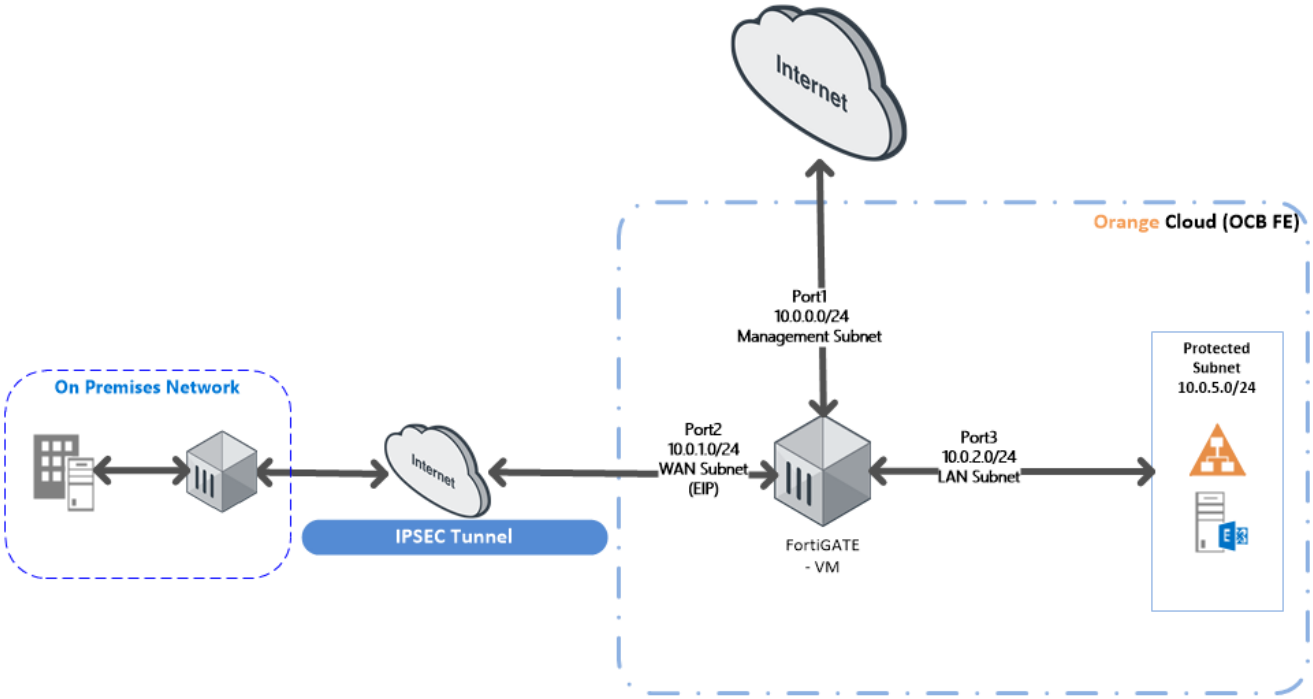


You are then ready to continue Fortigate instance configuration:



6 Solution Configuration

6.1 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.

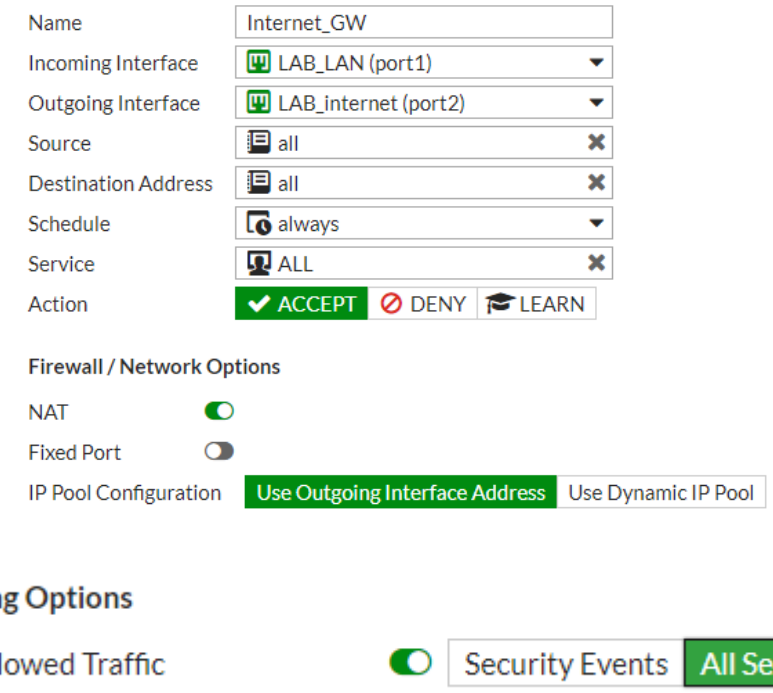
6.1.1 On Premises FortiGate configuration

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.

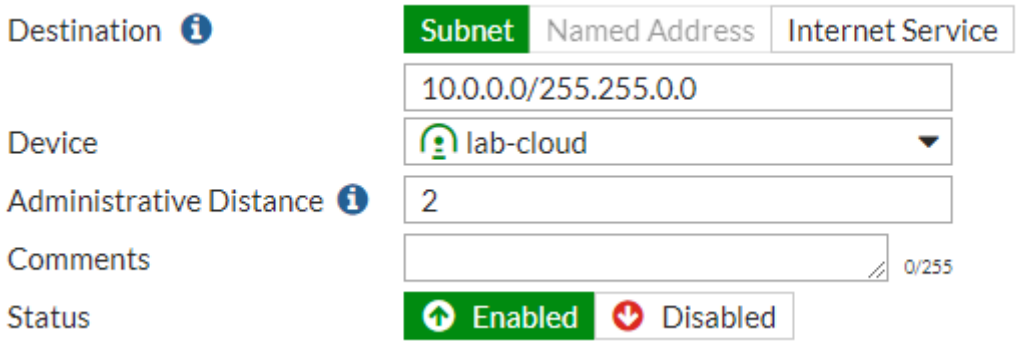
Go to Policy & Objects > IPv4 Policy and create a new policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet. Set the Incoming Interface to the internal interface (called internal on some FortiGate models) and the Outgoing Interface to the

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.



