



FortiGate

VM on OCB Flex Engine

Installation and Deployment Guide

24th September 2021

Orange Restricted

Version 4.0

document control

| date | version no. | author | change/addition |
|---------------------------------|-------------|---------------|---|
| 6 th December 2018 | 1.0 | Ahmad Samak | Creation |
| 1 st February 2020 | 2.0 | Ahmad Samak | Update the installation process of FortiGate VM on OCB FE. |
| 20 th 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 |
| 24 th September 2021 | 4.0 | David Bignell | Add section 6 Solution Configuration copied from separate FortiGate on OCB FE Configuration Guide v2 from 1 st Feb 2020 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

table of contents

| | | |
|----------|---|-----------|
| 1 | References | 4 |
| 2 | Introduction..... | 5 |
| 3 | FortiGate VM Overview | 6 |
| 3.1 | FortiGate VM models and Licensing | 6 |
| 3.2 | Register FortiGate VM with Customer Service and Support..... | 6 |
| 3.3 | Deployment package contents | 7 |
| 4 | Deployment Methods..... | 8 |
| 4.1 | Hybrid and VPC to VPC..... | 8 |
| 4.2 | On Cloud /On Cloud..... | 9 |
| 5 | Deploy the VM-Series Firewall on Orange Flex Engine | 10 |
| 5.1 | Create VPC | 10 |
| 5.2 | Install FortiGate VM on the VPC..... | 13 |
| 5.3 | Configure Network Interfaces manually | 17 |
| 6 | Solution Configuration | 22 |
| 6.1 | Hybrid and VPC to VPC Model | 22 |
| 6.1.1 | On Premises FortiGate configuration | 22 |
| | Creating a policy to allow traffic from the internal network to the Internet | 22 |
| 6.1.2 | Create a Static Route for the VPN Connection | 23 |
| 6.1.3 | Create user defined routes on OCB FE VPC | 23 |
| 6.1.4 | Creating Two policies to allow traffic from the internal network to OCB FE VPC and Vice Versa..... | 25 |
| 6.2 | Site-to-Site VPN-IPSEC Tunnel Configuration | 26 |
| 6.2.1 | Configuring the onprem. IPsec VPN | 26 |
| 6.2.2 | Configuring OCB FE IPSEC VPN..... | 29 |
| 6.2.3 | Results | 31 |
| 6.3 | IPsec VPN with FortiClient | 31 |
| 6.3.1 | Creating a user group for remote users..... | 32 |
| 6.3.2 | Adding a firewall address for the local network..... | 32 |
| 6.3.3 | Configuring the IPsec VPN using the IPsec VPN Wizard | 33 |
| 6.3.4 | Creating a security policy for access to the Internet..... | 35 |
| 6.3.5 | Configuring FortiClient..... | 35 |
| 6.3.6 | Results | 36 |

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 FortiGate 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:

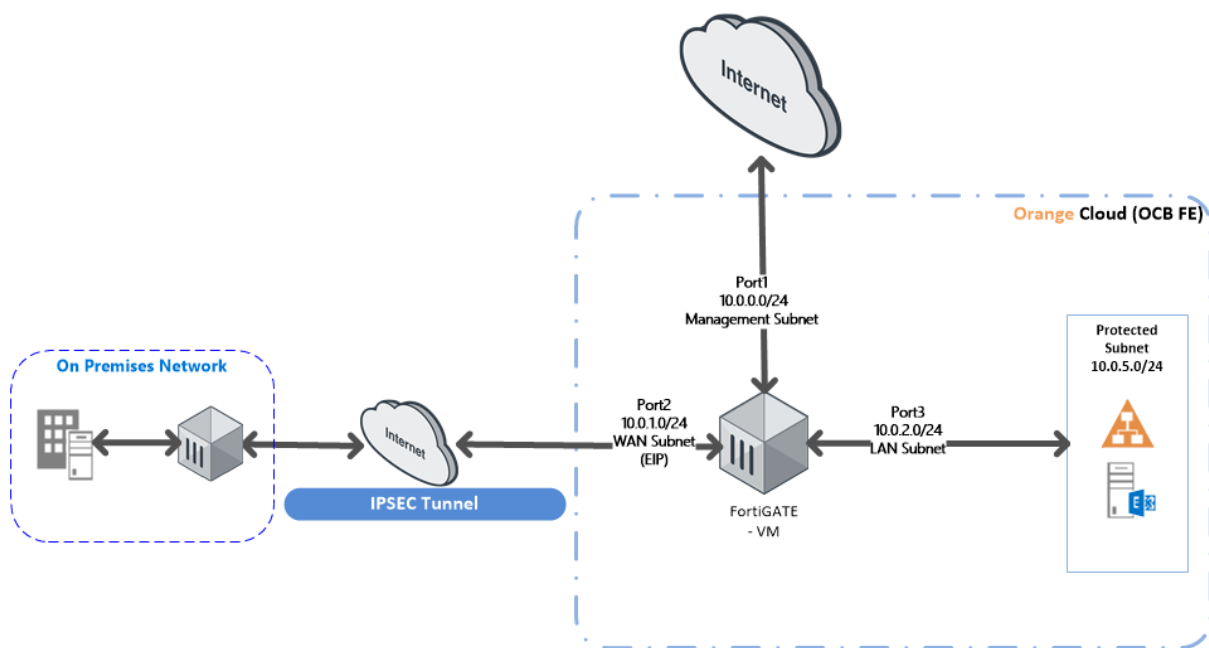
- create a 30GB log disk
- specify the virtual hardware settings

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

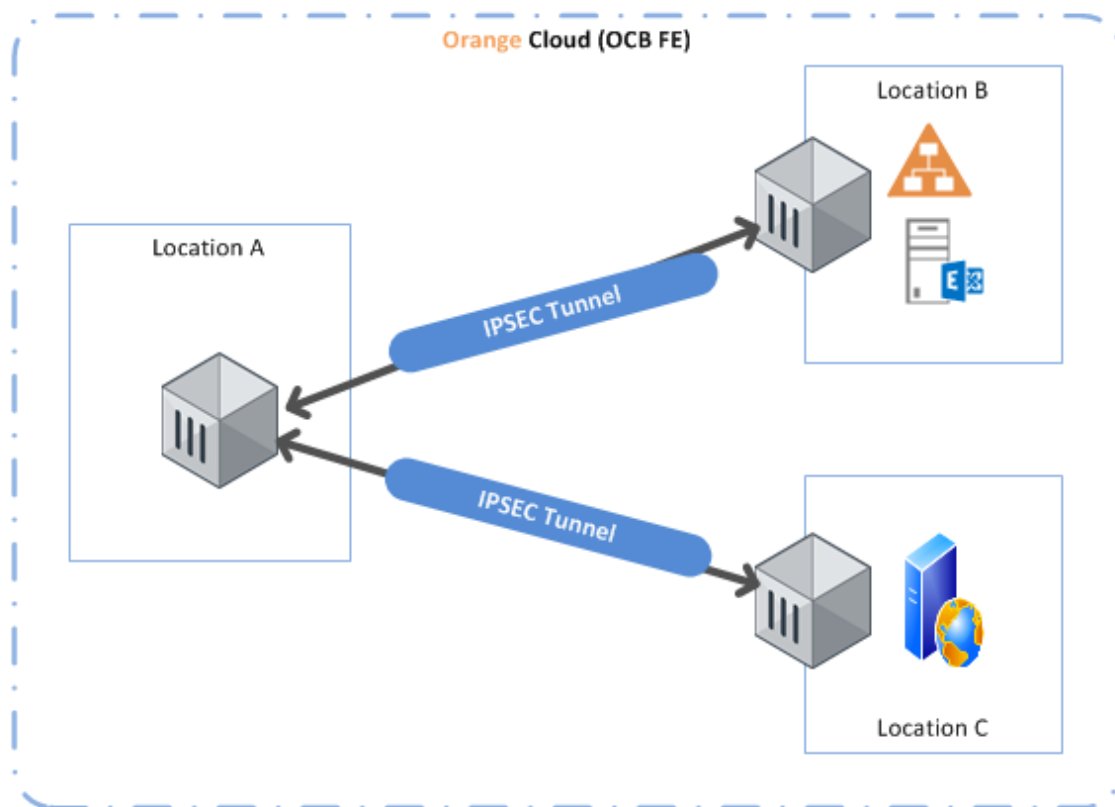
The FortiGate VM firewall on OCB FE allows you to securely extend your physical data center/private cloud into OCB FE using IPsec tunneling. To improve your data center security, if you have segmented your network and deployed your workloads in separate VPC's, you can secure traffic flowing between VPC's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

