FortiGate

VM on OCB Flex Engine Installation and Deployment Guide

6th December 2018

Version 1.0

document control

date	version no.	author	change/addition
6th December 2018	1.0	Ahmad Samak	Creation

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:

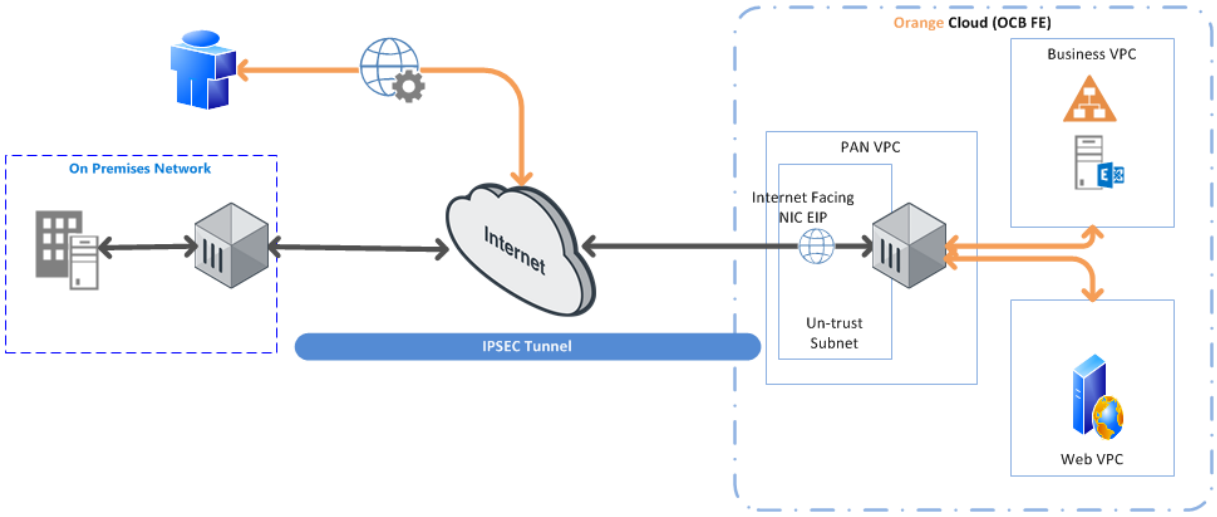
- create a 30GB log disk
- specify the virtual hardware settings

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.



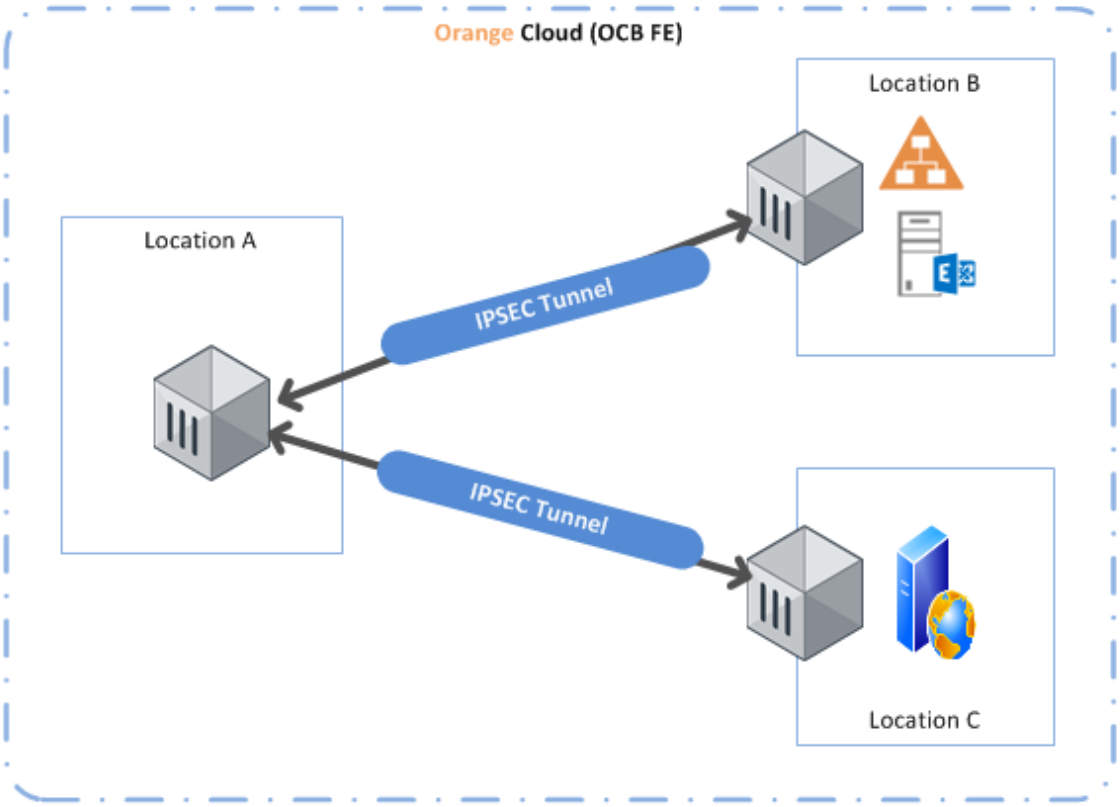
• Inter-Subnet —The Fortigate firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.

