



FortiGate

High Availability on OCB Flex Engine Installation Deployment and configuration Guide

document control

date	version no.	author	change/addition
6 th December 2019	1.0	Ahmad Samak	Creation
21 st September 2021	2.0	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

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 Method	8
4.1	High Availability (Active – Passive) deployment	8
4.2	Checking the prerequisites	9
5	Deploy the FortiGate VM Firewalls 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	21
6.1	Primary Fortigate ECS Configuration	21
6.2	Secondary FortiGate ECS Configuration	23
6.3	Configuring FortiGate firewall policies.....	26
6.4	Creating virtual IPS for Fortigates on OCB Flex Engine	28
6.4.1	Managing virtual IP	28
6.5	IPSEC Tunnel Configuration.....	30
6.5.1	Configuring the onpremises IPsec VPN	30
6.5.2	Configuring OCB FE IPSEC VPN.....	33
6.5.3	Adding user defined route on OCB FE to allow traffic between on premisis and OCB Flex engine.....	35

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:

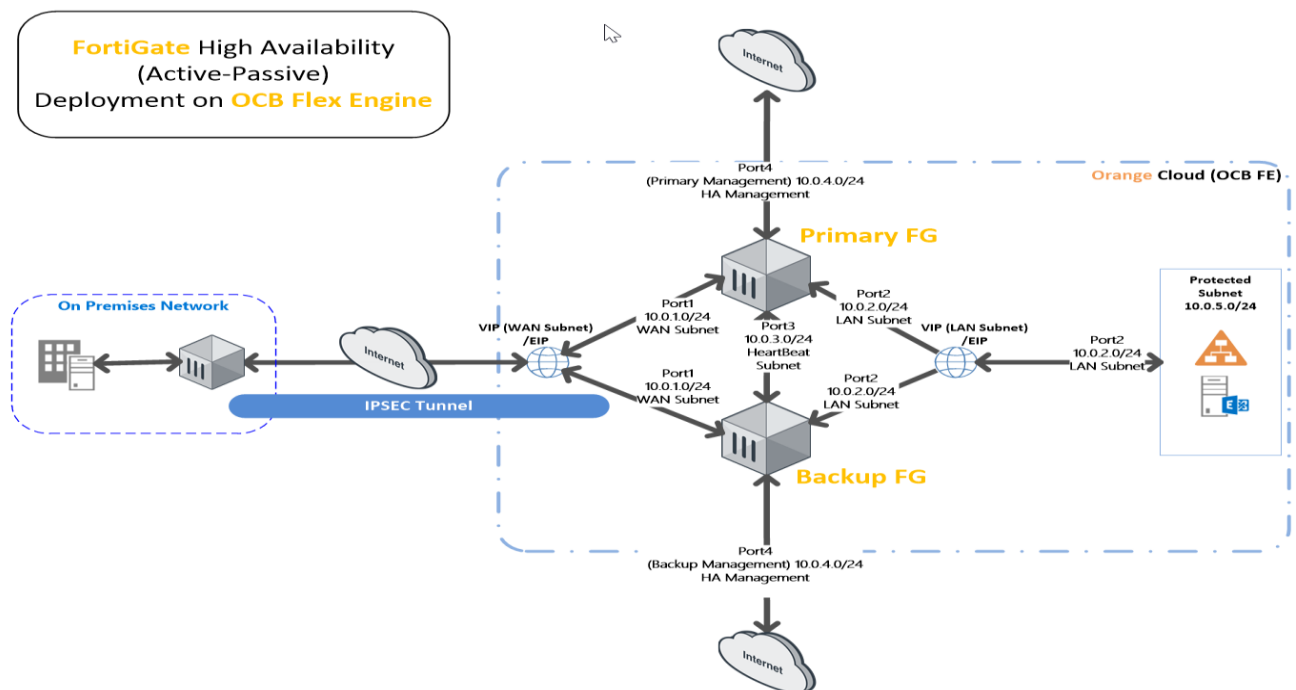
- create a 30GB log disk
- specify the virtual hardware settings

4 Deployment Method

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

4.1 High Availability (Active – Passive) deployment

A recommended installation requires four network interfaces per FortiGate-VM node. In addition to inbound and outbound data interfaces, the FortiGate-VMs use two interfaces for internal operations. Choose OCB Flex Engine ECS sizes that can equip four network interfaces. The table below outlines how the FortiGate-VMs use each port:



Port	Description
Port1	External data interface on the public network-facing side, 10.0.1.0/24. A public IP address (1.1.1.1) is associated with the active node's private IP address. FortiGate performs NAT for inbound and outbound traffic.
Port2	Internal data traffic interface on the protected network-facing side, 10.0.2.0/24. UDRs for networks behind the firewalls point to the active node port2 IP address.
Port3	Used for heartbeat between two FortiGate nodes on 10.0.3.0/24. This is the unicast communication. This heartbeat interface has its dedicated hbdev VDOM. You cannot use this interface for another purpose.
Port4	Dedicated management interface, placed on the subnet 10.0.4.0/24, to each FortiGate (2.2.2.2 for FortiGate A and 3.3.3.3 for FortiGate B) so that you can access them over the Internet for management purposes, such as logging in

Port	Description
	the FortiGate via SSH or the GUI and making configuration changes. In case of heartbeat failure, a passive firewall needs a dedicated port to communicate with OCB Flex Engine to issue failover-related commands. This port should always be available, regardless of the node status (active or passive), except when the node is unexpectedly down.

