

# FortiOS - AliCloud Cookbook

Version 6.2

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



November 29, 2019

FortiOS 6.2 AliCloud Cookbook

01-620-544167-20191129

# TABLE OF CONTENTS

<b>About FortiGate for AliCloud</b> .....	<b>6</b>
Instance type support .....	6
Region support .....	7
Models .....	7
Licensing .....	8
Order types .....	8
Creating a support account .....	8
Registering and downloading licenses .....	9
<b>Securing instances on AliCloud</b> .....	<b>10</b>
Configuring a virtual private cloud .....	10
Subscribing to the FortiGate-VM in the marketplace .....	11
Configuring routing to the FortiGate-VM on AliCloud .....	14
Connectivity test .....	14
Configuring the initial firewall policy on the FortiGate-VM .....	15
Configuring an ECS worker VM for VNC access .....	15
Testing malware scan for outgoing traffic .....	17
Testing application control for outgoing traffic .....	18
Enabling NAT inbound protection in FortiOS .....	19
<b>HA for FortiGate-VM on AliCloud</b> .....	<b>23</b>
Deploying and configuring FortiGate-VM on AliCloud using HAVIP .....	23
Setting up the VPC .....	24
Subscribing to the FortiGate-VM in the marketplace .....	29
Configuring the HAVIP on the AliCloud web console .....	38
Connectivity test .....	46
Deploying FortiGate-VM HA on AliCloud using routing tables and EIPs .....	46
Deploying FortiGate-VM HA on AliCloud between availability zones .....	55
<b>Deploying auto scaling on AliCloud</b> .....	<b>62</b>
Planning .....	63
Acronyms .....	63
Requirements .....	63
Deployment information .....	65
Deployment .....	66
Terraform variables .....	67
Verify the deployment .....	69
Destroying the cluster .....	71
Troubleshooting .....	72
Debugging cloud-init .....	72
TableStore destroy time .....	72
Resource availability .....	73
Timeout .....	73
How to reset the master election .....	73
Appendix .....	74
FortiGate Autoscale for AliCloud features .....	74

---

Architectural diagram .....	75
Master election .....	75
Manual deployment of auto scaling on AliCloud .....	76
<b>Security Fabric connector integration with AliCloud .....</b>	<b>82</b>
Configuring AliCloud Fabric connector using RAM roles .....	82
Pipelined automation using AliCloud Function Compute .....	82
<b>VPN for FortiGate-VM on AliCloud .....</b>	<b>83</b>
Connecting a local FortiGate to an AliCloud VPC VPN .....	83
Connecting a local FortiGate to an AliCloud FortiGate via site-to-site VPN .....	87
Configuring the local FortiGate .....	88
Configuring the AliCloud FortiGate .....	91
<b>Change log .....</b>	<b>96</b>



## About FortiGate for AliCloud

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate Next Generation Firewall technology delivers complete content and network protection. This solution is available for deployment on AliCloud.

In addition to advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, features including application control, firewall, antivirus, IPS, web filter, and VPN work in concert to identify and mitigate the latest complex security threats.

FortiGate for AliCloud supports active/passive high availability (HA) configuration using highly available virtual IP addresses (HAVIP). This enables FortiGate synchronization between the primary and secondary nodes for their configurations and sessions, and when the FortiGate detects a failure, the passive firewall instance becomes active.

Highlights of FortiGate for AliCloud include the following:

- Delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- New Docker application control signatures protect your container environments from newly emerged security threats. See [FortiGate-VM on a Docker environment](#).

## Instance type support

You can deploy FortiGate-VM (as bring your own license (BYOL)) on AliCloud on all available instances supported that the FortiGate-VM listing on the AliCloud marketplace supports. Supported instances on AliCloud for new deployments may change without notice.

For up-to-date information of instance type families, see the following:

- [Instance type families](#)
- [Fortinet FortiGate \(BYOL\) Next-Generation Firewall](#)

FortiGate-VM (as on-demand or pay-as-you-go (PAYG)) on AliCloud currently supports vCPU-2 and 4 only. For more information, visit:

- [Fortinet FortiGate-VM On-Demand \(2 vCore CPU\)](#)
- [Fortinet FortiGate-VM On-Demand \(4 vCore CPU\)](#)

You can apply a smaller FortiGate-VM license if you are OK with consuming less CPU than is present on your instance. For details, see [FortiGate-VM virtual licenses and resources](#).

## Region support

FortiGate-VM is available for purchase in all the regions/datacenters that the AliCloud global marketplace covers. Available regions are:

- Hong Kong
- Asia Pacific SE 1 (Singapore)
- US East 1 (Virginia)
- Asia Pacific NE 1 (Tokyo)
- US West 1 (Silicon Valley)
- EU Central 1 (Frankfurt)
- Middle East 1 (Dubai)
- Asia Pacific SE 2 (Sydney)
- Asia Pacific SE 3 (Kuala Lumpur)
- Asia Pacific SOU 1 (Mumbai)
- Asia Pacific SE 5 (Jakarta)
- North China 1
- North China 2
- China North 3 (Zhangjiakou)
- China North 5 (Huhehaote)
- East China 1
- East China 2
- South China 1

## Models

FortiGate-VM is available with different CPU and RAM sizes. You can deploy FortiGate-VM on various private and public cloud platforms. The following table shows the models conventionally available to order, also known as BYOL models. See [Order types on page 8](#).

Model name	vCPU	
	Minimum	Maximum
FG-VM01/01v/01s	1	1
FG-VM02/02v/02s	1	2
FG-VM04/04v/04s	1	4
FG-VM08/08v/08s	1	8
FG-VM16/16v/16s	1	16
FG-VM32/32v/32s	1	32
FG-VMUL/ULv/ULs	1	Unlimited



The v-series and s-series do not support virtual domains (VDMs) by default. To add VDMs, you must separately purchase perpetual VDM addition licenses. You can add and stack VDMs up to the maximum supported number after initial deployment.

---

Generally there are RAM size restrictions to FortiGate-BYOL licenses. However, these restrictions are not applicable to AliCloud deployments. Any RAM size with certain CPU models are allowed. Licenses are based on the number of CPUs only.

For information about each model's order information, capacity limits, and adding VDM, see the [FortiGate-VM datasheet](#).

## Licensing

You must have a license to deploy FortiGate for AliCloud.

## Order types

On AliCloud, there are usually two order types: BYOL and on-demand.

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series, available starting Q4 2019) licensing as opposed to on-demand. Subscription is month-based whereas PAYG is hour-based. BYOL licenses are available for purchase from resellers or your distributors, and prices are listed in the publicly available price list which is updated quarterly. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

On-demand is term-based and has two options: subscription and PAYG. With an on-demand subscription, the FortiGate-VM becomes available for use immediately after you create the instance. Term-based prices (hourly or annually) are mentioned in the marketplace product page.

In both BYOL and on-demand, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without use of software running on top of it (in this case the FortiGate-VM).

- For BYOL, you typically order a combination of products and services including support entitlement. New s-series SKUs contain the VM base and service bundle entitlements for easier ordering. To proceed with licensing a BYOL deployment, see [Registering and downloading licenses on page 9](#).
- To purchase on-demand, all you need to do is launch the product on the marketplace. However, you must contact Fortinet Support with your customer information to obtain support entitlement. See [Creating a support account on page 8](#). See *Support* on the [marketplace product page](#).



On-demand FortiGate-VM instances do not support the use of virtual domains (VDMs). If you plan to use VDMs, deploy BYOL instances instead.

---

## Creating a support account

FortiGate for AliCloud supports both on-demand and BYOL licensing models. See [Order types on page 8](#).



To make use of Fortinet technical support and ensure products function properly, you must complete certain steps to activate your entitlement. Our support team can identify your registration in the system thereafter.

First, if you do not have a Fortinet account, you can [create one](#).

For on-demand deployments, do the following:

1. Deploy and boot up the FortiGate on-demand VM instance and log into the FortiGate GUI management console.
2. On the Dashboard, copy the VM serial number.
3. Go to [Fortinet Service & Support](#) and create a new account or log in with an existing account.
4. Go to *Asset > Register/Activate* to start the registration process.
5. In the *Specify Registration Code* field, enter the serial number, and select *Next* to continue registering the product. Enter your details in the other fields.
6. After completing registration, contact Fortinet Customer Support and provide your FortiGate instance's serial number and the email address associated with your Fortinet account.

## Registering and downloading licenses

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you do not have a partner, contact [jerrywang@fortinet.com](mailto:jerrywang@fortinet.com) for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license (60-day term), you will receive a PDF with an activation code.

1. Go to [Fortinet Service & Support](#) and create a new account or log in with an existing account.
2. Go to *Asset > Register/Activate* to start the registration process. In the *Specify Registration Code field*, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiGate-VM.

After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

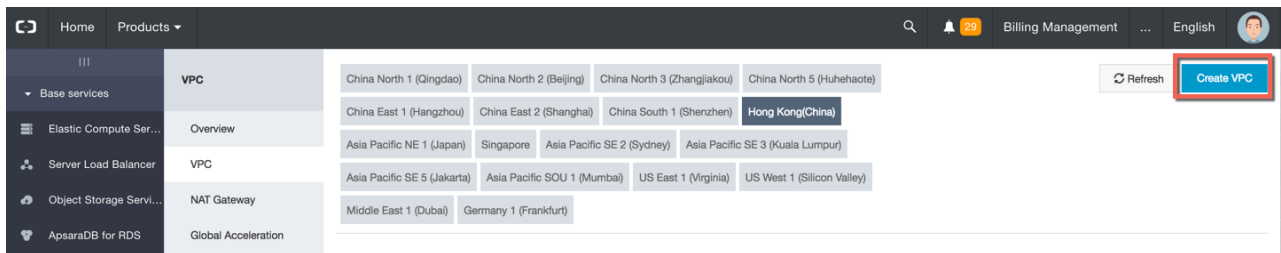
# Securing instances on AliCloud

This guide describes FortiGate-VM single deployment on AliCloud. This deployment consists of the following steps:

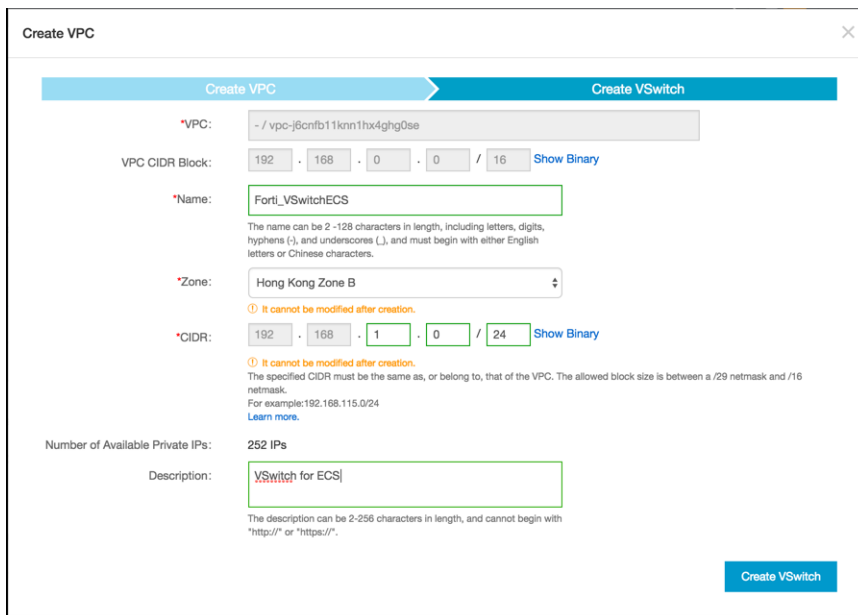
1. Configuring a virtual private cloud on page 10
2. Subscribing to the FortiGate-VM in the marketplace on page 11
3. Configuring routing to the FortiGate-VM on AliCloud on page 14
4. Connectivity test on page 14

## Configuring a virtual private cloud

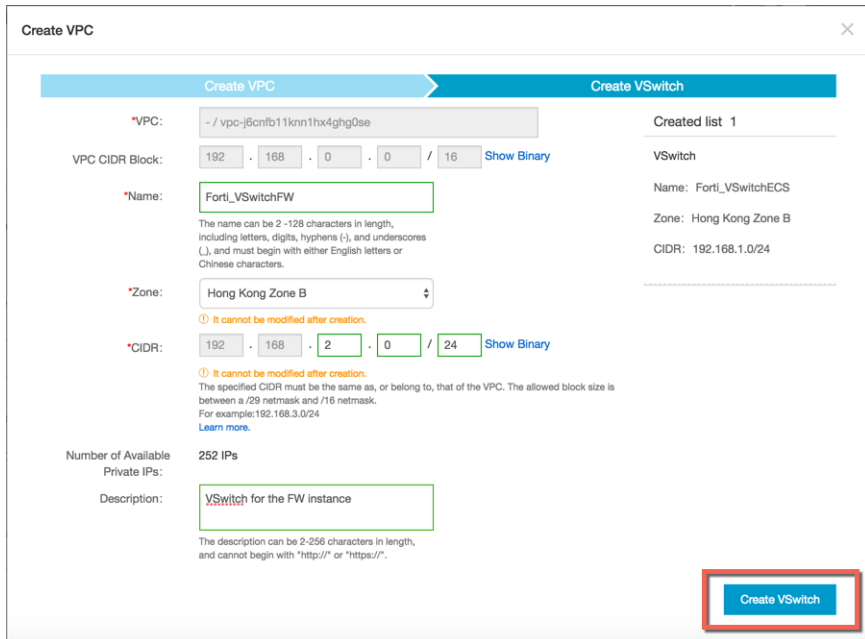
1. Assuming this is a new environment, the first step is to create the virtual private cloud (VPC). In the AliCloud web console, click *Create VPC*.



2. Enter a name for the VPC. Click *Create VPC*.
3. Click *Next Step*.
4. You will require at least two VSwitches: one for the ECS and one for the FortiGate-VM. Create the ECS VSwitch first as shown below.



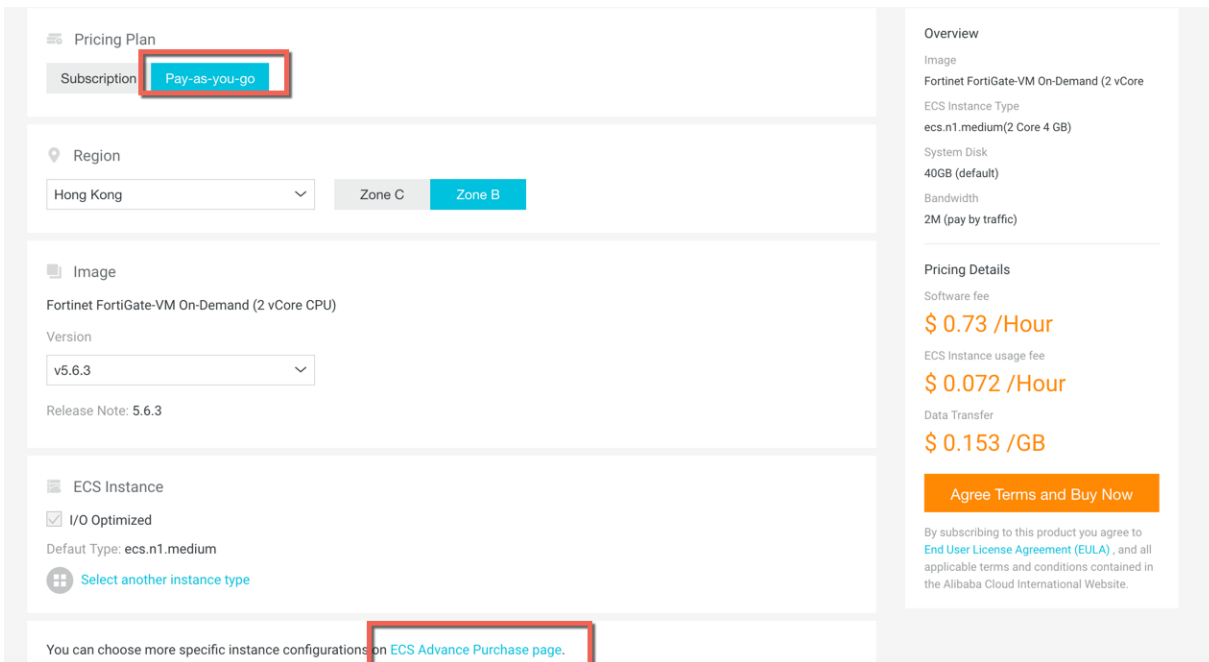
5. Click *Create More*.
6. Configure the VSwitch for the FortiGate-VM as shown below, then click *Create VSwitch*.



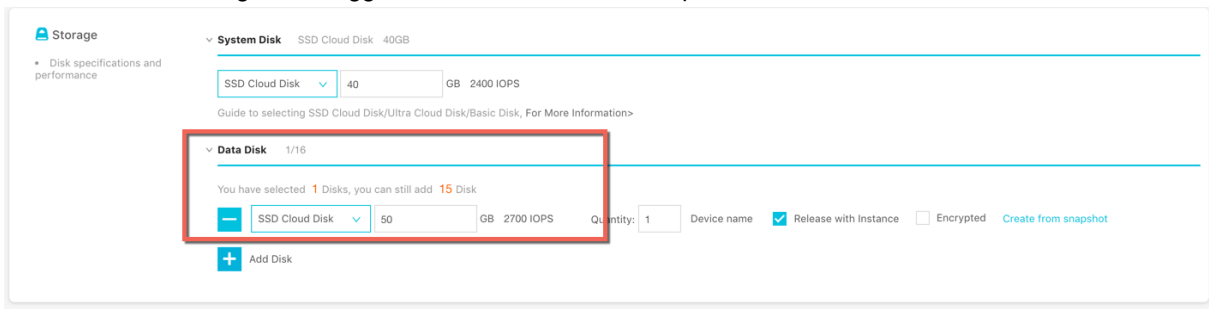
7. Click *Done*. VPC and VSwitch setup is complete.

## Subscribing to the FortiGate-VM in the marketplace

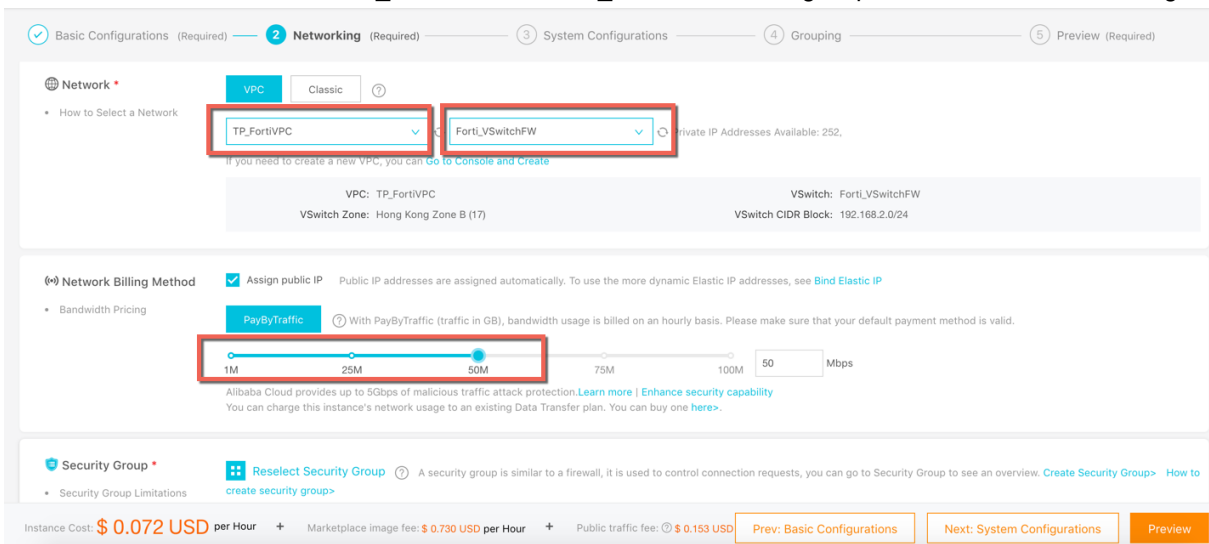
1. Go to the [AliCloud Marketplace](#) and search for Fortinet.
2. You will now create the FortiGate-VM instance. If you have your own FortiGate-VM license, select the BYOL image. Otherwise, select the on-demand image.
  - a. Click *Choose Your Plan*.
  - b. In this example, PAYG, Hong Kong, and Zone B were selected for the pricing plan, region, and zone, respectively. Zone B is the location of the VPC and VSwitches. Click *ECS Advance Purchase page* to customize the data disk and VPC information.



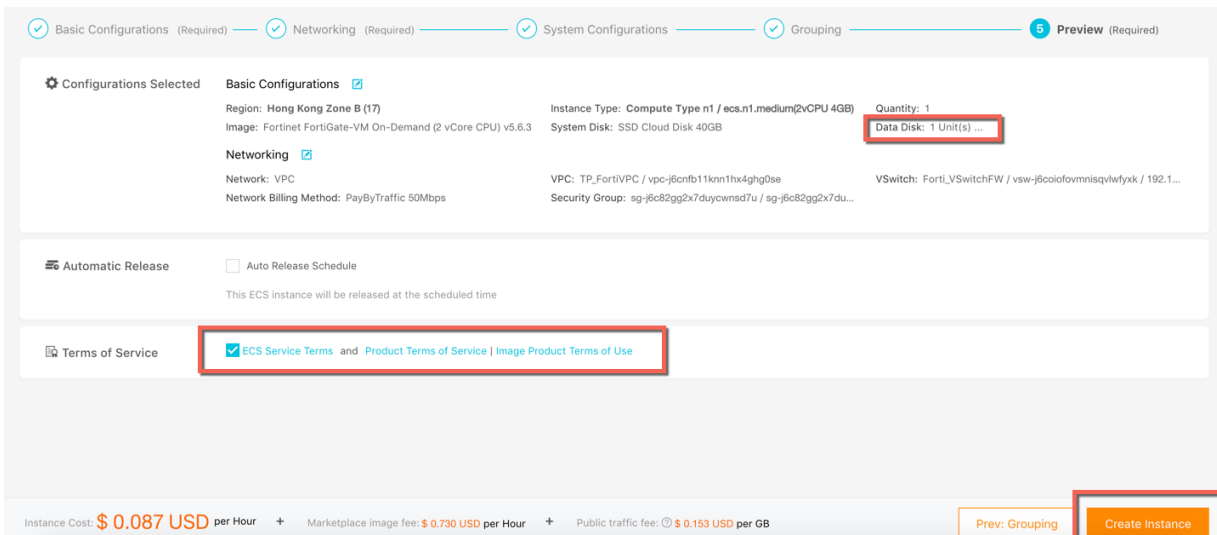
c. Add a data disk for logs. It is suggested to use SSD for better performance.



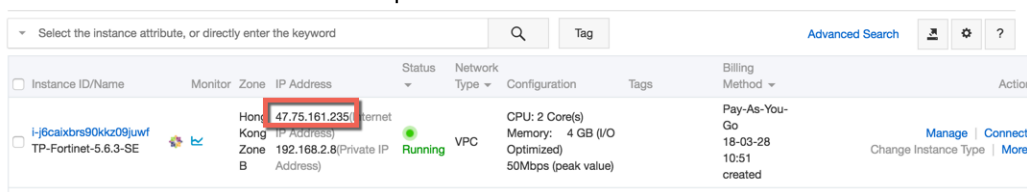
d. In the *Network* section, select TP\_FortiVPC and Forti\_VSwitchFW. Assign a public IP address to the image.



