FortiGate-Aliyun
Deployment Guide
# Table of Contents

- Setup Virtual Private Cloud (VPC) ................................................................. 3
- Subscribe to the Fortinet VM in marketplace .................................................. 7
- Setting up the HAVIP on Aliyun Web Console ............................................... 16
- Start configuration of Fortinet Firewall ......................................................... 24
- Add ECS worker VMs for testing ................................................................. 26
- Verify the security capabilities of the Fortinet ............................................... 29
  - Demonstrate the Anti-Virus feature ......................................................... 29
  - Demonstrate the Application Control access feature ............................... 31
  - Enable NAT inbound protection in Fortinet ........................................... 33
- Conclusions .................................................................................................. 37
Setup Virtual Private Cloud (VPC)

1. Assume this is the new environment, now let’s create the VPC first

   ![VPC configuration](image)

<table>
<thead>
<tr>
<th>Instance ID/Name</th>
<th>Destination CIDR Block</th>
<th>Status</th>
<th>Default VPC</th>
<th>Route Table</th>
<th>VSwitch</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/16</td>
<td>Available</td>
<td>No</td>
<td>1</td>
<td>3</td>
<td>Manage</td>
<td>Delete</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Available</td>
<td>No</td>
<td>1</td>
<td>2</td>
<td>Manage</td>
<td>Delete</td>
</tr>
<tr>
<td>192.168.0.0/16</td>
<td>Available</td>
<td>No</td>
<td>1</td>
<td>6</td>
<td>Manage</td>
<td>Delete</td>
</tr>
<tr>
<td>172.16.0.0/16</td>
<td>Available</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>Manage</td>
<td>Delete</td>
</tr>
</tbody>
</table>

2. The VPC named TP_FortiVPC

   ![VPC configuration](image)

   Region:
   China East 1 (Hangzhou)

   - Name: TP_FortiVPC
   - Destination CIDR Block: 192.168.0.0/16

3. We will need at least three VSwitches, one for the ECS, one for the FortiGate VM Inbound/Outbound interface, and one for FortiGate VM HA interface, let’s create the ECS VSwitch first (you can create the fourth VSwitch for FortiGate reversed management interface)
4. And this is the VSwitch for keeping the FortiGate VM Inbound/Outbound interface

5. And this is the VSwitch for keeping the FortiGate VM HA interface
6. The VPC is now ready, next section we will subscribe the FortiGate VM

Create VPC

6. The VPC is now ready, next section we will subscribe the FortiGate VM

Create VPC

Details

<table>
<thead>
<tr>
<th>VPC Name</th>
<th>TP_FortiVPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC ID</td>
<td>vpc-bp1ue3buvegqo4v1ha4wl</td>
</tr>
<tr>
<td>Status</td>
<td>Success Create NAT Gateway</td>
</tr>
</tbody>
</table>

VSwitch name | FortiGate_HA_SW
VSwitch ID   | vsw-bp1qg9k10u08j8br94oz
Status       | Success Purchase

VSwitch name | FortiGate_HA_SW
VSwitch ID   | vsw-bp1qg9k10u08j8br94oz
Status       | Success Purchase

VSwitch name | ECS_SW
VSwitch ID   | vsw-bp1qgejko10u08j8br94oz
Status       | Success Purchase

7. (optional) Create one more VSwitch for FortiGate Reserved Management interface.
Subscribe to the Fortinet VM in marketplace


9. If customer has their own FortiGate license they can choose the BYOL image, otherwise they can use On-Demand image offered
10. Click “Choose Your Plan” to continue

11. In this case I’ll use PAYG, select China East 1 (Hangzhou) and Zone F (Where the VPC and VSwitches located), and then click the link “ECS Advance Purchase page” because I want to customize the Data disk and VPC information.

12. Click 4 vCPU ECS type to launch the FortiGate instance (4 vCPU ECS can support maximum 3 NIC, 2 vCPU can support 2 NIC, so if you need FortiGate reserved management interface, please select 4 vCPU ECS type.)
13. Add a data disk for the Log (Suggest to use SSD for better performance)

14. Choose the TP_FortiVPC and FortiGate_internet_SW in Network section, also assign the Public IP to the image, this NIC will be port1 on FortiGate_VM, the default ENI.
15. Leave HTTPS/ICMP/SSH ports open to allow connect, and add one more ENI which is on ‘FortiGate_HA_SW’, this ENI will be port2 on FortiGate.