6.1.2 Create a Static Route for the VPN Connection

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

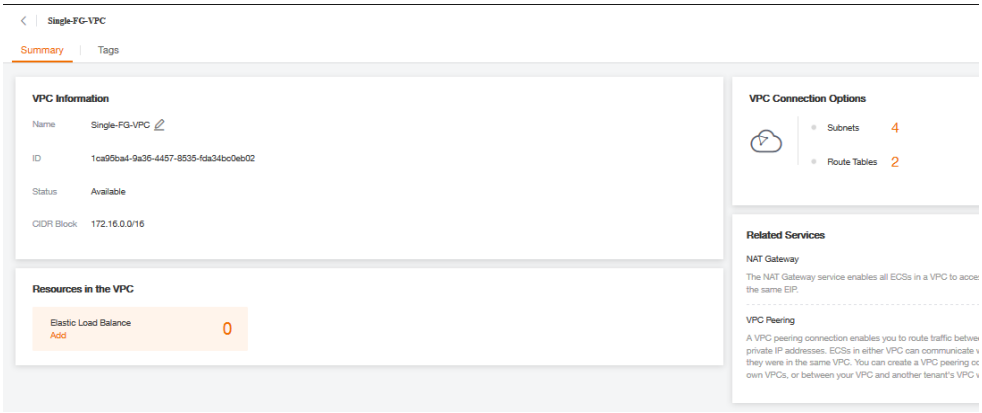


6.1.3 Create user defined routes on OCB FE VPC

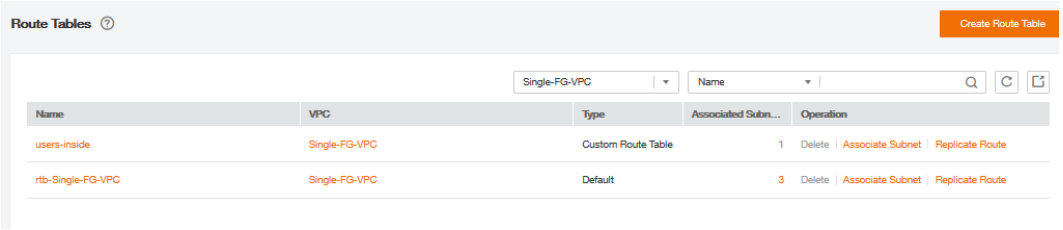
After applying the subnet level routing on OCB FE . We should have to add route table and create routes and associate to the internal (Protected subnet.

1- From Network > Virtual Private Cluod

2- Select your VPC

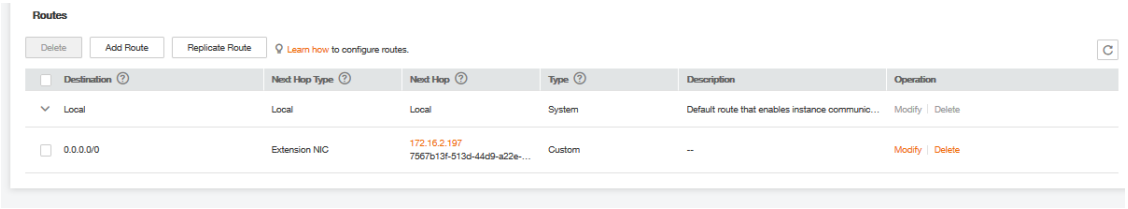


3- Choose route Tables

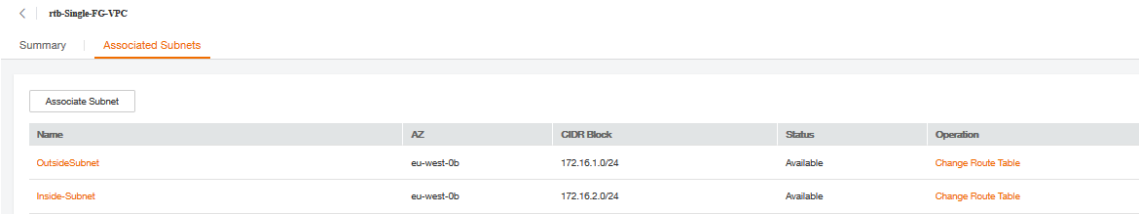


4- Select the route table of type Default

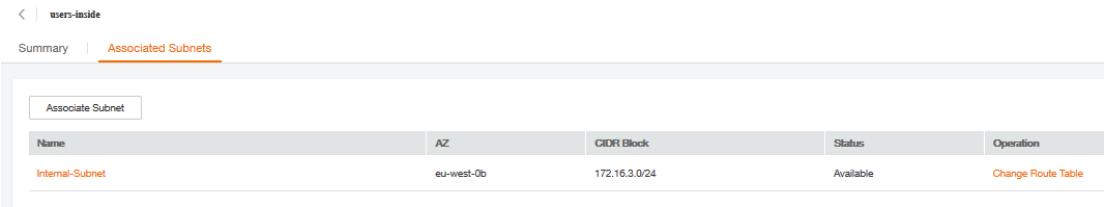
5- Add the following route



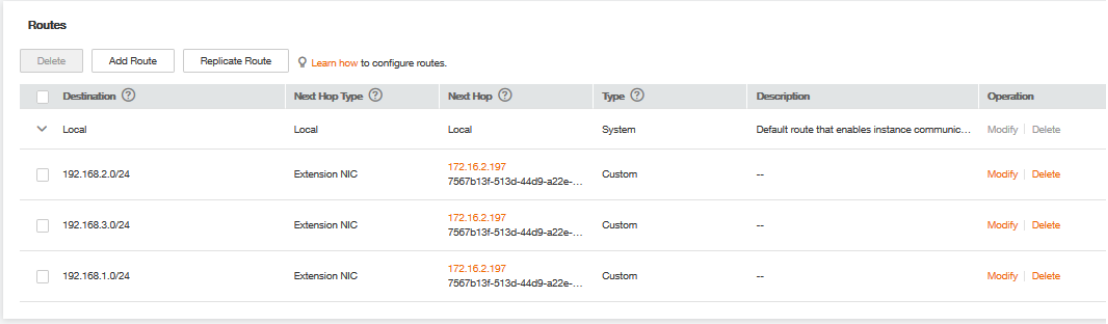
6- Make sure that the Default route table is associated to Internet facing and LAN Subnets.



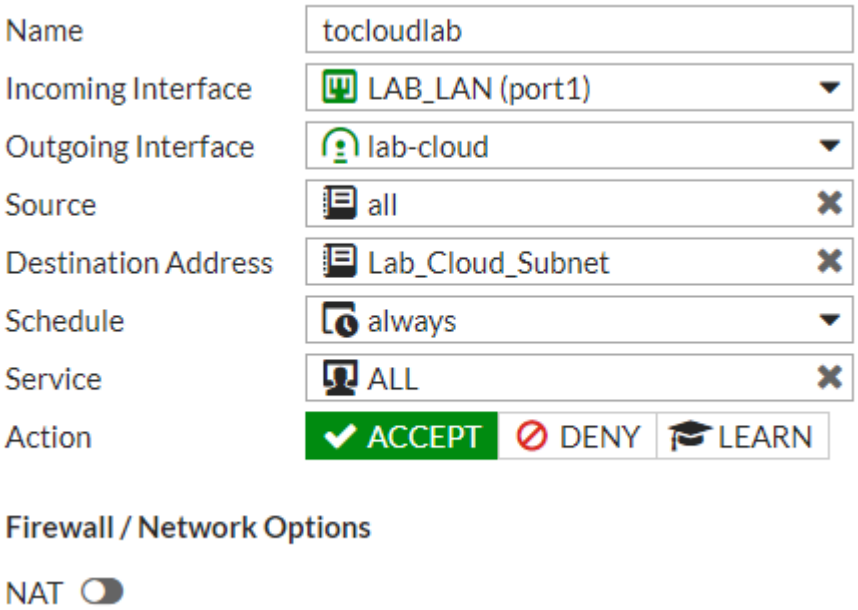
7- Create a new route table and associate to the Internal (Protected) Subnet