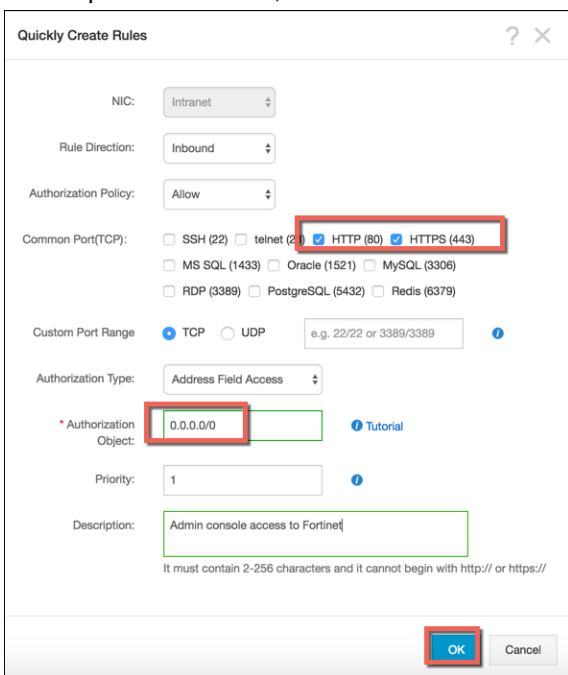
e. Continue to create the instance.



3. Click *Console* to return to the ECS instance list.
4. You can see that the VM has been created. Mark down the public IP address and the instance ID for later use. The instance ID is the FortiGate default password.



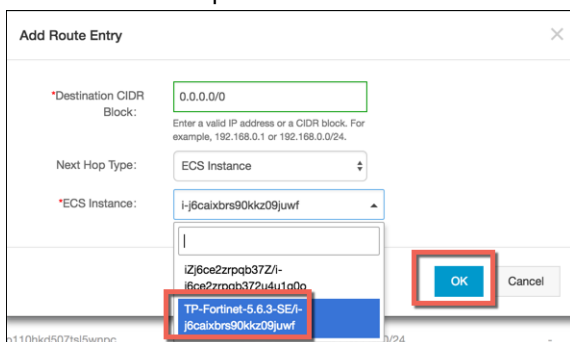
5. You must now configure the default security group. Go to *Security Groups*, then click *Configure Rules*.
  - a. Click *Quickly Create Rules*.
  - b. Enable ports 80 and 443, then click *OK*.



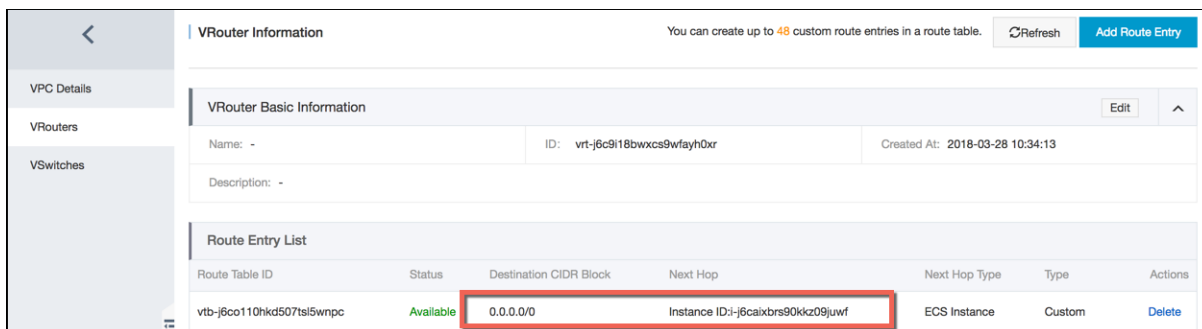
6. You can now access the FortiGate-VM in a web browser using the username "admin". The password is the instance ID.
7. Change the password after the initial login.

## Configuring routing to the FortiGate-VM on AliCloud

1. On the VPC entry, click *Manage*.
2. Click *Add Route Entry*.
3. Add 0.0.0.0/0 and point it to the FortiGate-VM.



This ensures ECS outbound traffic goes through the FortiGate.



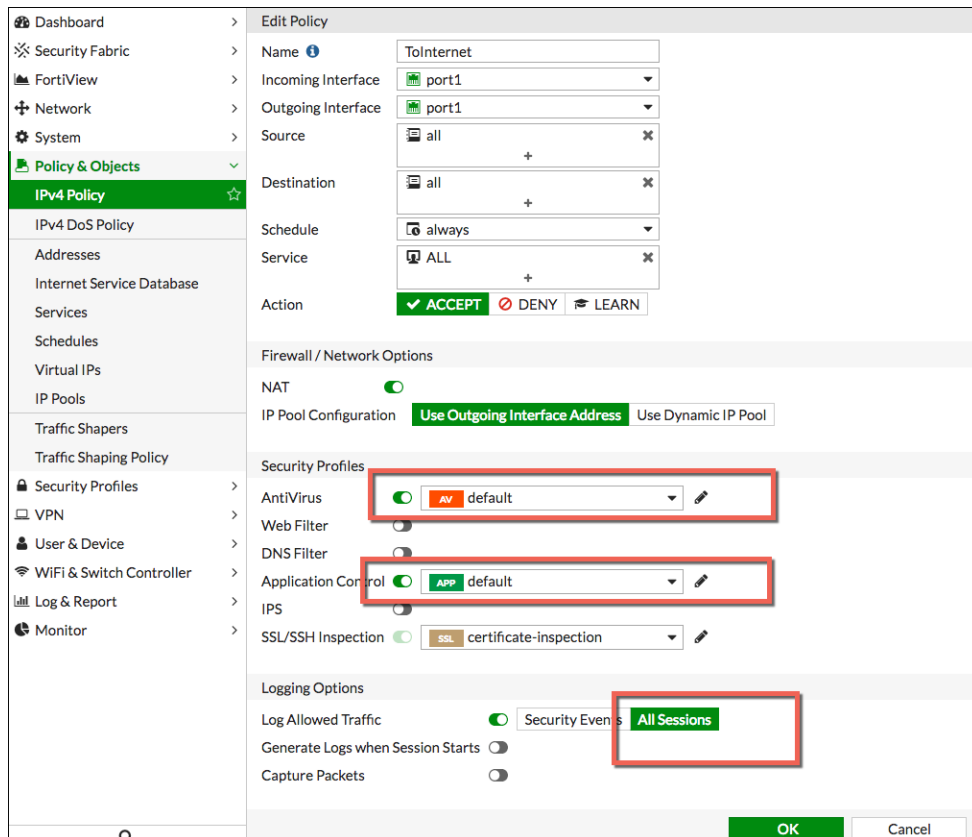
## Connectivity test

The following instructions test whether you configured the FortiGate-VM and VPC properly. Complete the following steps in order:

1. [Configuring the initial firewall policy on the FortiGate-VM on page 15](#)
2. [Configuring an ECS worker VM for VNC access on page 15](#)
3. [Testing malware scan for outgoing traffic on page 17](#)
4. [Testing application control for outgoing traffic on page 18](#)
5. [Enabling NAT inbound protection in FortiOS on page 19](#)

## Configuring the initial firewall policy on the FortiGate-VM

1. In FortiOS, add an IPv4 policy for outbound traffic.
2. Specify the following "ToInternet" policy with AntiVirus, Application Control, and logs allowed for all sessions. Click **OK**.

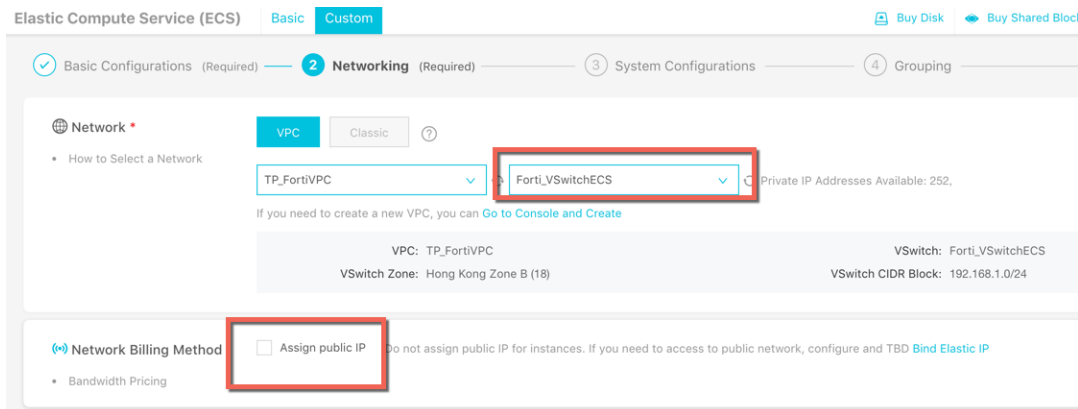


## Configuring an ECS worker VM for VNC access

1. In the AliCloud web console, click **Create Instance**.



2. Configure the ECS instance so that it does not use the same vSwitch as the FortiGate-VM. In this example, the ECS VSwitch was selected. There is no need to assign a public IP address since an ECS with a public IP address will not route through the FortiGate-VM.



3. Confirm the configuration, then create the instance.
4. Reset the VNC password and login password, then restart the instance.

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
i-j6cdmbags9axi0r8la TP-ECS-worker-SE			Hong Kong Zone B	192.168.1.36(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-28 11:51 created	Manage   Connect   More
i-j6caixbrs90kkz09juwv TP-Fortinet-5.6.3-SE			Hong Kong Zone B	47.75.161.235(Internet IP Address) 192.168.2.8(Private IP Address)	Running	VPC	2 vCPU 4 GB (I/O Optimized) ecs.n1.medium 50Mbps (peak value)	Pay-As-You-Go 18-03-28 10:51 created	Start   Stop   Restart   Release Setting   Buy the Same Configuration   Reset Password   Reset VNC Password   Modify Information
i-j6cfhyq9f0lj3xfypeb TP-Windows-TestFW			Hong Kong Zone B	10.1.213.107(Private IP Address)	Running	VPC	1 vCPU 4 GB (I/O Optimized) ecs.mn4.small	Pay-As-You-Go 18-03-27 16:56 created	Reset Password
i-j6cf7u83gahon904ktm TP-Fortinet-5.6.3			Hong Kong Zone B	47.75.165.167(Internet IP Address) 10.2.1.71(Private IP Address)	Running	VPC	2 vCPU 4 GB (I/O Optimized) ecs.sn1.medium 50Mbps (peak value)	Pay-As-You-Go 18-03-27 16:55 created	Reset VNC Password

5. Connect to the VNC and log into Windows.

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
i-j6cdmbags9axi0r8la TP-ECS-worker-SE			Hong Kong Zone B	192.168.1.36(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-28 11:51 created	Manage   Connect
			Hong Kong Zone B	47.75.161.235(Internet IP Address)	Running	VPC	2 vCPU 4 GB (I/O Optimized)	Pay-As-You-Go	

The VM should be able to connect to the Internet through the FortiGate-VM.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping hk.yahoo.com

Pinging oob-media-router-fp1-prod.media.wg1.b.yahoo.com [106.10.250.11] with 32 bytes of data:
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55

Ping statistics for 106.10.250.11:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms
Control-C
^C
C:\Users\Administrator>
```

FortiOS should also provide detailed log information.



Destination	Application	Bytes (Sent/Received)	Sessions	Bandwidth
hkg07s29-in-f10.1e100.net (172.217.161.170)	HTTPS.BROWSER	3.49 MB	1	0 bps
server-52-84-44-30.hkg53.r.cloudfront.net (52.84.44.30)	HTTPS.BROWSER	2.29 MB	1	80 bps
104.16.41.2	HTTPS.BROWSER	550.21 kB	1	0 bps
a23-52-171-145.deploy.static.akamaitechnologies.com (23.52.171.145)	HTTP.BROWSER_Firefox	462.45 kB	1	40 bps
server-52-222-238-44.hkg53.r.cloudfront.net (52.222.238.44)	HTTPS.BROWSER	461.57 kB	1	80 bps
server-52-222-238-35.hkg53.r.cloudfront.net (52.222.238.35)	HTTPS.BROWSER	281.06 kB	2	0 bps
server-52-84-43-118.hkg53.r.cloudfront.net (52.84.43.118)	HTTPS.BROWSER	223.99 kB	2	0 bps
hkg07s28-in-f8.1e100.net (172.217.31.232)	HTTPS.BROWSER	62.44 kB	1	0 bps
play.google.com (216.58.200.14)	HTTPS.BROWSER	26.01 kB	1	0 bps
ec2-34-208-49-39.us-west-2.compute.amazonaws.com (34.208.49.39)	HTTPS.BROWSER	21.47 kB	1	64 bps
server-52-222-238-152.hkg53.r.cloudfront.net (52.222.238.152)	HTTPS.BROWSER	20.38 kB	1	80 bps

## Testing malware scan for outgoing traffic

1. On the ECS worker node, visit this [website](#).
2. Click *Run Tests*. If there is no Application Firewall or AntiVirus protection, this test will fail.

**Test Cases & Results**

0/18 Tests Passed Expand All Collapse All Print All

**Plain - Plain test file** Run Tests >

**Clean file** Download Generated a minute ago

(Unknown) This is a screenshot from fortinet.com, taken in the last few minutes to show sample freshness. MD5: 5850b04d551430e7363a49ea6747753d  
SHA256: e0c4c34997e7cc72705527e9e4cc9b9d2ff8d32ac4dd3e08f9a49450dedfe5ae

**EICAR Infected file** Download Generated a minute ago

(Unknown) This is EICAR test file as well as a screenshot from fortinet.com, taken in the last few minutes to show sample freshness. MD5: 44d88612fea8a8f36de82e1278abb02f  
SHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

Please run this test

FortiGate will block the file from being downloaded.

**High Security Alert!!**

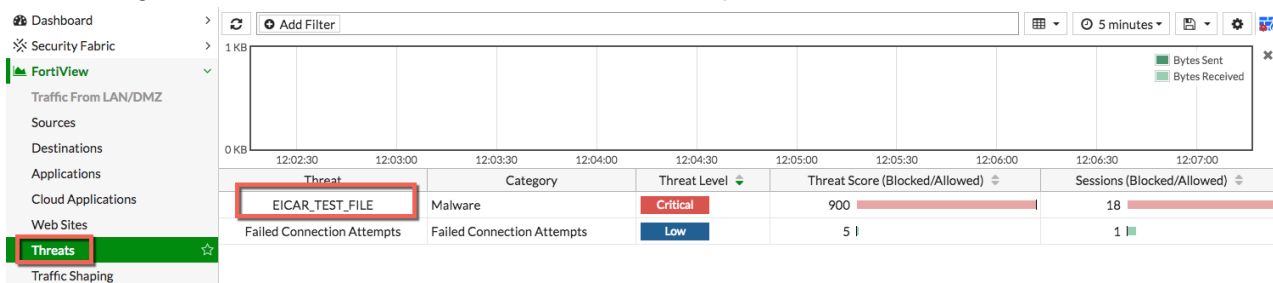
You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR\_TEST\_FILE".

URL: <http://metal.fortiguard.com/generated/eicar.com>  
File quarantined as: [http://www.fortinet.com/we?vn=EICAR\\_TEST\\_FILE](http://www.fortinet.com/we?vn=EICAR_TEST_FILE)

Client IP: 192.168.1.36  
Server IP: 104.236.145.4  
User name:  
Group name:

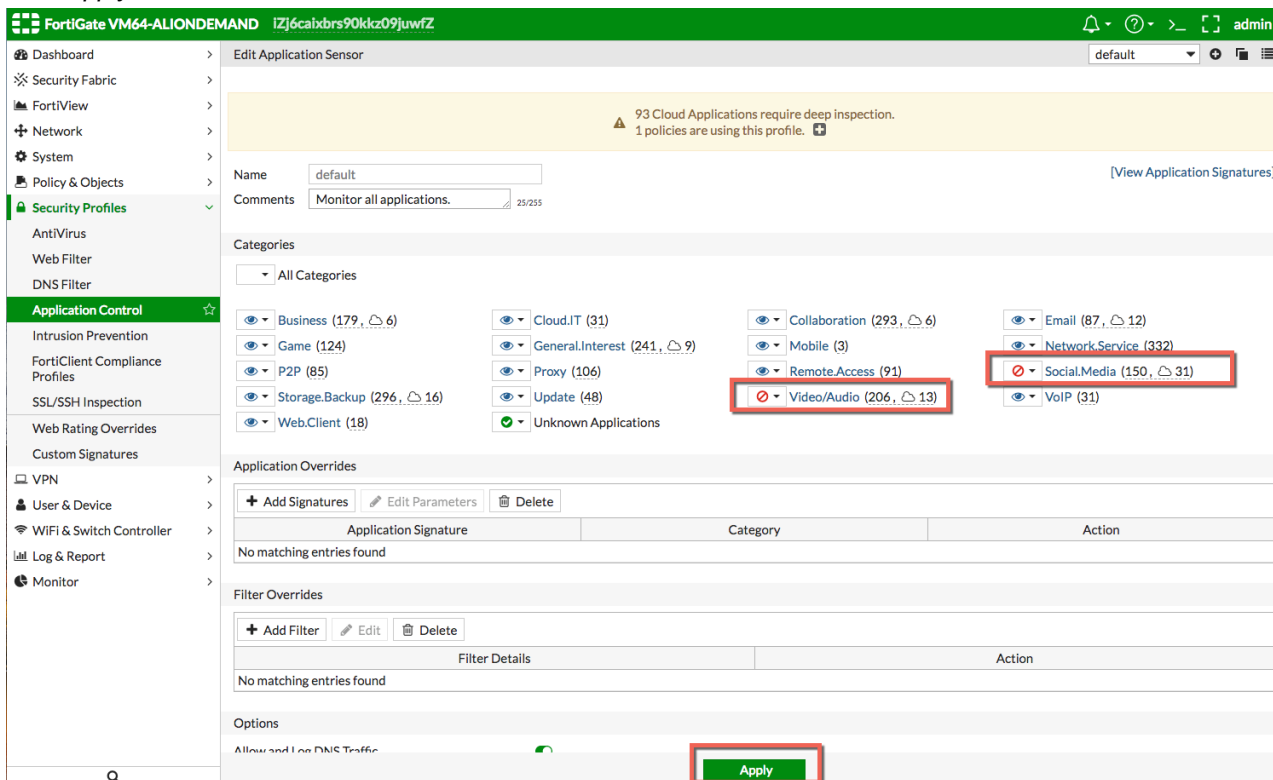
For the best AntiVirus scanning capabilities, ensure the AntiVirus definition is up-to-date in FortiOS.

3. In FortiOS, go to *FortiView > Threats*. You should see the attempted file download.

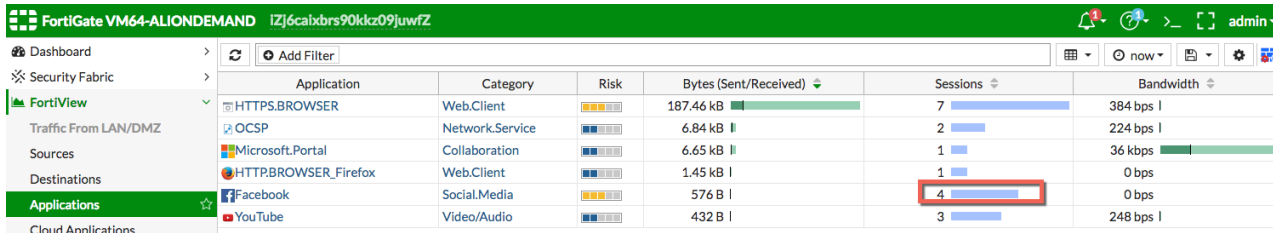


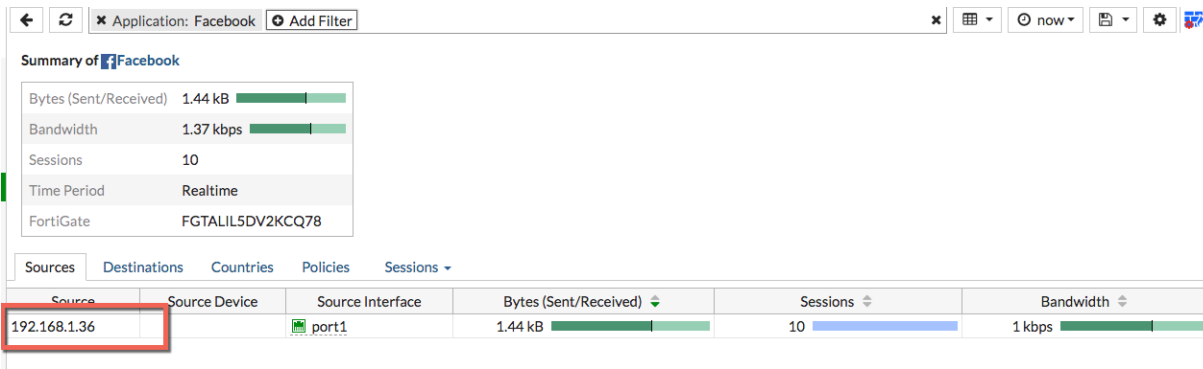
## Testing application control for outgoing traffic

1. In FortiOS, go to *Security Profiles > Application Control*. Under *Categories*, block *Video/Audio* and *Social Media*. Click *Apply*.



2. On the ECS, attempt to access Facebook and YouTube. It should not be able to connect. FortiOS shows the client trying to connect to Facebook and YouTube.

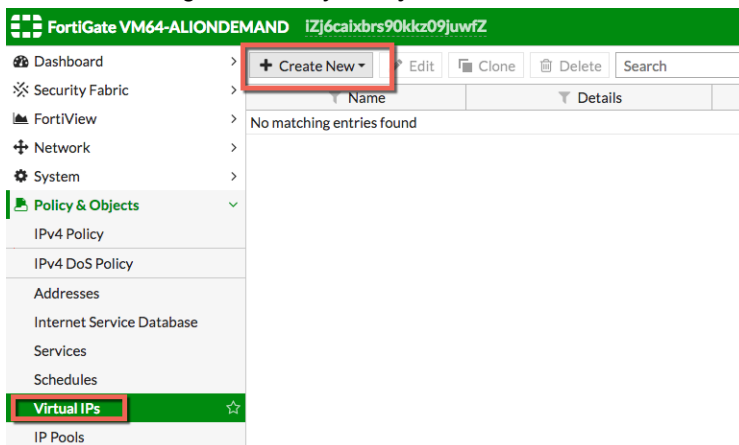




## Enabling NAT inbound protection in FortiOS

In this example, you will enable the FortiGate-VM to protect inbound RDP traffic. The same concept can be applied to HTTP/HTTPS and other services. This demonstrates how to configure the FortiGate-VM to monitor inbound and outbound traffic.

1. In FortiOS, navigate to *Policy & Objects > Virtual IPs*.



2. Map the FortiGate-VM's 3389 port to the ECS at 192.168.1.36.

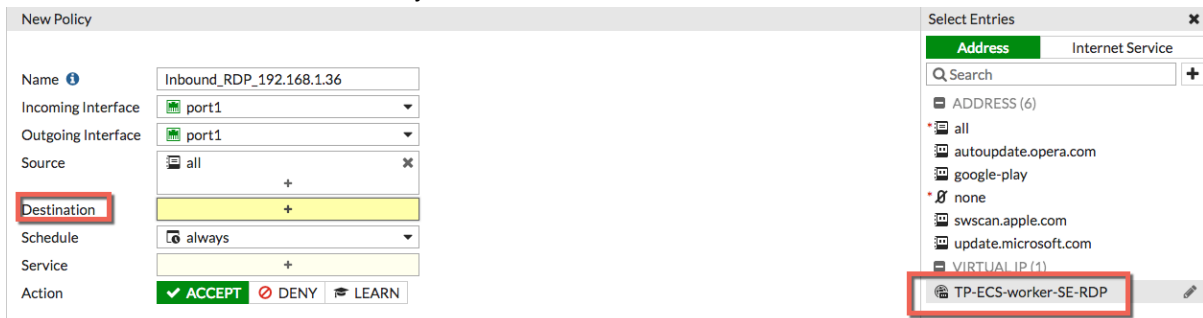
You can now see the newly created virtual IP address.

Name	External IP Address/Range	Mapped IP Address/Range	Protocol	External Service Port	Map to Port	Interface	Services	Ref.
TP-ECS-worker-SE-RDP	0.0.0.0 --> 192.168.1.36 (TCP; 3389 --> 3389)	192.168.1.36	TCP	3389	3389	port1		0

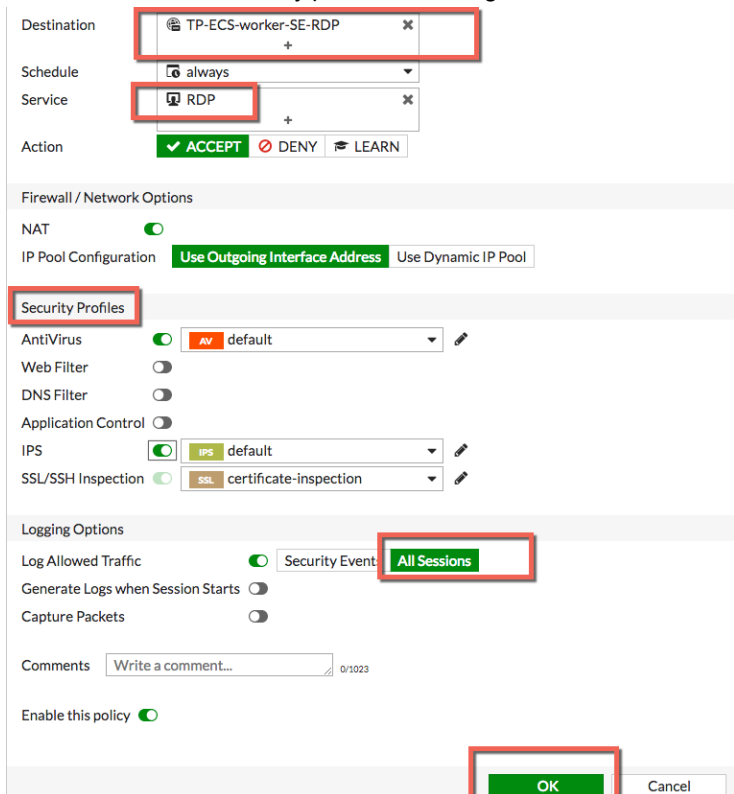
3. Configure the inbound policy for the RDP redirection. Go to *Policy & Objects* > *IPv4 Policy*, then click *Create New*.

ID	Name	Source	Destination	Schedule	Service	Act
1	ToInternet	all	all	always	ALL	✓ A
0	Implicit Deny	all	all	always	ALL	⊘ D

4. Name the rule, then choose the newly created virtual IP address as the destination.



5. Enable the desired security profiles, then log All Sessions for demonstration purposes.



The inbound rule is created successfully.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1	ToInternet	all	all	always	ALL	ACCEPT	Enabled	AV default APP default SSL certificate-inspection	All
2	Inbound_RDP_192.168...	all	TP-ECS-worker-SE-RDP	always	RDP	ACCEPT	Enabled	AV default IPS default SSL certificate-inspection	All
0	Implicit Deny	all	all	always	ALL	DENY			Disabled

You can now use the FortiGate public address to RDP into the ECS.

