


Instructions to get the installation completed manually

1. Upload license

Login as admin with password equal to instance id

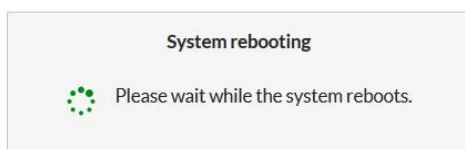
FortiGate VM License

 License is invalid for current VM configuration. Upload a new license or reconfigure the VM.

Upload License File

Select file

The instance reboots.




2. Configure inside interface port2


- It will be temporarily used for management.

Interface Name port2 (02:0E:B8:36:2C:A8)

Alias

Link Status Up 

Type Physical Interface


Role 


Address


Addressing mode

IP/Network Mask

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP  ☒ PING ☐ FMG-Access
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry


Receive LLDP 


Transmit LLDP 

3. Configure Static Route

- The route is required to establish SSH session from the internal virtual machine.


New Static Route


Dynamic Gateway  ☐

Destination  Subnet Internet Service



10.3.0.0/16

Gateway Address 10.3.4.1

Interface  inside (port2) ▼

Administrative Distance  10

Comments Write a comment... 0/255

Status  Enabled  Disabled

+ Advanced Options

OK Cancel

4. SSH to CLI on the inside interface from the virtual machine


```
ubuntu@ip-10-3-10-10:~$ ssh admin@10.3.4.10
The authenticity of host '10.3.4.10 (10.3.4.10)' can't be established.
ED25519 key fingerprint is SHA256:pQWKUGxcXuN740L77hXAKCNxbKfHbYlpiH1T7ZlntBA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.3.4.10' (ED25519) to the list of known hosts.
admin@10.3.4.10's password:
FG-A #
FG-A #
FG-A #
```

5. Configure hb port 3 and mgmt port4


- Both interfaces port3 and port4 are configured in the same way.
- Submit changes always in two steps.
- First, disable retrieval of default gateway from the server. It prevent the default route from being configured manually later on.

Interface Name port4 (02:B1:33:C8:CA:FE)

Alias mgmt


Link Status Up 


Type Physical Interface

Role  Undefined ▼


Address


Addressing mode Manual DHCP One-Arm Sniffer

Retrieve default gateway from server 



Override internal DNS 

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP  ☒ PING ☐ FMG-Access
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

Receive LLDP  Use VDOM Setting Enable Disable




- Second, disable DHCP and set the IP address manually.

Interface Name port4 (02:B1:33:C8:CA:FE)
Alias mgmt
Link Status Up 
Type Physical Interface
Role  Undefined

Address










Addressing mode **Manual** DHCP One-Arm Sniffer
IP/Network Mask 10.3.6.10/255.255.255.0

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP  ☒ PING ☐ FMG-Access
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry
Receive LLDP  **Use VDOM Setting** Enable Disable
Transmit LLDP  **Use VDOM Setting** Enable Disable

6. Configure static default gateway

New Static Route

Dynamic Gateway  
Destination  **Subnet** Internet Service
0.0.0.0/0.0.0.0
Gateway Address  Dynamic **Specify** 10.3.0.1
Interface  port1
Administrative Distance  10
Comments Write a comment...  0/255
Status  Enabled  Disabled

Advanced Options

OK

Cancel

7. Configure external port1

- Disable "Retrieve default gateway from the server".

Interface Name	port1 (02:AD:DC:91:B2:5A)
Alias	<input type="text" value="external"/>
Link Status	Up
Type	Physical Interface
Role	<input type="text" value="Undefined"/>

Address

Addressing mode	<input type="button" value="Manual"/> <input checked="" type="button" value="DHCP"/>
Status	Connected
Obtained IP/Netmask	10.3.0.10 255.255.255.0 <input type="button" value="Renew"/>
Expiry Date	2020/01/09 00:58:21
Acquired DNS	10.3.0.2
Default Gateway	10.3.0.1
Retrieve default gateway from server	<input type="radio"/>
Override internal DNS	<input checked="" type="radio"/>

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> FMG-Access
	<input type="checkbox"/> CAPWAP	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> FortiTelemetry		
Receive LLDP	<input checked="" type="button" value="Use VDOM Setting"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	

- Step2, Disable DHCP.