4.2 Checking the prerequisites

The following is required for a successful deployment:

- Availability to accommodate required OCB Flex Engine resources
 - VPC with five subnets (new or existing)
 - One for traffic to/through the active (primary) FortiGate
 - The second for the internal (LAN) ports facing the protected subnet.
 - Three public IP addresses
 - One for traffic to/through the active (primary) FortiGate
 - Two for management access to each FortiGate
 - All IP addresses must be static, not DHCP.
 - Two FortiGate-VM ECS's
 - You must deploy the two nodes in the same region and under the same VNet.
 - Each FortiGate-VM must have at least four network interfaces.
 - Decide the FortiGate login username and password.
- **IMPORTANT:** In this deployment on OCB Flex Engine, the FortiGate-VM can make API calls to change the route tables and the elastic IP address during a failover.

Once licensed and rebooted, you can proceed to configure the OCB Flex Engine settings to enable the cluster IP address and route table failover.

The following provides example installation for the primary and secondary FortiGates. Most of this configuration will be specific to your environment and so must be modified.

5 Deploy the FortiGate VM Firewalls on Orange Flex Engine

In our scenarios we have 1 VPC

- FGHA VPC that will host FortiGate VM Firewalls with 5 Subnets
- 2 FortiGate ECS's each ECS will have two disks one for the system and the other for the LOGS (SCSI)
- Protected Area Subnet.

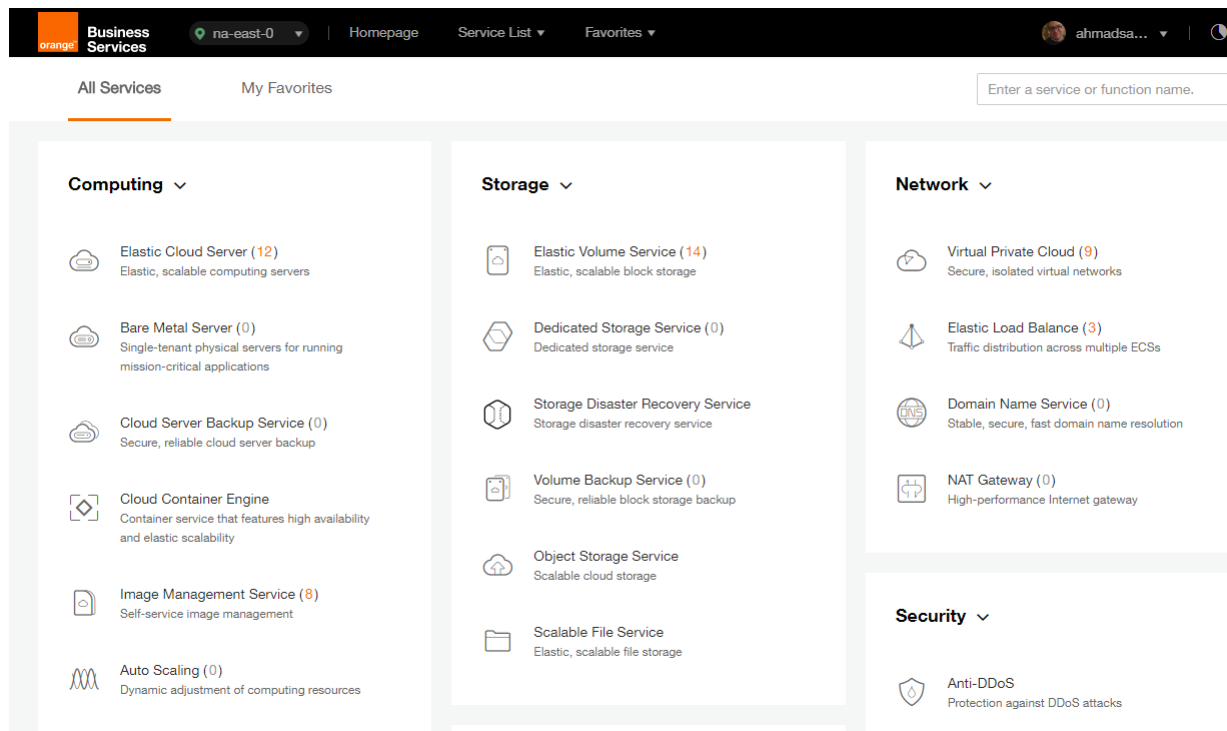
5.1 Create VPC

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

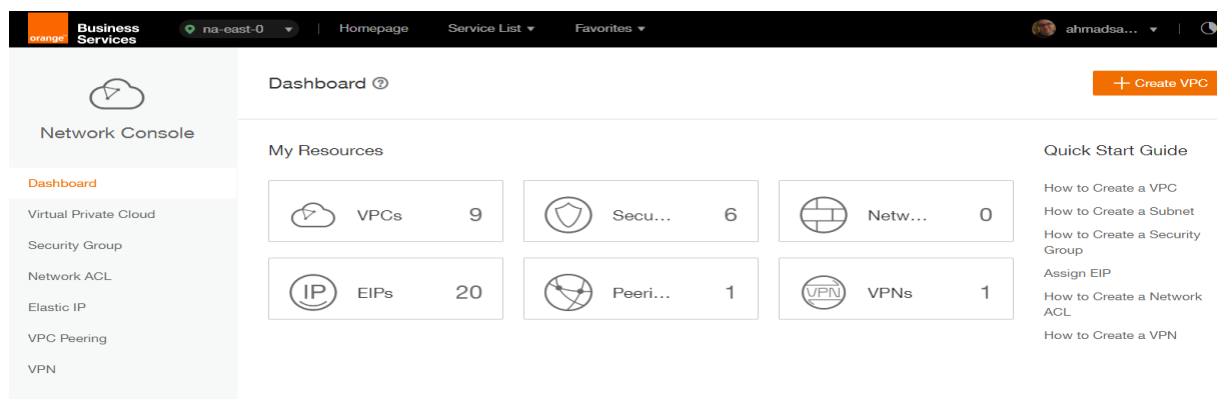
To use a VPC, first create it by following the procedure provided in this section. Then, create subnets, security groups, and VPNs, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