```

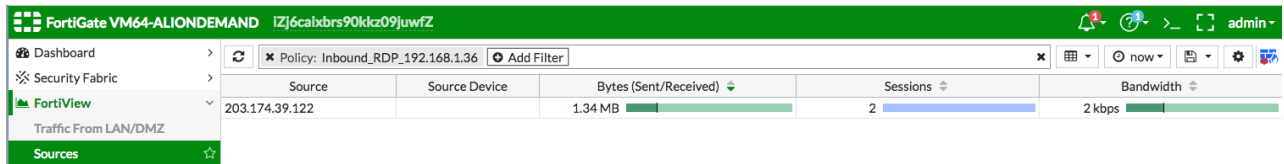
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping hk.yahoo.com

Pinging oob-media-router-fp1.prod.media.wg1.b.yahoo.com [106.10.250.11] with 32
bytes of data:
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55

Ping statistics for 106.10.250.11:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms
Control-C
^C
C:\Users\Administrator>
    
```

You can also view the logs and session information in FortiOS.



## HA for FortiGate-VM on AliCloud

There are different ways to configure active-passive HA on FortiGate-VM for AliCloud.

The first deployment scenario, described in [Deploying and configuring FortiGate-VM on AliCloud using HAVIP on page 23](#), depends on the HAVIP function that AliCloud provides. In this scenario, you must locate both the internal and external interface at port1. The primary and secondary FortiGates share the same IP address. Failover may be quicker than in the second scenario, since there are no EIPs or route tables to update. This scenario natively supports session pickup.

The second deployment scenario, described in [Deploying FortiGate-VM HA on AliCloud using routing tables and EIPs on page 46](#), achieves HA by introducing EIP moving and route table updating capabilities. In this scenario, you can locate the internal and external interface on different interfaces. Optionally, you can also leverage HAVIP for external traffic on port1 and internal traffic on port2 for increased efficiency and flexibility. This scenario supports session pickup, but in a more limited way than in the first scenario.

Consider the following when deciding which HA scenario to deploy:

- If you need session pickup capabilities and cannot disable NAT for incoming firewall policies, you must use the first scenario.
- If you need session pickup capabilities and can disable NAT for incoming firewall policies, you can use the second scenario with HAVIP on port1 and attach an EIP to the HAVIP. This scenario does not require EIP moving but does require route table updating for internal traffic. This scenario provides the best balance between flexibility and efficiency.
- If you cannot use port1 for external traffic, you must use the second scenario with EIP moving and route table updating. This may require more failover time.

## Deploying and configuring FortiGate-VM on AliCloud using HAVIP

You can configure active-passive HA with two FortiGate-VM instances using HAVIP, which is configurable on the AliCloud platform. FortiGate-VM configuration is synchronized between the two instances. When a primary/master FortiGate-VM is down, a failover to a secondary/slave FortiGate-VM occurs while sessions are kept, and the secondary unit is promoted to become the primary unit. HAVIP forwards traffic to the new primary FortiGate-VM while keeping switching time minimal.

In this scenario, the AliCloud VPC cannot create multiple route tables, and the VPC only supports one-arm deployment mode. HAVIP covers an inter-VPC service, and the VPC default route points to the HAVIP. VPC outbound traffic forwards to the HAVIP, then forwards to the primary FortiGate-VM. You must bind the HAVIP to an EIP for VPC inbound traffic.

## Setting up the VPC

- Assuming this is a new environment, the first step is to create the VPC. Click *Create VPC*.

The screenshot shows the AliCloud VPC console. On the left, there is a navigation menu with options: VPCs (selected), Route Tables, VSwitches, Shared Bandwidth P..., and Shared Data Transfer. The main area displays a table of VPCs. At the top, there are buttons for 'Create VPC', 'Refresh', and 'Custom'. A search bar is present with the text 'Enter a name or ID'. The table has columns for Instance ID/Name, Destination CIDR Block, Status, Default VPC, Route Table, VSwitch, and Actions. One VPC is listed with Instance ID 'vpc-12345678', Destination CIDR Block '192.168.0.0/16', Status 'Available', Default VPC 'No', Route Table '1', VSwitch '3', and Actions 'Manage Delete'.

- Name the VPC TP\_FortiVPC.

### VPC

#### Region

China East 1 (Hangzhou)

#### Name ?

TP\_FortiVPC 11/128 ✓

#### Destination CIDR Block ?

192.168.0.0/16

⚠ The CIDR cannot be changed once the VPC is created.

#### Description ?

VPC For demo Fortinet 21/256

- In this scenario, you need at least three VSwitches: one for the ECS, one for the FortiGate-VM inbound/outbound interface, and one for the FortiGate-VM HA interface. You can also create a fourth VSwitch for the FortiGate



reserved management interface. Create the ECS VSwitch first, as seen below.

• **Name** ?

ECS\_SW 6/128 ✓

• **Zone** ?

East China 1 Zone F ✓

**Zone Resource** ?

ECS ✓ RDS ✓ SLB ✓

• **Destination CIDR Block**

192 · 168 · 4 · 0 / 24 ✓

⚠ The CIDR cannot be changed once the VPC is created.

**Number of Available Private IPs**

252

**Description** ?

0/256



(You can only create three instances once.)

+ Add

🗑 Delete

4. Create the VSwitch for the FortiGate-VM inbound/outbound interface, as seen below.

### VSwitch

• **Name** ?

FortiGate\_Internet\_SW 21/128 ✓

• **Zone** ?

East China 1 Zone F ✓

**Zone Resource** ?

ECS ✓ RDS ✓ SLB ✓

• **Destination CIDR Block**

192 - 168 - 0 - 0 / 24 ✓

⚠ The CIDR cannot be changed once the VPC is created.

**Number of Available Private IPs**

252

**Description** ?

0/256



+ Add

🗑 Delete

5. Create the VSwitch for the FortiGate-VM HA interface, as seen below.

• **Name** ?

FortiGate\_HA\_SW 15/128 ✓

• **Zone** ?

East China 1 Zone F

**Zone Resource** ?

ECS ✓ RDS ✓ SLB ✓

• **Destination CIDR Block**

192 · 168 · 1 · 0 / 24 ✓

⚠ The CIDR cannot be changed once the VPC is created.

**Number of Available Private IPs**

252

**Description** ?

0/256



+ Add

🗑 Delete

6. (Optional) Create the VSwitch for the FortiGate reserved management interface.

### Create VSwitch



• VPC

TP\_FortiVPC/vpc-bp1ue3buvqego4vkha4wl

Destination CIDR Block

192.168.0.0/16

• Name ?

FortiGate\_Reserved\_MGMT\_SW 26/128 ✓

• Zone ?

East China 1 Zone F

Zone Resource ?

ECS ✓ RDS ✓ SLB ✓

• Destination CIDR Block

192 . 168 . 3 . 0 / 24

⚠ The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs

252

Description ?

0/256



OK Cancel

The VPC is now ready.

## Create VPC

**Details**

**VPC Name** TP\_FortiVPC  
**VPC ID** vpc-bp1ue3buvqego4vkha4wl  
**Status** Success [Create NAT Gateway](#)

**VSwitch name** FortiGate\_Internet\_SW  
**VSwitch ID** vsw-bp18zyff1ou2azweoun6r  
**Status** Success [Purchase](#)▼

**VSwitch name** FortiGate\_HA\_SW  
**VSwitch ID** vsw-bp1q5b9yoxinv9syb0jgc  
**Status** Success [Purchase](#)▼

**VSwitch name** ECS\_SW  
**VSwitch ID** vsw-bp1gejkl01u0j8brt4ioz  
**Status** Success [Purchase](#)▼

Contact Us

Complete

## Subscribing to the FortiGate-VM in the marketplace

1. Go to the [AliCloud Marketplace](#) and search for Fortinet.
2. You will now create the FortiGate-VM instance. If you have your own FortiGate-VM license, select the BYOL image. Otherwise, select the on-demand image.

- a. Click *Choose Your Plan*.
- b. In this example, PAYG, China East 1 (Hangzhou), and Zone F were selected for the pricing plan, region, and zone, respectively. Zone F is the location of the VPC and VSwitches. Click *ECS Advance Purchase page* to customize the data disk and VPC information.

Choose Your Plan

Pricing Plan

Subscription **Pay-as-you-go**

---

Region

China East 1 (Hangzhou) Zone G Zone B **Zone F** Zone E

---

Image

Fortinet FortiGate-VM On-Demand (2 vCore CPU)

Version: v5.6.3

Release Note: 5.6.3

---

ECS Instance

I/O Optimized

Default Type: ecs.sn1ne.large

[Select another instance type](#)

**Overview**

Image: Fortinet FortiGate-VM On-Demand (2 vCore)

ECS Instance Type: ecs.sn1ne.large(2 Core 4 GB)

System Disk: 40GB (default)

Bandwidth: 2M (pay by traffic)

---

**Pricing Details**

Software fee: **\$ 0.73 /Hour**

ECS Instance usage fee: **\$ 0.143 /Hour**

Data Transfer: **\$ 0.123 /GB**

**Agree Terms and Buy Now**

By subscribing to this product you agree to [End User License Agreement \(EULA\)](#), and all applicable terms and conditions contained in the Alibaba Cloud International Website.

You can choose more specific instance configurations on [ECS Advance Purchase page](#).

- c. Click the ECS type with 4 vCPU to launch the FortiGate instance. The 4 vCPU ECS can support a maximum of 3 NIC, while the 2 vCPU ECS can support 2 NIC. If the FortiGate reserved management interface is required, select the 4 vCPU ECS type.

**Region**

China East 1 (Hangzhou) Random China East 1 Zone G China East 1 Zone B **China East 1 Zone F** China East 1 Zone E

Select a region. Cloud services available in different regions do not have intranet communication with one another. Select a region close to your visitors to achieve the best download experience and lowest latency.

---

**Instance Type**

IO-Optimized Instance  vCPU:  Memory:  Instance type:

Current Generation: All Generations

Architecture: x86-Architecture Heterogeneous Computing

Category: General Purpose Compute Optimized Memory Optimized Big Data Local SSD High Clock Speed Entry-Level (Shared)

Family	Instance type	vCPU	Memory	Physical processor	Clock speed	Intranet bandwidth	Packet forwarding rate
<input type="radio"/> Compute Optimized Type sn1	ecs.sn1.medium	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps	100,000 PPS(Packets Per Second)
<input checked="" type="radio"/> Compute Optimized Type sn1	ecs.sn1.large	<b>4 vCPU</b>	<b>8 GiB</b>	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.8 Gbps	200,000 PPS(Packets Per Second)
<input type="radio"/> Network Enhanced sn1ne	ecs.sn1ne.large	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1 Gbps	300,000 PPS(Packets Per Second)

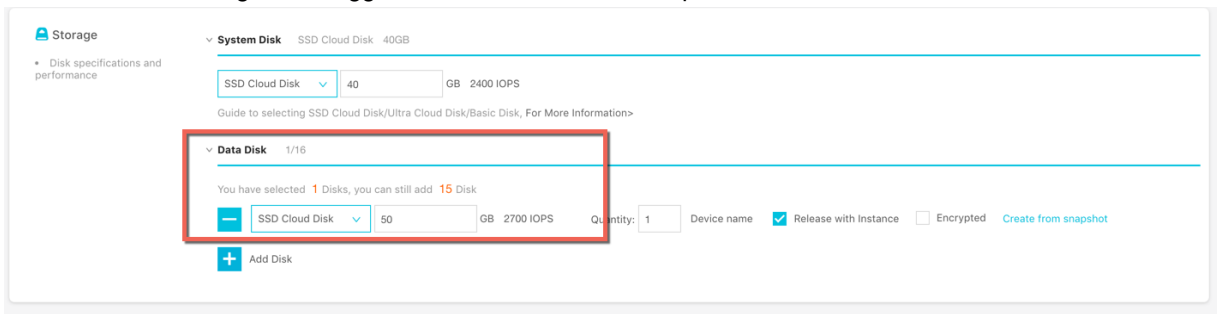
Bandwidth: 2Mbps PayBy/Traffic

Instance Cost: **\$ 0.262 USD per Hour** + Marketplace image fee: **\$ 0.730 USD per Hour** + Public traffic fee: **\$ 0.123 USD per GB**

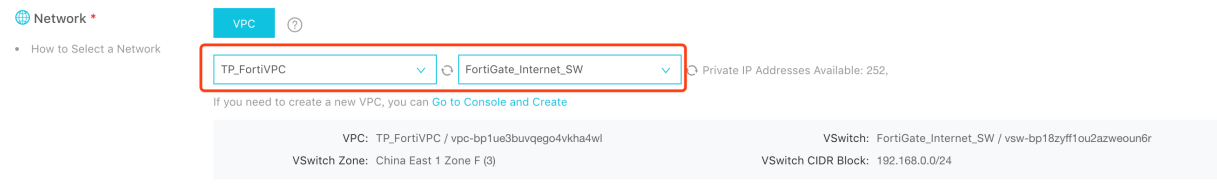
Save \$ 0.013 USD per Hour 👉 save 5% for ECS

Next: Networking Preview

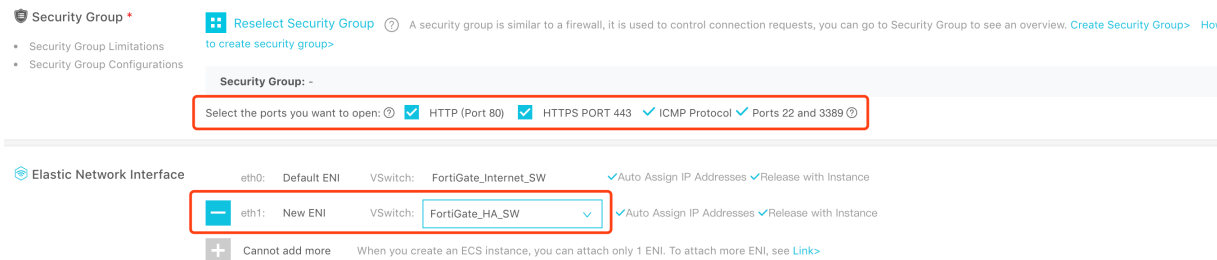
d. Add a data disk for logs. It is suggested to use SSD for better performance.



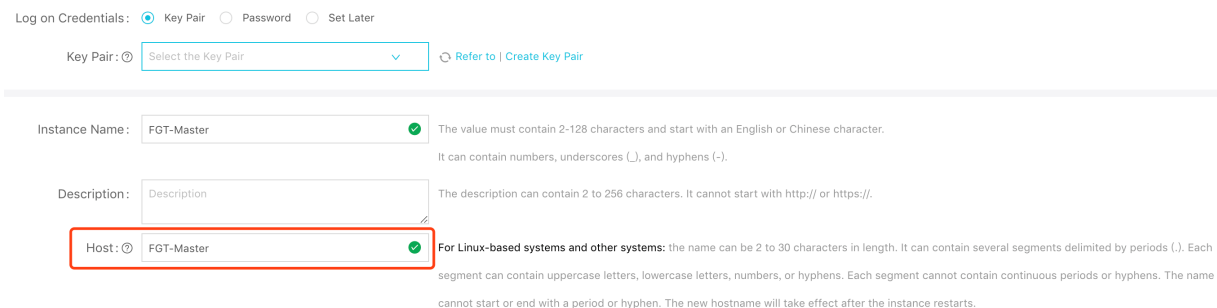
e. In the *Network* section, select TP\_FortiVPC and Forti\_internet\_SW. Assign a public IP address to the image. This NIC will be port1 on the FortiGate-VM, the default ENI.



f. Leave the HTTPS, ICMP, and SSH ports and protocols open to allow connection. Add another ENI on FortiGate\_HA\_SW. This ENI will be port2 on the FortiGate.



g. In the *Host* field, enter the FortiGate hostname.



**h. Click *ECS Service Terms*.**

Automatic Release     Auto Release Schedule  
 This ECS instance will be released at the scheduled time

---

Terms of Service     **ECS Service Terms**

[Purchase Notice](#)  
 You can view your bills and configure your billing in [Billing Management](#).  
 Alibaba Cloud Services forbids TCP port 25 and port 25 related mail services, if you need access to this port, a request needs to be submitted and approved first. [see more](#)>

**3. Click *Console* to return to the ECS instance list.**

**4. You can see that the VM has been created. Mark down the public IP address and the instance ID for later use. The instance ID is the FortiGate default password.**

Instance List Refresh Create Instance Bulk Action

Select the instance attribute, or directly enter the keyword Advanced Search

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
<input type="checkbox"/> i-bp1cj6it8c8hndkxom7 FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage   Connect Change Instance Type   More

**5. Repeat steps 1 and 2 to create another FortiGate instance, named FGT-Slave.**

Instance List Refresh Create Instance Bulk Action

Select the instance attribute, or directly enter the keyword Advanced Search

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
<input type="checkbox"/> i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247 (Internet IP Address) 192.168.0.151 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	Manage   Connect Change Instance Type   More
<input type="checkbox"/> i-bp1cj6it8c8hndkxom7 FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage   Connect Change Instance Type   More
<input type="checkbox"/> i-bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	192.168.5.144 (Private IP Address)	Stopped	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-04-04 07:50 created	Manage   Change Instance Type More
<input type="checkbox"/> i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84 (Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage   Connect Change Instance Type   More

Start Stop Restart Reset Password Renew Switch to Subscription Release Setting More

Total: 4 item(s), Per Page: 20 item(s) « ‹ 1 › »



6. You can create two ENI and attach them to the FortiGate instances. This step is optional.

a. Stop the two FortiGate instances.

Instance List

Instance ID/Name    Tags    Monitor    Zone    IP Address    Status    Network Type    Configuration    Billing Method    Actions

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
<input checked="" type="checkbox"/> i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247(Internet IP Address) 192.168.0.151(Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	Manage   Connect   More
<input checked="" type="checkbox"/> i-bp1cj6it8c8hndkxom7 FGT-Master			East China 1 Zone F	116.62.190.109(Internet IP Address) 192.168.0.150(Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage   Connect   More
<input type="checkbox"/> i-bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	47.98.103.62(Internet IP Address) 192.168.5.144(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large 5Mbps (peak value)	Pay-As-You-Go 18-04-04 07:50 created	Manage   Connect   More
<input type="checkbox"/> i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage   Connect   More

Start     Stop    Restart    Reset Password    Renew    Switch to Subscription    Release Setting    More

Total: 4 item(s), Per Page: 20 item(s)

b. Go to *Networks & Security > Network Interfaces* and create two ENI.

Elastic Compute Serv... | Network Interfaces

       Search

ID/Name	VSwitch/VPC	Zone	Security Group ID	Bound Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-1...	vsw-1...	East China 1 Zone F	sg-1...	i-1...		192.168.0.151	Primary	Running	Modify   Delete
eni-2...	vsw-1...	East China 1 Zone F	sg-1...			192.168.0.152	Secondary	Running	Modify   Delete
eni-3...	vsw-1...	East China 1 Zone F	sg-1...			192.168.0.153	Secondary	Running	Modify   Delete
eni-4...	vsw-1...	East China 1 Zone F	sg-1...			192.168.0.154	Secondary	Running	Modify   Delete

Create



Network Interface  
Name:

FGT-Master-Port3

2-128 characters, not http:// or https:// at the beginning, must be based on the size of letters beginning, may contain numbers, - or \_

\* VPC:

vpc-bp1ue3buvqego4vkha4wl / TP\_Fort...

\* VSwitch:

vsw-bp1n4o8m36029aq05akvk / FortiG...

CIDR: 192.168.3.0/24

IP:

Must be the free address in the address section of the VSwitch to which it belongs. By default, the free address in the switch is allocated randomly.

\* Security Group

sg-bp153m2jlzs6qlvntqt5

Description:

It must contain 2-256 characters and it cannot begin with http:// or https://

OK

Cancel

Create



Network Interface Name:

2-128 characters, not http:// or https:// at the beginning, must be based on the size of letters beginning, may contain numbers, - or \_

\* VPC:

\* VSwitch:

CIDR: 192.168.3.0/24

IP:

Must be the free address in the address section of the VSwitch to which it belongs. By default, the free address in the switch is allocated randomly.

\* Security Group:

Description:

It must contain 2-256 characters and it cannot begin with http:// or https://

c. Attach the two new ENI to the two FortiGate instances.

Network Interfaces

Name

ID/Name	VSwitch/VPC	Zone	Security Group ID	Bound Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-bp126a4rnnfhnelnoksk FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...			192.168.3.250	Secondary 00:16:3e:12:2b:bf	Available 2018-05-02	Modify <input type="button" value="Attach"/> <input type="button" value="Delete"/>
eni-bp126a4rnnfhnelnoksh FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...			192.168.3.249	Secondary 00:16:3e:10:13:3e	Available 2018-05-02	Modify <input type="button" value="Attach"/> <input type="button" value="Delete"/>

Attach



ID/Name: eni-bp126a4rnnfhnelnoksk/FGT-Slave-Port3

\*Select Instance:

i-bp167uui7rqzmp8ta0kw

FGT-Slave

FGT-Master

OK

Cancel

Attach



ID/Name: eni-bp126a4rnnfhnelnoksh/FGT-Master-Port3

\*Select Instance:

i-bp167uui7rqzmp8ta0kw

FGT-Slave

FGT-Master

OK

Cancel

Network Interfaces

Refresh Create

Update succes

Name Enter name Search

ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-bp126a4rnnfhnelnoksk/FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2j...	i-bp167uui7r...		192.168.3.250	Secondary 00:16:3e:12:2b:bf	In Use 2018-05-02	Modify   Detach   Delete
eni-bp126a4rnnfhnelnoksh/FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2j...	i-bp1cj6it8c...		192.168.3.249	Secondary 00:16:3e:10:13:3e	In Use 2018-05-02	Modify   Detach   Delete

d. Restart the two FortiGate instances.

Instance List

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
<input checked="" type="checkbox"/> i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247(Internet IP Address) 192.168.0.151(Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	Manage   Connect   More
<input checked="" type="checkbox"/> i-bp1cj6it8c8hndkxom7j FGT-Master			East China 1 Zone F	116.62.190.109(Internet IP Address) 192.168.0.150(Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2ne.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage   Connect   More
<input type="checkbox"/> i-bp1i12dakoem7nchepx8 SSL_VPN_Server			East China 1 Zone F	47.98.103.62(Internet IP Address) 192.168.5.144(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large 5Mbps (peak value)	Pay-As-You-Go 18-04-04 07:50 created	Manage   Connect   More
<input type="checkbox"/> i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage   Connect   More

Start Stop **Restart** Reset Password Renew Switch to Subscription Release Setting More

Total: 4 item(s), Per Page: 20 item(s)

- You can now access the FortiGate-VM in a web browser using the username "admin". The password is the instance ID.
- Change the password after the initial login.
- Set the IP address on three interfaces on the FortiGate.

**FortiGate VM64-ALIONDEMAND FGT-Master**

- Dashboard
- Security Fabric
- FortiView
- Network**
- Interfaces**
- DNS
- Packet Capture
- SD-WAN
- SD-WAN Status Check
- SD-WAN Rules
- Static Routes
- Policy Routes
- RIP
- OSPF

**Edit Interface**

Interface Name port3 (00:16:3E:10:13:3E)  
 Alias **MGMT**  
 Link Status Up  
 Type Physical Interface  
 Role Undefined

**Address**

Addressing mode **Manual** DHCP One-Arm Sniffer Dedicated to FortiSwitch  
 IP/Network Mask 192.168.3.249/24

**Administrative Access**

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

The screenshot shows the AliCloud console interface. On the left, there is a navigation menu with options like Overview, Instances, Auto Scaling, Block Storage, and Snapshots & Images. The main area displays 'Network Interfaces' with a table of interface details. Two interfaces are listed, both with private IP addresses highlighted in red boxes: 192.168.3.250 and 192.168.3.249. Below this, the FortiGate VM configuration is shown, including a dashboard and a 'Network' section with a table of physical interfaces. The table lists three interfaces: port1 (WAN/LAN), port2 (HA), and port3 (MGMT), each with its IP address and status.

ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(AII)	Status/Created At	Actions
eni-bp126a4rnnfnneinoksk FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2j...	i-bp167uui7r...		192.168.3.250	Secondary 00:16:3e:12:2b:bf	In Use 2018-05-02	Modify   Detach   Delete
eni-bp126a4rnnfnneinoksk FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2j...	i-bp1cj6it8c...		192.168.3.249	Secondary 00:16:3e:10:13:3e	In Use 2018-05-02	Modify   Detach   Delete

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (3)						
🟢	port1 (WAN/LAN)		192.168.0.150 255.255.255.0	Physical Interface	PING HTTPS SSH FMG-Access	1
🟢	port2 (HA)		192.168.1.249 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
🟢	port3 (MGMT)		192.168.3.249 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	0

## Configuring the HAVIP on the AliCloud web console

1. Create a new HAVIP address. Select the VPC and FortiGate-VM port 1 VSwitch, and set the HAVIP address.

The screenshot shows the 'HAVIP Addresses' configuration page in the AliCloud console. A 'Create HAVIP Address' button is highlighted with a red box. Below it is a table listing existing HAVIP addresses. The table has columns for Instance ID, IP Address, Status, Bind Instance, VPC, VSwitch, and Actions. The table is currently empty.

Instance ID	IP Address	Status	Bind Instance	VPC	VSwitch	Actions
-------------	------------	--------	---------------	-----	---------	---------

## Create HAVIP Address

**Region**

China East 1 (Hangzhou)

**VPC**

vpc-bp1ue3buvqego4vkha4wl

**VSwitch**

vsw-bp18zyff1ou2azweoun6r

**VSwitch CIDR Block**

192.168.0.0/24

**Private IP Address**

192 . 168 . 0 . 252

2. Set the HA configuration on the FortiGate via the VNC console on the AliCloud Web GUI, or via SSH.
  - a. Set the configuration on the primary FortiGate-As follows. In this example, 192.168.3.253 is the gateway on the VSwitch, while 192.168.1.250 is the secondary FortiGate's port2's IP address. Note the FortiGate with a higher priority value will be the primary 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
    next
  end
  set priority 200
  set monitor "port1"
  set unicast-hb enable
  set unicast-hb-peerip 192.168.1.250
end
```