Interface Name	port1 (02:AD:DC:91:B2:5A)
Alias	<input type="text" value="external"/>
Link Status	Up
Type	Physical Interface
Role	<input type="text" value="Undefined"/>

Address

Addressing mode	<input checked="" type="button" value="Manual"/> <input type="button" value="DHCP"/>
IP/Network Mask	<input type="text" value="10.3.0.10/255.255.255.0"/>

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> FMG-Access
	<input type="checkbox"/> CAPWAP	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> FortiTelemetry		
Receive LLDP	<input checked="" type="button" value="Use VDOM Setting"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	
Transmit LLDP	<input checked="" type="button" value="Use VDOM Setting"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	

Repeat the steps for second FortiGate-VM

8. Configure FortiGate VM-A & B through GUI and CLI

FG-A High Availability

```
FG-A # show system ha
config system ha
  set group-name "test"
  set mode a-p
  set hbdev "port3" 50
  set session-pickup enable
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
      set gateway 10.3.6.1
    next
  end
  set override disable
  set unicast-hb enable
  set unicast-hb-peerip 10.3.3.10
end
```

FG-B High Availability

```
FG-B # show system ha
config system ha
  set group-name "test"
  set mode a-p
  set hbdev "port3" 50
  set session-pickup enable
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
      set gateway 10.3.7.1
    next
  end
  set override disable
  set priority 50
  set unicast-hb enable
  set unicast-hb-peerip 10.3.2.10
end
```

9. Disassociate EIP from standby FG-B outside interface.

The EIP is disassociated automatically by the FG-B itself. It's recommended to do it manually though.

10. Check HA status

Connect to management interfaces (10.3.6.10 and 10.3.7.10 for FG-A and FG-B respectively)

FG-A

```
ubuntu@ip-10-3-10-10:~$ ssh admin@10.3.6.10
admin@10.3.6.10's password:
FG-A #
FG-A #
FG-A #
FG-A # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-AWS
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:22:0
Cluster state change time: 2020-01-09 06:31:32
Master selected using:
  <2020/01/09 06:31:32> FGVM01TM19008253 is selected as the master because it has the largest value of override priority.
  <2020/01/09 06:31:32> FGVM01TM19008253 is selected as the master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=10.3.3.10, myip=10.3.2.10, hasync_port='port3'
Configuration Status:
  FGVM01TM19008253(updated 4 seconds ago): in-sync
  FGVM01TM19008522(updated 3 seconds ago): in-sync
System Usage stats:
  FGVM01TM19008253(updated 4 seconds ago):
    sessions=23, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=8%
  FGVM01TM19008522(updated 3 seconds ago):
    sessions=14, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=8%
HBDEV stats:
  FGVM01TM19008253(updated 4 seconds ago):
    port3: physical/00, up, rx-bytes/packets/dropped/errors=289304/951/0/0, tx=392176/913/0/0
  FGVM01TM19008522(updated 3 seconds ago):
    port3: physical/00, up, rx-bytes/packets/dropped/errors=1102164/2097/0/0, tx=728293/2219/0/0
Master: FG-A, FGVM01TM19008253, HA cluster index = 1
Slave : FG-B, FGVM01TM19008522, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 10.3.2.10
Master: FGVM01TM19008253, HA operating index = 0
Slave : FGVM01TM19008522, HA operating index = 1
```

FG-B

```
FG-B # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-AWS
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:23:38
Cluster state change time: 2020-01-09 06:31:34
Master selected using:
  <2020/01/09 06:31:34> FGVM01TM19008253 is selected as the master because it has the largest value of override priority.
  <2020/01/09 06:30:56> FGVM01TM19008522 is selected as the master because it's the only member in the cluster.
  <2020/01/09 06:28:19> FGVM01TM19008253 is selected as the master because it has the largest value of override priority.
  <2020/01/09 06:28:19> FGVM01TM19008522 is selected as the master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=10.3.2.10, myip=10.3.3.10, hasync_port='port3'
Configuration Status:
  FGVM01TM19008522(updated 1 seconds ago): in-sync
  FGVM01TM19008253(updated 2 seconds ago): in-sync
System Usage stats:
  FGVM01TM19008522(updated 1 seconds ago):
    sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=8%
  FGVM01TM19008253(updated 2 seconds ago):
    sessions=4, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=8%
HBDEV stats:
  FGVM01TM19008522(updated 1 seconds ago):
    port3: physical/00, up, rx-bytes/packets/dropped/errors=1406331/2704/0/0, tx=939515/2815/0/0
  FGVM01TM19008253(updated 2 seconds ago):
    port3: physical/00, up, rx-bytes/packets/dropped/errors=493516/1548/0/0, tx=703973/1520/0/0
Slave : FG-B      , FGVM01TM19008522, HA cluster index = 0
Master: FG-A      , FGVM01TM19008253, HA cluster index = 1
number of vcluster: 1
vcluster 1: standby 10.3.2.10
Slave : FGVM01TM19008522, HA operating index = 1
Master: FGVM01TM19008253, HA operating index = 0
```

11. Configure the internal Routing Table in AWS

On the active instance identify the IP address of the internal interface.