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



- 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

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



Network Console

- Dashboard
- Virtual Private Cloud**
- Security Group
- Network ACL
- Elastic IP
- VPC Peering
- VPN

VPC 

[+ Create VPC](#)

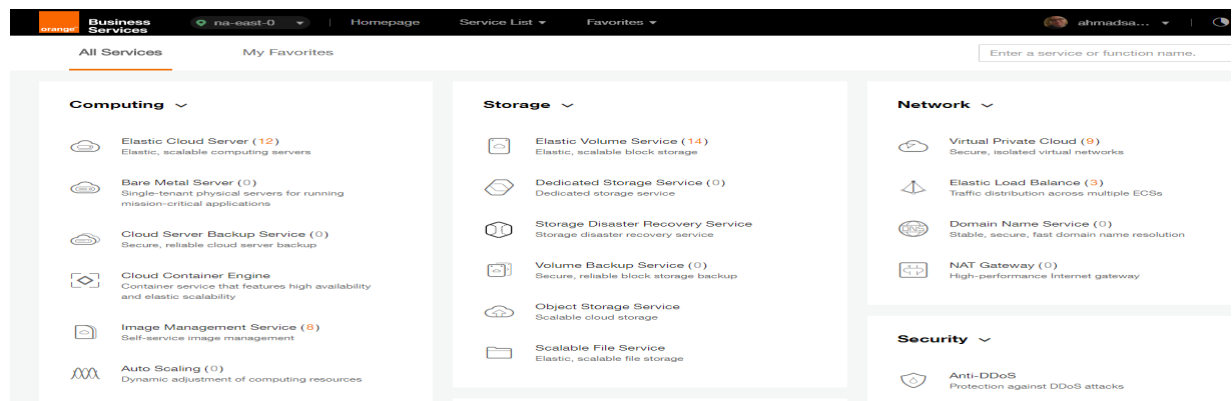
You can create 1 more VPCs.

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 h4cf28ed-h94f-445e-87ed-1dfb0c8c6efa	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**.



3. Click **Create ECS**.

Cloud Server Console

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

	Name/ID	AZ	Status	Specifications/Image	IP Address	Operation
Elastic Cloud Server						
Cloud Server Backup Service	<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
Bare Metal Server	<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
Elastic Volume Service	<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 (Priva...	Remote Login M
Dedicated Storage Service	<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
Volume Backup Service						
Image Management Service						
Auto Scaling						

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** eu-west-0b

Specifications

Enter a flavor name.

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	Com
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.

- 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.

- 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)



PAN-VM-8.0.1(100GB)

PAN-VM100-805(100GB)



Disk


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	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 <i>Virtual Private Cloud User</i>

Table 2 Parameter descriptions

Parameter	Description
	<p><i>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> <p>** 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 **</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> <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.

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 FortiGate ECS's you can access it through **Https** using the EIP of the WAN NIC. (username: admin / Password: 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) :

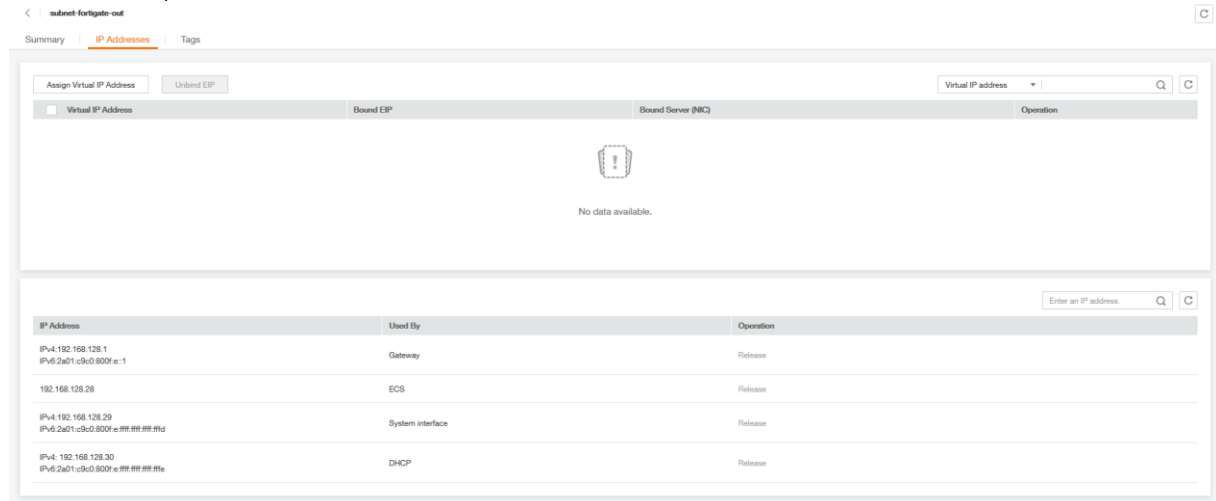
The screenshot shows the AWS Management Console for an ECS instance named 'ecs-fortigate-1'. The 'NICs' tab is active, showing two network interfaces:

- eni-fortigate-in**: Subnet: subnet-fortigate-in (192.168.128.0/27), Private IP Address: 192.168.128.28, Public IP Address: 90.84.177.140, Virtual IP Address: --, MAC Address: fa:16:3e:2a:d5:74.
- eni-fortigate-out**: Subnet: subnet-fortigate-out (192.168.128.0/27), Private IP Address: 192.168.128.52, Public IP Address: --, Virtual IP Address: --, MAC Address: fa:16:3e:2a:d5:74.