- b. Set the configuration on the secondary FortiGate-As follows. Here, 192.168.1.249 is the primary FortiGate's port2's IP address.

```
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
  next
end
set priority 100
set monitor "port1"
set unicast-hb enable
set unicast-hb-peerip 192.168.1.249
end

```

3. Reboot the two FortiGates.

4. Check the HA status by running `diagnose sys ha status` in the CLI. It should show the following:

```

FGT-Master # diagnose sys ha status
HA information
Statistics
  traffic.local = s:0 p:20456 b:7590378
  traffic.total = s:0 p:20467 b:7591052
  activity.fdb = c:0 q:0

Model=90019, Mode=2 Group=0 Debug=0
nocluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_master=1.
FGTALIG8XFM4RR79: Master, serialno_prio=1, usr_priority=200, hostname=FGT-Master
FGTALIZT2A540C07: Slave, serialno_prio=0, usr_priority=100, hostname=FGT-Slave

[Kernel HA information]
nocluster 1, state=work, master_ip=192.168.1.249, master_id=0:
FGTALIG8XFM4RR79: Master ha_prio/o_ha_prio=0/0
FGTALIZT2A540C07: Slave ha_prio/o_ha_prio=1/1

```

5. Set the HAVIP address to the port1 secondary IP address on the two FortiGates. On both FortiGates, configure the following. The secondary IP address configured below should be the same as the HAVIP address.

```

config system interface
  edit "port1"
    set secondary-IP enable
    config secondaryip
      edit 1
        set ip 192.168.0.252 255.255.255.0
        set allowaccess ping https ssh
      next
    end
  next
end

```



6. Bind the elastic IP address and the two FortiGate ECS to HAVIP.

a. Create a new EIP.

**Elastic IP Address**

Elastic IP Addresses

**Elastic IP Address List**

China North 1 (Qingdao)

China North 2 (Beijing)

China North 3 (Zhangjiakou)

China North 5 (Huhehaote)

Refresh Create EIP

China East 1 (Hangzhou)

China East 2 (Shanghai)

China South 1 (Shenzhen)

Hong Kong(China)

Asia Pacific NE 1 (Tokyo)

Asia Pacific SE 1 (Singapore)

Asia Pacific SE 2 (Sydney)

Asia Pacific SE 3 (Kuala Lumpur)

Asia Pacific SE 5 (Jakarta)

Asia Pacific SOU 1 (Mumbai)

US East 1 (Virginia)

US West 1 (Silicon Valley)

Middle East 1 (Dubai)

EU Central 1 (Frankfurt)

Elastic IP Address  Search Export

<input type="checkbox"/>	Instance ID	IP Address	Monitoring	Bandwidth	Billing Method(All)	Status(All)	Shared Bandwidth	Instance Bound	Instance Type	Actions
<input type="checkbox"/>	eip-bp1f5kuoatanoco05jgk2	47.97.186.150		Pay by Traffic 10Mbps	Pay-As-You-Go Created at 2018-05-02 16:23:24	Available	-	-	-	Bind   Unbind   More

**VPC**

VPCs

Route Tables

VSwitches

Shared Bandwidth P...

Shared Data Transfer...

Elastic IP Addresses

NAT Gateways

Global Acceleration

VPN

VPN Gateways

Customer Gateways

IPsec Connections

SSL Servers

SSL Clients

HAVIP Addresses

**HAVIP Addresses**

Create HAVIP Address
Refresh
Custom

Instance ID

Instance ID	IP Address	Status	Bind Instance	VPC	VSwitch	Actions
havip-bp1bwya8f7lppbl0qq6l5	192.168.0.252(Intranet IP)	Available	No ECS Bound	vpc-bp1ue3buvqego4vkha4wlTP_FortiVPC	vsw-bp18zzyff1ou2azweoun6rFortiGate_Interne...	Manage   More

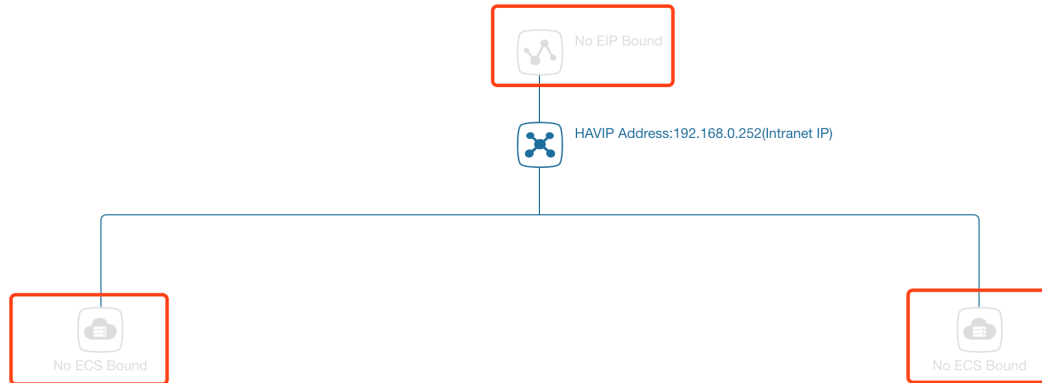
HAVIP Details

Refresh Delete

Information

ID	havip-bp1bwya8f7lppbl0qq6l5	Status	Available
Region	China East 1 (Hangzhou)	Intranet IPIP	192.168.0.252
VPC ID	vpc-bp1ue3buqego4vkha4wl	Created At	05/02/2018, 15:12:42
VSwitch	vsw-bp18zyff1ou2azweoun6r	Description	- Edit

Resources



b. Bind the EIP to the HAVIP.

Bind Elastic IP Address

**HAVIP Address**

havip-bp1bwya8f7lppbl0qq6l5

**Intranet IPIP**

192.168.0.252

**Elastic IP Address**

Select ^

- 47.97.186.150
- 116.62.161.94

- c. Bind the two FortiGates to the HAVIP.

### Bind an ECS Instance

---

**HAVIP Address**

havig-bp1bwya8f7lppbl0qq6l5

**Intranet IPIP**

192.168.0.252

● **ECS Instance**

i-bp167uui7rqzmp8ta0kw

### Bind an ECS Instance

---

**HAVIP Address**

havig-bp1bwya8f7lppbl0qq6l5

**Intranet IPIP**

192.168.0.252

● **ECS Instance**

Select

i-bp167uui7rqzmp8ta0kw

i-bp1cj6it8c8hndkxom7j

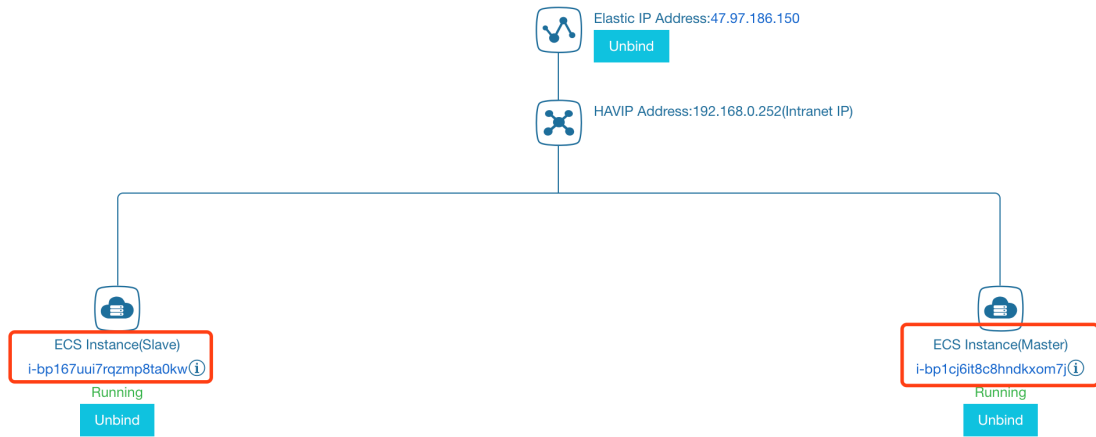
HAVIP Details

Refresh Delete

Information

ID	havig-bp1bwya8f7lppbl0qq6i5	Status	Allocated
Region	China East 1 (Hangzhou)	Intranet IPIP	192.168.0.252
VPC ID	vpc-bp1ue3buvqego4vkha4wl	Created At	05/02/2018, 15:12:42
VSwitch	vsw-bp18zyff1ou2azweoun6r	Description	- Edit

Resources



7. You must add the route entry to the FortiGate to ensure all outgoing traffic from ECS goes through the FortiGate.

### Route Table

#### Route Table Details

Route Table ID [vtb-bp1785omvus5wpyvwiogn](#) VPC ID [vpc-bp1ue3buvqego4vkha4wl](#)  
 Name - [Edit](#) Route Table Type System  
 Created At 05/02/2018, 13:48:20 Description - [Edit](#)

#### Route Entry List

Destination CIDR Block	Status	Next Hop	Type	Actions
192.168.0.0/24	● Available	-	System	
192.168.1.0/24	● Available	-	System	
192.168.3.0/24	● Available	-	System	
192.168.4.0/24	● Available	-	System	
100.64.0.0/10	● Available	-	System	

### Add Route Entry

● Destination CIDR Block

.  .  .  /

● Next Hop Type

● HAVIP Address

## Route Table

### Route Table Details

Route Table ID	vtb-bp1785omvus5wpywio9n	VPC ID	vpc-bp1ue3buvqego4vkha4wl
Name	- <a href="#">Edit</a>	Route Table Type	System
Created At	05/02/2018, 13:48:20	Description	- <a href="#">Edit</a>

### Route Entry List

Destination CIDR Block	Status	Next Hop	Type	Actions
0.0.0.0/0	● Creating	Instance ID:havip-bp1bwya8f7lppbl0qq6l5 Instance Type:HAVIP	Custom	<a href="#">Delete</a>
192.168.0.0/24	● Available	-	System	
192.168.1.0/24	● Available	-	System	
192.168.3.0/24	● Available	-	System	
192.168.4.0/24	● Available	-	System	
100.64.0.0/10	● Available	-	System	

## Connectivity test

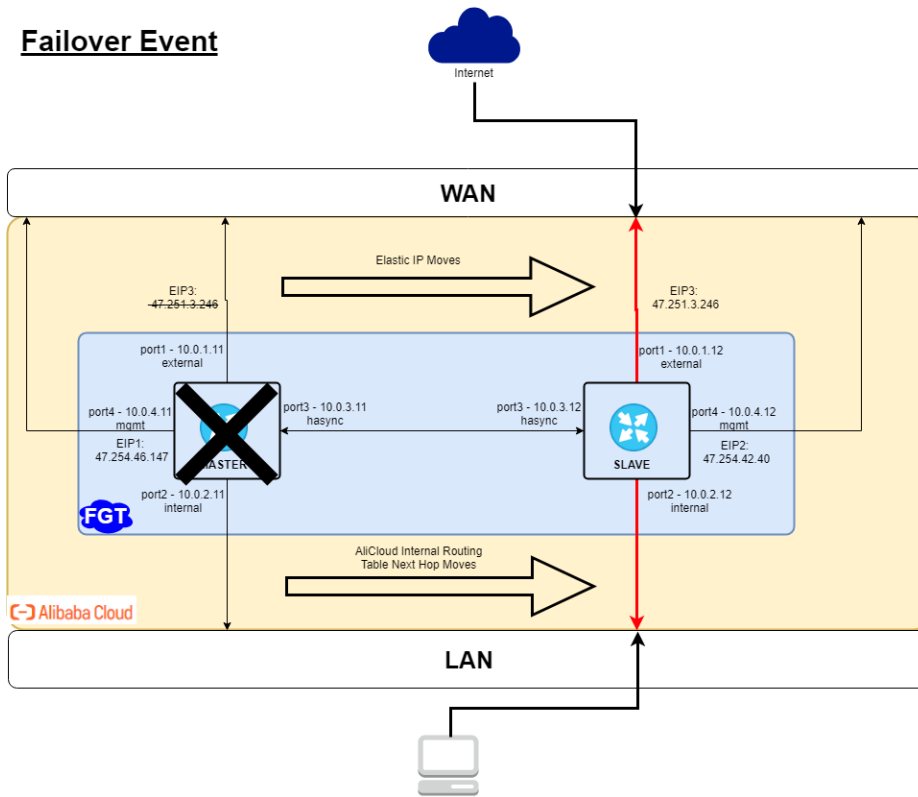
You can test whether you configured the FortiGate-VM instances and VPC properly. See [Connectivity test on page 14](#).

## Deploying FortiGate-VM HA on AliCloud using routing tables and EIPs

This guide provides a sample configuration of active-passive FortiGate-VM HA on AliCloud within one availability zone.

The following depicts the network topology for this sample deployment:

**Failover Event**



The following lists the IP address assignments for this sample deployment for FortiGate-A:

Port	AliCloud primary address	Subnet
port1	10.0.1.11	10.0.1.0/24 EIP3
port2	10.0.2.11	10.0.2.0/24
port3	10.0.3.11	10.0.3.0/24
port4	10.0.4.11	10.0.4.0/24 EIP1

The following lists the IP address assignments for this sample deployment for FortiGate-B:

Port	AliCloud primary address	Subnet
port1	10.0.1.12	10.0.24.0
port2	10.0.2.12	10.0.21.0/24
port3	10.0.3.12	10.0.22.0/24
port4	10.0.4.12	10.0.23.0/24

**To check the prerequisites:**

The following prerequisites must be met for this deployment:

- One VPC with one subnet each for management, external, internal, and heartbeat purposes
- Three public IP addresses:
  - EIP1 and EIP2 for FortiGate-A and FortiGate-B management
  - EIP3 for the HA external traffic IP address
- Two FortiGate-VM instances, both PAYG or BYOL
- The following summarizes minimum sufficient [RAM roles](#) for this deployment:
  - AliyunECSFullAccess
  - AliyunEIPFullAccess
  - AliyunVPCFullAccess



Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

**To configure FortiGate-VM HA in AliCloud:**

1. In the AliCloud management console, create a VPC with four VSwitches:

VSwitch	Purpose
net1-external	External data traffic on the public network-facing side.
net2-internal	External data traffic on the public network-facing side.
net3-heartbeat	Heartbeat between two FortiGate nodes. This is unicast communication.
net4-mgmt	Dedicated management interface.