• 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.

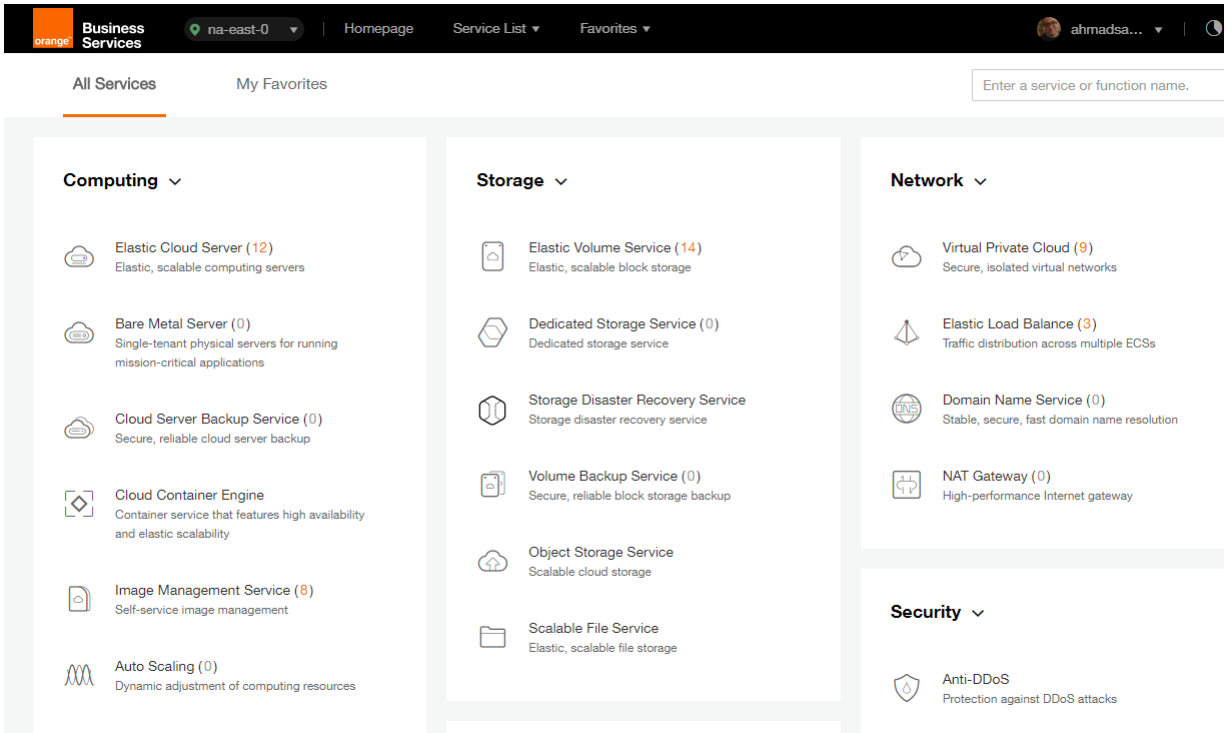
5.1 Create VPC

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

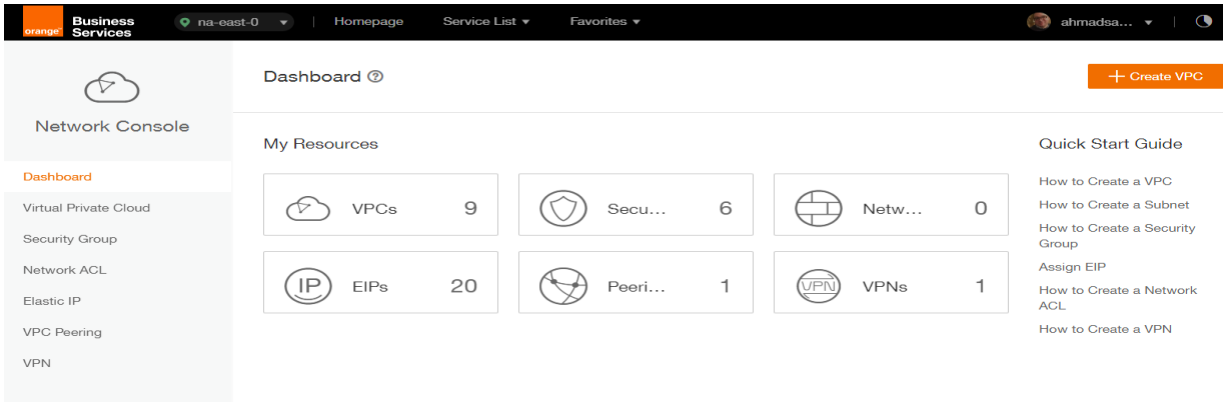
To use a VPC, first create it by following the procedure provided in this section. Then, create subnets, security groups, and VPNs, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

