FortiOS - AliCloud Cookbook

Version 6.4
# TABLE OF CONTENTS

## About FortiGate for AliCloud
- Instance type support .................................................. 5
- Region support .............................................................. 6
- Models ........................................................................ 6
- Licensing ....................................................................... 7
  - Order types .................................................................. 7
  - Creating a support account .......................................... 8
  - Registering and downloading a license ......................... 9
  - Migrating a FortiGate-VM instance between license types ... 9

## Securing instances on AliCloud ........................................... 11
- Configuring a virtual private cloud .................................... 11
- Subscribing to the FortiGate-VM in the marketplace ............... 13
- Configuring routing to the FortiGate-VM on AliCloud .......... 15
- Connectivity test ................................................................. 16
  - Configuring the initial firewall policy on the FortiGate-VM ... 16
  - Configuring an ECS worker VM for VNC access ............... 17
  - Testing malware scan for outgoing traffic ..................... 19
  - Testing application control for outgoing traffic ............... 20
  - Enabling NAT inbound protection in FortiOS ...................... 21

## HA for FortiGate-VM on AliCloud ...................................... 25
- Deploying and configuring FortiGate-VM on AliCloud using HAVIP 25
- Setting up the VPC ............................................................. 26
- Subscribing to the FortiGate-VM in the marketplace ............... 31
- Configuring the HAVIP on the AliCloud web console ............ 40
- Connectivity test ................................................................. 48
- Deploying FortiGate-VM HA on AliCloud using routing tables and EIPs 48
- Deploying FortiGate-VM HA on AliCloud between availability zones 57
- Configuring FortiGate-VM active-active HA .......................... 64

## Deploying auto scaling on AliCloud .................................... 65
- Planning ........................................................................ 65
  - Acronyms .................................................................... 65
  - Requirements ................................................................. 66
  - Deployment information ................................................ 67
- Deployment ..................................................................... 68
  - Terraform variables ....................................................... 69
- Verify the deployment .......................................................... 71
- Destroying the cluster ....................................................... 73

## Troubleshooting .................................................................... 74
- Debugging cloud-init .......................................................... 74
- TableStore destroy time .................................................... 74
- Resource availability .......................................................... 75
- Timeout ........................................................................ 75
- How to reset the master election ....................................... 75
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 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 7.

<table>
<thead>
<tr>
<th>Model name</th>
<th>vCPU</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>FG-VM01/01v/01s</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>FG-VM02/02v/02s</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>FG-VM04/04v/04s</td>
<td>1</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>FG-VM08/08v/08s</td>
<td>1</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>FG-VM16/16v/16s</td>
<td>1</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>FG-VM32/32v/32s</td>
<td>1</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>FG-VMUL/ULv/ULs</td>
<td>1</td>
<td>Unlimited</td>
<td></td>
</tr>
</tbody>
</table>
The v-series and s-series do not support virtual domains (VDOMs) by default. To add VDOMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDOMs 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 VDOM, 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) 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. The marketplace product page mentions hourly/annual term-based prices.

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. 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 a license 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 (VDOMs). If you plan to use VDOMs, deploy BYOL instances instead.

On-demand and BYOL licensing and payment models are not interchangeable. For example, once you spin up a FortiGate-VM on-demand instance, you cannot inject a BYOL license on the same VM. Likewise, you cannot convert a FortiGate-VM BYOL instance to on-demand.
When using a FortiGate-VM on-demand instance, the FortiOS GUI may display expiry dates for FortiGuard services. However, these expiries are automatically extended for as long as the on-demand instance's lifespan. You do not need to be concerned about the expiry of FortiGuard services.

Creating a support account

FortiGate for AliCloud supports both on-demand and BYOL licensing models. See Order types on page 7.

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 a license

You can obtain licenses for the BYOL licensing model through any Fortinet partner. If you do not have a partner, contact jerrywang@fortinet.com for assistance in purchasing a license.

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

To register and download a license:

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.
3. In the Registration page, enter the registration code that you received via email, and select Register to access the registration form.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
   a. Click Register to newly register the code to acquire a new serial number with a new license file.
   b. Click Renew to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.