16. Set the 'Host' as the hostname on FortiGate

17. Click ‘ECS Service Terms’

18. Click Console and back to the ECS instance list

19. You will see the VM created, mark down the Public IP and the instance ID (this will be FortiGate default password) and you will use later
20. Please repeat step 7-17 to create one more FortiGate instance, which name is FGT-Slave.

21. (Optional) Stop those two FortiGate instances
22. (Optional) Go to ‘Networks Interfaces’ page to create two ENI, and then attach the ENI on each FortiGate instance.
23. (Optional) Attach those two new ENI to two FortiGate.

Network Interfaces

<table>
<thead>
<tr>
<th>ID/Name</th>
<th>VSwitch/VPC</th>
<th>Zone</th>
<th>Security Group ID</th>
<th>Public IP Address</th>
<th>Private IP Address</th>
<th>Type/MAC(II)</th>
<th>Status/Created At</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>eni-bp126a49mfrnheinksk FGT-Slave-Port3</td>
<td>vsw-bp1n4o8m36029aq05akv / FortIg...</td>
<td>East China 1 Zone F</td>
<td>sg-bp153m2j...</td>
<td>192.168.3.250</td>
<td>Secondary</td>
<td>00:16:3e:12:2a:bf</td>
<td>Available 2018-05-02</td>
<td>Attach</td>
</tr>
<tr>
<td>eni-bp126a49mfrnheinksk FGT-Master-Port3</td>
<td>vsw-bp1n4o8m36029aq05akv</td>
<td>East China 1 Zone F</td>
<td>sg-bp153m2j...</td>
<td>192.168.3.249</td>
<td>Secondary</td>
<td>00:16:3e:10:13:3e</td>
<td>Available 2018-05-02</td>
<td>Attach</td>
</tr>
</tbody>
</table>
24. (Optional) Restart two FortiGate instance
25. Then we will be able to reach the Fortinet Web GUI by user admin/<instanceid>.

26. Set the ip address on three interfaces on FortiGate.
Setting up the HAVIP on Aliyun Web Console

27. Create a new HAVIP address, select the VPC and FortiGate Port1 VSwitch, and set the HAVIP address.
28. Set the HA configuration on FortiGate via VNC console on Aliyun Webgui, or via SSH.

FortiGate-Master:
```fortigate
config system ha
set group-name "ha"
set mode a-p
set hbdev "port2" 0
set session-pickup enable
set ha-mgmt-status enable
config ha-mgmt-interface
  edit 1
    set interface "port3"
    set gateway 192.168.3.253 --- gateway on vswitch
    next
end
set priority 200  --- the higher value will be Master
set monitor "port1"
set unicast-hb enable
set unicast-hb-peerip 192.168.1.250  --- IP address on FGT-Slave port2
end
```

FortiGate-Slave:
```fortigate
config system ha
set group-name "ha"
set mode a-p
set hbdev "port2" 0
set session-pickup enable
set ha-mgmt-status enable
config ha-mgmt-interface
  edit 1
    set interface "port3"
    set gateway 192.168.3.253 --- gateway on vswitch
    next
end
set priority 100
set monitor "port1"
set unicast-hb enable
set unicast-hb-peerip 192.168.1.249  --- IP address on FGT-Master port2
end
```
Then reboot two FortiGate.

Check the status of HA using ‘`diagnose sys ha status`’ in CLI, it shows following:

```
FGT-Master # diagnose sys ha status
HA information
  Model=90019, Mode=2 Group=0 Debug=0
  Vclustere=1, ses_pickup=1, delay=0

  [Debug Zone HA information]
  HA group member information: is_manage_master=1.
  FGTALIG8XF4MRR79: Master, serialno_prio=1, usr_priority=200, hostname=FGT-Master
  FGTALI5T2A540C07: Slave, serialno_prio=0, usr_priority=100, hostname=FGT-Slave

  [Kernel HA information]
  Vclustere 1, state=work, master_ip=192.168.1.249, master_id=0:
  FGTALIG8XF4MRR79: Master ha_prio/0 ha_prio=0/0
  FGTALI5T2A540C07: Slave ha_prio/0 ha_prio=1/1
```

29. Set the HAVIP address to port1 secondary ip address on two FortiGate.
On both FGT-Master and FGT-Slave:
```
config system interface
  edit "port1"
    set secondary-IP enable
  config secondaryip
    edit 1
      set ip 192.168.0.252 255.255.255.0 --- this ip address should be same with HAVIP address
      set allowaccess ping https ssh
      next
    end
  next
end
```