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



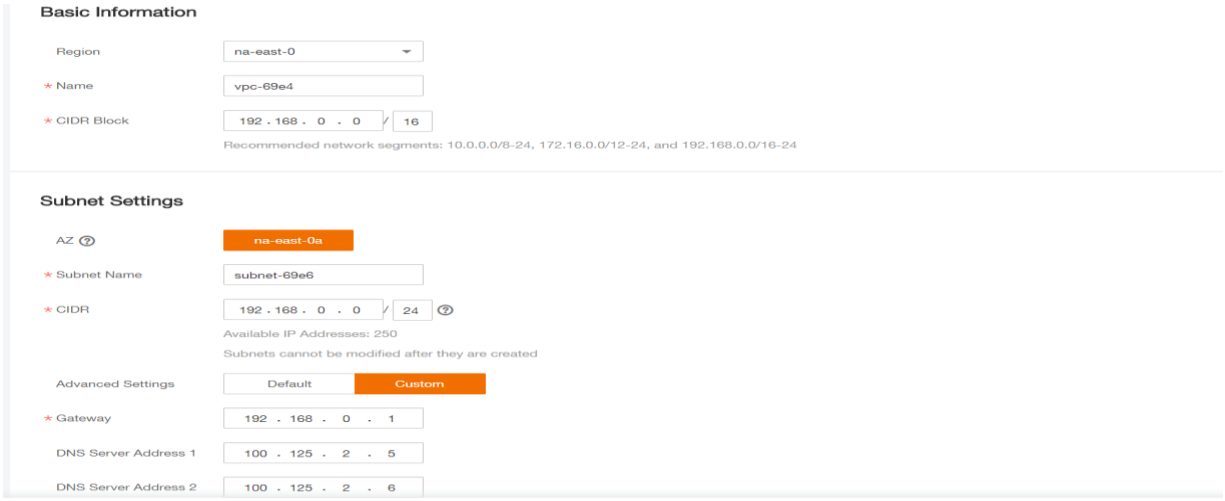
3. On the **Dashboard** page, click **Create VPC**.



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

Table 1 Parameter description

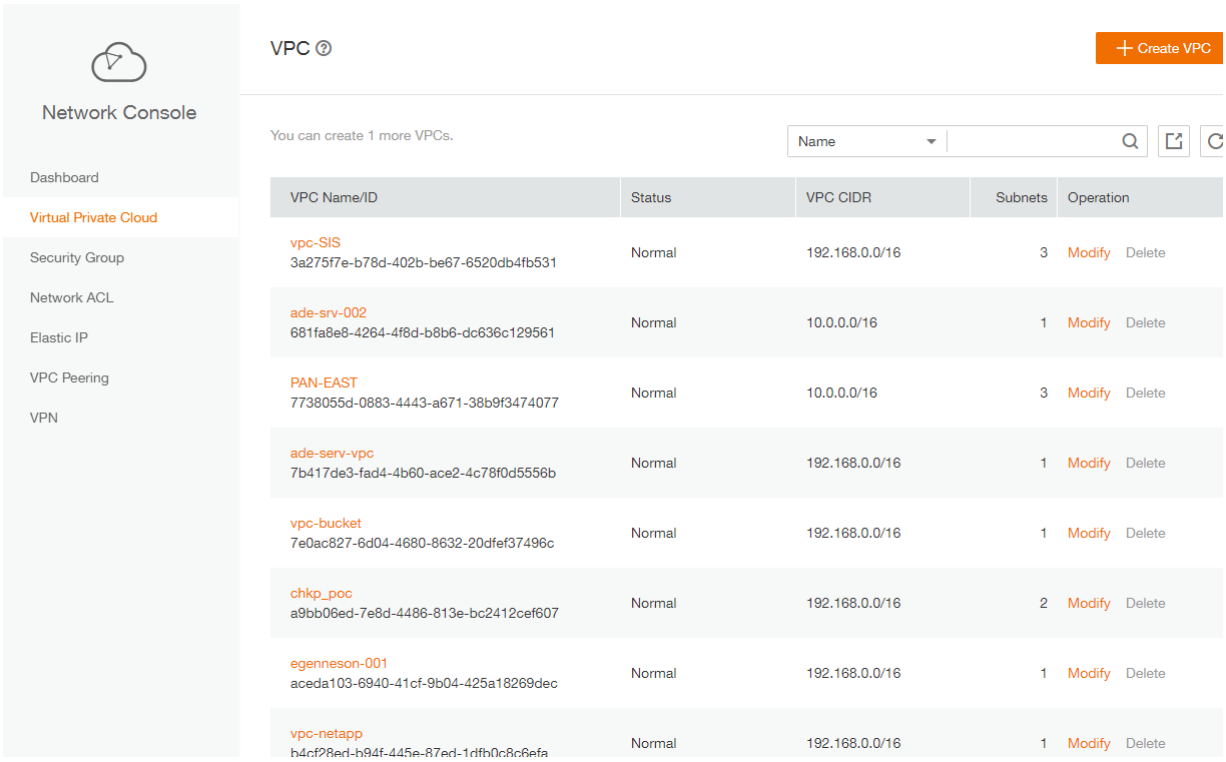
Parameter	Description	Example Value
Name	Specifies the VPC name.	VPC-001
VPC CIDR	Specifies the Classless Inter-Domain Routing (CIDR) block for the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset (for multiple subnets in the VPC). The following CIDR blocks are supported: 10.0.0.0/8–24 172.16.0.0/12–24 192.168.0.0/16–24	192.168.0.0/16
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**.