   ![Registration Confirmation](image)

   Registration Confirmation
   You wish to Register or Renew Fortinet product FortiGate VM Subscription with the license number. If you have existing FortiGate VM Subscription license under this account, therefore you have two options to proceed: Click Register to register a new license. A new serial number will be created. Or, Click Renew if you want to apply contract to an existing license. System will extend product expiration.

   ![Register Renew Buttons](image)

5. At the end of the registration process, download the license (.lic) file to your computer. You 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.

Migrating a FortiGate-VM instance between license types

When deploying a FortiGate-VM on public cloud, you determine the license type (on-demand or BYOL) during deployment. The license type is fixed for the VM's lifetime. The image that you use to deploy the FortiGate-VM on the public cloud marketplace predetermines the license type.

Migrating a FortiGate-VM instance from one license type to another requires a new deployment. You cannot simply switch license types on the same VM instance. However, you can migrate the configuration between two VMs running as different license types. There are also FortiOS feature differences between on-demand and BYOL license types. For example, a FortiGate-VM on-demand instance is packaged with Unified Threat Management protection and does not support VDOMs, whereas a FortiGate-VM BYOL instance supports greater protection levels and features depending on its contract.
To migrate FortiOS configuration to a FortiGate-VM of another license type:

1. Connect to the FortiOS GUI or CLI and back up the configuration. See Configuration backups.
2. Deploy a new FortiGate-VM instance with the desired license type. If deploying a BYOL instance, you must purchase a new license from a Fortinet reseller. You can apply the license after deployment via the FortiOS GUI.
3. Restore the configuration on the FortiGate-VM instance that you deployed in step 2 as described in Configuration backups.
4. If you deployed an on-demand instance in step 2, register the license. To receive support for an on-demand license, you must register the license as described in Creating a support account on page 8.
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 11
2. Subscribing to the FortiGate-VM in the marketplace on page 13
3. Configuring routing to the FortiGate-VM on AliCloud on page 15
4. Connectivity test on page 16

Configuring a virtual private cloud

To configure 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 the VPC name. Click Create VPC.
3. Click Next Step.
4. You need at least two VSwitches: one for the ECS and one for the FortiGate-VM. Create the ECS VSwitch first as shown.
5. Click *Create More*.

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

7. Click *Done*. VPC and VSwitch setup is complete.
Securing instances on AliCloud

Subscribing to the FortiGate-VM in the marketplace

To subscribe to the FortiGate-VM in the marketplace:

2. 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. This example selects PAYG, Hong Kong, and Zone B 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.

FortiOS 6.4 AliCloud Cookbook
Fortinet Technologies Inc.
d. In the **Network** section, select TP_FortiVPC and Forti_VSwitchFW. Assign a public IP address to the image.

![Network section screenshot]

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.

![ECS instance list screenshot]
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.

   ![Quickly Create Rules](image)

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.

![Add Route Entry](image)

This ensures ECS outbound traffic goes through the FortiGate.
Securing instances on AliCloud

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 16
2. Configuring an ECS worker VM for VNC access on page 17
3. Testing malware scan for outgoing traffic on page 19
4. Testing application control for outgoing traffic on page 20
5. Enabling NAT inbound protection in FortiOS on page 21

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

To configure 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 does 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.

5. Connect to the VNC and log into Windows.

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

FortiOS should also provide detailed log information.
Testing malware scan for outgoing traffic

To test 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.

FortiGate will block the file from being downloaded.

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.
Securing instances on AliCloud

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.

3. Configure the inbound policy for the RDP redirection. Go to Policy & Objects > IPv4 Policy, then click Create New.
4. Name the rule, then choose the newly created virtual IP address as the destination.

![Image showing the New Policy page with the destination set to the virtual IP address]

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

![Image showing the Security Profiles settings with All Sessions selected]

The inbound rule is created successfully.

![Image showing the FortiGate policy list with the inbound rule enabled]

You can now use the FortiGate public address to RDP into the ECS.
Securing instances on AliCloud

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 25, 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 48, 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

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

2. Name the VPC TP_FortiVPC.

3. 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

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

- **Name**: FortiGate_HA_SW

- **Zone**: East China 1 Zone F

**Zone Resource**
- ECS
- RDS
- SLB

- **Destination CIDR Block**
  
  192.168.1.0/24

- **Number of Available Private IPs**: 252

- **Description**: 0/256

Tips:
- The CIDR cannot be changed once the VPC is created.
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

The VPC is now ready.
Subscribing to the FortiGate-VM in the marketplace

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.