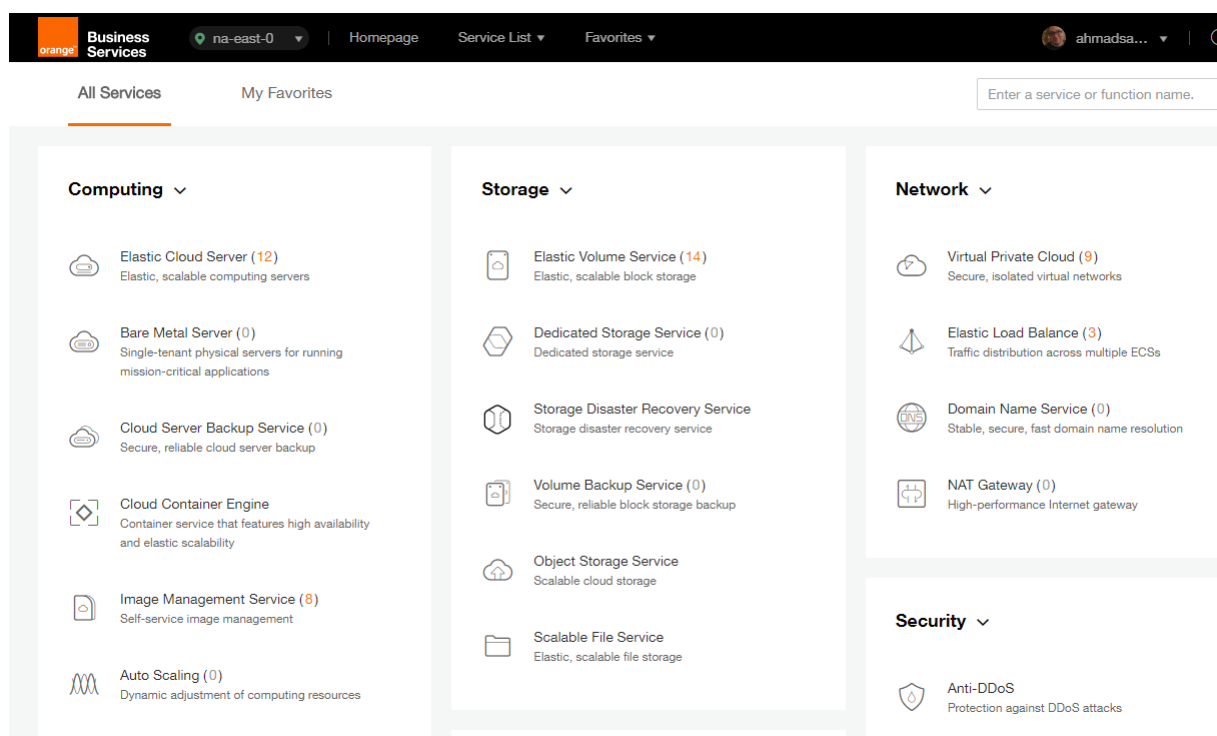
To use a VPC, first create it by following the procedure provided in this section. Then, create subnets, security groups, and VPNs, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

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

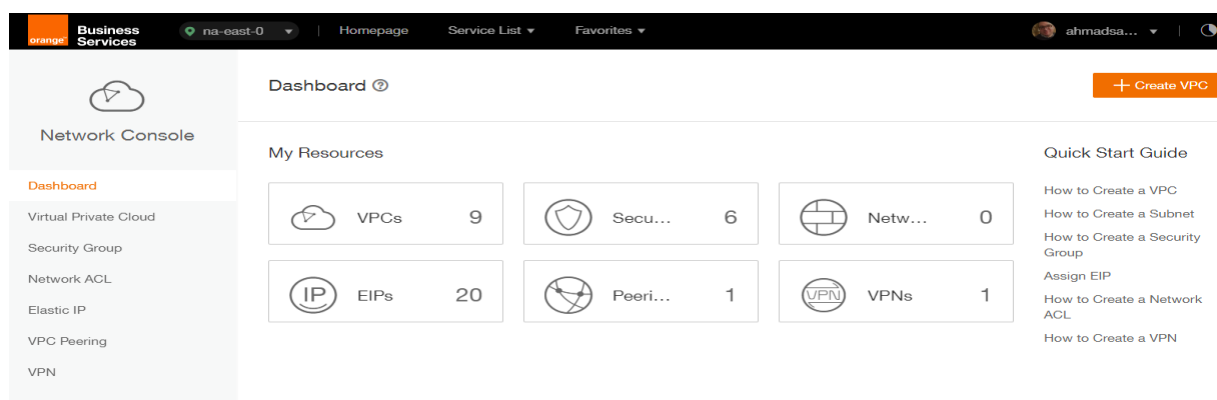
- Management Subnet
- Internet Facing Subnet
- LAN Subnet
- Protected Subnet

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 |

Basic Information


Region:

* Name:


* CIDR Block: /

Recommended network segments: 10.0.0.0/8-24, 172.16.0.0/12-24, and 192.168.0.0/16-24

Subnet Settings

AZ :

* Subnet Name:

* CIDR: / 

Available IP Addresses: 250
Subnets cannot be modified after they are created

Advanced Settings:

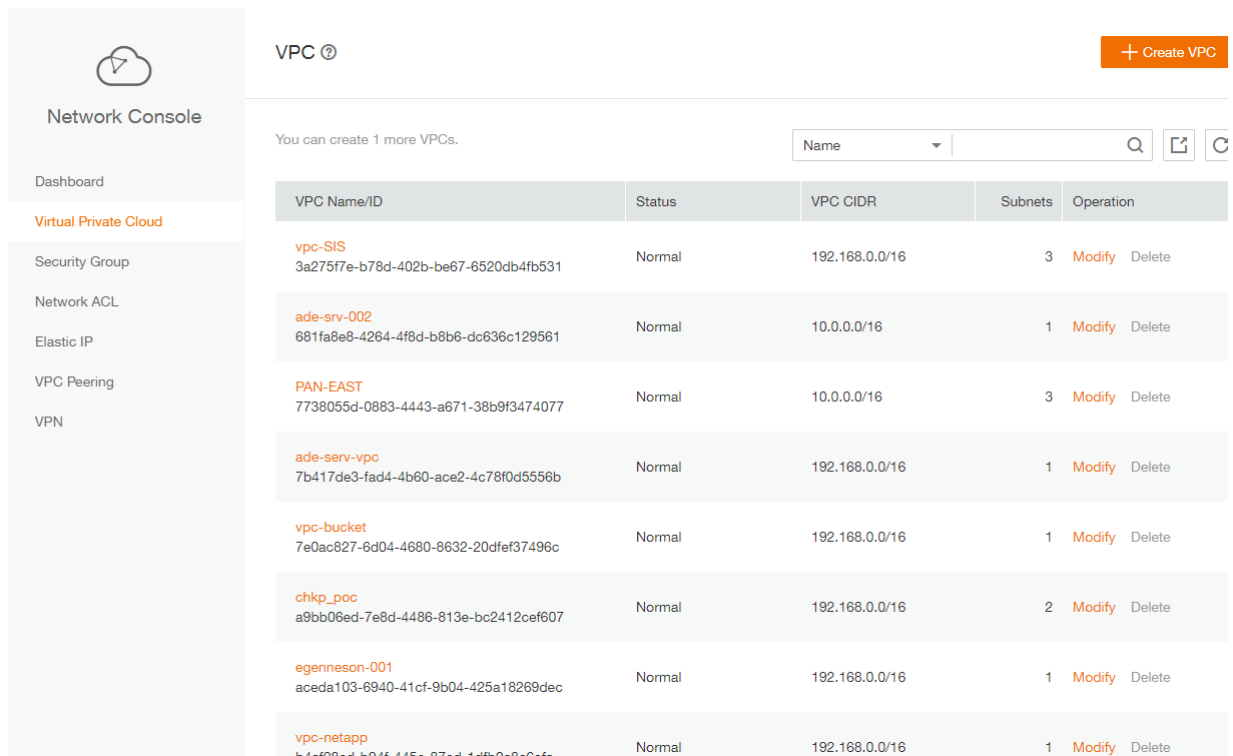
* Gateway:

DNS Server Address 1:

DNS Server Address 2:

- 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.
- Click **Create Now**.