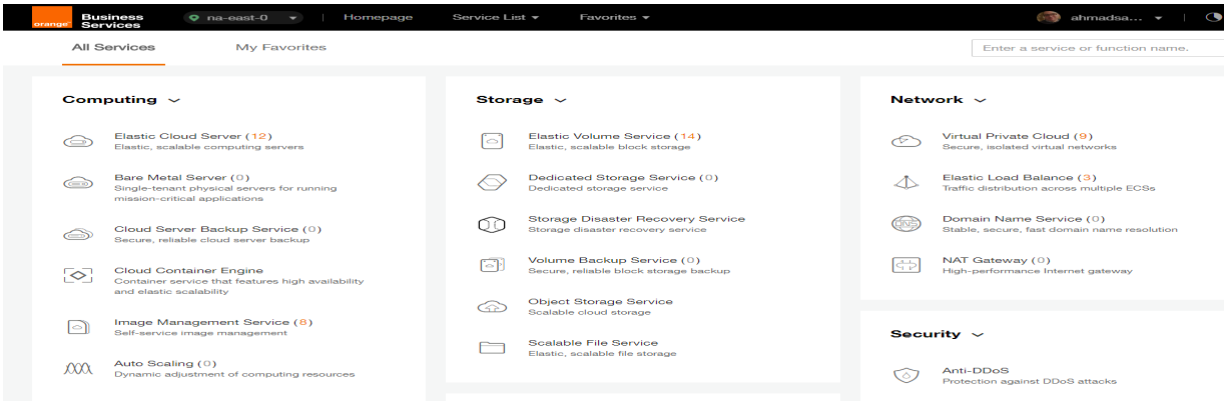
   The created VPC will be shown in the VPC List



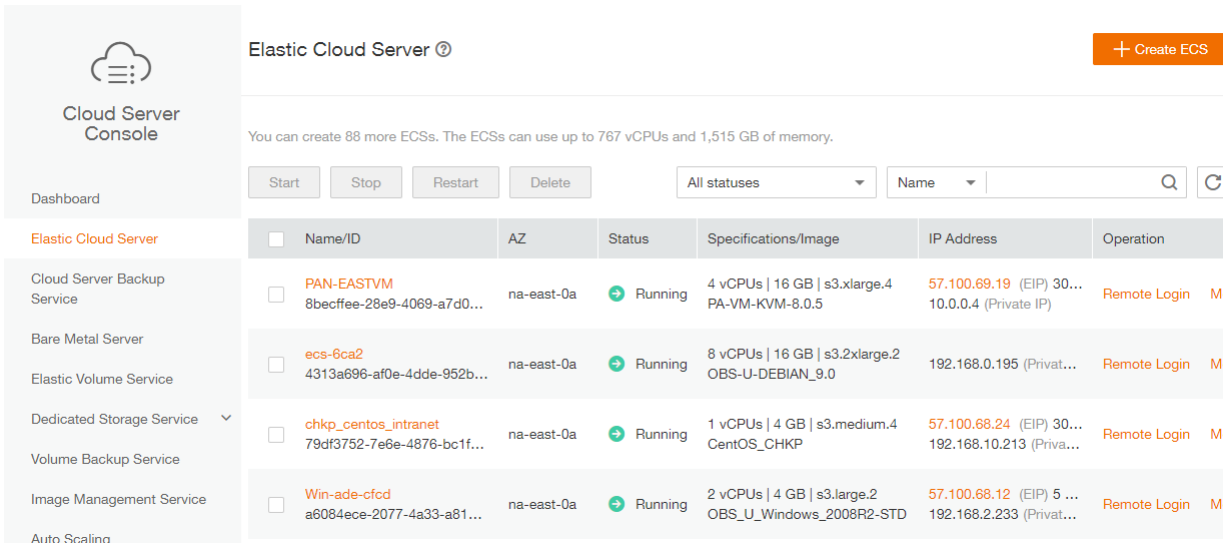
5.2 Install FortiGate VM on the VPC

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.