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

![Data Disk Screenshot]

**Data Disk**

You have selected 1 disk, you can still add 15 disk.

Add Disk

---

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.

![Network Configuration Screenshot]

**Network**

How to Select a Network

- TP_FortiVPC
- FortiGate_internet_SW

If you need to create a new VPC, you can Go to Create and Create.

Private IP Addresses Available: 256.

---

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.

![Security Group Screenshot]

**Security Group**

- Select the ports you want to open: HTTP (port 80), HTTPS (port 443), ICMP Protocol, Ports 22 and 3389

---

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

![Host Field Screenshot]

**Host**

Key Pair: Select the Key Pair

Log on Credentials: Key Pair, Password, Set Later

Instance Name: FG-Master

Description: The description can contain 2-255 characters. It cannot start with http:// or https://

Host: FG-Master

---
h. Click ECS Service Terms.

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. Repeat steps 1 and 2 to create another FortiGate instance, named FGT-Slave.
6. You can create two ENI and attach them to the FortiGate instances. This step is optional.
   a. Stop the two FortiGate instances.

   b. Go to Networks & Security > Network Interfaces and create two ENI.
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-bp1ue3buvqeg04vkha4wl / 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-bp153m2ljzs6qivntqt5

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.
d. Restart the two FortiGate instances.

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

1. Create a new HAVIP address. Select the VPC and FortiGate-VM port1 VSwitch, and set the HAVIP address.
Create HAVIP Address

Region
China East 1 (Hangzhou)

VPC
vpc-bp1ue3buqego4vkha4wl

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
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:

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
      next
end
```
6. Bind the elastic IP address and the two FortiGate ECS to HAVIP.
   a. Create a new EIP.
HA for FortiGate-VM on AliCloud

HAVIP Details

Information

<table>
<thead>
<tr>
<th>ID</th>
<th>havip-bp1bwya8f7lppbl0qq65</th>
<th>Status</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>China East 1 (Hangzhou)</td>
<td>Intranet IP</td>
<td>192.168.0.252</td>
</tr>
<tr>
<td>VPC ID</td>
<td>vpc-bp1b2uyog1ugkor1hu6w</td>
<td>Created At</td>
<td>05/02/2018, 15:12:42</td>
</tr>
<tr>
<td>VSwitch</td>
<td>vsw-bp1iyf1ou2azwqowdr</td>
<td>Description</td>
<td>Edit</td>
</tr>
</tbody>
</table>

Resources

b. Bind the EIP to the HAVIP.

Bind Elastic IP Address

HAVIP Address

havip-bp1bwya8f7lppbl0qq65

Intranet IP

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**

<table>
<thead>
<tr>
<th>HAVIP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>havip-bp1bwy8f7lppb0qq6i5</td>
</tr>
</tbody>
</table>

| Intranet IP/IP | 192.168.0.252 |

<table>
<thead>
<tr>
<th>ECS Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
</tr>
</tbody>
</table>

- i-bp167uui7rqzmp8taa0kw

### Bind an ECS Instance

<table>
<thead>
<tr>
<th>HAVIP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>havip-bp1bwy8f7lppb0qq6i5</td>
</tr>
</tbody>
</table>

| Intranet IP/IP | 192.168.0.252 |

<table>
<thead>
<tr>
<th>ECS Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
</tr>
</tbody>
</table>

- i-bp167uui7rqzmp8taa0kw
- i-bp1cj6it8c8hndkxxom7j
### HAVIP Details

#### Information

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>Region</th>
<th>VPC ID</th>
<th>VSwitch</th>
</tr>
</thead>
<tbody>
<tr>
<td>havip-bp1bwyx877ppl00gp85</td>
<td>Allocated</td>
<td>China East 1 (Hangzhou)</td>
<td>vpc-bp1uac3boursage04vht444l</td>
<td>vsw-bp18cyf7ou2azwoun6r</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Intranet IP</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.0.252</td>
<td>- Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Created At</td>
<td>05/02/2018, 15:12:42</td>
</tr>
</tbody>
</table>

#### Resources

- **Elastic IP Address:** 47.97.186.150
  - Unbind

- **HAVIP Address:** 192.168.0.252 (Intranet IP)

- **ECS Instance (Slave)**
  - ip-bp1bwyx877ppl00gp85 (Running)
  - Unbind

- **ECS Instance (Master)**
  - ip-bp18cyf7ou2azwoun6r (Running)
  - Unbind
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

<table>
<thead>
<tr>
<th>Route Table ID</th>
<th>vtb-bp1785omvus5wpywiohn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>- Edit</td>
</tr>
<tr>
<td>Created At</td>
<td>05/02/2018, 13:48:20</td>
</tr>
<tr>
<td>VPC ID</td>
<td>vpc-bp1ue3buxqgo4vkhq4wl</td>
</tr>
<tr>
<td>Route Table Type</td>
<td>System</td>
</tr>
<tr>
<td>Description</td>
<td>- Edit</td>
</tr>
</tbody>
</table>

#### Route Entry List

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

### Add Route Entry

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

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

- **HAVIP Address**
  
  ![HAVIP Address Input](image)
Connectivity test

You can test whether you configured the FortiGate-VM instances and VPC properly. See Connectivity test on page 16.

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

<table>
<thead>
<tr>
<th>Port</th>
<th>AliCloud primary address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>10.0.1.11</td>
<td>10.0.1.0/24 EIP3</td>
</tr>
<tr>
<td>port2</td>
<td>10.0.2.11</td>
<td>10.0.2.0/24</td>
</tr>
<tr>
<td>port3</td>
<td>10.0.3.11</td>
<td>10.0.3.0/24</td>
</tr>
<tr>
<td>port4</td>
<td>10.0.4.11</td>
<td>10.0.4.0/24 EIP1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>AliCloud primary address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>10.0.1.12</td>
<td>10.0.24.0</td>
</tr>
<tr>
<td>port2</td>
<td>10.0.2.12</td>
<td>10.0.21.0/24</td>
</tr>
<tr>
<td>port3</td>
<td>10.0.3.12</td>
<td>10.0.22.0/24</td>
</tr>
<tr>
<td>port4</td>
<td>10.0.4.12</td>
<td>10.0.23.0/24</td>
</tr>
</tbody>
</table>

To check the prerequisites:

The following prerequisites must be met for this deployment:
HA for FortiGate-VM on AliCloud

- 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:

<table>
<thead>
<tr>
<th>VSwitch</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>net1-external</td>
<td>External data traffic on the public network-facing side.</td>
</tr>
<tr>
<td>net2-internal</td>
<td>External data traffic on the public network-facing side.</td>
</tr>
<tr>
<td>net3-heartbeat</td>
<td>Heartbeat between two FortiGate nodes. This is unicast communication.</td>
</tr>
<tr>
<td>net4-mgmt</td>
<td>Dedicated management interface.</td>
</tr>
</tbody>
</table>
2. Add six ENIs.

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.

   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.

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.
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.

```bash
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
```
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.