Instance ID/Name	VPC	Status	IPv4 CIDR Block	Default VSwitch	Zone	Route Table	Route Table Type	Actions
vsw-rj96khrfv15gmnj3fk0x net4-mgmt	vpc-rj9h5m14eo5i u97hjaptw thua-vpc-ha	Available	10.0.4.0/24	No	Silicon Valley Zone A	vtb-rj9g99919c2uoq oetzra	System	Manage Delete Purchase
vsw-rj9973fmgxch9hloqj net3-heartbeat	vpc-rj9h5m14eo5i u97hjaptw thua-vpc-ha	Available	10.0.3.0/24	No	Silicon Valley Zone A	vtb-rj9g99919c2uoq oetzra	System	Manage Delete Purchase
vsw-rj9e6tqpf9v2xo0h1jr net2-internal	vpc-rj9h5m14eo5i u97hjaptw thua-vpc-ha	Available	10.0.2.0/24	No	Silicon Valley Zone A	vtb-rj9g11gufwqqe5ps 3q60i	Custom	Manage Delete Purchase
vsw-rj9tqi2vla806u969hrd net1-external	vpc-rj9h5m14eo5i u97hjaptw thua-vpc-ha	Available	10.0.1.0/24	No	Silicon Valley Zone A	vtb-rj9g99919c2uoq oetzra	System	Manage Delete Purchase



2. Add six ENIs.

Instance ID	VPC	Zone	Subnet	IP Address	Secondary IP Address	Creation Time	Actions
eni-rjdirvq0hyke8b18o fhua-net4-12	vsw-rj96khrf... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...	47.254.42.40	10.0.4.12	Secondary 00:16:3e:00:c0:a5	Bound May 31, 2019, 14:42 Manage Secondary Private IP Address   Delete
eni-rj9gsl6wcti7anp0ot7m fhua-net3-12	vsw-rj9973fz... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.3.12	Secondary 00:16:3e:00:14:b9	Bound May 31, 2019, 14:42 Manage Secondary Private IP Address   Delete
eni-rj94eztq3bv65yqd6k fhua-net2-12	vsw-rj9e6tqg... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.2.12	Secondary 00:16:3e:00:1d:8d	Bound May 31, 2019, 14:42 Manage Secondary Private IP Address   Delete
eni-rj9i1iuch9t3qd5doe3 fhua-net4-11	vsw-rj96khrf... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...	47.254.46.147	10.0.4.11	Secondary 00:16:3e:00:2b:a7	Bound May 31, 2019, 14:41 Manage Secondary Private IP Address   Delete
eni-rj91wj13wvjs7y1n23ow fhua-net3-11	vsw-rj9973fz... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.3.11	Secondary 00:16:3e:00:45:3e	Bound May 31, 2019, 14:41 Manage Secondary Private IP Address   Delete
eni-rj94jg06fag0v1jneyv fhua-net2-11	vsw-rj9e6tqg... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.2.11	Secondary 00:16:3e:00:c0:1a	Bound May 31, 2019, 14:39 Manage Secondary Private IP Address   Delete
eni-rj95mchbk2uqxqy6t8 -	vsw-rj9mwszu... vpc-rj9v23c9...	Silicon Valley Zone A	sg-rj9ee...	192.168.0.184		Primary 00:16:3e:00:c1:47	Bound May 31, 2019, 09:21 Manage Secondary Private IP Address   Delete

3. Create two routing tables:

- a. Create a routing table called "rtb-internal" for the net2-internal VSwitch. Set the NIC2 secondary IP address (10.0.2.23) as rtb-internal's default gateway. You can create this routing table after configuring NIC2 on FortiGate-A. Ensure that the default gateway is FortiGate-A's port2 ENI.

Route Table Details

Route Table ID: vtb-rj9q1tguvqqe5ps3q60i | VPC ID: vpc-rj9h5m14eo5lu97hjapjw

Name: rtb-internal | Route Table Type: Custom

Created At: 05/31/2019, 16:18:42 | Description: - Edit

Route Entry List | Associated VSwitches

Destination CIDR Block	Status	Next Hop	Type	Actions
0.0.0.0/0	Available	eni-rj94jg06fag0v1jneyv	Custom	Delete
10.0.1.0/24	Available	-	System	
10.0.2.0/24	Available	-	System	
10.0.3.0/24	Available	-	System	
10.0.4.0/24	Available	-	System	
100.64.0.0/10	Available	-	System	

- b. Create a routing table called "rtb-external" for the remaining VSwitches. Set this VCN's Internet gateway as its

default gateway. Ensure that this routing table can access the Internet.

Route Table Details

Route Table ID: vtb-rj9g999919c2uoqoetza VPC ID: vpc-rj9h5m14eo5lu97hjapw

Name: rtb-external Edit Route Table Type: System

Created At: 05/30/2019, 16:26:01 Description: - Edit

Route Entry List Associated VSwitches

Destination CIDR Block	Status	Next Hop	Type	Actions
10.0.1.0/24	Available	-	System	
10.0.2.0/24	Available	-	System	
10.0.3.0/24	Available	-	System	
10.0.4.0/24	Available	-	System	
100.64.0.0/10	Available	-	System	

### To deploy the FortiGate-VMs in AliCloud:

To take advantage of A-P HA, you need four vNICs (port1 to port4) on each FortiGate-VM that constitutes an A-P HA cluster. Configure all required network interfaces (AliCloud ENIs and FortiGate-VM network interface configuration) that support A-P HA. You must choose an AliCloud instance type that supports at least four vNICs.

Ensure the following:

- You have configured the security group on each subnet for egress and ingress interfaces appropriately. It is particularly important that the management interfaces have egress Internet access for API calls to the AliCloud metadata server.
- You attached four NICs for each FortiGate-VM, and assigned the static private IP address.
- EIP1 was bound to the FortiGate-A port4 management interface.
- EIP3 was bound to the FortiGate-A port1 external interface.
- EIP2 was bound to the FortiGate-B port4 management interface.



You can attach a public IP address on the primary FortiGate-VM's external interface instead of an EIP by creating an HAVIP address in the VPC, then binding this HAVIP address to both FortiGates' external interfaces. This approach may shorten the failover time depending on the network environment.

FGT-A

Instance Details

Network Interfaces

ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(All)	Status/Created At	Actions
eni-rj9dirvng0hykoddv7z		vsw-rj9tgit2-vpc-rj9h5m14	Silicon Valley Zone A	sg-rj99v...	47.251.3.246	10.0.1.11	Primary 00:16:3e:00:02:4d	Bound May 31, 2019, 15:02	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-rj9i1luoh9h3qd5doe3		vsw-rj96khrf-vpc-rj9h5m14	Silicon Valley Zone A	sg-rj99v...	47.254.46.147	10.0.4.11	Secondary 00:16:3e:00:2ba7	Bound May 31, 2019, 14:41	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-rj9i1wj13wjs7y1n25ow		vsw-rj9973f-vpc-rj9h5m14	Silicon Valley Zone A	sg-rj99v...		10.0.3.11	Secondary 00:16:3e:00:45:3e	Bound May 31, 2019, 14:41	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-rj94jg06faq0v1jneyv		vsw-rj9e6kag-vpc-rj9h5m14	Silicon Valley Zone A	sg-rj99v...		10.0.2.11	Secondary 00:16:3e:00:c0:1a	Bound May 31, 2019, 14:39	Modify   Unbind Manage Secondary Private IP Address   Delete

ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(All)	Status/Created At	Actions
eni-rj9f5x9cp9swekw6zh		vsw-rj9tgit2... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.1.12	Primary 00:163e00:36f1	Bound May 31, 2019, 14:47	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-rj9dirrv0nykei8bi8o		vsw-rj96khrf... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...	47.254.42.40	10.0.4.12	Secondary 00:163e00:c0a5	Bound May 31, 2019, 14:42	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-rj9ga16wct17anp0ot7m		vsw-rj9973fz... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.3.12	Secondary 00:163e00:14b9	Bound May 31, 2019, 14:42	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-rj9f4estg3bv65yqd6x		vsw-rj9e6tag... vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.2.12	Secondary 00:163e00:1d8d	Bound May 31, 2019, 14:42	Modify   Unbind Manage Secondary Private IP Address   Delete

### To configure FortiGate-A using the CLI:

The next steps show you how to configure A-P HA settings by using CLI commands on the GUI or via SSH. If using SSH, the FortiGate may lose connection due to routing table changes, so configuring HA via the GUI is recommended.

```

config system interface
  edit "port1"
    set mode static
    set ip 10.0.1.11 255.255.255.0
    set allowaccess ping https ssh snmp http fgfm
  next
  edit "port2"
    set ip 10.0.2.11 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
  edit "port3"
    set ip 10.0.3.11 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
  edit "port4"
    set ip 10.0.4.11 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
end

config router static
  edit 1
    set gateway 10.0.1.1
    set device "port1"
  next
end

config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable

```

```
    next
end
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set hbdev "port3" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.4.1
        next
    end
    set priority 128
    set unicast-hb enable
    set unicast-hb-peerip 10.0.3.12
end
```

### To configure FortiGate-B using the CLI:

The next steps show you how to configure A-P HA settings by using CLI commands on the GUI or via SSH. If using SSH, the FortiGate may lose connection due to routing table changes, so configuring HA via the GUI is recommended.

```
config system interface
    edit "port1"
        set mode static
        set ip 10.0.1.12 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
    next
    edit "port2"
        set ip 10.0.2.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port3"
        set ip 10.0.3.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.0.4.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config router static
    edit 1
        set gateway 10.0.1.1
        set device "port1"
    next
end

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
```

```

        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

config system ha
    set group-name "FGT-HA"
    set mode a-p
    set hbdev "port3" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.4.1
        next
    end
    set priority 64
    set unicast-hb enable
    set unicast-hb-peerip 10.0.3.21
end

```



You must set the FortiGate-B HA priority to a value lower than FortiGate-A's priority level. The node with the lower priority level is determined as the secondary node.

**To check the HA status and function:**

1. In FortiOS on the primary FortiGate, go to *System > HA*. Check that the HA status is synchronized.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
<input checked="" type="checkbox"/>	129	FGT-A	FGTALI1OLDMASIE8	Master	00:03:11:15	19	278.00 kbps
<input checked="" type="checkbox"/>	64	FGT-B	FGTALIYCQ_Y4V738	Slave	00:03:11:12	14	23.00 kbps

2. Log into a PC that is located in the internal subnet. Verify that the PC can access the Internet via FortiGate-A when FortiGate-A is the primary node.
3. Shut down FortiGate-A. Verify that FortiGate-B becomes the primary node. Use an API call to verify that the secondary private IP address moves to FortiGate-B.
4. Log into the PC. Verify that the PC can access the Internet via FortiGate-B when FortiGate-B is the primary node.
5. You can use the following diagnose commands to see if the secondary private IP address moves from FortiGate-A to FortiGate-B during failover:

```

FGT-B # diagnose debug application alicloud-ha -1
Debug messages will be on for 30 minutes.

```

```

FGT-B # Become HA master mode 2

```

```
===== start acs ha failover =====
send_vip_arp: vd root master 1 intf port1 ip 10.0.1.12
send_vip_arp: vd root master 1 intf port2 ip 10.0.2.12
acs meta info [instance id]: i-rj9f5xs9cp9xsweedlcs
acs meta info [ram role]: fhua-ecs-role
acs meta info [region]: us-west-1
acs meta info [vpc id]: vpc-rj9h5m14eo5lu97hjaptw
acs ecs endpoint is resolved at ecs.us-west-1.aliyuncs.com:47.88.73.18
acs vpc endpoint is resolved at vpc.aliyuncs.com:106.11.61.112
acs is parsing page 1 of total 3(1 page) instances
acs is checking tags on instance FGT-A
  Tag.FGT_port1: eni-rj9dirnvg0hykoddvv7z
  Tag.FGT_port2: eni-rj94jig06fag0vljneyv
  Tag.FGT_port3: eni-rj91wj13vwjs7y1n25ow
  Tag.FGT_port4: eni-rj9illiuoh9t3qd5doe3
acs is checking tags on instance FGT-B
  Tag.FGT_port1: eni-rj9f5xs9cp9xswekw6zh
  Tag.FGT_port2: eni-rj9j4eztztg3bv65yqd6x
  Tag.FGT_port3: eni-rj9gal6wcti7anp0ot7m
  Tag.FGT_port4: eni-rj9dirnvg0hykei8bl8o
acs is parsing page 1 of total 13(1 page) EIPs
acs local instance: FGT-B(i-rj9f5xs9cp9xsweedlcs)
  eni: 0, 10.0.1.12(eni-rj9f5xs9cp9xswekw6zh, port1)
  eni: 1, 10.0.2.12(eni-rj9j4eztztg3bv65yqd6x, port2)
  eni: 2, 10.0.3.12(eni-rj9gal6wcti7anp0ot7m, port3)
  eni: 3, 10.0.4.12(eni-rj9dirnvg0hykei8bl8o, port4) <--- eip(47.254.42.40)
acs peer instance: FGT-A(i-rj9illiuoh9t408ila60)
  eni: 0, 10.0.1.11(eni-rj9dirnvg0hykoddvv7z, port1) <--- eip(47.251.3.246)
  eni: 1, 10.0.2.11(eni-rj94jig06fag0vljneyv, port2)
  eni: 2, 10.0.3.11(eni-rj91wj13vwjs7y1n25ow, port3)
  eni: 3, 10.0.4.11(eni-rj9illiuoh9t3qd5doe3, port4) <--- eip(47.254.46.147)
acs is moving eip(47.251.3.246) from eni0(10.0.1.11) to eni0(10.0.1.12)
acs eip(47.251.3.246) status: Unassociating
acs eip(47.251.3.246) status: Unassociating
acs eip(47.251.3.246) status: Available
acs unassociated eip(47.251.3.246) from instance FGT-A successfully
acs eip(47.251.3.246) status: Associating
acs eip(47.251.3.246) status: Associating
acs eip(47.251.3.246) status: InUse
acs associated eip(47.251.3.246) to instance FGT-B successfully
acs local instance: FGT-B(i-rj9f5xs9cp9xsweedlcs)
  eni: 0, 10.0.1.12(eni-rj9f5xs9cp9xswekw6zh, port1) <--- eip(47.251.3.246)
  eni: 1, 10.0.2.12(eni-rj9j4eztztg3bv65yqd6x, port2)
  eni: 2, 10.0.3.12(eni-rj9gal6wcti7anp0ot7m, port3)
  eni: 3, 10.0.4.12(eni-rj9dirnvg0hykei8bl8o, port4) <--- eip(47.254.42.40)
acs peer instance: FGT-A(i-rj9illiuoh9t408ila60)
  eni: 0, 10.0.1.11(eni-rj9dirnvg0hykoddvv7z, port1)
  eni: 1, 10.0.2.11(eni-rj94jig06fag0vljneyv, port2)
```

```

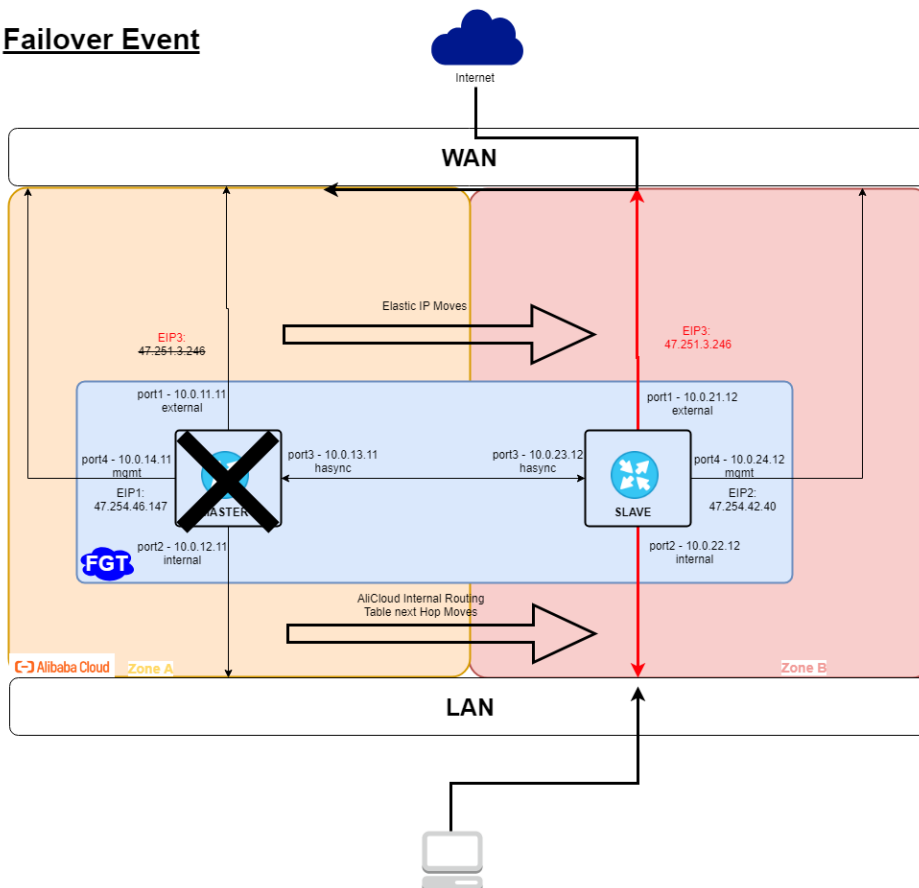
eni: 2, 10.0.3.11(eni-rj91wj13vwjs7y1n25ow, port3)
eni: 3, 10.0.4.11(eni-rj91lliuoh9t3qd5doe3, port4) <--- eip(47.254.46.147)
acs route table: vtb-rj9qltgufwqqe5ps3q60i
rule: cidr: 0.0.0.0/0, nexthop: 10.0.2.11(eni-rj94jig06fag0v1jneyv)
acs is deleting route table entry: 0.0.0.0/0 via 10.0.2.11
acs route table entry deleting
acs route table entry deleted
acs deleted route table entry: 0.0.0.0/0 via 10.0.2.11 successfully
acs is creating route table entry: 0.0.0.0/0 via 10.0.2.12
acs route table entry created
acs created route table entry: 0.0.0.0/0 via 10.0.2.12 successfully
acs route table: vtb-rj9qltgufwqqe5ps3q60i
rule: cidr: 0.0.0.0/0, nexthop: 10.0.2.12(eni-rj9j4eztztg3bv65yq6x)
===== exit acs ha failover =====
    
```

## Deploying FortiGate-VM HA on AliCloud between availability zones

This guide provides sample configuration of active-passive FortiGate-VM HA on AliCloud between availability zones (AZ)s:

The following depicts the network topology for this sample deployment:

### Failover Event



The following lists the IP address assignments for this sample deployment for FortiGate-A:

Port	AliCloud primary address	Subnet
port1	10.0.11.11	10.0.11.0/24 EIP3
port2	10.0.12.11	10.0.12.0/24
port3	10.0.13.11	10.0.13.0/24
port4	10.0.14.11	10.0.14.0/24 EIP1

The following lists the IP address assignments for this sample deployment for FortiGate-B:

Port	AliCloud primary address	Subnet
port1	10.0.21.12	10.0.21.0/24
port2	10.0.22.12	10.0.22.0/24
port3	10.0.23.12	10.0.23.0/24
port4	10.0.24.12	10.0.24.0/24 EIP2

#### To check the prerequisites:

The following prerequisites must be met for this deployment:

- One VPC with one subnet each for management, external, internal, and heartbeat purposes for each AZ
- Three public IP addresses:
  - EIP1 and EIP2 for FortiGate-A and FortiGate-B management
  - EIP3 for the HA external traffic IP address
- Two FortiGate-VM instances, both PAYG or BYOL
- The following summarizes minimum sufficient [RAM roles](#) for this deployment:
  - AliyunECSFullAccess
  - AliyunEIPFullAccess
  - AliyunVPCFullAccess



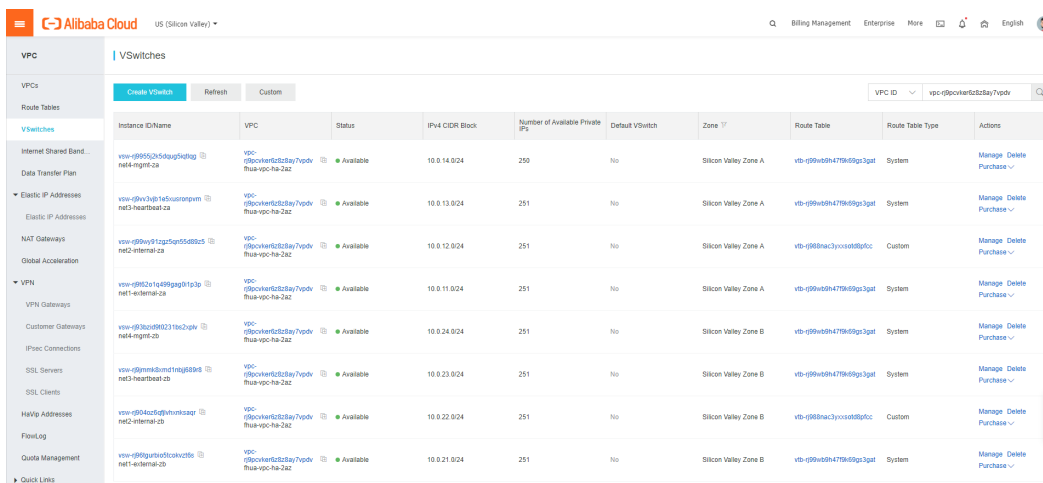
Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.



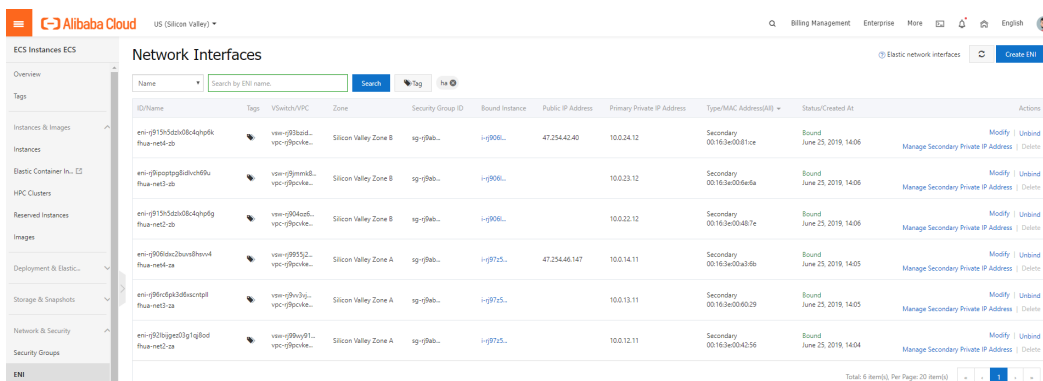
## To configure FortiGate-VM HA in AliCloud:

1. In the AliCloud management console, create a VPC with eight VSwitches (four for each AZ):

VSwitch	Purpose
net1-external-za	External data traffic on the public network-facing side.
net2-internal-za	Internal data traffic interface on the protected/trusted network-facing side.
net3-heartbeat-za	Heartbeat between two FortiGate nodes. This is unicast communication.
net4-mgmt-za	Dedicated management interface.
net1-external-zb	External data traffic on the public network-facing side.
net2-internal-zb	Internal data traffic interface on the protected/trusted network-facing side.
net3-heartbeat-zb	Heartbeat between two FortiGate nodes. This is unicast communication.
net4-mgmt-zb	Dedicated management interface.



2. Add six ENIs: three for each AZ:



3. Create two routing tables:

- a. Create a routing table called "rtb-internal" for the net2-internal VSwitch. Set the NIC2 secondary IP address (10.0.2.23) as rtb-internal's default gateway. You can create this routing table after configuring NIC2 on FortiGate-A. Ensure that the default gateway is FortiGate-A's port2 ENI.



ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(M)	Status/Created At	Actions
eni-g906id2b0u8l8p4 fha-net8-ca		vsw-g995j2... vpc-g9p0ck...	Silicon Valley Zone A	sg-g9f8b...	47.254.46.147	100.14.11	Secondary 00:16:3e:00a3:8b	Bound June 25, 2019, 14:05	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-g98id63d8dscpt8l fha-net3-ca		vsw-g9v3jg... vpc-g9p0ck...	Silicon Valley Zone A	sg-g9f8b...		100.13.11	Secondary 00:16:3e:0060:29	Bound June 25, 2019, 14:05	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-g93jgpe03j2jg9ed fha-net0-ca		vsw-g98uy91... vpc-g9p0ck...	Silicon Valley Zone A	sg-g9f8b...		100.12.11	Secondary 00:16:3e:0042:56	Bound June 25, 2019, 14:04	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-g9ku5e7jy9b1mdum3a		vsw-g98kz0... vpc-g9p0ck...	Silicon Valley Zone A	sg-g9f8b...	47.251.3.246	100.11.11	Primary 00:16:3e:0090:3c	Bound June 23, 2019, 12:10	Modify   Unbind Manage Secondary Private IP Address   Delete

ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(M)	Status/Created At	Actions
eni-g94j2zqy14y3ha fha-net4-ab		vsw-g96fg... vpc-g9p0ck...	Silicon Valley Zone B	sg-g9f8b...		100.21.12	Primary 00:16:3e:008c:ae	Bound June 25, 2019, 14:13	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-g913h5d5d08k4hp6k fha-net6-ab		vsw-g93zsd... vpc-g9p0ck...	Silicon Valley Zone B	sg-g9f8b...	47.254.42.40	100.24.13	Secondary 00:16:3e:0081:ce	Bound June 25, 2019, 14:06	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-g960cag8f8vch65u fha-net3-ab		vsw-g9fmm8... vpc-g9p0ck...	Silicon Valley Zone B	sg-g9f8b...		100.23.12	Secondary 00:16:3e:00e6:fa	Bound June 25, 2019, 14:06	Modify   Unbind Manage Secondary Private IP Address   Delete
eni-g913h5d5d08k4hp6g fha-net0-ab		vsw-g90kz0... vpc-g9p0ck...	Silicon Valley Zone B	sg-g9f8b...		100.22.12	Secondary 00:16:3e:0048:7e	Bound June 25, 2019, 14:06	Modify   Unbind Manage Secondary Private IP Address   Delete

## To configure FortiGate-A using the CLI:

The next steps show you how to configure A-P HA settings by using CLI commands on the GUI or via SSH. If using SSH, the FortiGate may lose connection due to routing table changes, so configuring HA via the GUI is recommended.

```

config system interface
  edit "port1"
    set mode static
    set ip 10.0.11.11 255.255.255.0
    set allowaccess ping https ssh snmp http fgfm
  next
  edit "port2"
    set ip 10.0.12.11 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
  edit "port3"
    set ip 10.0.13.11 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
  edit "port4"
    set ip 10.0.14.11 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
end

config router static
  edit 1
    set gateway 10.0.11.1
    set device "port1"
  next
end

config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"

```

```
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

config system ha
    set group-name "FGT-HA"
    set mode a-p
    set hbdev "port3" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.14.1
        next
    end
    set priority 192
    set unicast-hb enable
    set unicast-hb-peerip 10.0.23.12
end
```

### To configure FortiGate-B using the CLI:

The next steps show you how to configure A-P HA settings by using CLI commands on the GUI or via SSH. If using SSH, the FortiGate may lose connection due to routing table changes, so configuring HA via the GUI is recommended.

```
config system interface
    edit "port1"
        set mode static
        set ip 10.0.21.12 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
    next
    edit "port2"
        set ip 10.0.22.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port3"
        set ip 10.0.23.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.0.24.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config router static
    edit 1
        set gateway 10.0.21.1
        set device "port1"
    next
end
```

```

config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end

config system ha
  set group-name "FGT-HA"
  set mode a-p
  set hbdev "port3" 50
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
      set gateway 10.0.24.1
    next
  end
  set priority 64
  set unicast-hb enable
  set unicast-hb-peerip 10.0.13.21
end

```



You must set the FortiGate-B HA priority to a value lower than FortiGate-A's priority level. The node with the lower priority level is determined as the secondary node.

**To check the HA status and function:**

1. In FortiOS on the primary FortiGate, go to *System > HA*. Check that the HA status is synchronized.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
FortiGate VM64-ALIONDEMAND	192	FGT-A	FGTALIRNL7L40S9B	Master	00:00:37:36	11	29.00 kbps
FortiGate VM64-ALIONDEMAND	64	FGT-B	FGTALIAAFPJABDCE	Slave	00:00:37:46	12	24.00 kbps

2. Log into a PC that is located in the internal subnet. Verify that the PC can access the Internet via FortiGate-A when FortiGate-A is the primary node.
3. Shut down FortiGate-A. Verify that FortiGate-B becomes the primary node. Use an API call to verify that the secondary private IP address moves to FortiGate-B.
4. Log into the PC. Verify that the PC can access the Internet via FortiGate-B when FortiGate-B is the primary node.
5. You can use the `diagnose debug application alicloud-ha -1` command to see if the secondary private IP address moves from FortiGate-A to FortiGate-B during failover.

# Deploying auto scaling on AliCloud

You can deploy FortiGate-VM to support Auto Scaling on AliCloud.

Multiple FortiGate-VM instances can form an Auto Scaling group (ASG) to provide highly efficient clustering at times of high workloads. FortiGate-VM instances will be scaled out automatically according to predefined workload levels. Auto Scaling is achieved by using FortiGate-native high availability (HA) features such as `config-sync`, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events.

FortiGate Autoscale for AliCloud is available with FortiOS 6.2 and later versions for On-Demand (PAYG) instances. The standard deployment contains the following:

- A highly available architecture that spans two AZs
- A virtual private cloud (VPC) configured with public and private subnets
- A NAT gateway allowing egress traffic from the protected servers
- An external facing network load balancer is created as part of the deployment process. An internal facing network load balancer is optional.
- AliCloud Function Compute, which runs Fortinet-provided scripts for running Auto Scaling. Functions are used to handle Auto Scaling and failover management
- A TableStore (OTS) database which stores information on the Auto Scaling configurations such as the master or slave IP addresses

## Planning

The easiest way to deploy FortiGate Autoscale for AliCloud is with Terraform.

This deployment was tested using:

- Terraform 0.11
- Terraform provider for AliCloud 1.48.0

## Acronyms

The following acronyms are used throughout this document.

Acronym	Expansion
CIDR	Classless Inter-Domain Routing
DMZ	Demilitarized Zone
EIP	Elastic IP
ECS	Elastic Compute Service
ENI	Elastic Network Interface
ESS	Auto Scaling
FC	Function Compute
FGT	FortiGate
OSS	Object Storage Service
OTS	Open Table Service or TableStore, a NoSQL database by AliCloud
PAYG	Pay As You Go
RAM	Resource Access Management
SLB	Server Load Balancer

## Requirements

Installing and configuring FortiGate Autoscale for AliCloud requires knowledge of the following:

- Configuring a FortiGate using the CLI
- AliCloud services
- Terraform

It is expected that FortiGate Autoscale for AliCloud will be deployed by DevOps engineers or advanced system administrators who are familiar with the above.

## RAM account permissions

The solution can be deployed with an administrator account. As an administrator account has full permission to all resources under your AliCloud account, you may wish to create a separate RAM account with the following minimum required permissions:

- AliyunVPCFullAccess
- AliyunEIPFullAccess
- AliyunOSSFullAccess
- AliyunECSFullAccess
- AliyunSLBFullAccess
- AliyunOTSFullAccess
- AliyunESSFullAccess
- AliyunFCFullAccess
- AliyunRAMFullAccess
- AliyunBSSOrderAccess

## Region requirements

To deploy a FortiGate Auto Scaling cluster in AliCloud the region must support the following:

- TableStore
- OSS
- Function Compute
- Auto Scaling
- NAT Gateway

## Supported regions

The following regions contain all of the necessary services to run FortiGate Autoscale for AliCloud:

Acronym	Expansion
Asia Pacific NE 1 (Tokyo)	m-6weakry8j13jxmjlmi4o
Asia Pacific SE 2 (Sydney)	m-p0wb4dw13d6qc1sndaj6
Asia Pacific SOU 1 (Mumbai)	m-a2dbkrpr8wsobn9ygddc
EU Central 1 (Frankfurt)	m-gw8cizn7dguyeikpgozb
US East 1 (Virginia)	m-0xif6xxwhjlqhoaajrr6
US West 1 (Silicon Valley)	m-rj91iqplyxdp7crb0gvj



---

## Deployment information

Terraform will deploy the following resources:

- A VPC with two subnets split over two zones
- Two vswitches
- A NAT gateway
- An AutoScale cluster
- An AutoScale configuration
- Two AutoScale rules: Scale in and Scale out
- An OSS bucket
- A Function Compute service, function and HTTP trigger
- Two security groups: *Allow all*, and *Allow only internal connections*
- A TableStore instance and 5 tables
- Three Elastic IP addresses
- A RAM role with the ability to describe and create ENIs
- An external-facing server load balancer

## Deployment

1. Log into your AliCloud account. If you do not already have one, [create one](#) by following the instructions in the AliCloud article [Create a RAM user](#). The RAM account must have the minimum required permissions as listed in the section [RAM account permissions on page 64](#).
2. Create an AliCloud AccessKey. For details on creating one, refer to the AliCloud article [Create an AccessKey](#). This will create an AccessKeyID and an AccessKeySecret.
3. Install Terraform. For installation details, refer to the HashiCorp article [Installing Terraform](#).
4. Obtain the FortiGate Autoscale for AliCloud deployment package. Visit the [GitHub project release page](#) and download the `fortigate-autoscale-alicloud.zip` release for the version you want to use.
5. Unzip the file on your local PC. The following files and folders will be extracted:

```
├── alicloud_function_compute
├── alicloud_terraform
├── core
├── dist
├── LICENSE
├── node_modules
├── package.json
├── scripts
└── test
```

6. In your terminal, change to the `alicloud_terraform` folder:

```
cd alicloud_terraform
```

The `alicloud_terraform` folder contains the following files:

```
├── assets
│   └── configset
│       ├── baseconfig
│       ├── httproutingpolicy
│       ├── httpsroutingpolicy
│       ├── internalelbweb
│       └── storelogtofaz
├── main.tf
└── vars.tf
```

- `baseconfig` contains the `cloud-init` configuration for the FortiGate-VM and can be adjusted to support more advanced setups.
  - `main.tf` contains the majority of the deployment code. As part of the deployment it will upload the `baseconfig` to an OSS bucket to be used by the FortiGate-VM instances.
  - `vars.tf` contains the variables required for the deployment. For example: image ID (`instance_ami`), cluster name, instance, region, etc. For descriptions of the included variables, refer to the section [Terraform variables on page 67](#).
7. Edit the `vars.tf` file and customize variables for the deployment.



The OSS bucket name must be lowercase.

The Function Compute URL may not be more than 127 characters. The variable `cluster_name` is used to create this URL.

8. Initialize the providers and modules with the command `terraform init`:

```
terraform init
```

9. Submit the Terraform plan using the command below.

```
terraform plan -var "access_key=<access_key>" -var "secret_key=<secret_key>" -var "region=<region>"
```

10. Confirm and apply the plan:

```
terraform apply -var "access_key=<access_key>" -var "secret_key=<secret_key>" -var "region=<region>"
```

Output will be similar to below. A randomly generated three letter suffix is added to all resources and can be used to help identify your cluster resources.

```
Apply complete! Resources: 48 added, 0 changed, 0 destroyed.
```

```
Outputs:
```

```
Auto Scaling Group ID = asg-0x1lg2hk9z048yn6cuu1
AutoScale External Load Balancer IP = 47.89.136.18
PSK Secret = !_YfA7FQ0b_aYuei
Scale In Threshold = 35
Scale Out Threshold = 70
VPC name = FortigateAutoScale-rrr
```

## Terraform variables

Following are variables listed in the `vars.tf` file. They can be changed to suit the needs of your cluster.

Resource	Default	Description
<code>access_key</code>	Requires input	AliCloud AccessKey. For details on creating an AccessKey, refer to the AliCloud article <a href="#">Create an AccessKey</a> .
<code>secret_key</code>	Requires input	AliCloud Secret key created with the AccessKey. Used to access the API.
<code>region</code>	<code>us-east-1</code>	The AliCloud Region.
<code>scale_in_threshold</code>	35	Default aggregate CPU threshold (percentage) to scale in (remove) 1 instance.
<code>scale_out_threshold</code>	70	Default aggregate CPU threshold (percentage) to scale out (add) 1 instance.
<code>alicloud_account</code>	AliCloud account number	(datatype)
<code>cluster_name</code>	<code>FortigateAutoScale</code>	Name of the cluster to be used across objects.
<code>bucket_name</code>	<code>fortigateautoscale</code>	Name of the OSS bucket. Must be lowercase.
<code>instance_ami</code>	Requires input	If specified, this will be the image used by the build. Otherwise, the script will obtain the latest FortiGate AMI.

---

Resource	Default	Description
instance	ecs.sn1ne	The instance Family type to be used by the Auto Saling configuration.
vpc_cidr	172.16.0.0/16	VPC CIDR block, it is divided into two /21 subnets.
vswitch_cidr_1	172.16.0.0/21	First Vswitch located in zone A of the region.
vswitch_cidr_2	172.16.8.0/21	Second Vswitch located in zone B of the region.
table_store_ instance_type	Capacity	Accepted values are <i>HighPerformance</i> or <i>Capacity</i> .

Variables can also be referenced from the command line using:

```
terraform plan -var "<var name>=<value>"
```

## Verify the deployment

1. Log in to the AliCloud console and navigate to *TableStore*.
2. Navigate to the *FortiGateMasterElection* table.
3. Make note of the master FortiGate-VM IP address and ensure the *voteState* is *done*. See below for an example:

### FortiGateMasterElection

Table Data Insert Search Update Delete

Data Source: FortiGateMasterElection Table can display up to 50 rows.

Row Detail	asgName(Primary Key)	instanceId	ip	subnetId	voteEndTime	voteState	vpId
Row Detail	Master	i-0xi2pts0vr46rxhht3...	172.16.14.111	candidateInstance.su...	1.561416933046E12	done	candidateInstance.vi...

Total: 1 item(s), Per Page: 10 item(s) << < 1 > >>

4. Navigate to the *FortiGateAutoscale* table and confirm that instances that have been added to the cluster. Following is an example of a healthy cluster:

Table Data Insert Search Update Delete

Data Source: FortiGateAutoscale Table can display up to 50 rows.

Row Detail	instanceId(Primary K...	HeartBeatLossCount	MasterIp	NextHeartBeatTime	SyncState	autoScalingGroupName	heartBeatInterval
Row Detail	i-0xi2pts0vr46rxhht3...	0.0	172.16.14.111	1.561418453349E12	in-sync	FortigateAutoScale-g...	10.0
Row Detail	i-0xial3fyiqsf3tgbiz...	0.0	172.16.14.111	1.561418451745E12	in-sync	FortigateAutoScale-g...	10.0

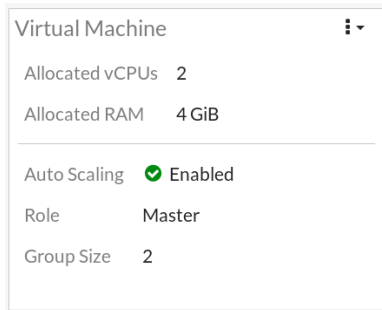
Total: 2 item(s), Per Page: 10 item(s) << < 1 > >>



The *MasterIp* column displays the IP address of the master FortiGate-VM.  
When an instance is removed from a cluster its record will not be erased from this table.

5. Log in to the master FortiGate-VM instance using the public IP address from step 3. The default admin port is *8443* and the default username/password will be *admin/<instance-id>*.

6. From the web interface you can tell the Instance role and current cluster size:



7. From the CLI type the following to get the role status and current *callback-url*:

```
get system auto-scale
```

Output will be similar to the following:

```
status          : enable
role            : master
sync-interface  : port1
callback-url    : https://*****.ap-southeast-5-internal.fc.aliyuncs.com/2016-08-15/proxy/FortigateAutoScale-smc/FortiGateASG-rrr/
hb-interval    : 10
psksecret      : *
```

## Destroying the cluster

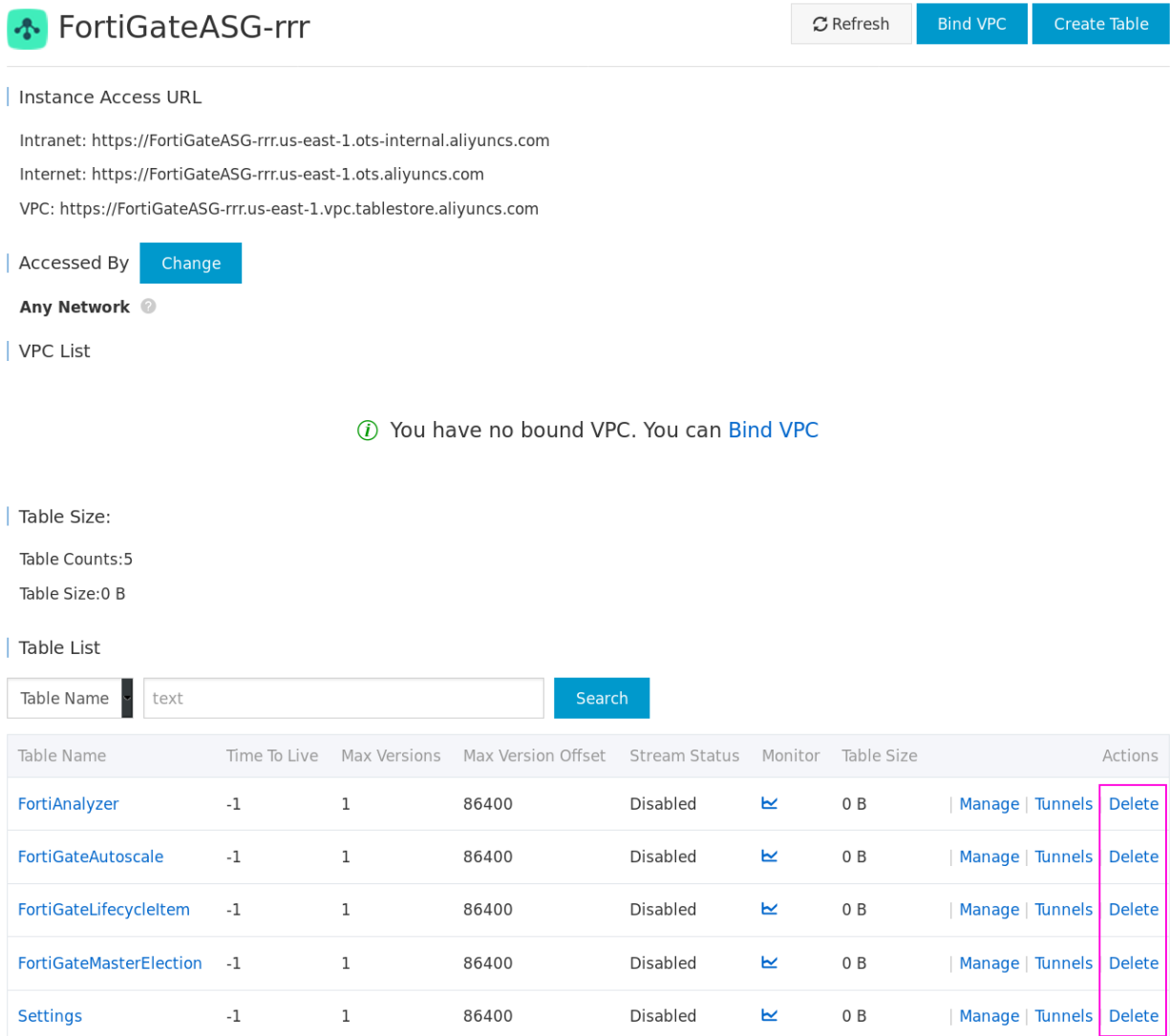
To destroy the cluster, first enter and verify:

```
terraform destroy -var "access_key=<access_key>" -var "secret_key=<secret_key>" -var "region-  
n=<region>"
```

There are restrictions on deleting tables when they have data. As such, TableStore must then be deleted manually from the console.

To remove TableStore:

1. Navigate to your Table and click *Delete* for each table:



The screenshot shows the console interface for 'FortiGateASG-rrr'. At the top right, there are buttons for 'Refresh', 'Bind VPC', and 'Create Table'. Below this, there are sections for 'Instance Access URL', 'Accessed By', 'Any Network', and 'VPC List'. A message states: 'You have no bound VPC. You can Bind VPC'. There is also a 'Table Size' section showing 'Table Counts:5' and 'Table Size:0 B'. At the bottom, there is a 'Table List' section with a search bar and a table of tables.

Table Name	Time To Live	Max Versions	Max Version Offset	Stream Status	Monitor	Table Size	Actions
FortiAnalyzer	-1	1	86400	Disabled		0 B	Manage   Tunnels   Delete
FortiGateAutoscale	-1	1	86400	Disabled		0 B	Manage   Tunnels   Delete
FortiGateLifecycleItem	-1	1	86400	Disabled		0 B	Manage   Tunnels   Delete
FortiGateMasterElection	-1	1	86400	Disabled		0 B	Manage   Tunnels   Delete
Settings	-1	1	86400	Disabled		0 B	Manage   Tunnels   Delete

2. After deleting the tables, return to the *Instance* page and click *Release*:

ⓘ This region supports high-performance instances and capacity instances.

Related Links: [Product Page](#)

Instance Name	Instance Type	Instance Description	Status	Created At	Monitor	Actions
FortiGateASG-rrr	Capacity	TableStore Instance Terraf...	Running	2019-06-20 12:45:51		<a href="#">Manage</a> <a href="#">Release</a>

## Troubleshooting

### Debugging cloud-init

Retrieving the `cloud-init` log can be useful when issues are occurring at boot up. To retrieve the log, log in to the FortiGate-VM and type the following into the CLI:

```
diag debug cloudinit show
```

Output will look similar to the following:

```
>> Checking metadata source ali
>> ALI user data obtained
>> Fos-instance-id: i-p0w3dr3bf9rck4jub4vb
>> Cloudinit trying to get config script from https://*****.ap-southeast-2-intern-
al.fc.aliyuncs.com/2016-08-15/proxy/FortigateAutoScale-wke/FortigateAutoScale-rrr/
>> Cloudinit download config script successfully
>> Found metadata source: ali
>> Run config script
>> Finish running script
>> FortiGate-VM64-ALI $ config system dns
>> FortiGate-VM64-ALI (dns) $      unset primary
>> FortiGate-VM64-ALI (dns) $      unset secondary
>> FortiGate-VM64-ALI (dns) $ end
>> FortiGate-VM64-ALI $ config system auto-scale
>> FortiGate-VM64-ALI (auto-scale) $      set status enable
>> FortiGate-VM64-ALI (auto-scale) $      set sync-interface port 1
>> FortiGate-VM64-ALI (auto-scale) $      set role master
>> FortiGate-VM64-ALI (auto-scale) $      set callback-url
https://*****.ap-southeast-2-internal.fc.aliyuncs.com/2016-08-15/proxy/Fortig-
ateAutoScale-wke/FortigateAutoScale-rrr/
```

### TableStore destroy time

TableStore deletion can take up to 10 minutes and may appear as follows:

```
alicloud_ots_instance.tablestore: Still destroying... (ID: FortiGateASG-rrr, 7m0s elapsed)
alicloud_ots_instance.tablestore: Still destroying... (ID: FortiGateASG-rrr, 7m10s elapsed)
alicloud_ots_instance.tablestore: Still destroying... (ID: FortiGateASG-rrr, 7m20s elapsed)
```



---

If you are seeing these messages after 10 minutes, it is likely that TableStore contains data. You will need to manually delete TableStore and then re-run the `terraform destroy` command. For details on manually deleting TableStore, refer to the section [Destroying the cluster on page 71](#).