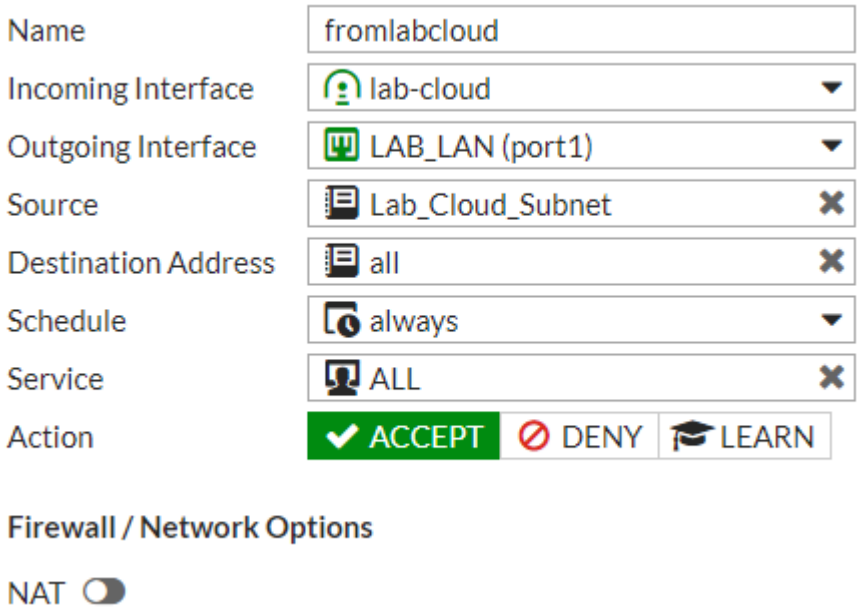


8- Add the following routes to the custom route table to allow traffic to the destination subnets (On premisis Subnets) through the Inside NIC.

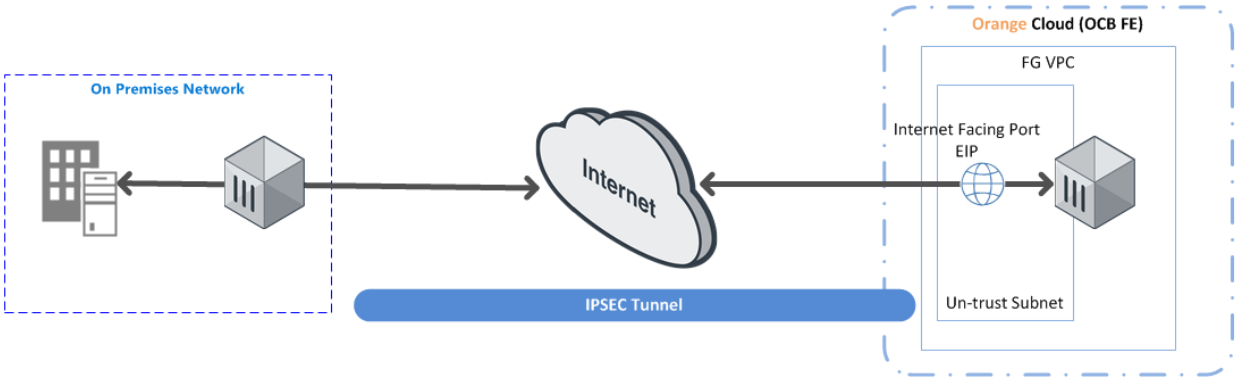


6.1.4 Creating Two policies to allow traffic from the internal network to OCB FE VPC and Vice Versa





6.2 Site-to-Site VPN-IPSEC Tunnel Configuration

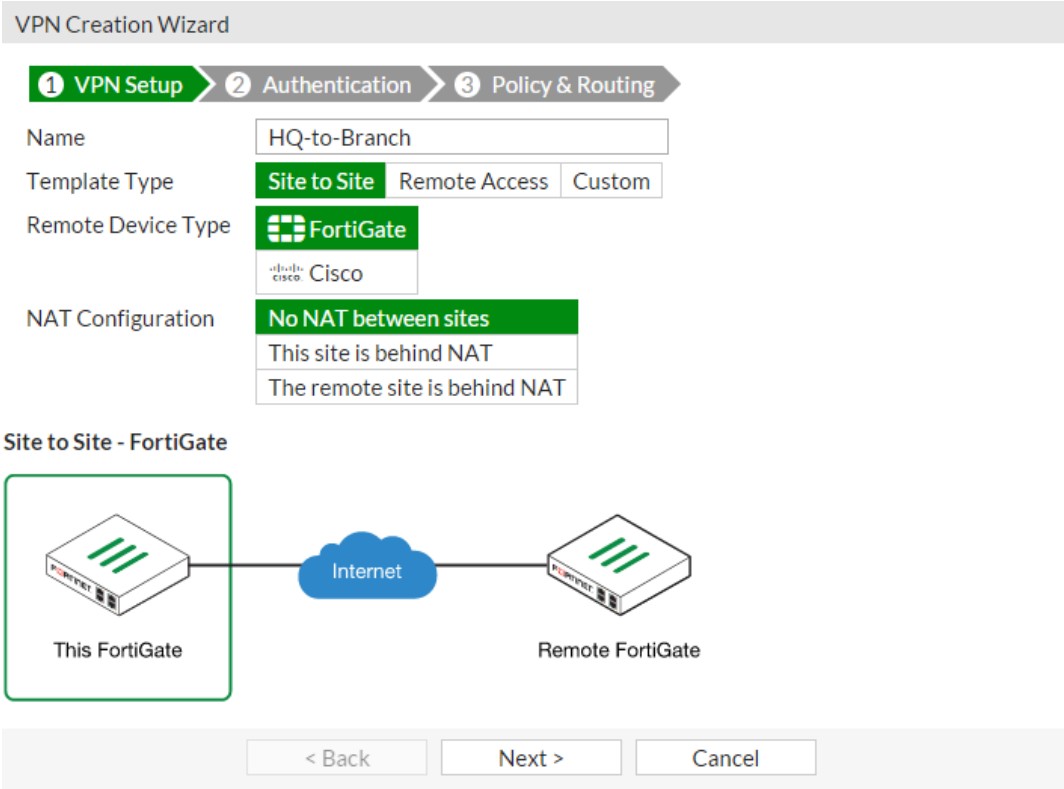


IPSec Tunnel configuration will be performed on Both the firewalls as per the diagram above,