```plaintext
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
```
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.

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-ri9f5xs9cp9xsweedlcs
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-rj9f5xs9cp9xsweedlcs
  Tag.FGT_port2: eni-rj9j4jig06faq0vljneyv
  Tag.FGT_port3: eni-rj91wj13ywjs7y1n25ow
  Tag.FGT_port4: eni-rj9iiliuoh9t3qd5doe3
acs is checking tags on instance FGT-B
  Tag.FGT_port1: eni-rj9f5xs9cp9xsweedlcs
  Tag.FGT_port2: eni-rj9j4jig06faq0vljneyv
  Tag.FGT_port3: eni-rj91wj13ywjs7y1n25ow
  Tag.FGT_port4: eni-rj9iiliuoh9t3qd5doe3
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-rj9f5xs9cp9xsweedlcs, port1)
  eni: 1, 10.0.2.12(eni-rj9j4jig06faq0vljneyv, port2)
  eni: 2, 10.0.3.12(eni-rj9ga16wcti7anp0ot7m, port3)
  eni: 3, 10.0.4.12(eni-rj9dirnvg0hykei8bl8o, port4) <--- eip(47.254.42.40)
acs peer instance: FGT-A(i-rj9iiliuoh9t40811a60)
  eni: 0, 10.0.1.11(eni-rj9dirnvg0hykei8bl8o, port1) <--- eip(47.251.3.246)
  eni: 1, 10.0.2.11(eni-rj9j4jig06faq0vljneyv, port2)
  eni: 2, 10.0.3.11(eni-rj9ga16wcti7anp0ot7m, port3)
  eni: 3, 10.0.4.11(eni-rj9dirnvg0hykei8bl8o, 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-rj9f5xs9cp9xsweedlcs, port1) <--- eip(47.251.3.246)
  eni: 1, 10.0.2.12(eni-rj9j4jig06faq0vljneyv, port2)
  eni: 2, 10.0.3.12(eni-rj9ga16wcti7anp0ot7m, port3)
  eni: 3, 10.0.4.12(eni-rj9dirnvg0hykei8bl8o, port4) <--- eip(47.254.42.40)
acs peer instance: FGT-A(i-rj9iiliuoh9t40811a60)
  eni: 0, 10.0.1.11(eni-rj9dirnvg0hykei8bl8o, port1)
  eni: 1, 10.0.2.11(eni-rj9j4jig06faq0vljneyv, port2)
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:
HA for FortiGate-VM on AliCloud

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

<table>
<thead>
<tr>
<th>Port</th>
<th>AliCloud primary address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>10.0.11.11</td>
<td>10.0.11.0/24 EIP3</td>
</tr>
<tr>
<td>port2</td>
<td>10.0.12.11</td>
<td>10.0.12.0/24</td>
</tr>
<tr>
<td>port3</td>
<td>10.0.13.11</td>
<td>10.0.13.0/24</td>
</tr>
<tr>
<td>port4</td>
<td>10.0.14.11</td>
<td>10.0.14.0/24 EIP1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>AliCloud primary address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>10.0.21.12</td>
<td>10.0.21.0/24</td>
</tr>
<tr>
<td>port2</td>
<td>10.0.22.12</td>
<td>10.0.22.0/24</td>
</tr>
<tr>
<td>port3</td>
<td>10.0.23.12</td>
<td>10.0.23.0/24</td>
</tr>
<tr>
<td>port4</td>
<td>10.0.24.12</td>
<td>10.0.24.0/24 EIP2</td>
</tr>
</tbody>
</table>

IPsec VPN phase 1 configuration does not synchronize between primary and secondary FortiGates across AZs. Phase 2 configuration does synchronize.

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):

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

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.
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.

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.
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"
```
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.

```
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
config router static
  edit 1
    set gateway 10.0.21.1
    set device "port1"
  next
end
```
HA for FortiGate-VM on AliCloud

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.

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.
Configuring FortiGate-VM active-active HA

See Active-active egress route failover for AliCloud.
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.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>EIP</td>
<td>Elastic IP</td>
</tr>
<tr>
<td>ECS</td>
<td>Elastic Compute Service</td>
</tr>
</tbody>
</table>
Deploying auto scaling on AliCloud

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENI</td>
<td>Elastic Network Interface</td>
</tr>
<tr>
<td>ESS</td>
<td>Auto Scaling</td>
</tr>
<tr>
<td>FC</td>
<td>Function Compute</td>
</tr>
<tr>
<td>FGT</td>
<td>FortiGate</td>
</tr>
<tr>
<td>OSS</td>
<td>Object Storage Service</td>
</tr>
<tr>
<td>OTS</td>
<td>Open Table Service or TableStore, a NoSQL database by AliCloud</td>
</tr>
<tr>
<td>PAYG</td>
<td>Pay As You Go</td>
</tr>
<tr>
<td>RAM</td>
<td>Resource Access Management</td>
</tr>
<tr>
<td>SLB</td>
<td>Server Load Balancer</td>
</tr>
</tbody>
</table>

**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:
Deploying auto scaling on AliCloud

- 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:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific NE 1 (Tokyo)</td>
<td>m-6weakry8j13jxmj1mi4o</td>
</tr>
<tr>
<td>Asia Pacific SE 2 (Sydney)</td>
<td>m-p0wb4dw13d6qc1sndaj6</td>
</tr>
<tr>
<td>Asia Pacific SOU 1 (Mumbai)</td>
<td>m-a2dbkrpr8wsobn9ygddc</td>
</tr>
<tr>
<td>EU Central 1 (Frankfurt)</td>
<td>m-gw8cizn7dguyeikpgozb</td>
</tr>
<tr>
<td>US East 1 (Virginia)</td>
<td>m-0xif6xxwhj1qhoaqjrr6</td>
</tr>
<tr>
<td>US West 1 (Silicon Valley)</td>
<td>m-rj91iqplyxdp7crb0gvj</td>
</tr>
</tbody>
</table>

**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 66.

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 69.