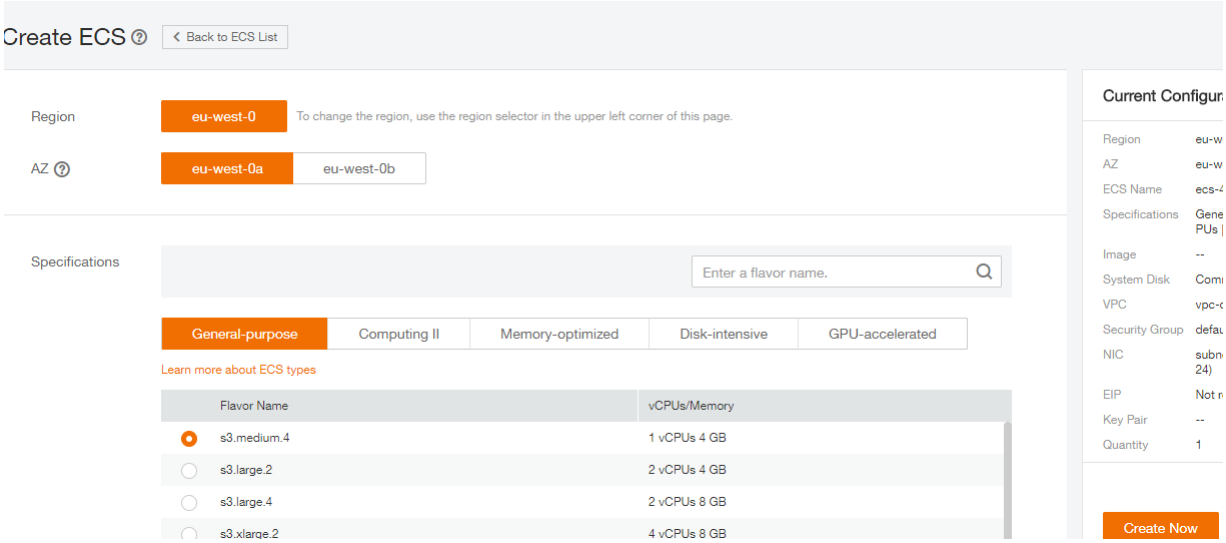
1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.



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.

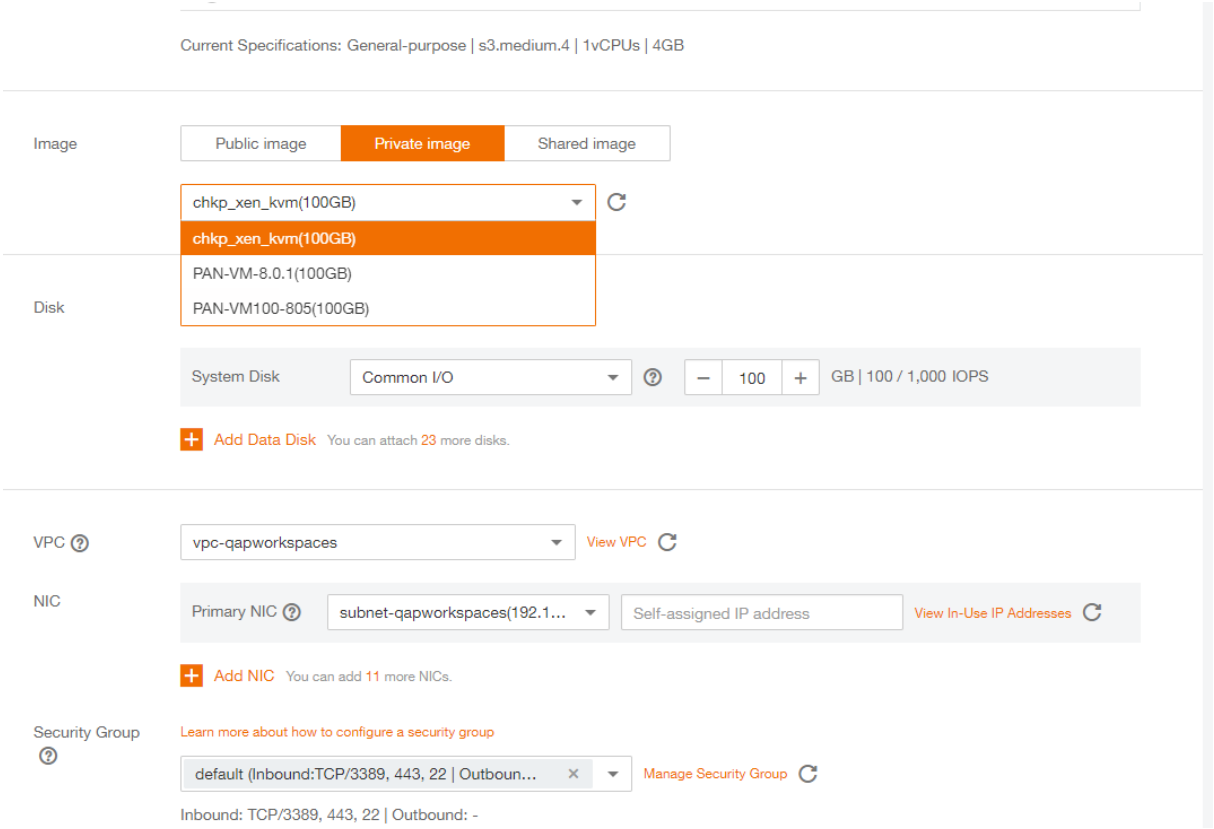
   For example, if the Local Disk value is 3 x 1800 GB, three HDDs are attached to the ECS and the capacity of each HDD is 1800 GB.