The created VPC will be shown in the VPC List



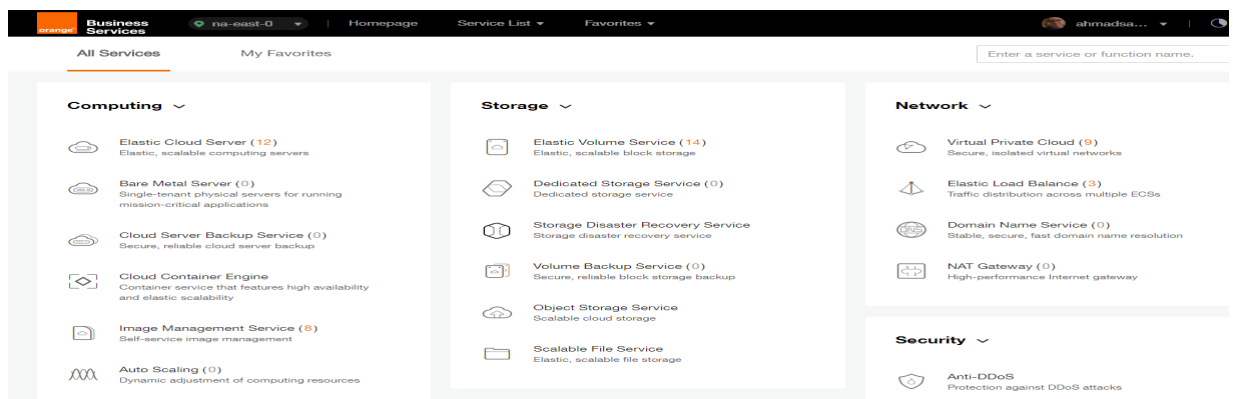
The screenshot shows the AWS Network Console interface. On the left is a sidebar with navigation links: Dashboard, Virtual Private Cloud (highlighted), Security Group, Network ACL, Elastic IP, VPC Peering, and VPN. The main area is titled 'VPC' and shows a message 'You can create 1 more VPCs.' Below this is a table listing existing VPCs. Each row includes the VPC Name/ID, Status, VPC CIDR, Subnets, and Operation links (Modify, Delete).

| VPC Name/ID | Status | VPC CIDR | Subnets | Operation |
|---|--------|----------------|---------|---|
| vpc-sis 3a275f7e-b78d-402b-be67-6520db4fb531 | Normal | 192.168.0.0/16 | 3 | Modify Delete |
| ade-srv-002 681fa8e8-4264-4f8d-b8b6-dc636c129561 | Normal | 10.0.0.0/16 | 1 | Modify Delete |
| PAN-EAST 7738055d-0883-4443-a671-38b9f3474077 | Normal | 10.0.0.0/16 | 3 | Modify Delete |
| ade-srv-vpc 7b417de3-fad4-4b60-ace2-4c78f0d5556b | Normal | 192.168.0.0/16 | 1 | Modify Delete |
| vpc-bucket 7e0ac827-6d04-4680-8632-20dfe37496c | Normal | 192.168.0.0/16 | 1 | Modify Delete |
| chkp_poc a9bb06ed-7e8d-4486-813e-bc2412cef607 | Normal | 192.168.0.0/16 | 2 | Modify Delete |
| egenneson-001 aceda103-6940-41cf-9b04-425a18269dec | Normal | 192.168.0.0/16 | 1 | Modify Delete |
| vpc-netapp b4cf28ed-b9df-445e-87ed-1dfb0c8c6afa | Normal | 192.168.0.0/16 | 1 | Modify Delete |

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**.



The screenshot shows the AWS Business Services console. The top navigation bar includes 'Business Services', a region selector ('na-east-0'), and links for 'Homepage', 'Service List', and 'Favorites'. Below the navigation bar, there are tabs for 'All Services' and 'My Favorites'. The main content area is divided into three columns: 'Computing', 'Storage', and 'Network'. The 'Computing' column is expanded, showing a list of services including Elastic Cloud Server (12), Bare Metal Server (0), Cloud Server Backup Service (0), Cloud Container Engine, Image Management Service (8), and Auto Scaling (0). The 'Storage' column shows Elastic Volume Service (14), Dedicated Storage Service (0), Storage Disaster Recovery Service, Volume Backup Service (0), Object Storage Service, and Scalable File Service. The 'Network' column shows Virtual Private Cloud (9), Elastic Load Balance (3), Domain Name Service (0), and NAT Gateway (0). A search bar is located at the top right of the main content area.

3. Click **Create ECS**.

Elastic Cloud Server [?](#) [+ Create ECS](#)

You can create 88 more ECSs. The ECSs can use up to 767 vCPUs and 1,515 GB of memory.

Start Stop Restart Delete All statuses Name

| <input type="checkbox"/> | Name/ID | AZ | Status | Specifications/Image | IP Address | Operation |
|--------------------------|--|------------|---------|---|---|----------------|
| <input type="checkbox"/> | PAN-EASTVM 8becfee-28e9-4069-a7d0... | na-east-0a | Running | 4 vCPUs 16 GB s3.xlarge.4 PA-VM-KVM-8.0.5 | 57.100.69.19 (EIP) 30... 10.0.0.4 (Private IP) | Remote Login M |
| <input type="checkbox"/> | ecs-6ca2 4313a696-af0e-4dde-952b... | na-east-0a | Running | 8 vCPUs 16 GB s3.2xlarge.2 OBS-U-DEBIAN_9.0 | 192.168.0.195 (Privat... | Remote Login M |
| <input type="checkbox"/> | chkp_centos_intranet 79df3752-7e6e-4876-bc1f... | na-east-0a | Running | 1 vCPUs 4 GB s3.medium.4 CentOS_CHKP | 57.100.68.24 (EIP) 30... 192.168.10.213 (Privat... | Remote Login M |
| <input type="checkbox"/> | Win-ade-cfcd a6084ece-2077-4a33-a81... | na-east-0a | Running | 2 vCPUs 4 GB s3.large.2 OBS_U_Windows_2008R2-STD | 57.100.68.12 (EIP) 5 ... 192.168.2.233 (Privat... | Remote Login M |

The ECS creation page is displayed.

Create ECS [?](#) [← Back to ECS List](#)

Region **eu-west-0** To change the region, use the region selector in the upper left corner of this page.

AZ **eu-west-0a**

Specifications

General-purpose Computing II Memory-optimized Disk-intensive GPU-accelerated

[Learn more about ECS types](#)

| Flavor Name | vCPUs/Memory |
|--|--------------|
| <input checked="" type="radio"/> s3.medium.4 | 1 vCPUs 4 GB |
| <input type="radio"/> s3.large.2 | 2 vCPUs 4 GB |
| <input type="radio"/> s3.large.4 | 2 vCPUs 8 GB |
| <input type="radio"/> s3.xlarge.2 | 4 vCPUs 8 GB |

Current Configuration

| | |
|----------------|----------|
| Region | eu-w |
| AZ | eu-w |
| ECS Name | ecs-4 |
| Specifications | Gene PUs |
| Image | -- |
| System Disk | Comi |
| VPC | vpc-c |
| Security Group | defau |
| NIC | subn 24) |
| EIP | Not n |
| Key Pair | -- |
| Quantity | 1 |

[Create Now](#)

- Confirm the region.