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**).

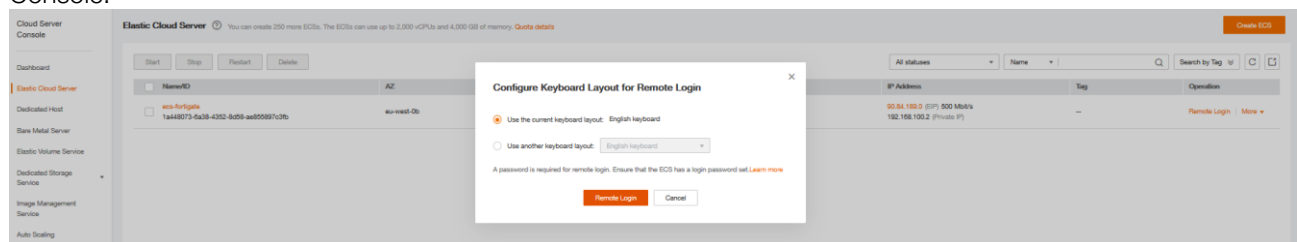
Note that “Source/Destination Check” option must be deactivated on all Fortigate ECS NIC.

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

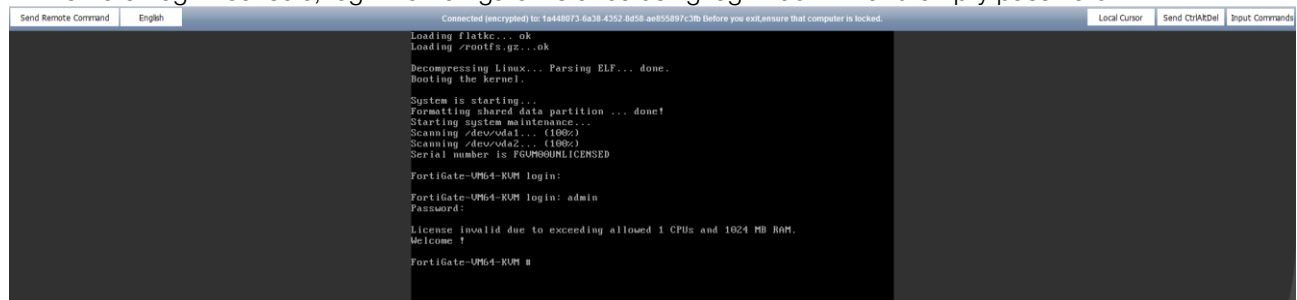


In this example, the subnet gateway address is **192.168.128.1**.

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:



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

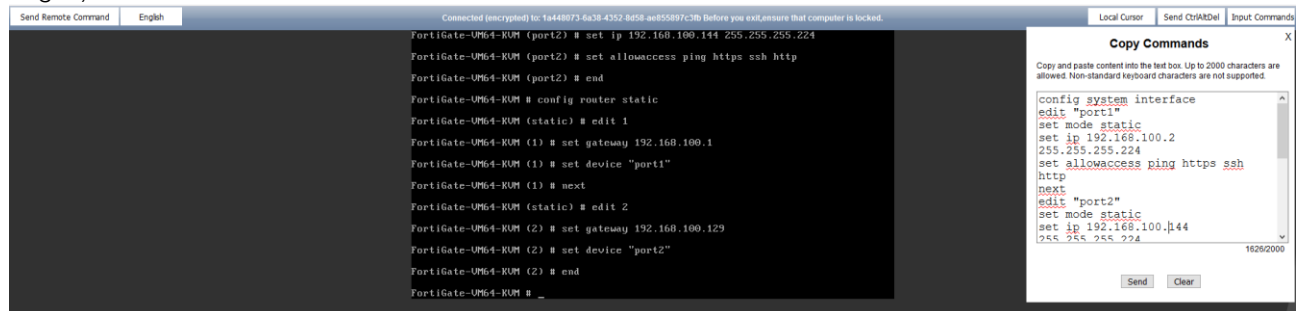
set allowaccess ping https ssh http

```

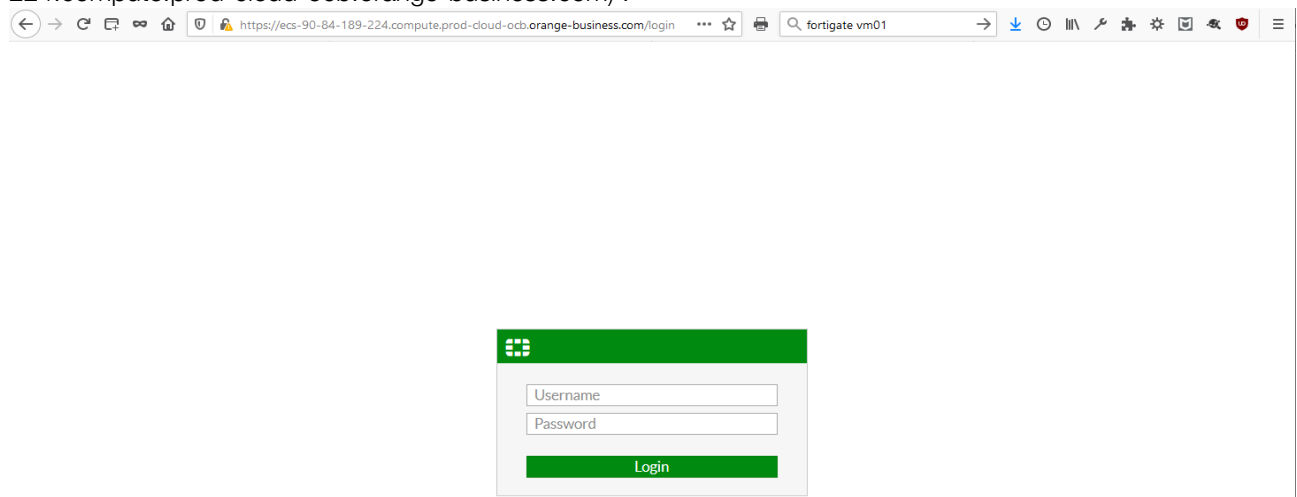
end
config router static
edit 1
set gateway 192.168.128.1
set device "port1"
end