30. Bind ‘Elastic IP’ and two FortiGate ECS to HAVIP
Create a new EIP
**HAVIP Addresses**

<table>
<thead>
<tr>
<th>Instance ID</th>
<th>IP Address</th>
<th>Status</th>
<th>Bind Instance</th>
<th>VPC</th>
<th>VSwitch</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>havip-bp1wy8gf7lppolopqosf</td>
<td>192.168.0.252(Intranet IP)</td>
<td>Available</td>
<td>No ECS Bound</td>
<td>vpc-bp1wy8gf7lppolopqosf</td>
<td>vswitch-bp1wy8gf7lppolopqosf</td>
<td>Manage</td>
</tr>
</tbody>
</table>

**HAVIP Details**

**Information**

- **ID**: havip-bp1wy8gf7lppolopqosf
- **Region**: China East 1 (Hangzhou)
- **VPC ID**: vpc-bp1wy8gf7lppolopqosf
- **VSwitch**: vswitch-bp1wy8gf7lppolopqosf
- **Status**: Available
- **Intranet IP**: 192.168.0.252
- **Created At**: 05/02/2018, 15:12:42
- **Description**: -

**Resources**

- **HAVIP Address**: 192.168.0.252(Intranet IP)
- **No EIP Bound**

**Bind EIP to HAVIP,**
Bind Elastic IP Address

HAVIP Address
havip-bp1bwy877ppbi0qq6i5

Intranet IP
192.168.0.252

Elastic IP Address

<table>
<thead>
<tr>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.97.186.150</td>
</tr>
<tr>
<td>116.62.161.94</td>
</tr>
</tbody>
</table>

Bind two FortiGate to HAVIP,
Bind an ECS Instance

HAVIP Address
havip-bp1bwy877ppbi0qq6i5

Intranet IP
192.168.0.252

ECS Instance

<table>
<thead>
<tr>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>i-bp167uu7rzmp8ta0kw</td>
</tr>
</tbody>
</table>

Bind an ECS Instance

HAVIP Address
havip-bp1bwy877ppbi0qq6i5

Intranet IP
192.168.0.252

ECS Instance

<table>
<thead>
<tr>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>i-bp1cj6f38cb1ndkoom7</td>
</tr>
</tbody>
</table>
31. Also we need to add the route entry to FortiGate, this make sure all out-going traffic from ECS will go through Fortinet
## Route Table

### Route Table Details

<table>
<thead>
<tr>
<th>Route Table ID</th>
<th>vtb-bp1785omuxqpyw1ogn</th>
<th>VPC ID</th>
<th>vpc-bp1ue3buveqgos4vkl4s48f1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Edit</td>
<td>Route Table Type</td>
<td>System</td>
</tr>
<tr>
<td>Created At</td>
<td>05/02/2018, 13:48:20</td>
<td>Description</td>
<td>Edit</td>
</tr>
</tbody>
</table>

### Route Entry List

<table>
<thead>
<tr>
<th>Destination CIDR Block</th>
<th>Status</th>
<th>Next Hop</th>
<th>Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/24</td>
<td>✔️ Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>✔️ Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>✔️ Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>✔️ Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>100.64.0.0/10</td>
<td>✔️ Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
</tbody>
</table>

### Add Route Entry

- **Destination CIDR Block**
  
  ![CIDR Block Input](image)

- **Next Hop Type**
  
  ![Next Hop Type](image)

- **HAVIP Address**
  
  ![HAVIP Address](image)
## Route Table

**Route Table Details**

<table>
<thead>
<tr>
<th>Route Table ID</th>
<th>vtb-bp178j0mvus5wpyvwiog</th>
<th>VPC ID</th>
<th>vpc-bp1ua3buqego4vkha4wi</th>
<th>Name</th>
<th>Route Table Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created At</td>
<td>05/02/2018, 13:48:20</td>
<td></td>
<td></td>
<td></td>
<td>System</td>
<td></td>
</tr>
</tbody>
</table>

**Route Entry List**

<table>
<thead>
<tr>
<th>Destination CIDR Block</th>
<th>Status</th>
<th>Next Hop</th>
<th>Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>Creating</td>
<td>55 Instance ID: havip-bp1bwya8f77ppbi0qq6i</td>
<td>Custom</td>
<td>Delete</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>100.64.0.0/10</td>
<td>Available</td>
<td>-</td>
<td>System</td>
<td></td>
</tr>
</tbody>
</table>
Start configuration of Fortinet Firewall

32. You can change password here after logging in

![](image1.png)

33. After logging in again by new password, you can change the time zone and language as well in System -> Settings

![](image2.png)
34. Now we need to add the IPv4 Policy for the outbound traffic.