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

- 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.

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

- 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 previously 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

Current Specifications: General-purpose | s3.medium.4 | 1vCPUs | 4GB

Image

Public image **Private image** Shared image


chkp_xen_kvm(100GB) 


chkp_xen_kvm(100GB)



Disk

PAN-VM-8.0.1(100GB)



PAN-VM100-805(100GB)


System Disk Common I/O  - 100 + GB | 100 / 1,000 IOPS


 **Add Data Disk** You can attach 23 more disks.



VPC  vpc-qapworkspaces  [View VPC](#)

NIC

Primary NIC  subnet-qapworkspaces(192.1... Self-assigned IP address [View In-Use IP Addresses](#) 

 **Add NIC** You can add 11 more NICs.

Security Group  [Learn more about how to configure a security group](#)

default (Inbound:TCP/3389, 443, 22 | Outbound:...)  [Manage Security Group](#) 

Inbound: TCP/3389, 443, 22 | Outbound: -

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 | <p>Provides a network, including subnet and security group, for an ECS.</p> <p>You can select an existing VPC, or click View VPC and create a desired one.</p> <p>For more information about VPC, see <i>Virtual Private Cloud User Guide</i>.</p> <p>NOTE:</p> <p>DHCP must be enabled in the VPC to which the ECS belongs.</p> |
| Security Group | <p>Controls instance access within or between security groups by defining access rules. This enhances instance security.</p> <p>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.</p> <p>NOTE:</p> <p>Before initializing an ECS, ensure that the security group rule in the outbound direction meets the following requirements:</p> <ul style="list-style-type: none"> • Protocol: TCP • Port Range: 80 • Remote End: 169.254.0.0/16 <p>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:</p> <ul style="list-style-type: none"> • Protocol: ANY • Port Range: ANY • Remote End: 0.0.0.0/16 |
| NIC | <p>Consists of a primary NIC and one or more extension NICs.</p> <p>MTU Settings: optional</p> <p>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.</p> <p>An MTU can only be a number, ranging from 1280 to 8888.</p> |
| EIP | <p>A static public IP address bound to an ECS in a VPC. Using the EIP, the ECS provides services externally.</p> <p>The following options are provided:</p> |

Table 2 Parameter descriptions

| Parameter | Description |
|-----------|---|
| | <ul style="list-style-type: none"> • 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. <p>** In our scenario: We assigned 2 EIP's one for the management NIC and the other for the Internet Facing NIC.</p> |

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.

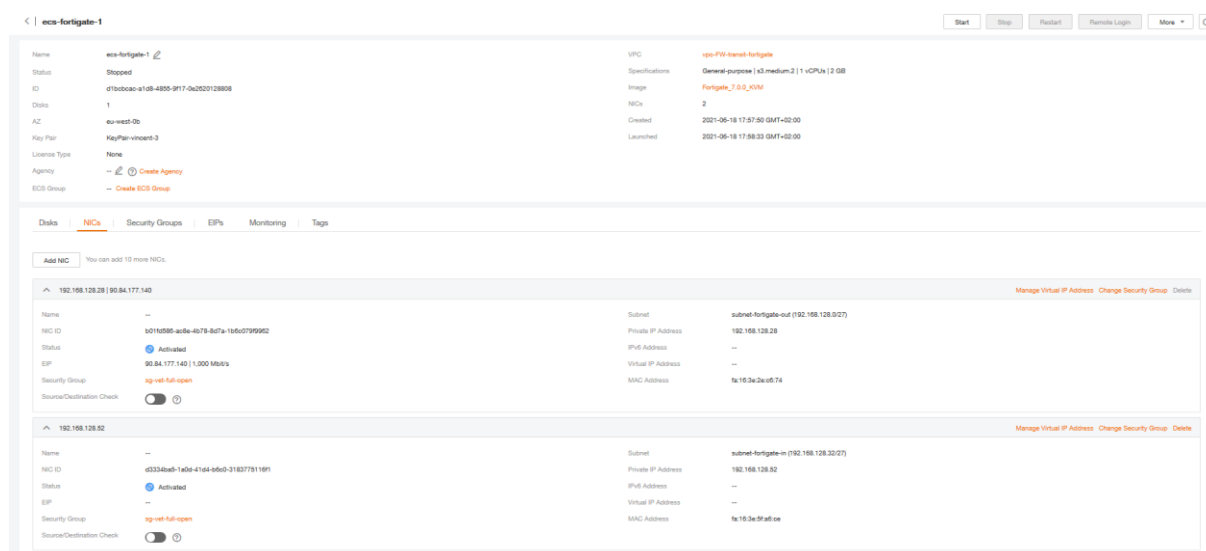
15. After creating the Fortigate VM you can access it through **Https** using the EIP of the Management NIC. (username: admin / no password)

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.

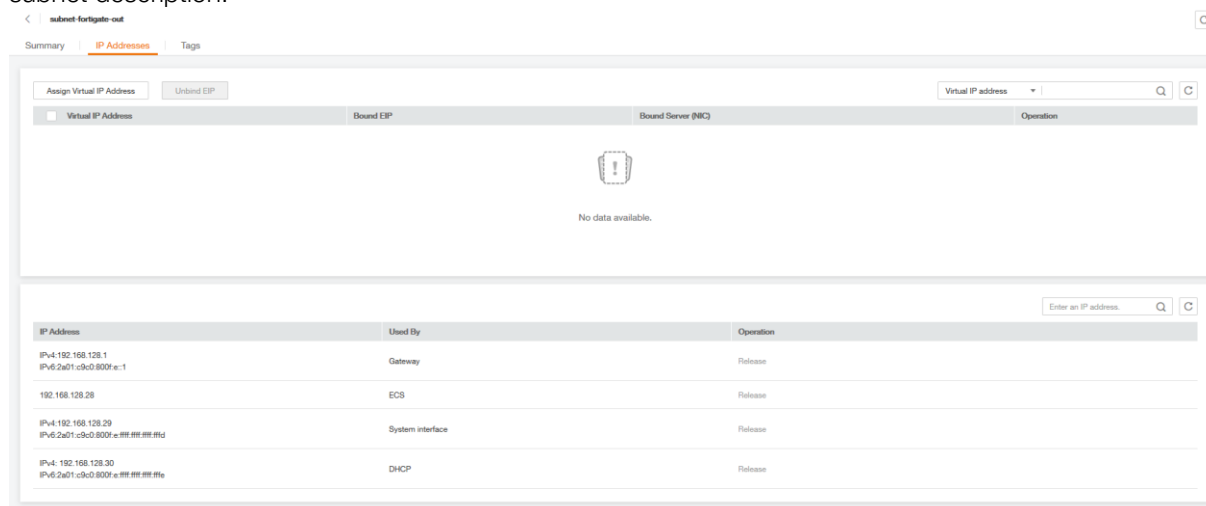
Those IP addresses can be retrieved on the Cloud Server Console page, in Fortigate ECS description (NIC tab) :



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**).

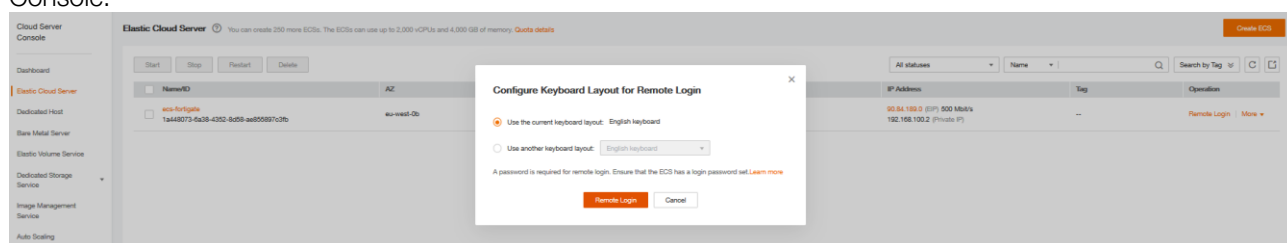
Note that “Source/Destination Check” option must be deactivated on all Fortigate ECS NIC.