6.2.1 Configuring the onprem. IPsec VPN

1. From the On premises FortiGate

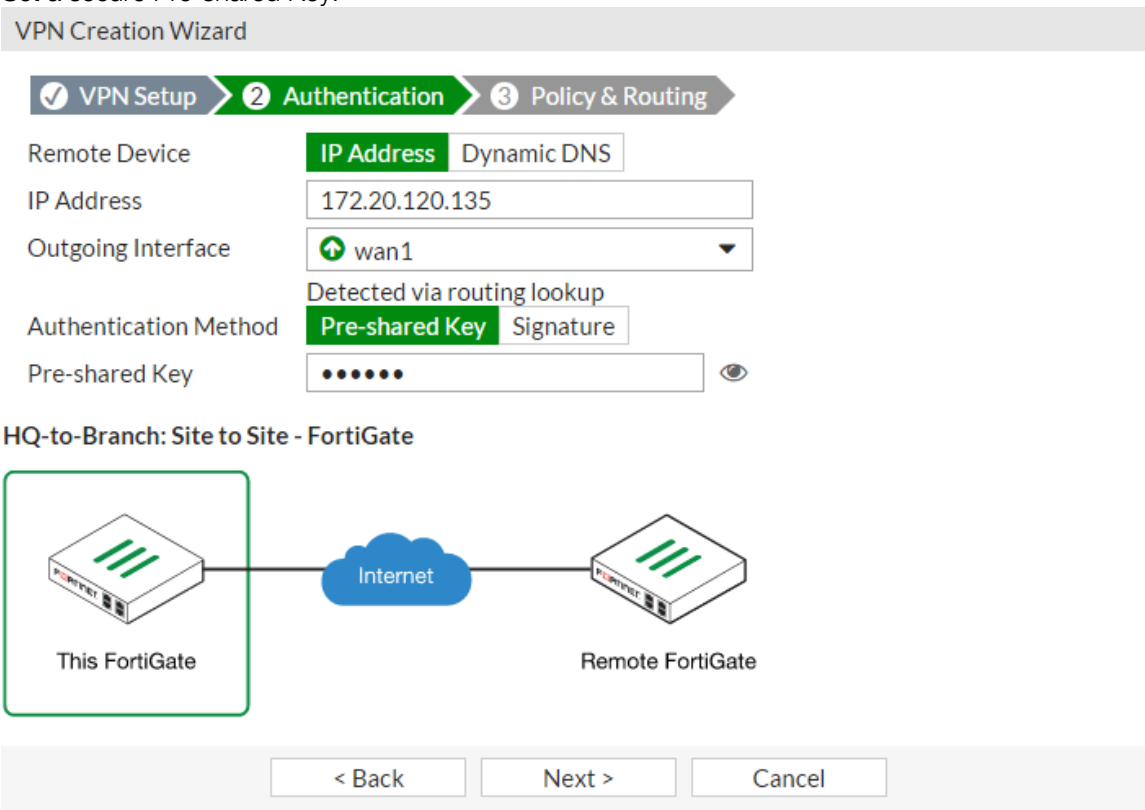
Go to VPN > IPSEC Wizard



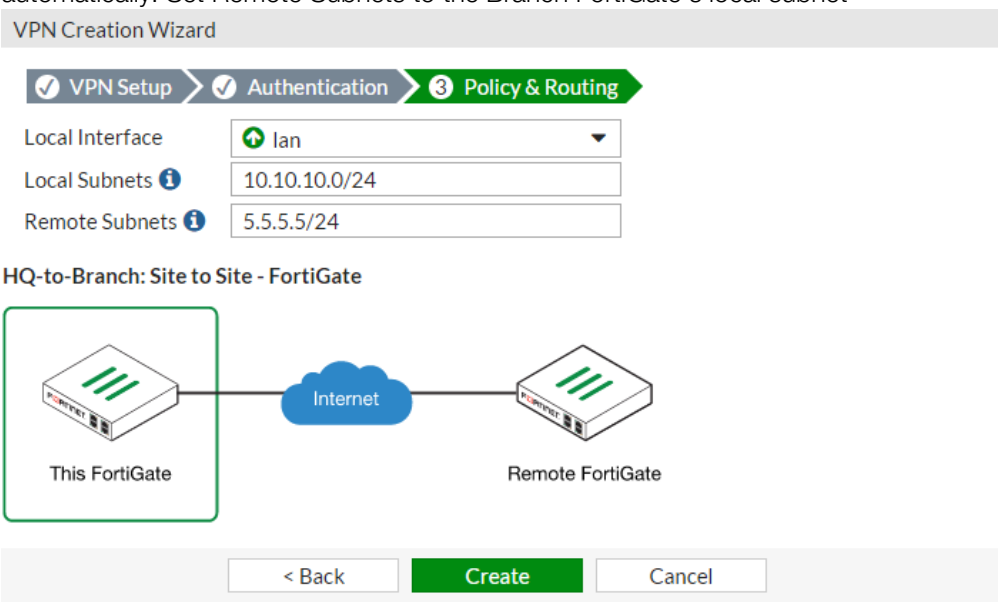
Select the **Site to Site** template, and select **FortiGate**

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.

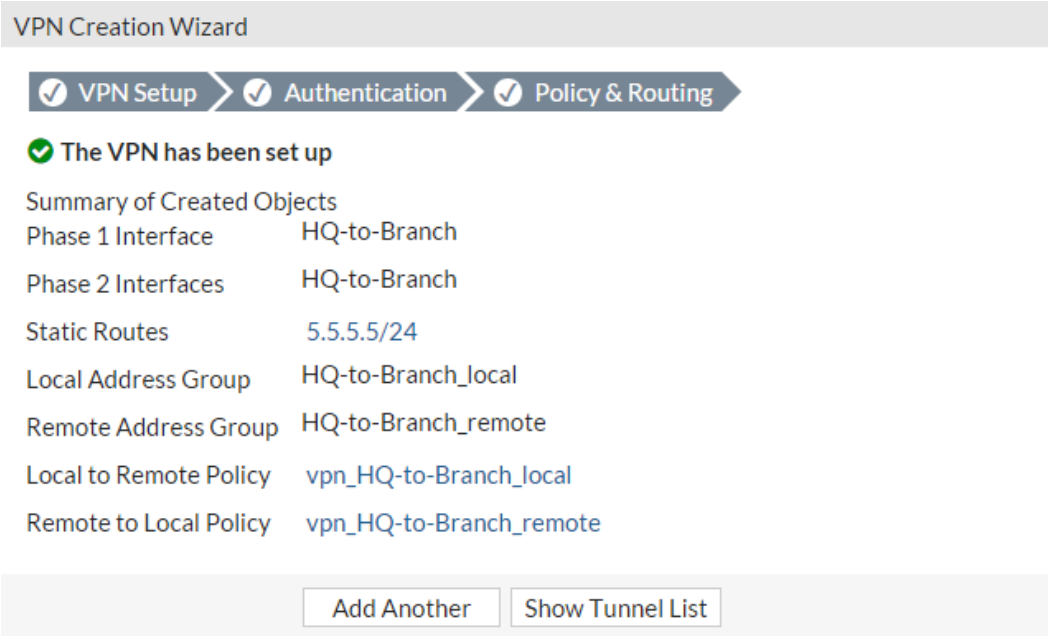
Set a secure Pre-shared Key.