FG-A

HA: Master

FortiGate VM64-AWS

1 3 5 7 9 11 13 15 17

2 4 6 8 10 12 14 16 18

+ Create New

Edit

Delete

Status	Name	Members	IP/Netmask	Type	
Physical (4)					
	port1 (external)		10.3.0.10 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FI
	port2 (inside)		10.3.4.10 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP
	port3 (hb)		10.3.2.10 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP
	port4 (mgmt)		10.3.6.10 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP

Identify the relevant eni-*

Details	Flow Logs	Tags	
Network interface ID	eni-023f1528d7b40e734	Subnet ID	subnet-07e766e7787f57d9d
VPC ID	vpc-057539529f9ae960d	Availability Zone	eu-west-1a
MAC address	02:8a:6d:ef:f7:ee	Description	-
Security groups	sg_fortigate_vm. view inbound rules. view outbound rules	Network interface owner	620312619173
Status	in-use	Primary private IPv4 IP	10.3.4.10
Private DNS (IPv4)	-	IPv4 Public IP	-
Secondary private IPv4 IPs	-	IPv6 IPs	-
Elastic Fabric Adapter	Disabled	Source/dest. check	true
Attachment ID	eni-attach-0f75d0e3fc3e0fb5e	Instance ID	i-0df4d4bc9c5364e1a
Attachment owner	620312619173	Device index	1
Attachment status	attached	Delete on termination	false
Elastic IP owner	-	Allocation ID	-
Association ID	-	Outpost ID	-

Add the default route to the routing table rt-inside with the next-hp pointing to active FortiGate VM internal interface.

[Route Tables](#) > [Edit routes](#)

Edit routes

Destination	Target	Status	Propagated	
10.3.0.0/16	local	active	No	
44.3.0.0/16	local	active	No	
193.15.240.60/32	igw-013dfb55f82f04ee8	active	No	✕
0.0.0.0/0	eni-023f1528d7b40e734		No	✕
<button>Add route</button>				

* Required

[Cancel](#)

[Save routes](#)

12. Configure firewall policy

Name	To Internet
Incoming Interface	inside (port2)
Outgoing Interface	external (port1)
Source	VPC
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

Address VPC

Type Subnet

Subnet 10.3.0.0/16

Interface inside (port2)

Comments All subnets from the VPC

References 1

Edit

Firewall / Network Options

NAT ☒

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

Preserve Source Port ☐

Protocol Options ☒ PRX default

13. Initiate ping from a VM

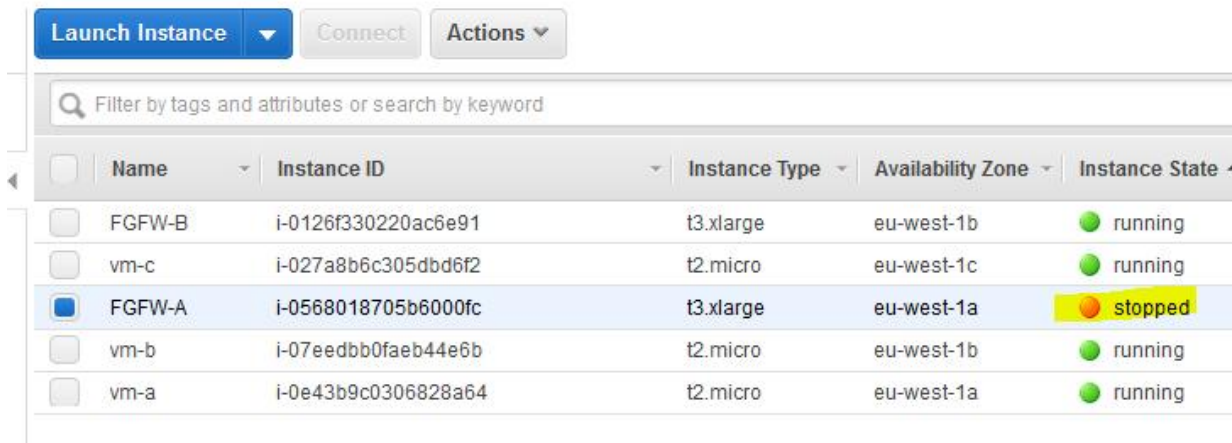
```
ubuntu@ip-10-3-10-10:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=47 time=0.820 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=47 time=0.762 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=47 time=0.797 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2056ms
rtt min/avg/max/mdev = 0.762/0.793/0.820/0.023 ms
ubuntu@ip-10-3-10-10:~$
```

Outgoing traffic is logged in the forwarding logs.