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:

```

Connected (encrypted) to: 1a448073-6a38-4352-8d58-a6855897c3b6 Before you exit, ensure that computer is locked.
Send Remote Command English Local Cursor Send Ctrl+Del Input Commands

Loading flatk... ok
Loading /rootfs.gz... ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Formatting shared data partition ... done!
Starting system maintenance...
Scanning /dev/uda1... (100%)
Scanning /dev/uda2... (100%)
Serial number is FGUM90UNLICENSED

FortiGate-UM64-KUM login:
FortiGate-UM64-KUM login: admin
Password:
License invalid due to exceeding allowed 1 CPUs and 1824 MB RAM.
Welcome !

FortiGate-UM64-KUM #

```

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"):

```

Connected (encrypted) to: 1a448073-6a38-4352-8d58-a6855897c3b6 Before you exit, ensure that computer is locked.
Send Remote Command English Local Cursor Send Ctrl+Del Input Commands

FortiGate-UM64-KUM (port2) # set ip 192.168.100.144 255.255.255.224
FortiGate-UM64-KUM (port2) # set allowaccess ping https ssh http
FortiGate-UM64-KUM (port2) # end
FortiGate-UM64-KUM # config router static
FortiGate-UM64-KUM (static) # edit 1
FortiGate-UM64-KUM (1) # set gateway 192.168.100.1
FortiGate-UM64-KUM (1) # set device "port1"
FortiGate-UM64-KUM (1) # next
FortiGate-UM64-KUM (static) # edit 2
FortiGate-UM64-KUM (2) # set gateway 192.168.100.129
FortiGate-UM64-KUM (2) # set device "port2"
FortiGate-UM64-KUM (2) # end
FortiGate-UM64-KUM #

```

Copy Commands

Copy and paste content into the text box. Up to 2000 characters are allowed. Non-standard keyboard characters are not supported.

```

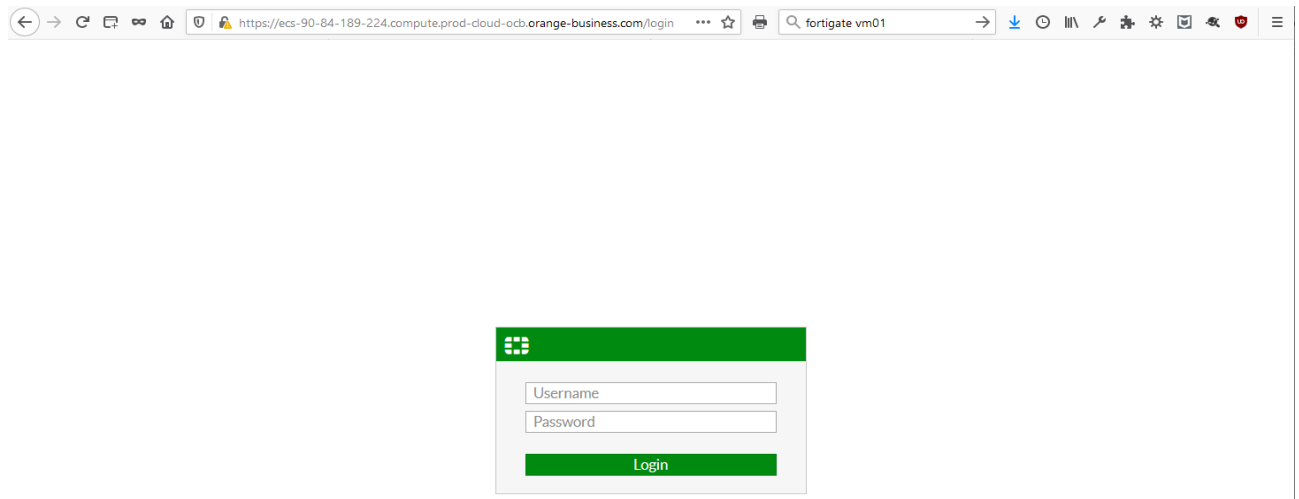
config system interface
edit "port1"
set mode static
set ip 192.168.100.2
255.255.255.224
set allowaccess ping https ssh
http
next
edit "port2"
set mode static
set ip 192.168.100.144
255.255.255.224

```

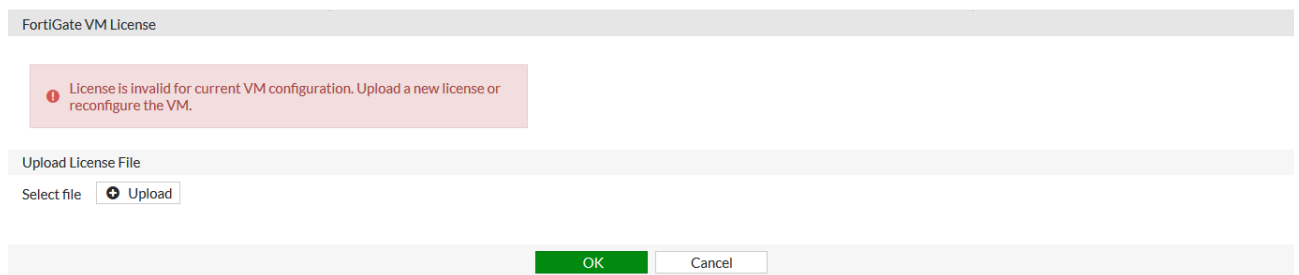
1828/2000

Send Clear

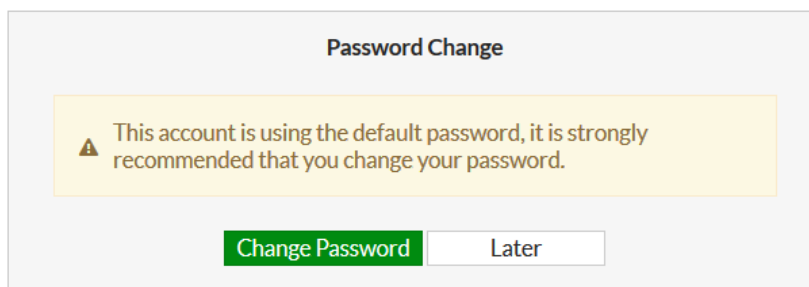
Once NIC configuration done, you can connect to Fortigate Web Console, using reverse DNS name of EIP associated with ECS main NIC (example: EIP=90.84.189.224 => reverse DNS=ecs-90-84-189-224.compute.prod-cloud-ocb.orange-business.com) :



In Fortigate Web console, log in using username “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:



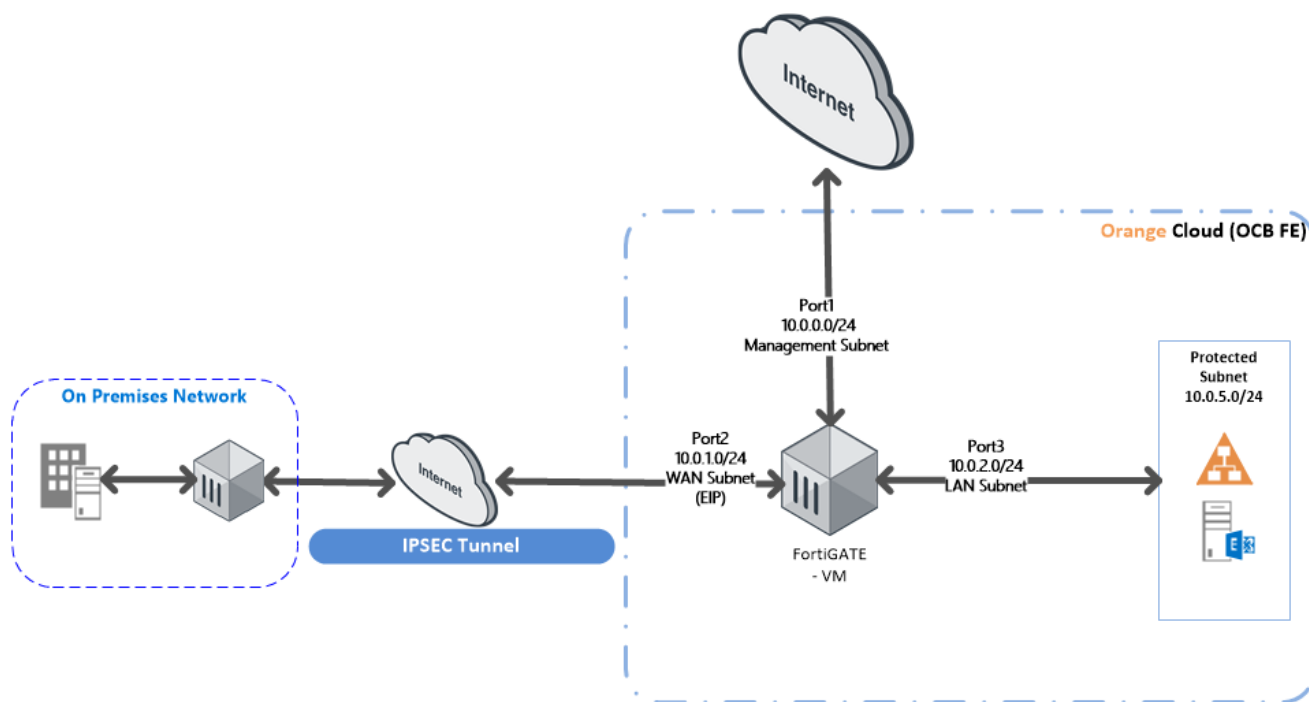
You are then ready to continue Fortigate instance configuration:

The screenshot displays the FortiGate VM64-KVM dashboard for instance FGVM1VTM21001487. The interface includes a left-hand navigation menu with options like Dashboard, Main, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The main content area is divided into several panels:

- System Information:** Displays Hostname (FGVM1VTM21001487), Serial Number (FGVM1VTM21001487), Firmware (v6.0.3 build0200 (GA)), Mode (NAT (Flow-based)), System Time (2021/08/04 06:47:47), Uptime (00:00:09:43), and WAN IP (90.84.189.224).
- Licenses:** Shows FortiCare Support status and a list of licenses including Firmware & General Updates, IPS, AntiVirus, and Web Filtering. It also displays FortiClient (0/10) and FortiToken (0/2) counts.
- Virtual Machine:** Displays FGVM1V License status and resource allocation: Allocated vCPUs (1/1) at 100% and Allocated RAM (2 GiB / 2 GiB) at 98%.
- FortiCloud:** Shows Status as Not Activated.
- Security Fabric:** Displays a list of security components and a message indicating FortiGate Telemetry is disabled.
- Security Rating:** Shows No Security Rating Results Found with a Run Now button.

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.

| | |
|---------------------|---|
| Name | Internet_GW |
| Incoming Interface | LAB_LAN (port1) |
| Outgoing Interface | LAB_internet (port2) |
| Source | all |
| Destination Address | all |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒

Fixed Port ☐

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Logging Options

Log Allowed Traffic ☒ Security Events ☐ 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.

| | |
|-------------------------|---|
| Destination | Subnet Named Address Internet Service |
| | 10.0.0.0/255.255.0.0 |
| Device | lab-cloud |
| Administrative Distance | 2 |
| Comments | |
| Status | <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled |

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 Cloud

2- Select your VPC

< Single-FG-VPC

Summary | Tags

VPC Information

Name: Single-FG-VPC

ID: 1ca95ba4-9a36-4457-8535-fda34b0eb02

Status: Available

CIDR Block: 172.16.0.0/16

VPC Connection Options

Subnets: 4

Route Tables: 2

Resources in the VPC

Elastic Load Balance: 0

Related Services

NAT Gateway
The NAT Gateway service enables all EC2s in a VPC to access the same Internet.

VPC Peering
A VPC peering connection enables you to route traffic between private IP addresses. EC2s in either VPC can communicate with each other if they were in the same VPC. You can create a VPC peering connection between your VPC and another tenant's VPC.

3- Choose route Tables

Route Tables ? Create Route Table

Single-FG-VPC

| Name | VPC | Type | Associated Subnets | Operation |
|-------------------|---------------|--------------------|--------------------|---|
| users-inside | Single-FG-VPC | Custom Route Table | 1 | Delete Associate Subnet Replicate Route |
| rtb-Single-FG-VPC | Single-FG-VPC | Default | 3 | Delete Associate Subnet Replicate Route |

4- Select the route table of type Default

5- Add the following route

Routes

Delete Add Route Replicate Route ? Learn how to configure routes.

| Destination | Next Hop Type | Next Hop | Type | Description | Operation |
|-------------|---------------|---|--------|--|-----------------|
| Local | Local | Local | System | Default route that enables instance communication... | Modify Delete |
| 0.0.0.0/0 | Extension NIC | 172.16.2.197 7867b13f-513d-44d9-a22e-... | Custom | -- | Modify Delete |

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

< rtb-Single-FG-VPC

Summary | Associated Subnets

Associate Subnet

| Name | AZ | CIDR Block | Status | Operation |
|---------------|------------|---------------|-----------|--------------------|
| OutsideSubnet | eu-west-0b | 172.16.1.0/24 | Available | Change Route Table |
| Inside-Subnet | eu-west-0b | 172.16.2.0/24 | Available | Change Route Table |

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

Single-FG-VPC

| Name | VPC | Type | Associated Subnets | Operation |
|--------------|---------------|--------------------|--------------------|---|
| users-inside | Single-FG-VPC | Custom Route Table | 1 | Delete Associate Subnet Replicate Route |

< | users-inside

Summary | Associated Subnets

Associate Subnet

| Name | AZ | CIDR Block | Status | Operation |
|-----------------|------------|---------------|-----------|------------------------------------|
| Internal-Subnet | eu-west-0b | 172.16.3.0/24 | Available | Change Route Table |

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

Routes

Delete Add Route Replicate Route [Learn how to configure routes.](#)

| Destination | Next Hop Type | Next Hop | Type | Description | Operation |
|---|---------------|---|--------|---|-----------------|
| Local | Local | Local | System | Default route that enables instance communic... | Modify Delete |
| <input type="checkbox"/> 192.168.2.0/24 | Extension NIC | 172.16.2.197 7567b13f-513d-44d9-a22e-... | Custom | -- | Modify Delete |
| <input type="checkbox"/> 192.168.3.0/24 | Extension NIC | 172.16.2.197 7567b13f-513d-44d9-a22e-... | Custom | -- | Modify Delete |
| <input type="checkbox"/> 192.168.1.0/24 | Extension NIC | 172.16.2.197 7567b13f-513d-44d9-a22e-... | Custom | -- | Modify Delete |

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

| | |
|---------------------|---|
| Name | tocloudlab |
| Incoming Interface | LAB_LAN (port1) |
| Outgoing Interface | lab-cloud |
| Source | all |
| Destination Address | Lab_Cloud_Subnet |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