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

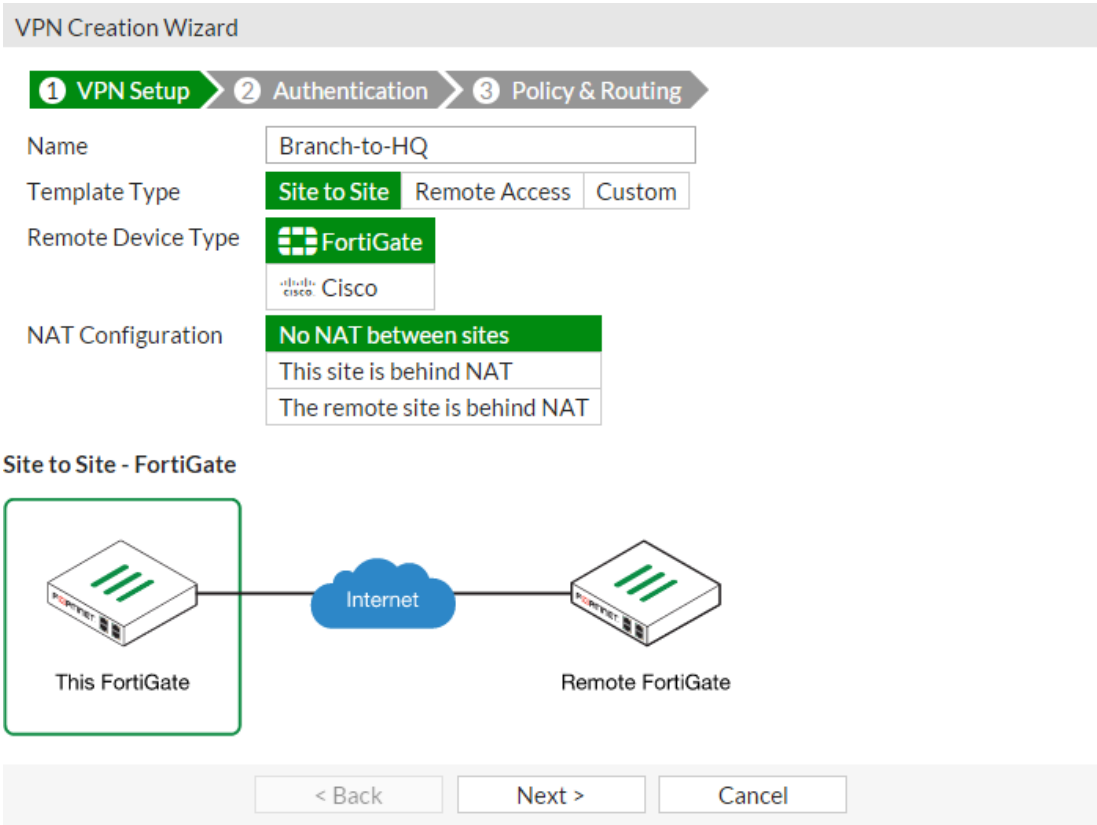


4. A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.

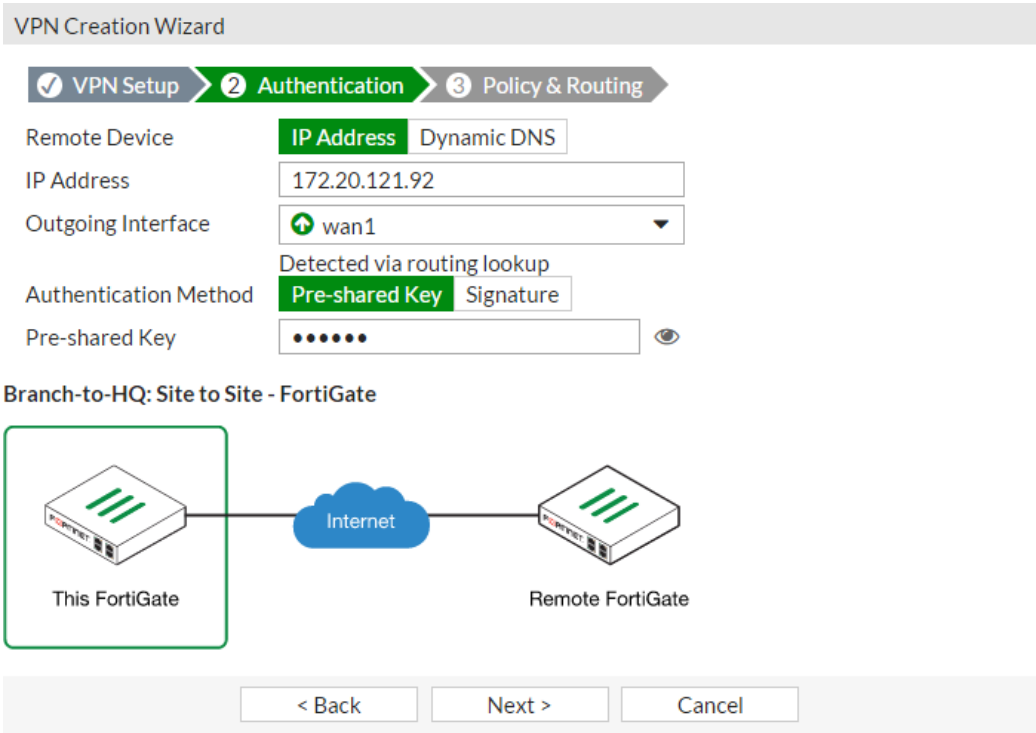


6.2.2 Configuring OCB FE IPSEC VPN

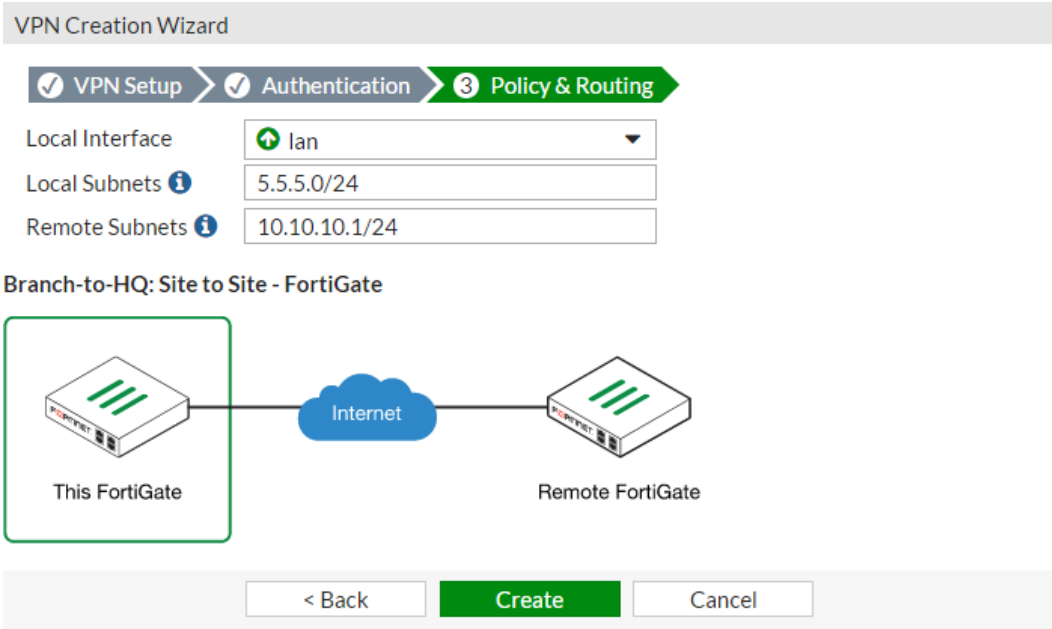
1. On the Branch FortiGate, go to **VPN > IPsec Wizard**. Select the **Site to Site** template, and select **FortiGate**