```

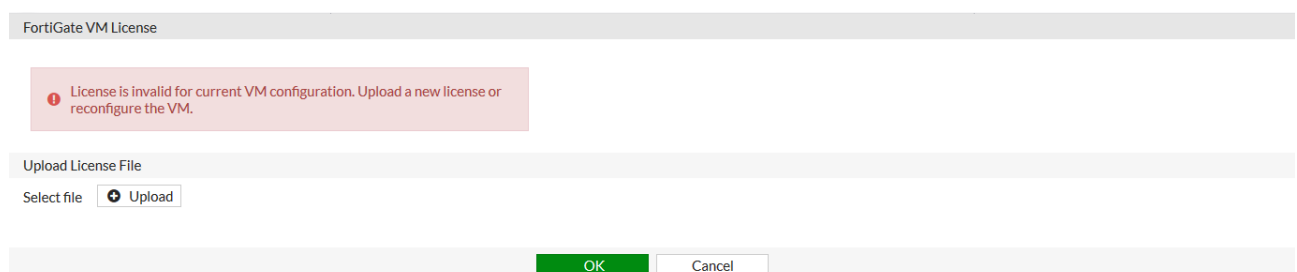
To ease this, use “Input Commands” button (available if you select “English keyboard” layout for “Remote Login”):



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 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:

Password Change

 This account is using the default password, it is strongly recommended that you change your password.

6 Solution Configuration

Immediately after initial deployment, your new FortiGate ECS's should have only one interface (port1) active with the IP address provided via DHCP. However, you should configure your new firewalls to use static IP addresses instead. FortiGate HA configuration relies on static settings, which DHCP invalidates. You must change your network configuration to use static IP addresses. You can accomplish this using the FortiGate CLI or GUI.

Connect via SSH to the IP address associated with FortiGate A's port1.

The below are configurations made in the CLI **before** changing port1 to a static IP address. The variables are based on the example diagram. Replace these with your own values.

6.1 Primary Fortigate ECS Configuration

```
config system interface
edit "port2"
set mode static
set ip 10.0.2.4 255.255.255.0
set allowaccess ping ssh
set alias "internal"
next
edit "port3"
set mode static
set ip 10.0.3.4 255.255.255.0
set allowaccess ping probe-response
set alias "hasyncport"
next
edit "port4"
set mode static
set ip 10.0.4.4 255.255.255.0
set allowaccess ping https ssh snmp fgfm radius-acct capwap ftm
```

```
set alias "management"

next

end

config router static

edit 1

set gateway 10.0.1.1

set device port1

next

edit 2

set dst 10.0.5.0 255.255.255.0

set gateway 10.0.2.1

set device "port2"

next

end

config system ha

set group-name "HAtest"

set mode a-p

set hbdev "port3" 100

set session-pickup enable

set session-pickup-connectionless enable

set ha-mgmt-status enable

config ha-mgmt-interfaces

edit 1

set interface "port4"

set gateway 10.0.4.1

next
```

```
end

set override disable

set priority 200

set unicast-hb enable

set unicast-hb-peerip 10.0.3.5

end
```

The italicized commands were introduced to unicast HA for public cloud FortiGate-VM. When these lines are present, the FGCP cluster does not use virtual IP and MAC addresses. Instead, both firewall nodes have distinguished IP addresses that point to the counterpart's heartbeat IP address.

After finishing the configuration on FortiGate A, connect via SSH to FortiGate B:

```
# exec ssh 10.0.1.5
```

6.2 Secondary FortiGate ECS Configuration

```
config system interface

edit "port2"

set mode static

set ip 10.0.2.5 255.255.255.0

set allowaccess ping ssh

set alias "internal"

next

edit "port3"

set mode static

set ip 10.0.3.5 255.255.255.0

set allowaccess ping probe-response

set alias "hasyncport"

next
```

```
edit "port4"

set mode static

set ip 10.0.4.5 255.255.255.0

set allowaccess ping https ssh snmp fgfm radius-acct capwap ftm

set alias "management"

next

end

config router static

edit 1

set gateway 10.0.1.1

set device port1

next

edit 2

set dst 10.0.5.0 255.255.255.0

set gateway 10.0.2.1

set device "port2"

next

end

config system ha

set group-name "HAtest"

set mode a-p

set hbdev "port3" 100

set session-pickup enable

set session-pickup-connectionless enable

set ha-mgmt-status enable

config ha-mgmt-interfaces
```



```

edit 1

set interface "port4"

set gateway 10.0.4.1

next

end

set override disable

set priority 200

set unicast-hb enable

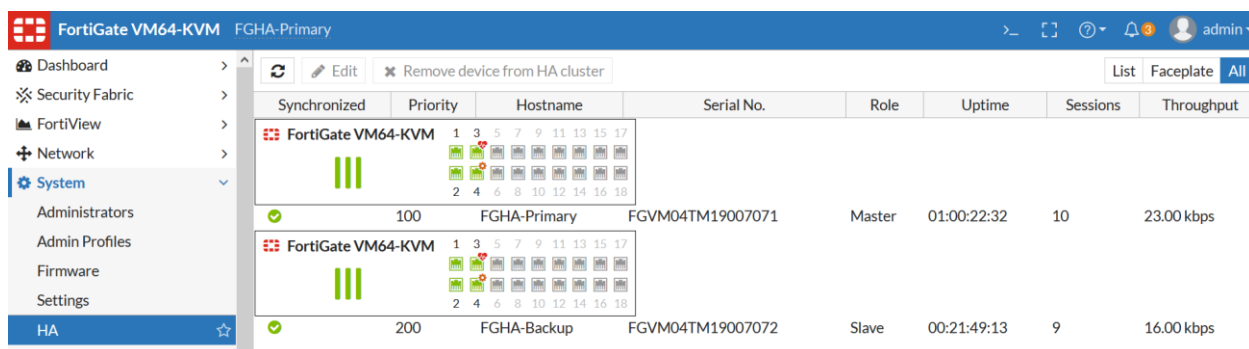
set unicast-hb-peerip 10.0.3.4

end