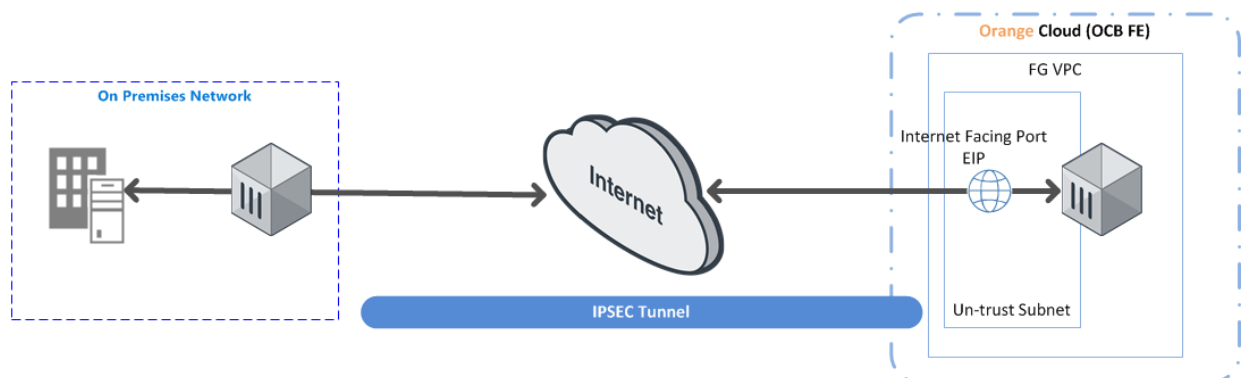
NAT ☐

| | |
|---------------------|---|
| Name | fromlabcloud |
| Incoming Interface | lab-cloud |
| Outgoing Interface | LAB_LAN (port1) |
| Source | Lab_Cloud_Subnet |
| Destination Address | all |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☐

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

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing

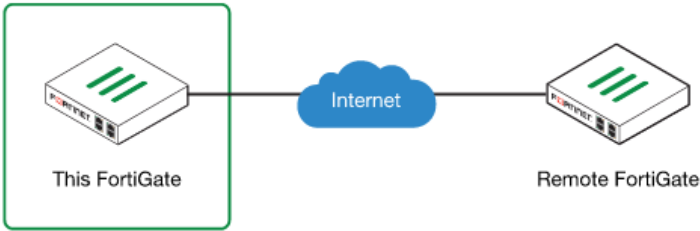
Name: HQ-to-Branch

Template Type: **Site to Site** Remote Access Custom

Remote Device Type: **FortiGate** Cisco

NAT Configuration: **No NAT between sites**
This site is behind NAT
The remote site is behind NAT

Site to Site - FortiGate



< Back Next > Cancel

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.

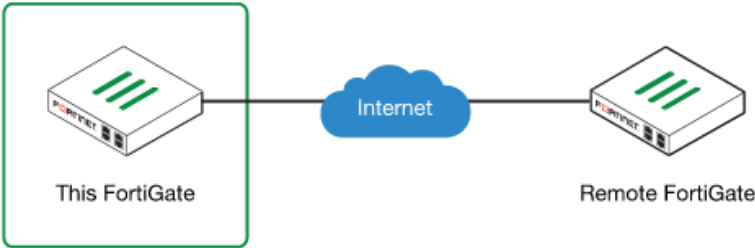
Set a secure Pre-shared Key.

VPN Creation Wizard

☒ VPN Setup
 ☒ 2 Authentication
 ☐ 3 Policy & Routing

Remote Device IP Address Dynamic DNS
 IP Address
 Outgoing Interface ↑ wan1 ▼
 Detected via routing lookup
 Authentication Method Pre-shared Key Signature
 Pre-shared Key 👁

HQ-to-Branch: Site to Site - FortiGate



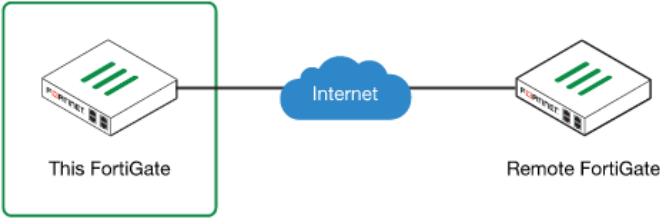
3. In the Policy & Routing step, set the Local Interface. The Local Subnets will be added automatically. Set Remote Subnets to the Branch FortiGate's local subnet

VPN Creation Wizard

☒ VPN Setup
 ☒ Authentication
 ☒ 3 Policy & Routing

Local Interface ↑ lan ▼
 Local Subnets ⓘ
 Remote Subnets ⓘ

HQ-to-Branch: Site to Site - FortiGate



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

VPN Creation Wizard

☒ VPN Setup
 >
 ☒ Authentication
 >
 ☒ Policy & Routing

☒ The VPN has been set up

Summary of Created Objects

| | |
|------------------------|-------------------------|
| Phase 1 Interface | HQ-to-Branch |
| Phase 2 Interfaces | HQ-to-Branch |
| Static Routes | 5.5.5.5/24 |
| Local Address Group | HQ-to-Branch_local |
| Remote Address Group | HQ-to-Branch_remote |
| Local to Remote Policy | vpn_HQ-to-Branch_local |
| Remote to Local Policy | vpn_HQ-to-Branch_remote |

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**

VPN Creation Wizard

☒ 1 VPN Setup
 >
 ☐ 2 Authentication
 >
 ☐ 3 Policy & Routing

Name:

Template Type:
 ☒ Site to Site
 ☐ Remote Access
 ☐ Custom

Remote Device Type:
 ☒ FortiGate
 ☐ Cisco

NAT Configuration:
 ☒ No NAT between sites
 ☐ This site is behind NAT
 ☐ The remote site is behind NAT

Site to Site - FortiGate

- 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.

VPN Creation Wizard

VPN Setup > **2 Authentication** > 3 Policy & Routing

Remote Device **IP Address** Dynamic DNS

IP Address 172.20.121.92

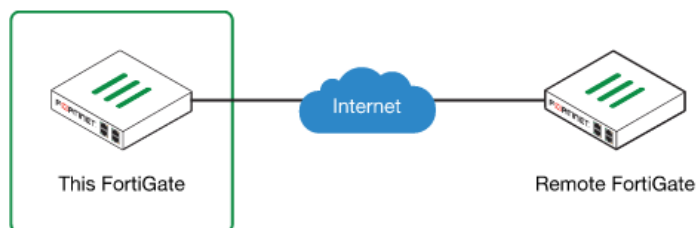
Outgoing Interface wan1

Detected via routing lookup

Authentication Method **Pre-shared Key** Signature

Pre-shared Key •••••

Branch-to-HQ: Site to Site - FortiGate



< Back

Next >

Cancel

- 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

VPN Creation Wizard

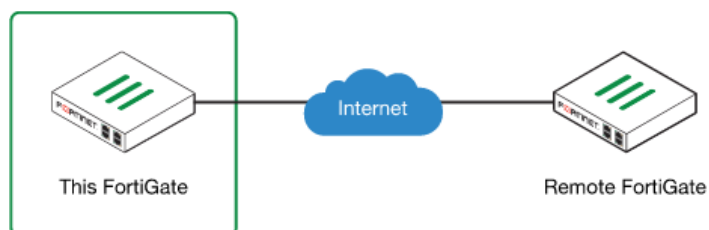
VPN Setup > Authentication > **3 Policy & Routing**