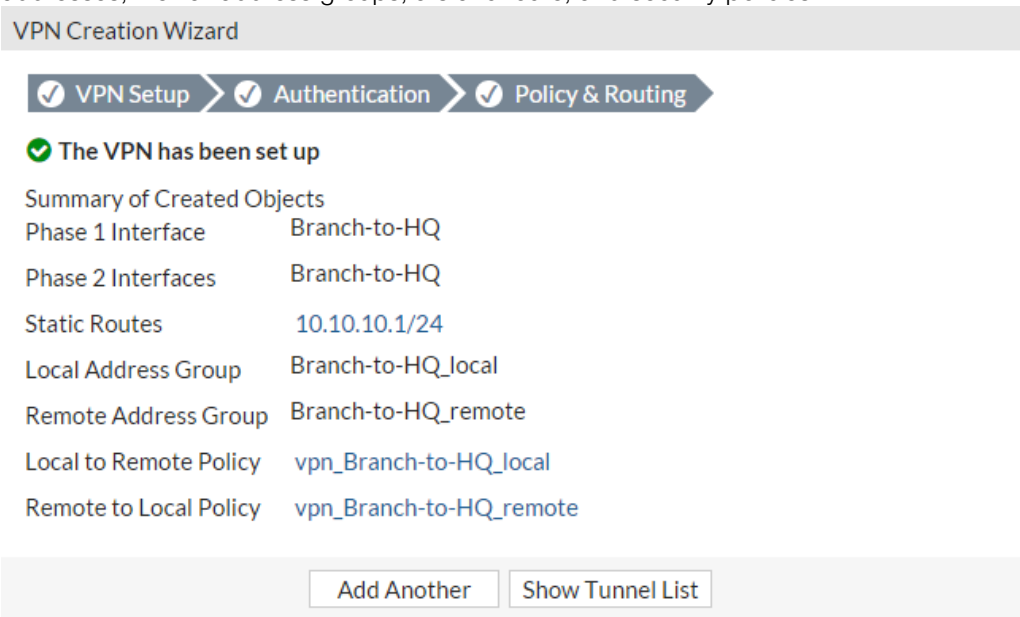
2. In the **Authentication** step, set **IP Address** to the IP of the on prem. FortiGate. After you enter the gateway, an available interface will be assigned as the Outgoing Interface. If you wish to use a different interface, select Change. Set the same Pre-shared Key that was used for HQ's VPN.



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

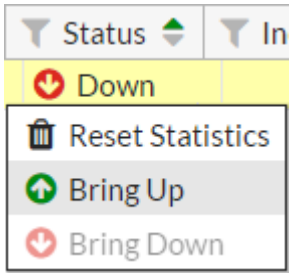


4. A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



6.2.3 Results

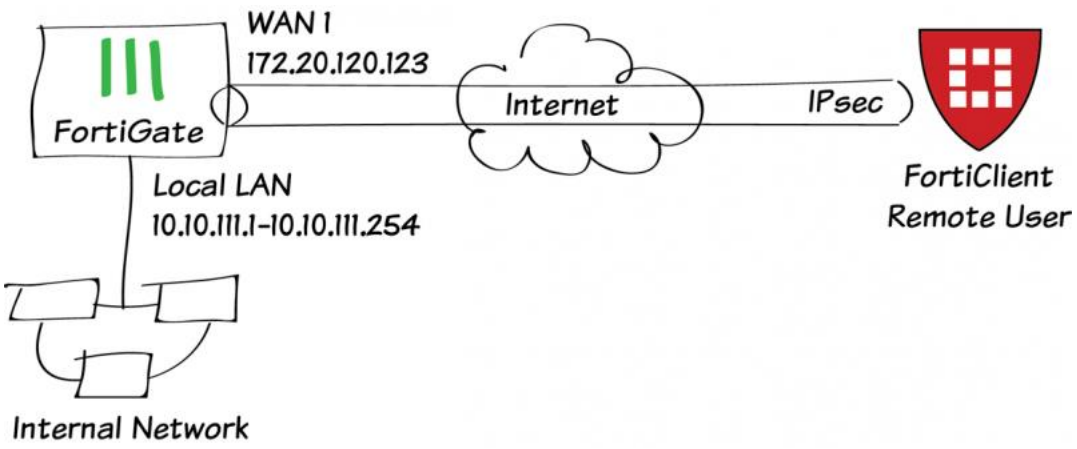
On either FortiGate, go to **Monitor** > **IPsec Monitor** to verify the status of the VPN tunnel. Right-click under **Status** and select **Bring Up**.



6.3 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.

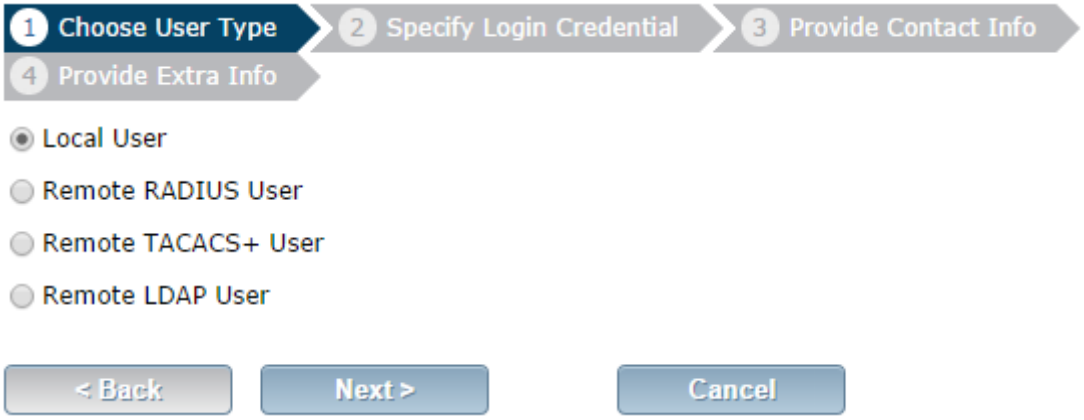
The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet. When the tunnel is configured, you will connect using the FortiClient application.



6.3.1 Creating a user group for remote users

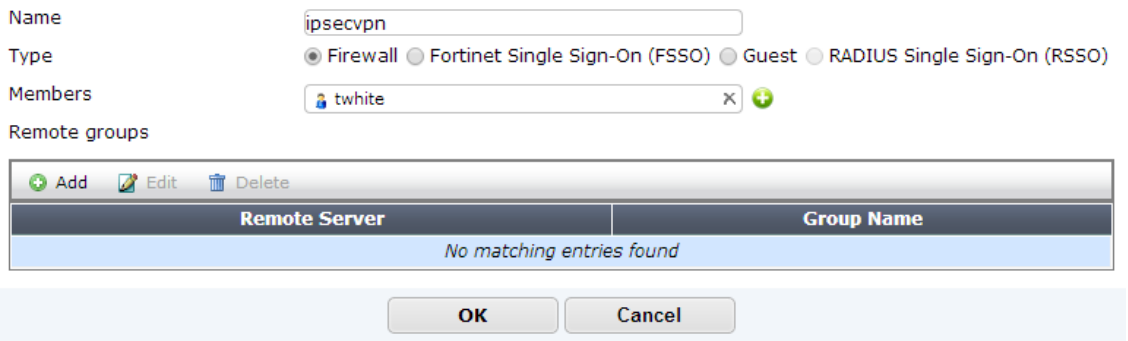
1. Go to **User & Device** > **User** > **User Definition**.