```

The FortiGate with the lower set priority value is determined as the secondary node, as FortiGate B is in the example.

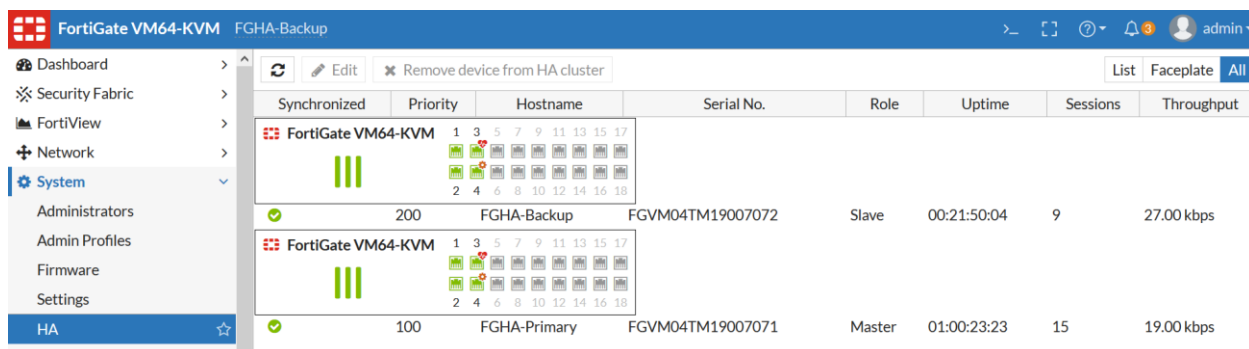
Since your HA configuration has now specified your port4 as the dedicated management interface, you can exit the current SSH session and start a new one to your dedicated management IP address, FGTMgmtPublicIp. You can also now change the port1 IP address to a static IP address.





The screenshot shows the FortiGate VM64-KVM HA configuration interface. The left sidebar lists various system settings, with 'HA' selected. The main table displays the HA cluster configuration for two FortiGate VM64-KVM instances.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
	100	FGHA-Primary	FGVM04TM19007071	Master	01:00:22:32	10	23.00 kbps
	200	FGHA-Backup	FGVM04TM19007072	Slave	00:21:49:13	9	16.00 kbps

Primary FortiGate (Master) & Secondary FortiGate (Slave)



The screenshot shows the FortiGate VM64-KVM HA configuration interface from the perspective of the Secondary FortiGate (Slave). The left sidebar lists various system settings, with 'HA' selected. The main table displays the HA cluster configuration for two FortiGate VM64-KVM instances.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
	200	FGHA-Backup	FGVM04TM19007072	Slave	00:21:50:04	9	27.00 kbps
	100	FGHA-Primary	FGVM04TM19007071	Master	01:00:23:23	15	19.00 kbps

6.3 Configuring FortiGate firewall policies

First, configure Primary Fortigate. In the FortiGate ECS console, select *Policy & Objects > IPv4 Policy* and create two new policies, as shown in this example. Create one policy for outgoing traffic from the private subnet, through the public subnet, to the Internet. Create another policy for incoming traffic from the Internet, through the public subnet, to the private subnet

Dashboard > **New Policy**

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

IPv4 Policy >

IPv4 DoS Policy >

Addresses >

Internet Service Database >

Services >

Schedules >

Virtual IPs >

IP Pools >

Traffic Shapers >

Traffic Shaping Policy >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Name 1

Incoming Interface port2

Outgoing Interface port1

Source all

Destination all

Schedule always

Service ALL

Action ☒ ACCEPT ☐ DENY ☐ LEARN

Firewall / Network Options

NAT ☒

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

Security Profiles

AntiVirus ☒ AV default

Web Filter ☒ WEB default

DNS Filter ☒ DNS default

Application Control ☒ APP default

IPS ☐

SSL/SSH Inspection ☐ certificate-inspection

Logging Options

Log Allowed Traffic ☒ Security Events ☐ All Sessions

Generate Logs when Session Starts ☐

Capture Packets ☐

Comments Write a comment... 0/1023

Enable this policy ☒

OK **Cancel**

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Traffic Shapers

Traffic Shaping Policy

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

New Policy

Name

2

Incoming Interface

port1

Outgoing Interface

port2

Source

all

Destination

all

Schedule

always

Service

ALL

Action

ACCEPT

DENY

LEARN

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Security Profiles

AntiVirus

AV

default

Web Filter

WEB

default

DNS Filter

DNS

default

Application Control

APP

default

IPS

IPS

default

SSL/SSH Inspection

SSL

certificate-inspection

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Generate Logs when Session Starts

Capture Packets

Comments

Write a comment...