Local Interface wan

Local Subnets 5.5.5.0/24

Remote Subnets 10.10.10.1/24

Branch-to-HQ: Site to Site - FortiGate

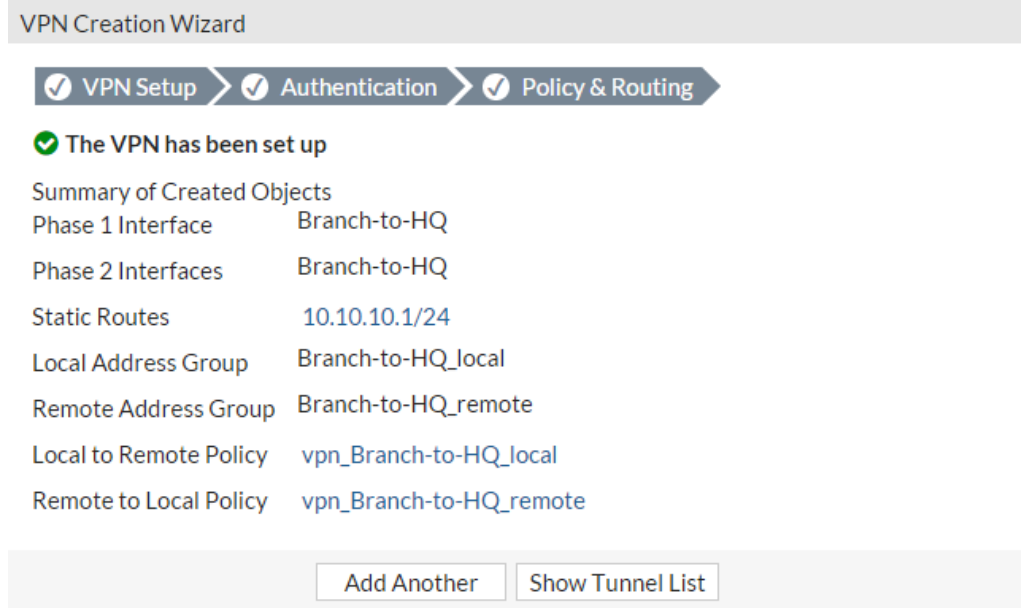


< Back

Create

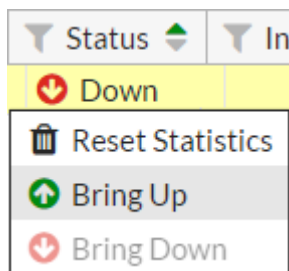
Cancel

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

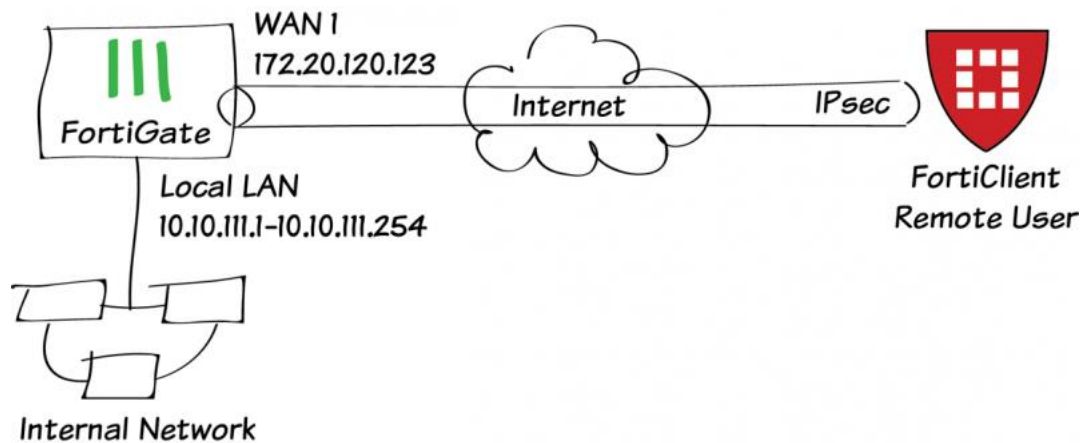
On either FortiGate, go to **Monitor > IPsec Monitor** to verify the status of the VPN tunnel. Right-click under **Status** and select **Bring Up**.



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**.

The screenshot shows the 'User Creation Wizard' in the FortiGate GUI. The first step, 'Choose User Type', is active. It displays four radio button options: 'Local User' (selected), 'Remote RADIUS User', 'Remote TACACS+ User', and 'Remote LDAP User'. Below the options are three buttons: '< Back', 'Next >', and 'Cancel'.

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.

The screenshot shows the 'User Group' configuration page. The 'Name' field is 'ipsecvpn'. The 'Type' is set to 'Firewall' (selected). The 'Members' field contains 'twhite'. Below this is a table for 'Remote groups' with columns 'Remote Server' and 'Group Name'. The table is empty, showing the message 'No matching entries found'. At the bottom are 'Add', 'Edit', and 'Delete' icons, and 'OK' and 'Cancel' buttons.

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.

| | |
|-------------------|---|
| Category | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name | <input type="text" value="Local LAN"/> |
| Type | <input type="text" value="Subnet"/> |
| Subnet / IP Range | <input type="text" value="10.10.111.0/255.255.255.0"/> |
| Interface | <input type="text" value="port1"/> |
| Visibility | <input checked="" type="checkbox"/> |
| Comments | <input type="text" value="Write a comment..."/> 0/255 |

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.

1 VPN Setup

2 Authentication

3 Policy & Routing

4 Client Options

| | |
|----------|---|
| Name | <input type="text" value="ipsecvpn"/> |
| Template | <div><div> Dialup - FortiClient (Windows, Mac OS, Android)</div><div> Site to Site - FortiGate</div><div> Dialup - iOS (Native)</div><div> Dialup - Android (Native L2TP/IPsec)</div><div> Dialup - Cisco Firewall</div><div> Site to Site - Cisco</div><div> Custom VPN Tunnel (No Template)</div></div> |

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.

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

Incoming Interface: wan1

Authentication Method: ☒ Pre-shared Key ☐ Signature

Pre-shared Key:

☒ Hide Characters

User Group: ipsecvpn

< Back Next > Cancel

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.*

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

Local Interface: port1

Local Address: Local LAN

Client Address Range: 10.10.111.1-10.10.111.254

Subnet Mask: 255.255.255.255

DNS Server: ☒ Use System DNS ☐ Specify

☐ Enable IPv4 Split Tunnel

☒ Allow Endpoint Registration

< Back Next > Cancel

8. Click Next and select Client Options as desired.

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

☒ Save Password

☐ Auto Connect

☐ Always Up (Keep Alive)

< Back Create Cancel

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.

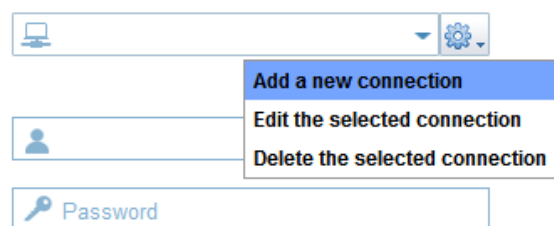
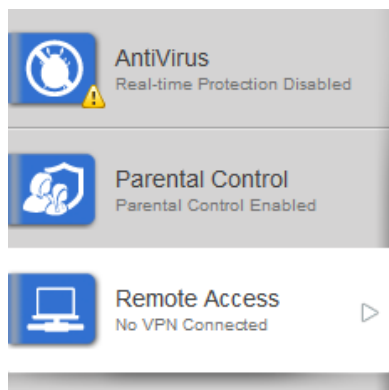
| | | |
|---------------------|-----------------------|---|
| Incoming Interface | ipsecvpn | + |
| Source Address | FortiClient VPN_range | + |
| Source User(s) | Click to add... | |
| Source Device Type | Click to add... | |
| Outgoing Interface | wan1 | + |
| Destination Address | all | + |
| Schedule | always | |
| Service | ALL | + |
| Action | ✓ ACCEPT | |

Firewall / Network Options

☒ 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

Connection Name: IPsec VPN to Work

Type: ☐ SSL-VPN ☒ IPsec VPN

Description:

Remote Gateway: 172.20.120.123

Authentication Method: Pre-Shared Key

Pre-Shared Key:

Authentication (XAuth): ☒ Prompt on login ☐ Save login

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

AntiVirus: Real-time Protection Disabled

Parental Control: Parental Control Enabled

Remote Access: No VPN Connected

IPsec VPN to Work

Username: twhite

Password:

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

AntiVirus: Real-time Protection Disabled

Parental Control: Parental Control Enabled

Remote Access: VPN Connected

IPsec VPN to Work

10.10.111.16

Duration: 00:00:23

Bytes Received: 8344




Bytes Sent: 157192

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

| Name | Type | Remote Gateway | Status | Incoming Data | 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 |