## Resource availability

If a region runs out of a specified resource an error like the one below will be displayed. In this case the cluster will need to be deployed into a different region.

```
1 error occurred:
  * alicloud_slb.default: 1 error occurred:
  * alicloud_slb.default: [ERROR] terraform-provider-alicloud/alicloud/resource_alicloud_slb.go:324: Resource alicloud_slb CreateLoadBalancer Failed!!! [SDK alibaba-cloud-sdk-go ERROR]:
SDK.ServerError
ErrorCode: OperationFailed.ZoneResourceLimit
Recommend:
RequestId: 83972A94-0640-49DA-8586-DCF535D14886
Message: The operation failed because of resource limit of the specified zone.
```

## Timeout

If a timeout such as the one below occurs, re-run the command.

```
Error: Error applying plan:

1 error occurred:
  * alicloud_vswitch.vsw2: 1 error occurred:
  * alicloud_vswitch.vsw2: [ERROR] terraform-provider-alicloud/alicloud/resource_alicloud_vswitch.go:58:
[ERROR] terraform-provider-alicloud/alicloud/resource_alicloud_vswitch.go:170:
[ERROR] terraform-provider-alicloud/alicloud/service_alicloud_ecs.go:51: Resource us-east-1b DescribeZones Failed!!! [SDK alibaba-cloud-sdk-go ERROR]:
net/http: request canceled (Client.Timeout exceeded while reading body)
```

## How to reset the master election

To reset the master election, refer to the section [Verify the deployment on page 69](#) to locate the master record and delete the record. A new master FortiGate-VM will be elected and a new record will be created as a result.

# Appendix



## FortiGate Autoscale for AliCloud features

### Major components

- *The Auto Scaling group.* The Auto Scaling group contains one to many FortiGate-VMs (PAYG licensing model). This Auto Scaling group will dynamically scale-out or scale-in based on the scaling metrics specified in the scaling rules.
- The *configset* folder contains files that are loaded as the initial configuration for a new FortiGate-VM instance.
  - *baseconfig* is the base configuration. This file can be modified as needed to meet your network requirements. Placeholders such as {SYNC\_INTERFACE} are explained in the [Configset placeholders on page 74](#) table below.
- *Tables in TableStore.* These tables are required to store information such as health check monitoring, master election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.

### Configset placeholders

When the FortiGate-VM requests the configuration from the Auto Scaling function, the placeholders in the table below will be replaced with associated environment variables stored in Function Compute.

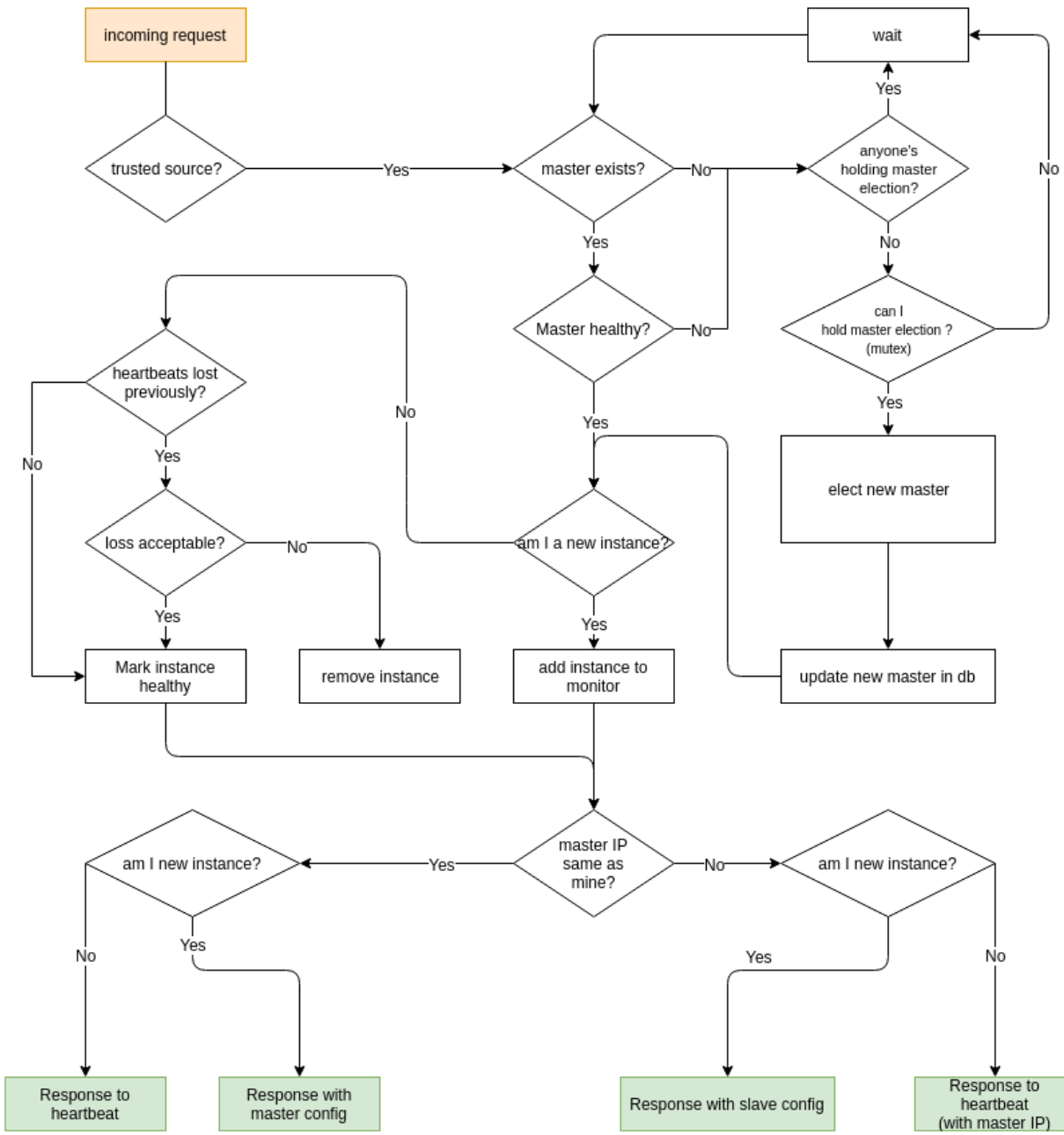
Placeholder	Type	Description
{SYNC_INTERFACE}	Text	The interface for FortiGate-VMs to synchronize information. All characters must be lowercase.
{CALLBACK_URL}	URL	The endpoint URL to interact with the Auto Scaling handler script. Automatically generated during the Terraform deployment.
{PSK_SECRET}	Text	The Pre-Shared key used in FortiOS. Randomly generated during the Terraform deployment.   Changes to the PSK secret after FortiGate Autoscale for AliCloud has been deployed are not reflected here. For new instances to be spawned with the changed PSK secret, this environment variable will need to be manually updated.
{ADMIN_PORT}	Number	A port number specified for administration login. A positive integer such as 443 etc. Default value: 8443.   Changes to the admin port after deployment are not reflected here. For new instances to be spawned with the changed admin port, this environment variable will need to be updated.

# Architectural diagram

## Master election

### FortiGate Autoscale

with heartbeat response & failover management



---

## Manual deployment of auto scaling on AliCloud

Following is a sample configuration for deploying Auto Scaling on AliCloud:

1. Create a scaling group in the AliCloud console.
2. Create a scaling configuration in the AliCloud console.
3. Create scaling rules in the AliCloud console.
4. Configure a FortiGate-VM in the Auto Scaling group as the primary member.
5. Scale out a new FortiGate-VM, configure it as a secondary member, and synchronize the configuration from the primary to the secondary FortiGate-VM.
6. Run diagnose commands to confirm that Auto Scaling is functioning.

### To create a scaling group in the AliCloud console:

1. Log into the AliCloud console.
2. Go to *Auto Scaling > Scaling Groups > Create Scaling Group*.
3. Set the following parameters for the Auto Scaling group:
  - a. *Scaling Group Name*: Enter a name for the scaling group. The sample configuration is named *FGT-ASG*.
  - b. *Maximum Instances*: Enter the maximum number of instances that can comprise the group. In the sample configuration, four (4) is the maximum number.
  - c. *Minimum Instances*: Enter the minimum number of instances that can comprise the group. In the sample configuration, one (1) is the minimum number.
  - d. *Instance Configuration Source*: Leave at the default value.
  - e. *Network Type*: Leave at the default value, which is VPC.
  - f. Select the VPC and VSwitch as desired.

Create Scaling Group
✕

**\*Scaling Group Name:**

The name can be 2 to 40 characters in length. It must start with a letter, number or Chinese character. It can also contain periods (.), underscores (\_), and hyphens (-).

**\*Maximum Instances:**

Valid range: 0 to 1000

**\*Minimum Instances:**

Valid range: 0 to 1000

**\*Default Cooldown Time (Seconds):**

The value must be an integer no less than 0.

**Removal Policy:** First Pick  Then Pick  To Remove

[How can I ensure that a manually added ECS instance will not be removed from the scaling group?](#)

**\* Instance Configuration Source:**  Custom Scaling Configuration  Launch Template

**\* Network Type:**  VPC  VPC A scaling group can support multiple VSwitches.

**\* VPC:** VPC ID:  [Create VPC network](#)

VSwitch:

**Multi-Zone Scaling Policy:**  Priority  Distribution Balancing  Cost Optimization

**Reclaim Mode:**  Release Mode  Shutdown and Reclaim Mode

**SLB Instances:**  [Manage SLB instances](#)

Only SLB instances that have been configured with listeners can be used by scaling groups.

**RDS Instances:**  [Manage RDS databases](#)

Databases in the scaling group: configured=0, maximum=10

4. Click **OK**.

**To create a scaling configuration in the AliCloud console:**

1. After creating an Auto Scaling group, AliCloud displays a popup for creating a new scaling configuration before activating Auto Scaling. In the popup, click *Create Now*.
2. Select the instance type.
3. Select the desired FortiGate-VM image.
4. Ensure that *Assign Public IP* is selected.
5. Select the desired security group.

## 6. Click Next: System Configurations.

Auto Scaling | Scaling Group Name: FGT-ASG

1 Basic Configurations (Required) | 2 System Configurations | 3 Preview (Required)

**Billing Method**:  Pay-As-You-Go  Preemptible Instance

**Instance Type**

Filter Instances:

Architecture:  x86-Architecture  Heterogeneous Computing  ECS Bare Metal Instance  Super Computing Cluster

Category:  General Purpose  Compute Optimized  Memory Optimized  Big Data  Local SSD  Storage Enhancement  High Clock Speed  Entry-Level (Shared)

Family	Instance Type	vCPU	Memory	Physical Processor	Clock Speed	Internal Network Bandwidth	Packets Rate
<input checked="" type="radio"/> Network Enhanced sn2ne	ecs.sn2ne.large	2 vCPU	8 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1 Gbps	300,000 PPS
<input type="radio"/> Network Enhanced sn2ne	ecs.sn2ne.xlarge	4 vCPU	16 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1.5 Gbps	500,000 PPS
<input type="radio"/> Network Enhanced sn2ne	ecs.sn2ne.2xlarge	8 vCPU	32 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	2 Gbps	1,000,000 PPS
<input type="radio"/> Network Enhanced sn2ne	ecs.sn2ne.3xlarge	12 vCPU	48 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	2.5 Gbps	1,300,000 PPS
<input type="radio"/> Compute Optimized Type sn2	ecs.sn2.medium	2 vCPU	8 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps	100,000 PPS
<input type="radio"/> Compute Optimized Type sn2	ecs.sn2.large	4 vCPU	16 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.8 Gbps	200,000 PPS

Bandwidth: 5Mbps Pay-By-Traffic | Total: \$0.124 USD per Hour + Public traffic fee: \$0.077 USD per GB

**Next: System Configurations** | Preview

## 7. (Optional) set the key pair.

Auto Scaling | Scaling Group Name: FGT-ASG

1 Basic Configurations (Required) | 2 System Configurations | 3 Preview (Required)

**Tags**

Tags are sorted by upper and lowercase key values. For example, you can add a tag with the key as "Name" and the value "Webserver". Tag keys must be unique and cannot exceed 64 characters. Tag values can be blank and cannot exceed 128 characters. Tag key and tag value cannot include "Alibaba cloud" or start with "https://" or "http://". You can create up to 20 tags, these tags will be applied to all the instances and disks created.

Log on Credentials:  Key Pair  Inherit Password From Image  Set Later

Key Pair:  [Refer to | Create Key Pair](#)

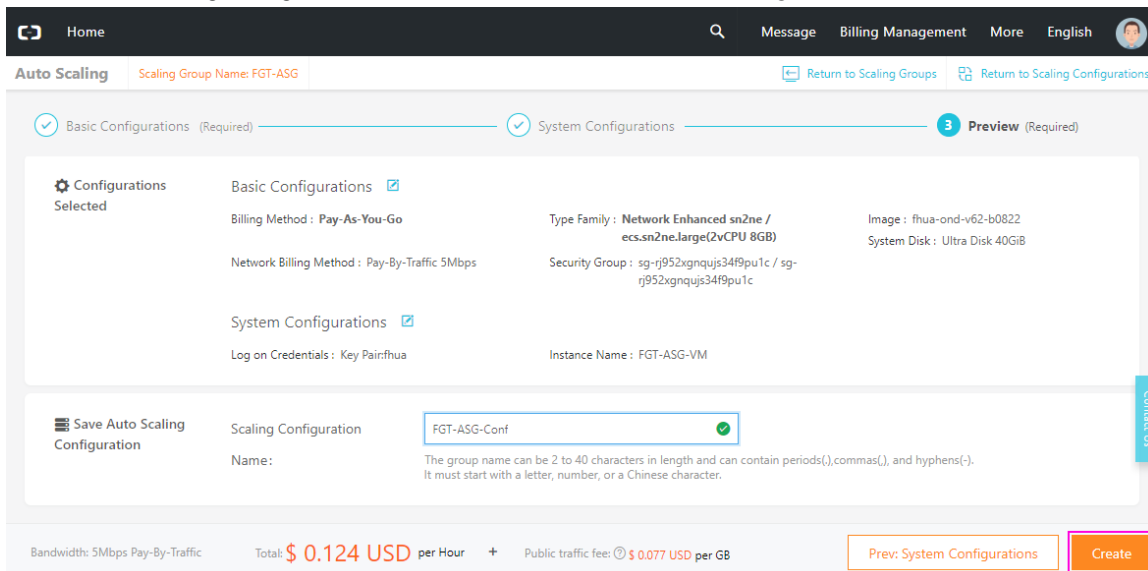
Instance Name:   The name can be 2 to 128 characters in length and can contain letters, Chinese characters, numbers, hyphens (-), underscores (\_), and periods (.). It must start with a letter or Chinese character.

> Advanced (based on instance RAM roles or cloud-init)

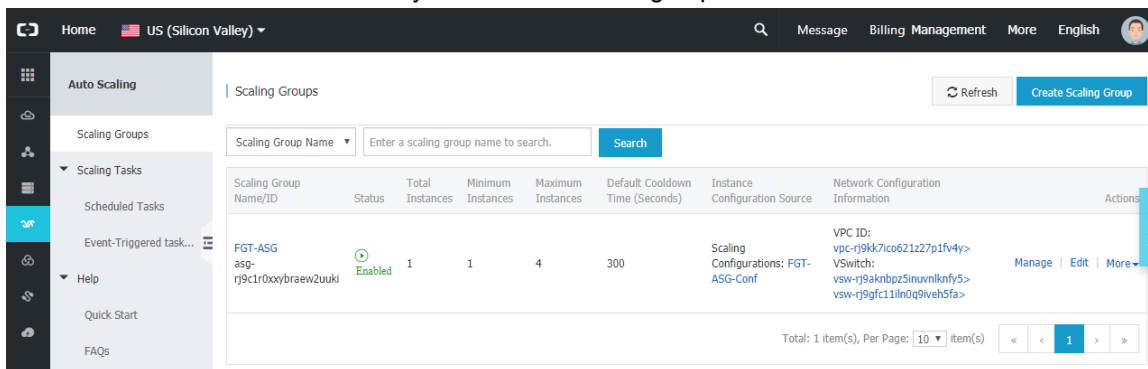
Bandwidth: 5Mbps Pay-By-Traffic | Total: \$0.124 USD per Hour + Public traffic fee: \$0.077 USD per GB

Prev: Basic Configurations | **Next: Preview** | Preview

8. Preview the scaling configuration, then click *Create* and *Enable Configuration*.



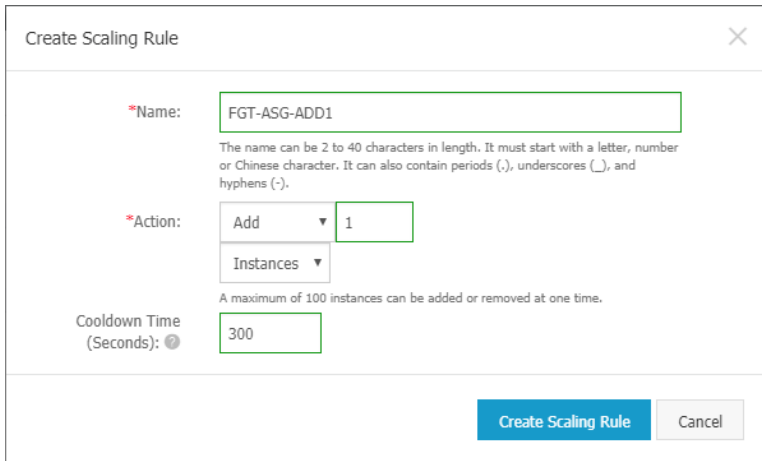
9. Go to *Auto Scaling > Scaling Groups* to ensure that AliCloud has created the Auto Scaling group and that the first FortiGate-VM has been automatically launched under the group.



**To create scaling rules in the AliCloud console:**

1. In *Auto Scaling > Scaling Groups*, click the group name.
2. Click *Scaling Rules* from the right-side menu.
3. In the *Create Scaling Rule* dialog, enter a scaling rule name.
4. Configure an action. In the sample configuration, the scaling rule is configured to add one (1) FortiGate-VM instance.
5. Enter a cool down time, then click *Create Scaling Rule*. You could also configure another scaling rule which can be

executed to remove one (1) FortiGate-VM instance.



### To configure a FortiGate-VM in the Auto Scaling group as the primary member:

1. Log into the FortiGate-VM.
2. Run the following commands in the CLI to enable Auto Scaling and configure this FortiGate-VM as the primary member of the Auto Scaling group:

```
config system auto-scale
  set status enable
  set role master
  set sync-interface "port1"
  set psksecret xxxxxx
end
```

### To scale out a new FortiGate-VM, configure it as a secondary member, and synchronize the configuration:

1. In *Auto Scaling > Scaling Groups*, click the group name, then execute the scaling rule created earlier. AliCloud creates a new FortiGate-VM instance.
2. Log into the new FortiGate-VM.
3. Run the following commands in the CLI to enable Auto Scaling and configure this FortiGate-VM as the secondary member of the Auto Scaling group. The `master-ip` value should be the primary FortiGate-VM's private IP address:

```
config system auto-scale
  set status enable
  set role slave
  set sync-interface "port1"
  set master-ip 192.168.1.204
  set psksecret xxxxxx
end
```

The secondary FortiGate-VM will be synced with the primary FortiGate-VM. The secondary FortiGate-VM can receive configurations from the primary FortiGate-VM.

### To run diagnose commands:

You can run the following `diagnose` commands to determine if the primary and secondary FortiGate-VMs are able to synchronize configurations:

```
FortiGate-VM64-ALION~AND # diag deb app hasync -1
slave's configuration is not in sync with master's, sequence:0
```



---

```
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
logout all admin users
```

# Security Fabric connector integration with AliCloud

## Configuring AliCloud Fabric connector using RAM roles

See the [FortiOS Cookbook](#) for information on the AliCloud Fabric connector.

The following summarizes minimum sufficient [RAM roles](#) for Fabric connector integration with AliCloud:

- [AliyunECSReadOnlyAccess](#)
- [AliyunEIPReadOnlyAccess](#)
- [AliyunVPCReadOnlyAccess](#)



Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

---

## Pipelined automation using AliCloud Function Compute

See [GitHub](#).

# VPN for FortiGate-VM on AliCloud

## Connecting a local FortiGate to an AliCloud VPC VPN

This recipe provides sample configuration of a site-to-site VPN connection from a local FortiGate to an AliCloud VPC VPN via IPsec with static routing.

Instances that you launch into an AliCloud VPC can communicate with your own remote network via a site-to-site VPN between your on-premise FortiGate-And AliCloud VPC VPN. You can enable access to your remote network from your VPC by configuring a VPN gateway and customer gateway to the VPC, then configuring the site-to-site VPC VPN.

The following prerequisites must be met for this configuration:

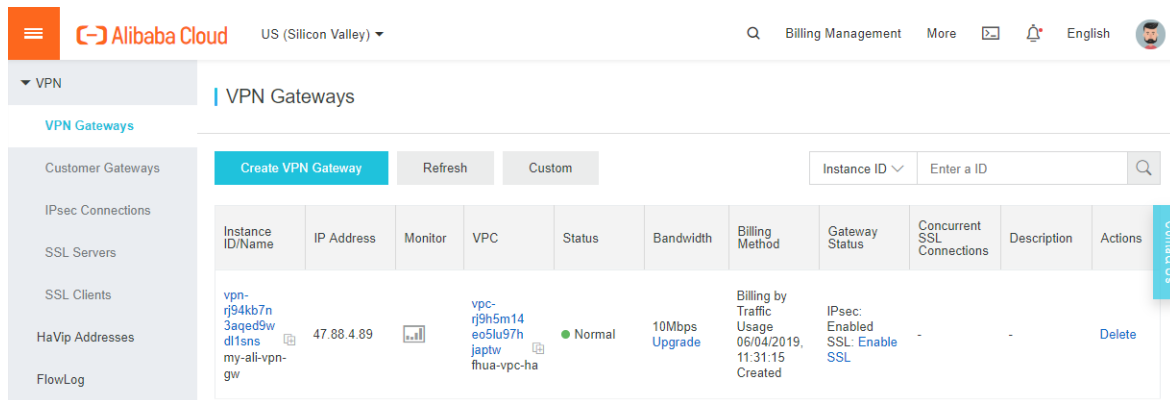
- An AliCloud VPC with some configured subnets, routing tables, security group rules, and so on
- An on-premise FortiGate with an external IP address

This recipe consists of the following steps:

1. [Create a VPN gateway.](#)
2. [Create a customer gateway.](#)
3. [Create a site-to-site VPN connection on AliCloud.](#)
4. [Configure the on-premise FortiGate.](#)
5. [Run diagnose commands.](#)

### To create a VPN gateway:

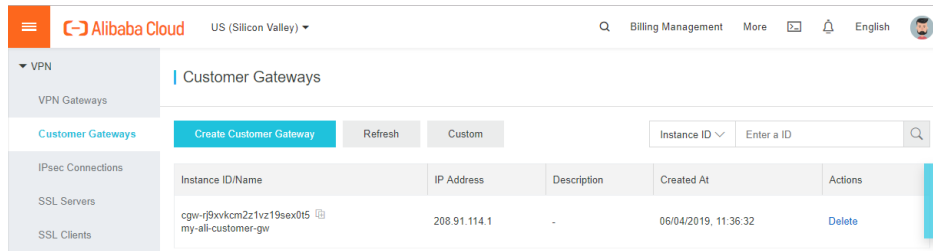
1. In the AliCloud management console, go to *VPN > VPN Gateways*.
2. Click *Create VPN Gateway*.
3. Create a virtual private gateway and attach it to the VPC from which you want to create the site-to-site VPN connection.