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*

Table 2 Parameter descriptions

Parameter	Description
	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. ** In our scenario: We created only two NIC cards one for the Management and the Other is for the Untrust Interfaces. The other two NIC cards will be created using API request on the Business and Web VPC's then will be assigned to the Fortigate VM **
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: • **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.

Table 2 Parameter descriptions

Parameter	Description
	** In our scenario: We assigned 2 EIP's one for the management NIC and the other for the Un trust 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 Palo Alto VM you can access it through **Https** using the EIP of the Management NIC. (username: admin / Password: admin)

5.3 Business and Web VPC's Ports creation and assignment to Palo Alto VM

In this section, we will explain how to create ports (NIC's) in the Server Farm VPC's and then assign the created NIC's to the Palo Alto VPC in order to be assignd as a port inside the Palo Alto VM.

The ports cannot be created using the normal FE GUI so we will use API requests to create the two Ports.

Prerequesite:

Inorder to create API requests and apply them to the VPC's. A Linux VM contains openstack client and configured to access the region conatining the target VPC's must be prepared for that purpose.

For more details about creating openstack client please check the URL:
https://docs.openstack.org/newton/user-guide/common/cli-install-openstack-command-line-clients.html

5.3.1 Port creation & assignment steps

In this part I will how how to create a port on a VPC using the API request.

1. Login through SSH to the Linux VM that is already created in one of your VPC's

2. Download openStack package using the following commands:

```
yum install python-devel python-pip
pip install python-openstackclient
```

3. After the openStack client is downloaded and installed. Create .env file.

```
vim filename.env
```

4. Add the following information inside the .env file

```
export OS_USER_DOMAIN_NAME=xxxxxxxxx ----
export OS_DOMAIN_NAME="xxxxxxxxxxx"     ----
export OS_AUTH_URL=https://iam.eu-west-0.prod-cloud-ocb.orange-business.com/v3
export OS_TENANT_NAME=eu-west-0
export OS_PROJECT_NAME=eu-west-0
export OS_INTERFACE=public
# No changes needed beyond this point
export NOVA_ENDPOINT_TYPE=publicURL
export OS_ENDPOINT_TYPE=publicURL
export CINDER_ENDPOINT_TYPE=publicURL
export OS_VOLUME_API_VERSION=2
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
#alias openstack='openstack --insecure'
export OS_USERNAME=ahmadsamak
export OS_PASSWORD=xxxxxxx--  -----
```

5. Save the .env file

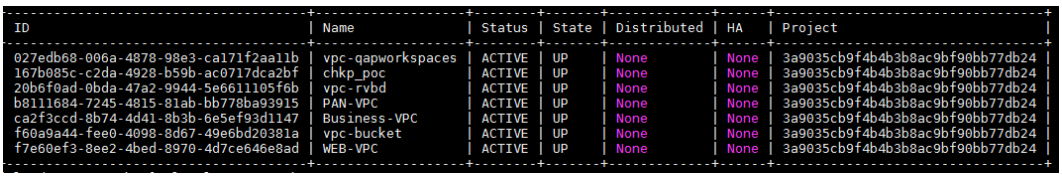
6. Type the command

```
source filename.env
```

7. Show the list of VPC's in the authenticated region

```
envfilename router list
```

This will display all the VPC's created in the authenticated region with their ID's



ID	Name	Status	State	Distributed	HA	Project
027edb68-006a-4878-98e3-ca171f2aa11b	vpc-qapworkspaces	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24
167b085c-c2da-4928-b59b-ac0717dca2bf	chkp_poc	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24
20b6f0ad-0bda-47a2-9944-5e6611105f6b	vpc-rvbd	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24
b8111684-7245-4815-81ab-bb778ba93915	PAN-VPC	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24
ca2f3ccd-8b74-4d41-8b3b-6e5ef93d1147	Business-VPC	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24
f60a9a44-fee0-4098-8d67-49e6bd20381a	vpc-bucket	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24
f7e60ef3-8ee2-4bed-8970-4d7ce646e8ad	WEB-VPC	ACTIVE	UP	None	None	3a9035cb9f4b4b3b8ac9bf90bb77db24