0/1023

Enable this policy

OK

Cancel

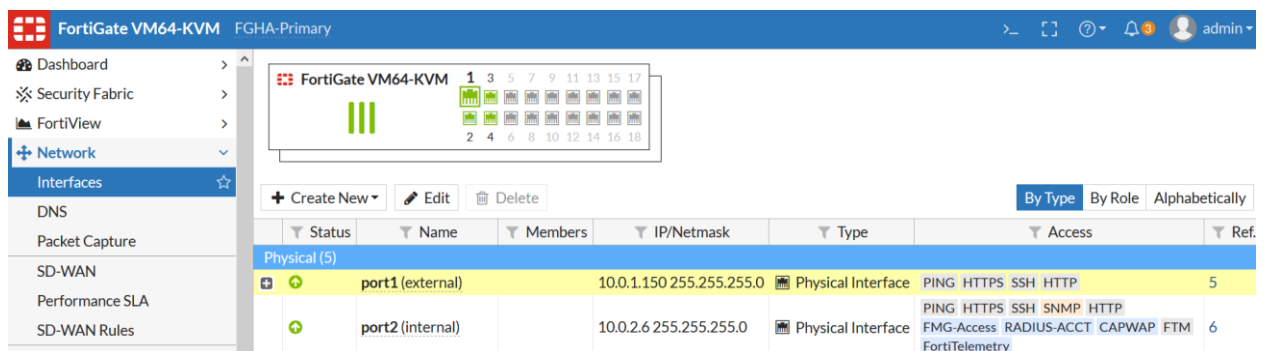
6.4 Creating virtual IPS for Fortigates on OCB Flex Engine

You have to create 2 virtual IPS on OCB Flex Engine for the Fortigate HA configuration. The purpose behind these virtual IPS is to assign 1 virtual IP to the WAN Port (Port1) and the Inside Port (Port2) then assigning Elastic IP's two these virtual IPS.

Important:

When you assign the virtual IP's with their elastic IP's to Port1 and Port2 in the Primary Fortigate ECS. It will synchronize the same configuration to the Secondary Fortigate.

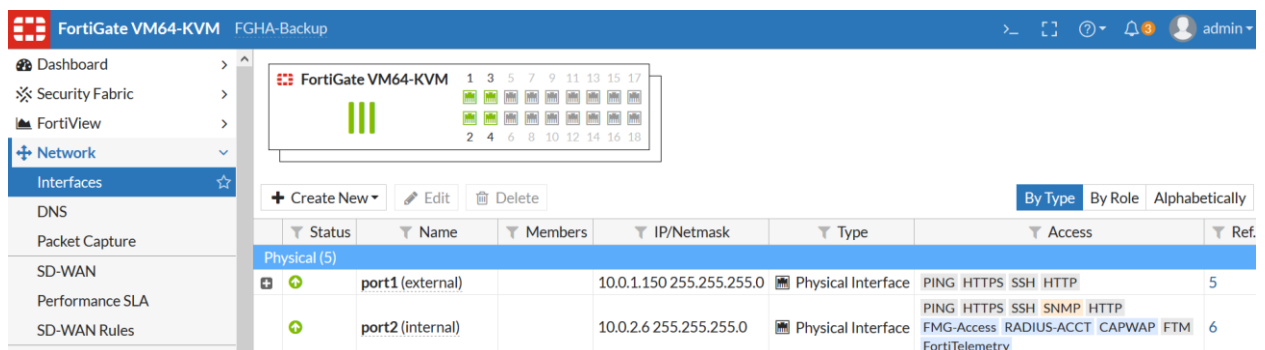
The images below show the primary and backup fortigates after configuring the virtual IP and assigning to the Primary fortigate.



The screenshot shows the FortiGate VM64-KVM FGHA-Primary configuration page. The left sidebar lists various configuration sections, with 'Network' and 'Interfaces' selected. The main area displays a table of physical interfaces.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (5)						
+	port1 (external)		10.0.1.150 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	5
+	port2 (internal)		10.0.2.6 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP FMG-Access RADIUS-ACCT CAPWAP FTM FortiTelemetry	6

Primary Fortigate



The screenshot shows the FortiGate VM64-KVM FGHA-Backup configuration page. The left sidebar lists various configuration sections, with 'Network' and 'Interfaces' selected. The main area displays a table of physical interfaces.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (5)						
+	port1 (external)		10.0.1.150 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	5
+	port2 (internal)		10.0.2.6 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP FMG-Access RADIUS-ACCT CAPWAP FTM FortiTelemetry	6

Backup Fortigate

6.4.1 Managing virtual IP

A virtual IP address provides the second IP address for one or more ECS NICs, improving high availability between the ECSs.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. On the **Elastic Cloud Server** page, click the name of the target ECS.

The page providing details about the ECS is displayed.

4. Click the **NICs** tab. Then, click **Manage Virtual IP Address**. (In our case we will bind virtual IPS for both Port1 and Port 2)
5. In the **Manage Virtual IP Address** dialog box, select **Bind virtual IP address**.
6. Set the IP address.

This IP address is a virtual one. Multiple ECSs deployed to work in active/standby mode can be bound with the same virtual IP address for disaster recovery.