### To create a customer gateway:

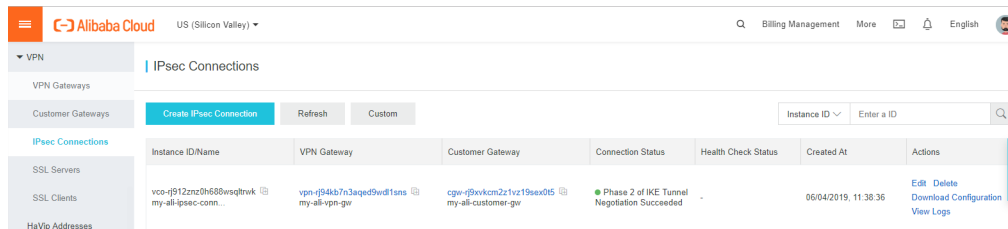
This example refers to the on-premise FortiGate for the VPC VPN to connect to as the customer gateway.

1. Go to *VPN > Customer Gateways*.
2. Click *Create Customer Gateway*.
3. Configure the customer gateway as shown:



**To create a site-to-site VPN connection on AliCloud:**

1. Go to *VPN > IPsec Connections*.
2. Click *Create IPsec Connection*.
3. Create an IPsec connection between the VPN and customer gateways.
4. Under *Actions*, click *Download Configuration*.



5. Note the IPsec-related parameters. You will use these parameters to configure the on-premise FortiGate in the next step:

```
{
  "LocalSubnet": "0.0.0.0/0",
  "RemoteSubnet": "0.0.0.0/0",
  "IpsecConfig": {
    "IpsecPfs": "group2",
    "IpsecEncAlg": "aes",
    "IpsecAuthAlg": "sha1",
    "IpsecLifetime": 86400
  },
  "Local": "x.x.x.x",
  "Remote": "47.88.4.89",
  "IkeConfig": {
    "IkeAuthAlg": "sha1",
    "LocalId": "x.x.x.x",
    "IkeEncAlg": "aes",
    "IkeVersion": "ikev1",
    "IkeMode": "main",
    "IkeLifetime": 86400,
    "RemoteId": "47.88.4.89",
    "Psk": "xxxxxxxxxxxxxxxxxxxx",
    "IkePfs": "group2"
  }
}
```

```

}
}

```

### To configure the on-premise FortiGate:

1. In the FortiOS CLI, configure the on-premise FortiGate with the above IPsec-related parameters. When setting `remote-gw` and `psksecret`, use the values found for `RemoteId` and `Psk` above, respectively. The example on-premise FortiGate uses `port9` as its external interface:

```

config vpn ipsec phase1-interface
  edit "AliCloudVPN"
    set interface "port9"
    set keylife 86400
    set peertype any
    set net-device enable
    set proposal aes128-sha1
    set dhgrp 14 2
    set remote-gw 47.88.4.89
    set psksecret xxxxxxxxxxxxxxxxxxxx
  next
end
config vpn ipsec phase2-interface
  edit "AliCloudVPN"
    set phase1name "AliCloudVPN"
    set proposal aes128-sha1
    set dhgrp 14 2
    set keepalive enable
    set keylifeseconds 3600
  next
end
config firewall address
  edit "AliCloudVPN-local-subnet-1"
    set allow-routing enable
    set subnet 10.6.30.0 255.255.255.0
  next
end
config firewall address
  edit "AliCloudVPN-remote-subnet-1"
    set allow-routing enable
    set subnet 10.0.1.0 255.255.255.0
  next
end
config router static
  edit 2
    set device "AliCloudVPN"
    set dstaddr "AliCloudVPN-remote-subnet-1"
  next
end
config firewall policy
  edit 10

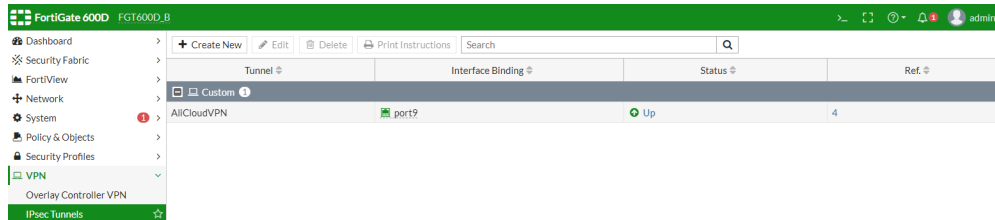
```

```

set name "AliCloudVPN-local-ali"
set srcintf "mgmt1"
set dstintf "AliCloudVPN"
set srcaddr "AliCloudVPN-local-subnet-1"
set dstaddr "AliCloudVPN-remote-subnet-1"
set action accept
set schedule "always"
set service "ALL"
next
edit 20
set name "AliCloudVPN-ali-local"
set srcintf "AliCloudVPN"
set dstintf "mgmt1"
set srcaddr "AliCloudVPN-remote-subnet-1"
set dstaddr "AliCloudVPN-local-subnet-1"
set action accept
set schedule "always"
set service "ALL"
next
end

```

- If the IPsec tunnel does not appear automatically, run the `diagnose vpn tunnel up AliCloudVPN` command.
- In the FortiOS GUI, go to *VPN > IPsec Tunnels*. Verify that the tunnel is up. The on-premise FortiGate can now access the AliCloud VM with its private IP address. The AliCloud VM can also access the on-premise FortiGate with its private IP address.



### To run diagnose commands:

```

FGT600D_B # diagnose vpn ike gateway list

vd: root/0
name: AliCloudVPN
version: 1
interface: port9 10
addr: 172.16.200.212:4500 -> 47.88.4.89:4500
created: 1087s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 9110/9110/9110 ms
IPsec SA: created 1/2 established 1/1 time 30/30/30 ms

id/spi: 0 d9d4ae9111a51b0b/de39f4ac9deffc18
direction: initiator
status: established 1087-1078s ago = 9110ms
proposal: aes128-shal
key: 9bf9b58431949e77-a0c21ded48368db1

```

```

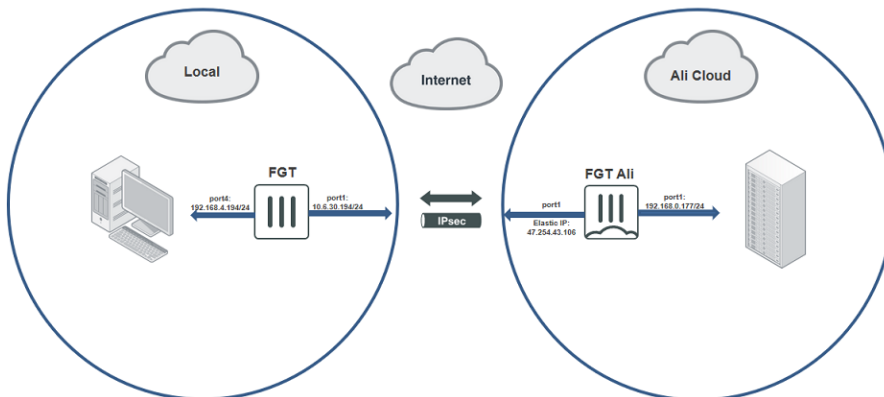
lifetime/rekey: 28800/27421
DPD sent/recv: 00000000/00000000

FGT600D_B # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=AliCloudVPN ver=1 serial=1 172.16.200.212:4500->47.88.4.89:4500 dst_mtu=1500
bound_if=10 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_dev
frag-rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=14 ilast=1084 olast=270 ad=/0
stat: rxp=1 txp=43 rxb=16452 txb=4389
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=AliCloudVPN proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=6 options=10227 type=00 soft=0 mtu=1422 expire=2399/0B replaywin=2048
      seqno=2c esn=0 replaywin_lastseq=00000001 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=3298/3600
  dec: spi=ac5426a9 esp=aes key=16 417b83810bf1f17b30e8b0974716d37d
      ah=sha1 key=20 a3e1d5ca5d85907a35c7720e9c640d0fafbb0ee3
  enc: spi=c999e156 esp=aes key=16 837b20f727c957f700f6c89acbb9e9a9
      ah=sha1 key=20 7f4634601d6962575c00761f7270d36a683c3d65
  dec:pkts/bytes=1/16376, enc:pkts/bytes=43/7648
  npu_flag=03 npu_rgwty=47.88.4.89 npu_lgwy=172.16.200.212 npu_selid=0 dec_npuid=1 enc_npuid=1
    
```

## Connecting a local FortiGate to an AliCloud FortiGate via site-to-site VPN

This guide provides sample configuration of a site-to-site VPN connection from a local FortiGate to an AliCloud FortiGate via site-to-site IPsec VPN with static routing. The following depicts the network topology for this sample deployment:



The following prerequisites must be met for this configuration:

- A FortiGate located on AliCloud with port1 connected to local LAN and a public IP address mapped to port1.
- A local FortiGate in a local environment. Determine if your FortiGate has a publicly accessible IP address or if it is behind NAT. In this example, the on-premise FortiGate is behind NAT.

This recipe consists of the following steps:

1. [Configure the local FortiGate.](#)
2. [Configure the AliCloud FortiGate.](#)
3. [Establish a VPN connection between the local and AliCloud FortiGates.](#)
4. [Run diagnose commands.](#)

## Configuring the local FortiGate

**To configure the local FortiGate using the GUI:**

1. Configure the interfaces:
  - a. In FortiOS, go to *Network > Interfaces*.
  - b. Edit port1. From the *Role* dropdown list, select *WAN*. In the *IP/Network Mask* field, enter 10.6.30.194/255.255.255.0 for the interface that is connected to the Internet.
  - c. Edit port4. From the *Role* dropdown list, select *LAN*. In the *IP/Network Mask* field, enter 192.168.4.194/255.255.255.0 for the interface that is connected to the local subnet.
2. Configure a static route to connect to the Internet:
  - a. Go to *Network > Static Routes*.
  - b. Click *Create New*.
  - c. In the *Destination* field, enter 0.0.0.0/0.0.0.0.
  - d. From the *Interface* dropdown list, select *port1*.
  - e. In the *Gateway Address* field, enter 10.6.30.254.
3. Configure IPsec VPN:
  - a. Go to *VPN > IPsec Wizard*.
  - b. Configure *VPN Setup*:
    - i. In the *Name* field, enter the desired name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *This site is behind NAT*. Click *Next*. For non-dialup situations where the local FortiGate has an external IP address, select *No NAT between sites*.
  - c. Configure *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. In the *IP Address* field, enter 47.254.43.106. This is the AliCloud FortiGate port1 public IP address.
    - iii. From the *Outgoing Interface* dropdown list, select *port1*.
    - iv. For *Authentication Method*, select *Pre-shared Key*.
    - v. In the *Pre-shared Key* field, enter 123456. Click *Next*.
  - d. Configure *Policy & Routing*:
    - i. From the *Local Interface* dropdown list, select *port4*. This autofills the *Local Subnets* field with 192.168.4.0/24.



- ii. In the *Remote Subnets* field, enter 192.168.4.0/24. This is the AliCloud FortiGate port1 subnet.
- iii. For *Internet Access*, select *None*. Click *Create*.

### To configure the local FortiGate using the CLI:

#### 1. Configure the interfaces:

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.6.30.194 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set type physical
    set role wan
    set snmp-index 1
  next
  edit "port4"
    set vdom "root"
    set ip 192.168.4.194 255.255.255.0
    set allowaccess ping https ssh snmp fgfm ftm
    set type physical
    set device-identification enable
    set lldp-transmission enable
    set role lan
    set snmp-index 4
  next
end
```

#### 2. Configure a static route to connect to the Internet:

```
config router static
  edit 1
    set gateway 10.6.30.254
    set device "port1"
  next
end
```

#### 3. Configure IPsec VPN:

```
config vpn ipsec phase1-interface
  edit "to_ali"
    set interface "port1"
    set peertype any
    set net-device enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set comments "VPN: to_ali (Created by VPN wizard)"
    set wizard-type static-fortigate
    set remote-gw 47.254.43.106
    set psksecret xxxxxx
  next
end
```

```
config vpn ipsec phase2-interface
  edit "to_ali"
    set phase1name "to_ali"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
    set comments "VPN: to_ali (Created by VPN wizard)"
    set src-addr-type name
    set dst-addr-type name
    set src-name "to_ali_local"
    set dst-name "to_ali_remote"
  next
end
config router static
  edit 2
    set device "to_ali"
    set comment "VPN: to_ali (Created by VPN wizard)"
    set dstaddr "to_ali_remote"
  next
  edit 3
    set distance 254
    set comment "VPN: to_ali (Created by VPN wizard)"
    set blackhole enable
    set dstaddr "to_ali_remote"
  next
end
config firewall policy
  edit 1
    set name "vpn_to_ali_local"
    set uuid c6b2d36e-6c65-51e9-5a78-9a0881a0b07c
    set srcintf "port4"
    set dstintf "to_ali"
    set srcaddr "to_ali_local"
    set dstaddr "to_ali_remote"
    set action accept
    set schedule "always"
    set service "ALL"
    set comments "VPN: to_ali (Created by VPN wizard)"
  next
  edit 2
    set name "vpn_to_ali_remote"
    set uuid c6bf126e-6c65-51e9-8652-cb88546929b4
    set srcintf "to_ali"
    set dstintf "port4"
    set srcaddr "to_ali_remote"
    set dstaddr "to_ali_local"
    set action accept
    set schedule "always"
    set service "ALL"
```

```
        set comments "VPN: to_ali (Created by VPN wizard)"
    next
end
```

## Configuring the AliCloud FortiGate

### To configure the AliCloud FortiGate using the GUI:

1. Configure the interface:
  - a. In FortiOS, go to *Network > Interfaces*.
  - b. Edit port1.
  - c. From the *Role* dropdown list, select *LAN*.
  - d. Ensure that *Addressing mode* is set to *DHCP* and that the FortiGate can list the assigned IP address.
2. Configure IPsec VPN:
  - a. Go to *VPN > IPsec Wizard*.
  - b. Configure *VPN Setup*:
    - i. In the *Name* field, enter the desired name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *The remote site is behind NAT*. Click *Next*.
  - c. Configure *Authentication*:
    - i. From the *Incoming Interface* dropdown list, select *port1*.
    - ii. For *Authentication Method*, select *Pre-shared Key*.
    - iii. In the *Pre-shared Key* field, enter 123456. Click *Next*.
  - d. Configure *Policy & Routing*:
    - i. From the *Local Interface* dropdown list, select *port1*. This autofills the *Local Subnets* field with 192.168.4.0/24.
    - ii. In the *Remote Subnets* field, enter 192.168.4.0/24. This is the local FortiGate port4 subnet.
    - iii. For *Internet Access*, select *None*. Click *Create*.

### To configure the AliCloud FortiGate using the CLI:

1. Configure the interface and ensure that the FortiGate can list the assigned IP address:

```
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh fgfm
        set type physical
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 1
    next
```

```

end

diagnose ip address list
IP=192.168.0.177->192.168.0.177/255.255.255.0 index=3 devname=port1

```

## 2. Configure IPsec VPN:

```

config vpn ipsec phase1-interface
  edit "to_local"
    set type dynamic
    set interface "port1"
    set peertype any
    set net-device enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set dpd on-idle
    set comments "VPN: to_local (Created by VPN wizard)"
    set wizard-type dialup-fortigate
    set psksecret xxxxxx
    set dpd-retryinterval 60
  next
end
config vpn ipsec phase2-interface
  edit "to_local"
    set phase1name "to_local"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
    set comments "VPN: to_local (Created by VPN wizard)"
    set src-addr-type name
    set dst-addr-type name
    set src-name "to_local_local"
    set dst-name "to_local_remote"
  next
end
config firewall policy
  edit 1
    set name "vpn_to_local_local"
    set uuid e07aaa72-833c-51e9-ad33-4c1e96b656da
    set srcintf "port1"
    set dstintf "to_local"
    set srcaddr "to_local_local"
    set dstaddr "to_local_remote"
    set action accept
    set schedule "always"
    set service "ALL"
    set comments "VPN: to_local (Created by VPN wizard)"
  next
  edit 2
    set name "vpn_to_local_remote"
    set uuid e086b2b8-833c-51e9-3aaf-49e3cd4c5c70
    set srcintf "to_local"

```

```

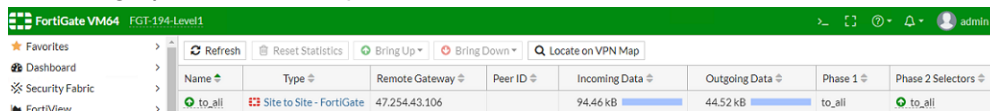
set dstintf "port1"
set srcaddr "to_local_remote"
set dstaddr "to_local_local"
set action accept
set schedule "always"
set service "ALL"
set comments "VPN: to_local (Created by VPN wizard)"
next
end

```

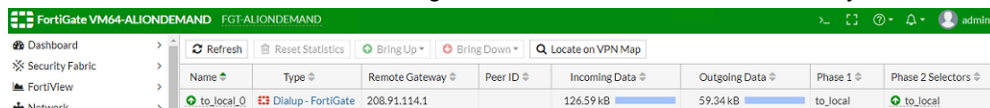
### To establish the VPN connection between the FortiGates:

The tunnel is down until you initiate connection from the local FortiGate.

1. In FortiOS on the local FortiGate, go to *Monitor > IPsec Monitor*.
2. Click the created tunnel.
3. Click *Bring Up*. The tunnel is up.



4. In FortiOS on the AliCloud FortiGate, go to *Monitor > IPsec Monitor* to verify that the tunnel is up.



### To run diagnose commands:

1. Show the local FortiGate VPN status:

```

FGT-194-Level1 # diagnose vpn ike gateway list
vd: root/0
name: to_all
version: 1
interface: port1 3
addr: 10.6.30.194:4500 -> 47.254.43.106:4500
created: 4057s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 21180/21180/21180 ms
IPsec SA: created 1/3 established 1/3 time 20/26/30 ms
  id/spi: 2 fd018d163ea303aa/9d7a245f889ee6c4
  direction: initiator
  status: established 4057-4036s ago = 21180ms
  proposal: aes128-sha256
  key: c7bab4dd8883b727-3b249220088216f8
  lifetime/rekey: 86400/82063
  DPD sent/recv: 00000000/00000009
FGT-194-Level1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----

```

```

name=to_ali ver=1 serial=1 10.6.30.194:4500->47.254.43.106:4500 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options
[0210]=create_dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=14 ilast=0 olast=0 ad=/0
stat: rxp=3382 txp=3404 rxb=432896 txb=204240
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=to_ali proto=0 sa=1 ref=2 serial=3
  src: 0:192.168.4.0/255.255.255.0:0
  dst: 0:192.168.0.0/255.255.255.0:0
  SA: ref=3 options=10226 type=00 soft=0 mtu=1422 expire=39471/0B
replaywin=2048
  seqno=d14 esn=0 replaywin_lastseq=00000d0d itn=0 qat=0
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=8427ce41 esp=aes key=16 961323608ef02c111ce4cc393cd79293
    ah=sha1 key=20 9cffabaa0163df6a92e1917efa333148b58ff9da
  enc: spi=e2723047 esp=aes key=16 f93b233906039c179924923a4f09ebae
    ah=sha1 key=20 c2c6225e26927de6381bf44c6ccd6d0a325e2e27
  dec:pkts/bytes=3325/199500, enc:pkts/bytes=3347/428416

```

## 2. Show the AliCloud FortiGate VPN status:

```

FGT-ALIONDEMAND # diagnose vpn ike gateway list
vd: root/0
name: to_local_0
version: 1
interface: port1 3
addr: 192.168.0.177:4500 -> 208.91.114.1:64916
created: 4103s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 120/120/120 ms
IPsec SA: created 1/3 established 1/3 time 20/26/30 ms
  id/spi: 0 fd018d163ea303aa/9d7a245f889ee6c4
  direction: responder
  status: established 4103-4103s ago = 120ms
  proposal: aes128-sha256
  key: c7bab4dd8883b727-3b249220088216f8
  lifetime/rekey: 86400/82026
  DPD sent/recv: 00000009/00000000
FGT-ALIONDEMAND # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=to_local ver=1 serial=1 192.168.0.177:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/528 options
[0210]=create_dev frag-rfc accept_traffic=1
proxyid_num=0 child_num=1 refcnt=11 ilast=4118 olast=4118 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
-----

```

```
name=to_local_0 ver=1 serial=2 192.168.0.177:4500->208.91.114.1:64916 dst_
mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/976 options
[03d0]=create_dev no-sysctl rgwy-chg rport-chg frag-rfc accept_traffic=1
parent=to_local index=0
proxyid_num=1 child_num=0 refcnt=14 ilast=0 olast=0 ad=/0
stat: rxp=3459 txp=3459 rxb=442752 txb=207540
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=9
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=to_local proto=0 sa=1 ref=2 serial=3 add-route
src: 0:192.168.0.0/255.255.255.0:0
dst: 0:192.168.4.0/255.255.255.0:0
SA: ref=3 options=282 type=00 soft=0 mtu=1422 expire=39694/0B replaywin=2048
seqno=d4b esn=0 replaywin_lastseq=00000d52 itn=0 qat=0
life: type=01 bytes=0/0 timeout=43187/43200
dec: spi=e2723047 esp=aes key=16 f93b233906039c179924923a4f09ebae
ah=sha1 key=20 c2c6225e26927de6381bf44c6ccd6d0a325e2e27
enc: spi=8427ce41 esp=aes key=16 961323608ef02c111ce4cc393cd79293
ah=sha1 key=20 9cffabaa0163df6a92e1917efa333148b58ff9da
dec:pkts/bytes=3402/204120, enc:pkts/bytes=3402/435456
```

# Change log

Date	Change Description
2019-03-26	Initial release.
2019-06-05	Added <a href="#">Connecting a local FortiGate to an AliCloud VPC VPN on page 83</a> and <a href="#">Connecting a local FortiGate to an AliCloud FortiGate via site-to-site VPN on page 87</a> .
2019-06-07	Added <a href="#">Deploying FortiGate-VM HA on AliCloud using routing tables and EIPs on page 46</a> .
2019-06-28	Added <a href="#">Security Fabric connector integration with AliCloud on page 82</a> .
2019-07-02	Updated <a href="#">Instance type support on page 6</a> .
2019-07-22	Updated <a href="#">Deploying FortiGate-VM HA on AliCloud using routing tables and EIPs on page 46</a> and <a href="#">Security Fabric connector integration with AliCloud on page 82</a> .
2019-07-30	Updated <a href="#">Deploying auto scaling on AliCloud on page 62</a> . Added <a href="#">Deploying FortiGate-VM HA on AliCloud between availability zones on page 55</a> .
2019-09-26	Added <a href="#">Pipelined automation using AliCloud Function Compute on page 82</a> .
2019-10-17	Updated <a href="#">Deploying auto scaling on AliCloud on page 62</a> .
2019-11-29	Updated <a href="#">Order types on page 8</a> and <a href="#">Models on page 7</a> .





**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.