8. Show the list of subnets inside the VPC's

```
envfilename subnet list
```

This will display all the subnets created in the authenticated region with their ID's and IP ranges

```
+--------------------------------------+----------------------+--------------------------------------+-----------------+
| ID                                   | Name                 | Network                              | Subnet          |
+--------------------------------------+----------------------+--------------------------------------+-----------------+
| 0bed7520-0c84-4cdd-882e-112178cae08f | subnet-qapworkspaces | 471327fb-5d29-442b-a363-6d38500a441a | 192.168.0.0/24  |
| 3b313bec-7957-4356-bd49-b70dc4c33214 | internet             | 40dd760d-df92-499b-a790-0ceb6bbb9a69 | 192.168.0.0/24  |
| 40aa735e-eaf1-48f7-b04d-cce56be9030c | Business-Subnet      | 958e6c3b-d55e-428e-8635-c39835684fb3 | 10.1.0.0/24     |
| 59e5d263-bb79-49b5-8d56-276106b76a39 | Management           | 95cbb89f-cd7b-48a5-8887-eeda934f577c | 172.16.0.0/24   |
| 70ea84f3-fd8a-4e2b-af9e-68f5911e497f | subnet-f351          | 2669fefc-6335-41e7-a07e-a1de0c174b00 | 192.168.0.0/24  |
| 85edd8b9-382e-4c69-956f-69d3845ebb96 | VPN                  | b9547899-2cf1-4629-bc54-4a8778a1607a | 172.16.4.0/24   |
| 9a400447-2408-4ed0-a13e-104c4a714724 | Untrust              | cdd74181-bdb6-433d-9b40-268c14194c34 | 172.16.1.0/24   |
| 9b440bc7-344a-4ffe-8b47-3ff51a957434 | Web-Subnet           | 354c2859-89f7-4821-a400-9b028c46af7e | 10.0.0.0/24     |
| c33a7676-b731-4bb9-a571-f86a0a675e52 | intranet             | 8e7f023f-5614-4c2d-969f-e931b15d9928 | 192.168.10.0/24 |
| ca280392-0ba1-4a2e-ad0b-e355e44ca7dc | subnet-bucket        | a9100ce2-9806-4090-8738-18ad81448c10 | 192.168.0.0/24  |
+--------------------------------------+----------------------+--------------------------------------+-----------------+
```

9. Show the list of servers inside the VPC's

`envfilename server list`

This will display all the servers hosted in the VPC's with their ID's and IP addresses

```
| ID                                   | Name        | Status  | Networks                                                                    | Image
| Flavor       |
| c654919f-e47d-49ac-aaab-15beae9d510b | AD-Business | ACTIVE  | ca2f3ccd-8b74-4d41-8b3b-6e5ef93d1147=10.1.0.4, 90.84.194.220
                                                                                                                               | OBS_U_Windows_2012R2-STD_UNI
| s1.xlarge    |
| 41c40106-5c41-4a61-9808-cc73093d52c4 | WebServer   | ACTIVE  | f7e60ef3-8ee2-4bed-8970-4d7ce646e8ad=10.0.0.4, 90.84.192.59
                                                                                                                               | OBS_U_Windows_2012R2-STD_UNI
| s1.xlarge    |
| 35205328-2ee9-40ec-a24f-45724a849930 | open-stack  | ACTIVE  | f7e60ef3-8ee2-4bed-8970-4d7ce646e8ad=10.0.0.5, 90.84.193.160
                                                                                                                               | OBS_U_CentOS_7.3
| c1.large     |
| 47d6003d-f91e-411b-a830-08132a2e0680 | PAN-VM100   | ACTIVE  | b8111684-7245-4815-81ab-bb778ba93915=172.16.0.4, 172.16.1.4, 172.16.4.4, 90.84.46.122, 90
.84.46.130, 90.84.192.137; f7e60ef3-8ee2-4bed-8970-4d7ce646e8ad=10.0.0.231; ca2f3ccd-8b74-4d41-8b3b-6e5ef93d1147=10.1.0.72 | PAN-VM100-805
| s3.2xlarge.2 |
| 10897d57-f928-4325-8d64-13fce1cd59b1 | ecs-win2016 | ACTIVE  | 027edb68-006a-4878-98e3-ca171f2aa11b=192.168.0.179, 90.84.244.20
                                                                                                                               |
| c1.2xlarge   |
| 2275349a-ab75-436e-af30-42f67b8c9031 | chkp_img    | SHUTOFF | 167b085c-c2da-4928-b59b-ac0717dca2bf=192.168.0.45, 192.168.10.61, 90.84.246.214
                                                                                                                               | chkp_xen_kvm
| c1.xlarge    |
```