35. Specific the following “ToInternet” policy, let’s enable the AntiVirus and Application Control here for Demo, also enabled All Sessions log too, then click “OK”.
Add ECS worker VMs for testing

36. Just create ECS as usual

37. Remember, **cannot use the same VSwitch of the Fortinet**, in this case I selected the ECS Vswitch. And don’t need to assign public IP because ECS with Public IP will not route through Fortinet

38. Confirm and create the instance
39. Then reset the VNC password, login password and restart the instance.

<table>
<thead>
<tr>
<th>Instance ID/Name</th>
<th>Tags</th>
<th>Monitor Zone</th>
<th>IP Address</th>
<th>Status</th>
<th>Network Type</th>
<th>Configuration</th>
<th>Billing Method</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP-ECS-worker-SE</td>
<td></td>
<td></td>
<td>192.168.1.36</td>
<td>Running</td>
<td>VPC</td>
<td>2 vCPU 8 GB (O)</td>
<td>Pay-As-You-Go</td>
<td></td>
</tr>
<tr>
<td>TP-Fortinet-5.6.3</td>
<td></td>
<td></td>
<td>47.75.161.225</td>
<td>Running</td>
<td>VPC</td>
<td>2 vCPU 4 GB (O)</td>
<td>Pay-As-You-Go</td>
<td></td>
</tr>
<tr>
<td>TP-Window-TestFW</td>
<td></td>
<td></td>
<td>10.1.213.107</td>
<td>Running</td>
<td>VPC</td>
<td>1 vCPU 4 GB (O)</td>
<td>Pay-As-You-Go</td>
<td></td>
</tr>
<tr>
<td>TP-Fortinet-5.6.3-SE</td>
<td></td>
<td></td>
<td>47.75.161.187</td>
<td>Running</td>
<td>VPC</td>
<td>2 vCPU 4 GB (O)</td>
<td>Pay-As-You-Go</td>
<td></td>
</tr>
</tbody>
</table>

40. Then connect to the VNC, login to the Windows.

41. You should find it is able to connect internet through the Fortinet.
42. You should also find the detail log information in the Fortinet as well!
Verify the security capabilities of the Fortinet

Demonstrate the Anti-Virus feature

43. In the ECS, visit the website http://metal.fortiguard.com/tests/

44. Click the run tests, if there is no Firewall Antivirus protection the test will fail

![Test Cases & Results](image)

45. As the ECS is protected by Fortinet, you will see it is blocked

![High Security Alert](image)

To have the best Anti-Virus scanning capabilities, make sure the anti-virus definition is up-to-date in Fortinet
46. And we also can see the Threats in Fortinet console
Demonstrate the Application Control access feature

47. Go to Security Profiles -> Application Control, let’s select to block the Video/Audio and Social Media. And click Apply.

48. Then try to access facebook and youtube in the ECS, you will see they are not able to connect.
49. In the Fortinet console, we will see which clients trying to connect to facebook as well
Enable NAT inbound protection in Fortinet

In this sample, I’ll try to enable the Fortinet to protect inbound RDP traffic, the same concept can be applied to HTTP/HTTPS and other services too, this is very useful because most customers want Fortinet to monitor both inbound and outbound traffic.

50. Setup the NAT and point to the RDP address of the ECS, Click Virtual IPs under Policy&Objects.

51. We map the 3389 port of the Fortinet to the ECS 192.168.1.36.
52. Can see the Virtual IP there now

53. Now we will configure the inbound policy for the RDP redirection

54. Name the rule and then choose the Virtual IP we created as the destination

55. Similarly, enable the security profiles you want, and then use All Sessions as Log allowed traffic for demo purpose.
56. The inbound rule is created successfully
57. And now you should be able to use the Fortinet Public IP address to RDP the ECS.

58. Logs and sessions information can also be viewed in Fortinet.
Conclusions

Fortinet is a powerful software that widely used by many international customers, financial and securities industries as well. By leveraging this VM, we should be able to strengthen the confidence of customer for using Cloud.