2. Create a new **Local User** with the **User Creation Wizard**.



3. Proceed through each step of the wizard, carefully entering the appropriate information.

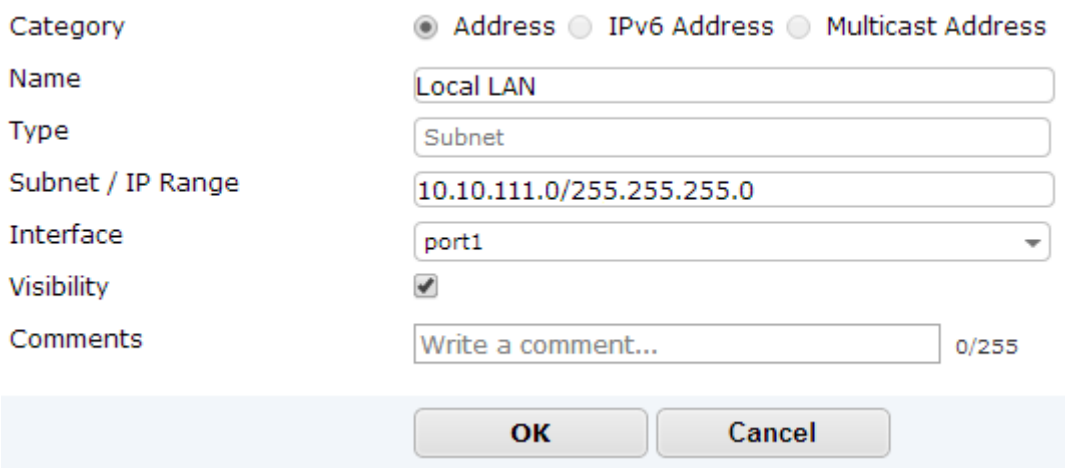
4. Go to User & Device > User > User Groups. Create a user group for remote users and add the user you created.



6.3.2 Adding a firewall address for the local network

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

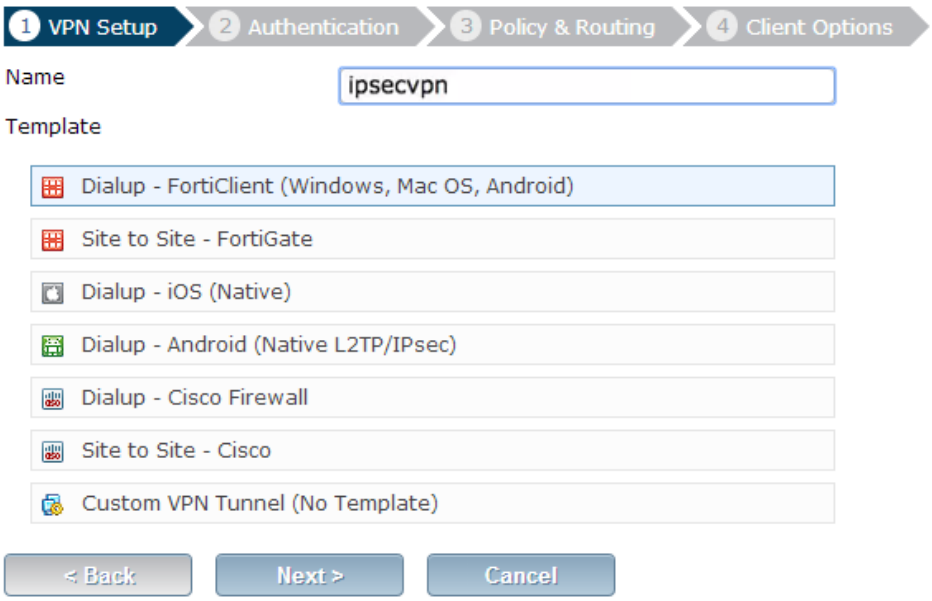
2. Add a firewall address for the Local LAN, including the subnet and local interface.



6.3.3 Configuring the IPsec VPN using the IPsec VPN Wizard

1. Go to VPN > IPSec > Wizard.

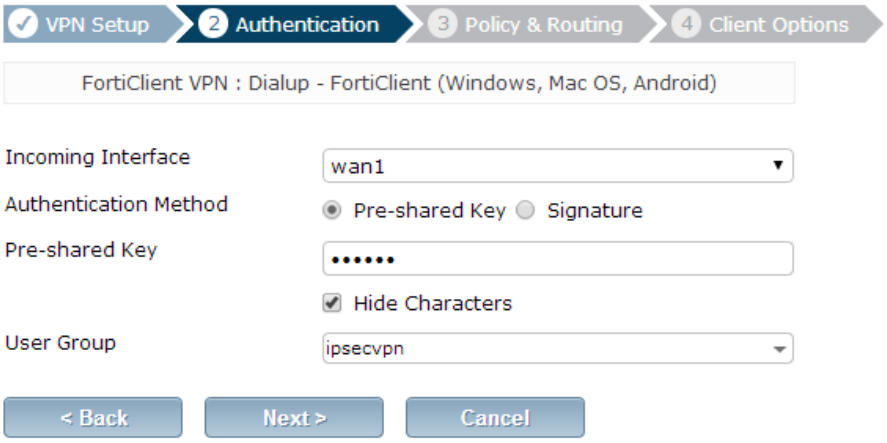
2. Name the VPN connection* and select Dial Up – FortiClient (Windows, Mac OS, Android) and click Next.



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

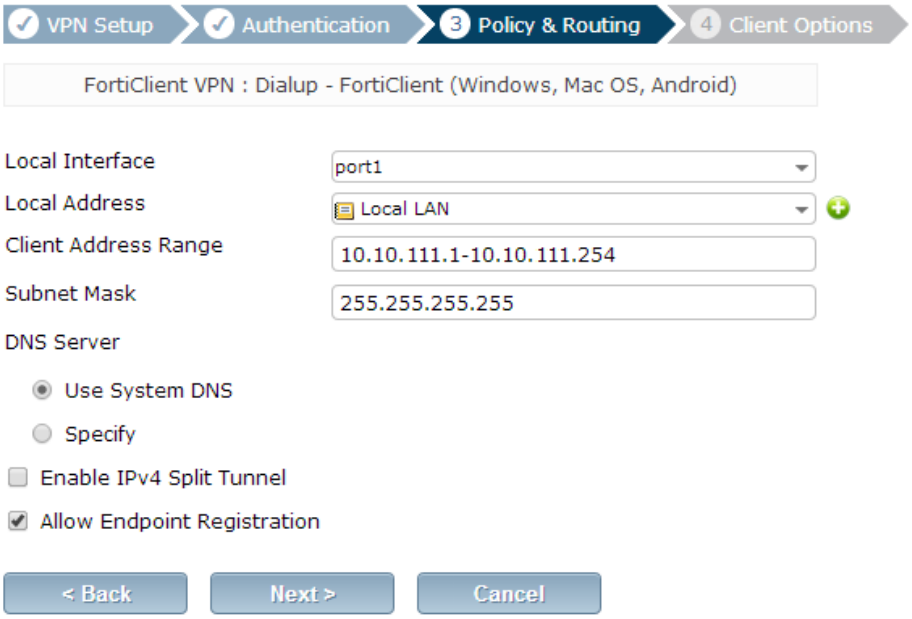
4. Select Pre-shared Key for the Authentication Method.