7. Click **OK**.

Subnet > WAN-Subnet

Summary **IP Addresses** Tags

Assign Virtual IP Address Virtual IP address

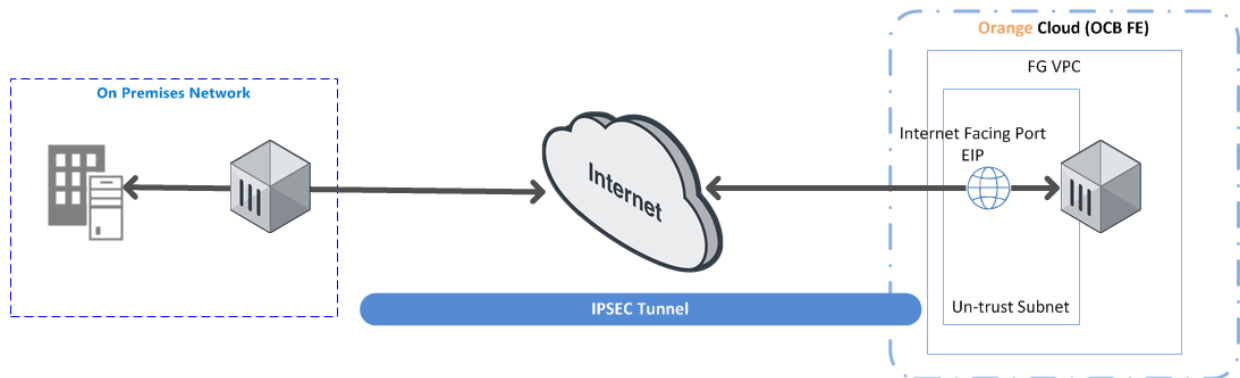
Virtual IP Address	Bound EIP	Bound Server (NIC)	Operation
10.0.1.150	90.84.196.130	FGHA-Backup (10.0.1.5) View All (2)	Unbind from EIP More

Bound Server

Name

Name	Type	Status	Private IP Address	Operation
FGHA-Primary	ECS	Running	10.0.1.4	Unbind
FGHA-Backup	ECS	Running	10.0.1.5	Unbind

6.5 IPSEC Tunnel Configuration



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

6.5.1 Configuring the onpremises 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

This FortiGate Remote FortiGate

< Back Next > Cancel

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

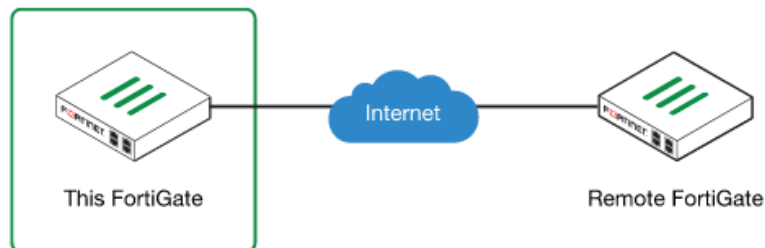
2. In the **Authentication** step, set **IP Address** to the IP of the Branch FortiGate. After you enter the gateway, an available interface will be assigned as the Outgoing Interface. If you wish to use a different interface, select it from the drop-down menu. Set a secure Pre-shared Key.

VPN Creation Wizard

✓ VPN Setup > ② Authentication > ③ Policy & Routing

Remote Device	IP Address Dynamic DNS
IP Address	172.20.120.135
Outgoing Interface	↑ wan1
Detected via routing lookup	
Authentication Method	Pre-shared Key Signature
Pre-shared Key	•••••

HQ-to-Branch: Site to Site - FortiGate



< Back

Next >

Cancel

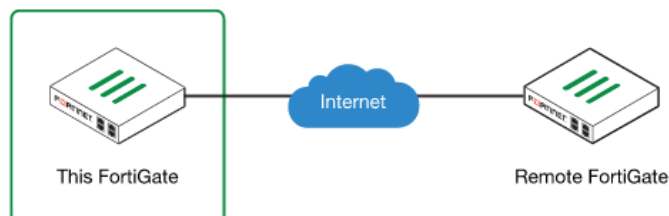
3. In the **Policy & Routing** step, set the Local Interface. The Local Subnets will be added automatically. Set Remote Subnets to the Branch FortiGate's local subnet.

VPN Creation Wizard

✓ VPN Setup > ✓ Authentication > ③ Policy & Routing

Local Interface	↑ lan
Local Subnets ⓘ	10.10.10.0/24
Remote Subnets ⓘ	5.5.5.5/24

HQ-to-Branch: 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.

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

[Add Another](#)[Show Tunnel List](#)

6.5.2 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

< Back Next > Cancel

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.

VPN Creation Wizard

✓ VPN Setup > 2 Authentication > 3 Policy & Routing

Remote Device

IP Address

Outgoing Interface

Detected via routing lookup

Authentication Method

Pre-shared Key

Branch-to-HQ: Site to Site - FortiGate

< Back Next > Cancel

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

VPN Creation Wizard

✓ VPN Setup > ✓ Authentication > 3 Policy & Routing

Local Interface

Local Subnets

Remote Subnets

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.

VPN Creation Wizard

✓ VPN Setup > ✓ Authentication > ✓ Policy & Routing

✓ The VPN has been set up

Summary of Created Objects

Phase 1 Interface	Branch-to-HQ
Phase 2 Interfaces	Branch-to-HQ
Static Routes	10.10.10.1/24
Local Address Group	Branch-to-HQ_local
Remote Address Group	Branch-to-HQ_remote
Local to Remote Policy	vpn_Branch-to-HQ_local
Remote to Local Policy	vpn_Branch-to-HQ_remote

[Add Another](#)
[Show Tunnel List](#)

6.5.3 Adding user defined route on OCB FE to allow traffic between on premisis and OCB Flex engine

Route Tables > **rtb-FGHA-VPC**

Summary Associated Subnets

Name	rtb-FGHA-VPC	Type	Default
ID	e2147df1-8a0d-460b-a82c-6fedb2220bc0	VPC	FGHA-VPC
Description	--		

Routes

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

<input type="checkbox"/> Destination	Next Hop ...	Next Hop	Type	Description	Operation
<input checked="" type="checkbox"/> Local	Local	Local	System	Default route that ...	Modify Delete
<input type="checkbox"/> 172.16.1.0/24	Virtual IP ...	10.0.2.6 a204078e...	Custom	--	Modify Delete