Date/Time		Source	Device	Destination	Application Name	Result	Policy
2020/01/07 14:50:33		10.3.10.10		8.8.8.8		✓ 588 B / 588 B	To Internet (1)
2020/01/07 14:50:21		10.3.10.10		8.8.8.8		✓ Accept: session start	To Internet (1)
2020/01/07 14:49:26		10.3.10.10		8.8.8.8		✓ Accept: session start	To Internet (1)

14. HA failover test

Stop the master instance through AWS console.



Launch Instance ▾ Connect Actions ▾

Filter by tags and attributes or search by keyword

	Name ▾	Instance ID ▾	Instance Type ▾	Availability Zone ▾	Instance State ▴
<input type="checkbox"/>	FGFW-B	i-0126f330220ac6e91	t3.xlarge	eu-west-1b	● running
<input type="checkbox"/>	vm-c	i-027a8b6c305dbd6f2	t2.micro	eu-west-1c	● running
<input checked="" type="checkbox"/>	FGFW-A	i-0568018705b6000fc	t3.xlarge	eu-west-1a	● stopped
<input type="checkbox"/>	vm-b	i-07eedbb0faeb44e6b	t2.micro	eu-west-1b	● running
<input type="checkbox"/>	vm-a	i-0e43b9c0306828a64	t2.micro	eu-west-1a	● running

Activate awsd debugging.

```
255 ubuntu@ip-10-3-10-10:~$ ssh admin@10.3.7.10
admin@10.3.7.10's password:
FG-B #
FG-B #
FG-B #
FG-B #
FG-B #
FG-B # di de en

FG-B # di de application awsd -1
Debug messages will be on for 30 minutes.

FG-B #
FG-B #
FG-B #
FG-B # Become HA master
send_vip_arp: vd root master 1 intf port1 ip 10.3.1.10
send_vip_arp: vd root master 1 intf port2 ip 10.3.5.10
awsd get instance id i-0126f330220ac6e91
awsd get iam role NextGenFirewallHA
awsd get region eu-west-1
awsd get vpc id vpc-0bfa0c90a160e582f
awsd doing ha failover for vdom root
awsd associate elastic ip for port1
awsd associate elastic ip allocation eipalloc-0f7140ed02e5ea7c0 to 10.3.1.10 of eni eni-0eec9e5b7a796d291
awsd associate elastic ip successfully
awsd associate elastic ip for port2
awsd update route table rtb-061c31bc5c6b27bad, replace route of dst 0.0.0.0/0 to eni-009d4682c3561e457
awsd update route successfully

FG-B #
```

There's a break for ~ approx. 14 seconds.

```
64 bytes from 8.8.8.8: icmp_seq=188 ttl=47 time=0.923 ms
64 bytes from 8.8.8.8: icmp_seq=189 ttl=47 time=0.892 ms
64 bytes from 8.8.8.8: icmp_seq=190 ttl=47 time=0.956 ms
64 bytes from 8.8.8.8: icmp_seq=191 ttl=47 time=0.936 ms
64 bytes from 8.8.8.8: icmp_seq=192 ttl=47 time=1.40 ms
64 bytes from 8.8.8.8: icmp_seq=193 ttl=47 time=0.941 ms
64 bytes from 8.8.8.8: icmp_seq=194 ttl=47 time=0.890 ms
64 bytes from 8.8.8.8: icmp_seq=195 ttl=47 time=0.949 ms
64 bytes from 8.8.8.8: icmp_seq=196 ttl=47 time=0.938 ms
64 bytes from 8.8.8.8: icmp_seq=197 ttl=47 time=0.919 ms
64 bytes from 8.8.8.8: icmp_seq=211 ttl=47 time=1.52 ms
64 bytes from 8.8.8.8: icmp_seq=212 ttl=47 time=1.48 ms
64 bytes from 8.8.8.8: icmp_seq=213 ttl=47 time=1.50 ms
64 bytes from 8.8.8.8: icmp_seq=214 ttl=47 time=1.53 ms
64 bytes from 8.8.8.8: icmp_seq=215 ttl=47 time=1.56 ms
64 bytes from 8.8.8.8: icmp_seq=216 ttl=47 time=1.51 ms
64 bytes from 8.8.8.8: icmp_seq=217 ttl=47 time=1.47 ms
^C
--- 8.8.8.8 ping statistics ---
217 packets transmitted, 204 received, 5% packet loss, time 219408ms
rtt min/avg/max/mdev = 0.807/0.955/2.010/0.171 ms
ubuntu@ip-10-3-10-10:~$
```

U® 18.04 0:- 1:- 2:-*