10. Create a port inside a subnet in a VPC using their ID's

`envfilename port create --fixedip subnet=subnetID --network=VPCID portname`

11. Show the list of created ports and determine the newly created Port ID from its name

`openstack port list`

```
[cloud@open-stack ~]$ openstack port list
| ID                                   | Name                                 | MAC Address       | Fixed IP Addresses
                        | Status |
| 00ac49c2-9551-48d6-a615-b2e3336fd053 |                                      | fa:16:3e:de:ac:b4 | ip_address='172.16.1.254', subnet_id='9a400447-2408-4e
d0-a13e-104c4a714724'   | DOWN   |
| 01d7fccb-6e39-40eb-a96c-3bc25bb9a7af |                                      | fa:16:3e:cc:89:df | ip_address='192.168.0.92', subnet_id='0bed7520-0c84-4c
dd-882e-112178cae08f'   | ACTIVE |
| 10799c1f-bbb7-4daa-9e64-60267fa577a3 |                                      | fa:16:3e:b3:38:a0 | ip_address='192.168.0.254', subnet_id='70ea84f3-fd8a-4
e2b-af9e-68f5911e497f'  | DOWN   |
| 1fbc9bb5-5e80-4d7a-a9c3-f979def248e3 | NIC3                                 | fa:16:3e:08:8c:a8 | ip_address='10.0.0.231', subnet_id='9b440bc7-344a-4ffe
-8b47-3ff51a957434'     | ACTIVE |
| 276f3ef0-8b70-4a85-a1e9-f66eeaa0fe35 |                                      | fa:16:3e:f6:d5:40 | ip_address='192.168.0.254', subnet_id='ca280392-0ba1-4
a2e-ad0b-e355e44ca7dc'  | DOWN   |
| 2e9e9717-e6c6-4372-89f1-34845ee3e6cd | 59e5d263-bb79-49b5-8d56-276106b76a39 | fa:16:3e:91:22:fb | ip_address='172.16.0.1', subnet_id='59e5d263-bb79-49b5
-8d56-276106b76a39'     | DOWN   |
| 30c7ac17-7148-4535-b5d3-2e98f319bbf8 |                                      | fa:16:3e:b5:68:00 | ip_address='172.16.1.244', subnet_id='9a400447-2408-4e
d0-a13e-104c4a714724'   | ACTIVE |
| 3aae0d08-b5b2-4a0a-a138-5db59a5a59e8 |                                      | fa:16:3e:77:cd:57 | ip_address='192.168.0.179', subnet_id='0bed7520-0c84-4
cdd-882e-112178cae08f'  | ACTIVE |
```

12. Assign the port created to the needed ECS (example: Palo Alto VM)

`envfilename server add port ECSID PORTID`

13. Now the port has been created in one VPC then assigned to an ECS as a NIC card in another VPC.

14. Check the ECS NICs from FE console you will find a new NIC has been added with an IP from another VPC as shown below.

15. Restart the Fortigate VM firewall to give the chance to the new port to correctly reflect its macaddress to the proper logical network interface on the vm-series firewall.

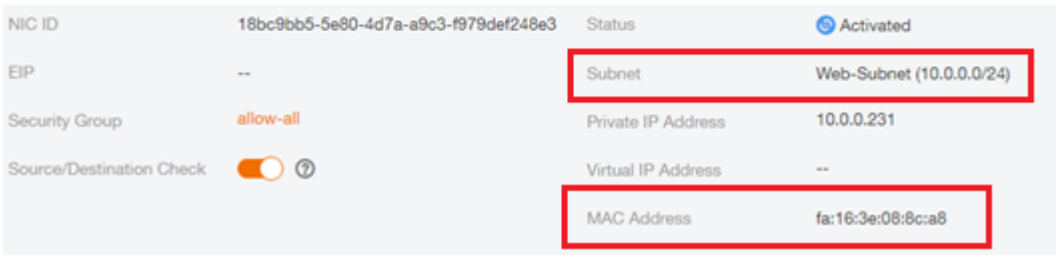
16. After restarting the Fortigate VM firewall access it through CLI and check the network interfaces and thier macadresses to see which interface has the same macaddress like the created port.

```
Show interface all
```

```
total configured hardware interfaces: 5

name                    id    speed/duplex/state        mac address
-------------------------------------------------------------------------
ethernet1/1             16    10000/full/up             fa:16:3e:1d:e4:a4
ethernet1/2             17    10000/full/up             fa:16:3e:f0:99:66
ethernet1/3             18    10000/full/up             fa:16:3e:08:8c:a8
ethernet1/4             19    10000/full/up             fa:16:3e:df:32:ff
tunnel                  4     [n/a]/[n/a]/up            e4:a7:49:6f:cf:04

aggregation groups: 0
```



From the above snapshots we can see that the created Port from Web VPC has its macaddress assigned to network interface ethernet1/3 so that the network interface ethernet1/3 should be configured as the web-zone facing interface on the FortiGate VM firewall.

Very Important Notice

Make sure that the mac address of the new port is correctly reflectd to the network interfaces in FortiGate VM firewall.