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

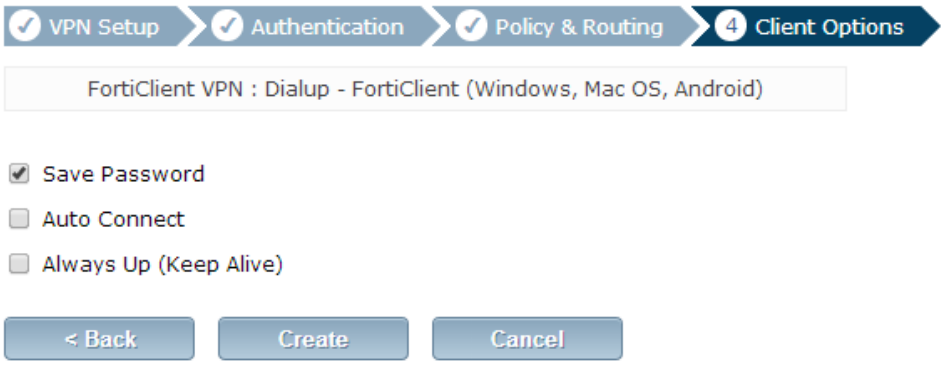


6. Set Local Interface to an internal interface (in the example, port 1) and set Local Address to the local LAN address.

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

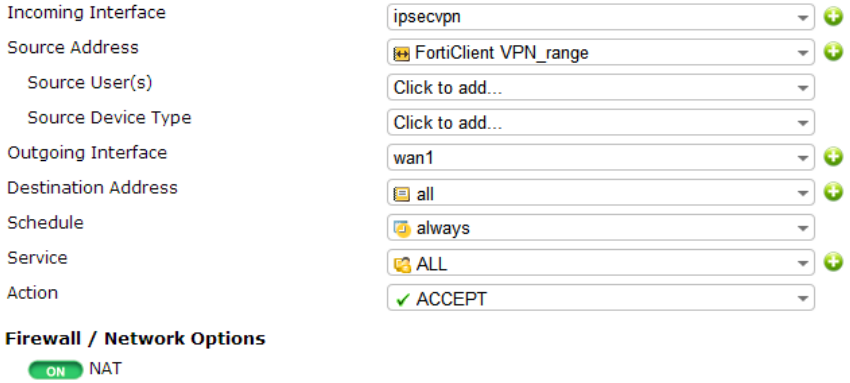


8. Click Next and select Client Options as desired.



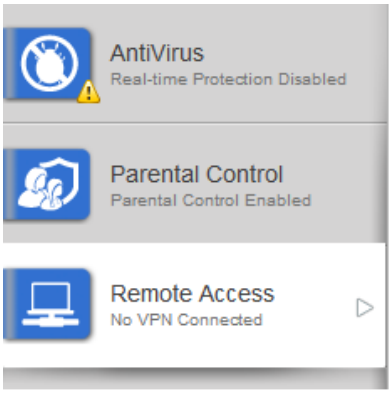
6.3.4 Creating a security policy for access to the Internet

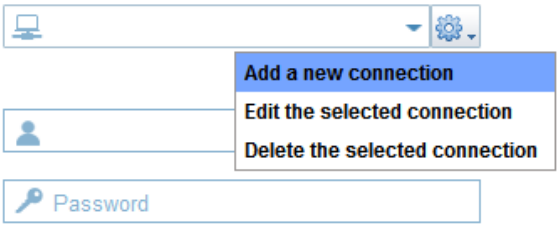
1. Go to Policy & Objects > Policy > IPv4.
2. Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.
3. Set Incoming Interface to the tunnel interface and set Source Address to all.
4. Set Outgoing Interface to wan1 and Destination Address to all.
5.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



6.3.5 Configuring FortiClient

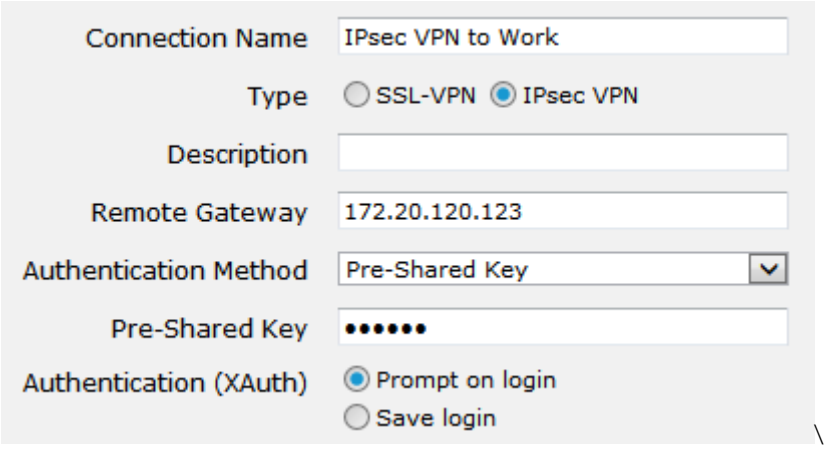
1. Open FortiClient, go to Remote Access and Add a new connection



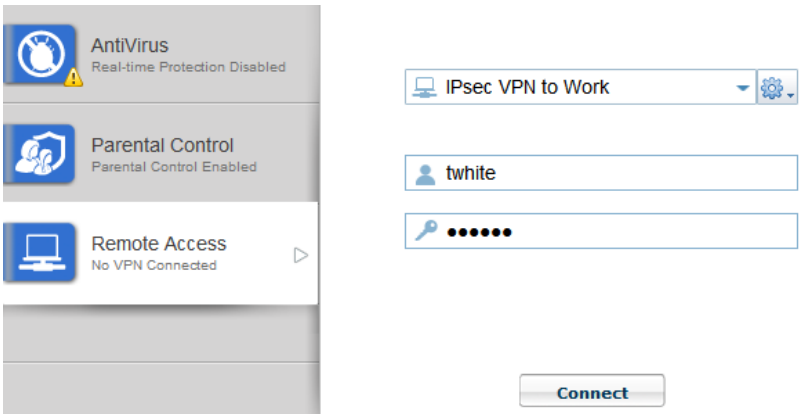


2. Provide a Connection Name and set the Type to IPsec VPN.
3. Set Remote Gateway to the FortiGate IP address.

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

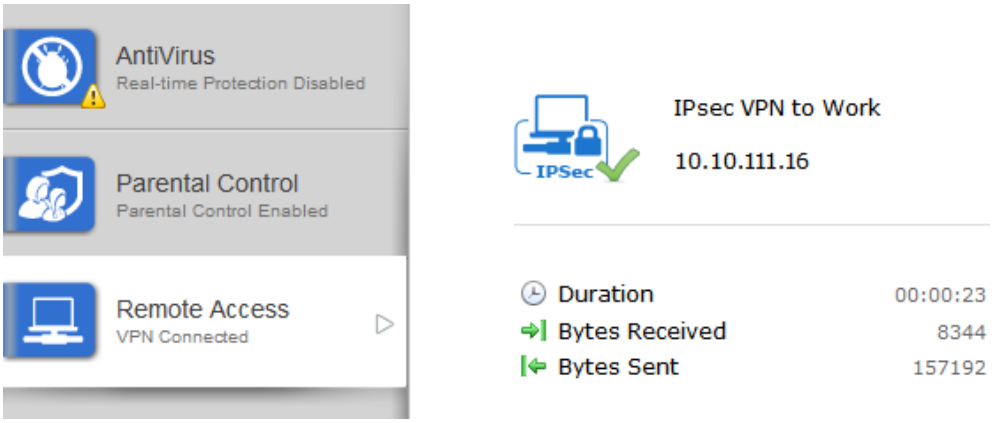


5. Select the new connection, enter the username and password, and click Connect.



6.3.6 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