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 = !_YfA7FQ8b_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.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access_key</td>
<td>Requires input</td>
<td>AliCloud AccessKey. For details on creating an AccessKey, refer to the AliCloud article Create an AccessKey.</td>
</tr>
<tr>
<td>secret_key</td>
<td>Requires input</td>
<td>AliCloud Secret key created with the AccessKey. Used to access the API.</td>
</tr>
<tr>
<td>region</td>
<td>us-east-1</td>
<td>The AliCloud Region.</td>
</tr>
<tr>
<td>scale_in_threshold</td>
<td>35</td>
<td>Default aggregate CPU threshold (percentage) to scale in (remove) 1 instance.</td>
</tr>
<tr>
<td>scale_out_threshold</td>
<td>70</td>
<td>Default aggregate CPU threshold (percentage) to scale out (add) 1 instance.</td>
</tr>
<tr>
<td>alicloud_account</td>
<td>AliCloud account number</td>
<td>(datatype)</td>
</tr>
<tr>
<td>cluster_name</td>
<td>FortigateAutoScale</td>
<td>Name of the cluster to be used across objects.</td>
</tr>
<tr>
<td>bucket_name</td>
<td>fortigateautoscale</td>
<td>Name of the OSS bucket. Must be lowercase.</td>
</tr>
<tr>
<td>instance_ami</td>
<td>Requires input</td>
<td>If specified, this will be the image used by the build. Otherwise, the script will obtain the latest FortiGate AMI.</td>
</tr>
<tr>
<td>Resource</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>instance</td>
<td>ecs.sn1ne</td>
<td>The instance Family type to be used by the Auto Saling configuration.</td>
</tr>
<tr>
<td>vpc_cidr</td>
<td>172.16.0.0/16</td>
<td>VPC CIDR block, it is divided into two /21 subnets.</td>
</tr>
<tr>
<td>vswitch_cidr_1</td>
<td>172.16.0.0/21</td>
<td>First Vswitch located in zone A of the region.</td>
</tr>
<tr>
<td>vswitch_cidr_2</td>
<td>172.16.8.0/21</td>
<td>Second Vswitch located in zone B of the region.</td>
</tr>
<tr>
<td>table_store_instance_type</td>
<td>Capacity</td>
<td>Accepted values are <em>HighPerformance</em> or <em>Capacity</em>.</td>
</tr>
</tbody>
</table>

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](image)

   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.

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:

   ![FortiGateAutoscale Table](image)

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:

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocated vCPUs</td>
<td>2</td>
</tr>
<tr>
<td>Allocated RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>Auto Scaling</td>
<td>Enabled</td>
</tr>
<tr>
<td>Role</td>
<td>Master</td>
</tr>
<tr>
<td>Group Size</td>
<td>2</td>
</tr>
</tbody>
</table>

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=<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:

   ![FortiGateASG-rrr](image)

   - Instance Access URL
   - Intranet: https://FortiGateASG-rrr.us-east-1.ots-internal.aliyuncs.com
   - Internet: https://FortiGateASG-rrr.us-east-1.ots.aliyuncs.com
   - VPC: https://FortiGateASG-rrr.us-east-1.vpc.tablestore.aliyuncs.com

   - Accessed By: Change
   - Any Network: 🌐
   - VPC List

   - You have no bound VPC. You can Bind VPC

   ![Table List](image)

   - Table Size:
     - Table Count: 3
     - Table Size: 0 B

   - Table List
     - | 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 |
       | FortiGateLifecycle  | -1           | 1            | 86400              | Disabled      | 💰       | 0 B        | Manage  | Tunnels | Delete |
       | FortiGateMasterElec | -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:

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-internaI.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/FortigateAutoScale-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 73.

**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:
      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:
      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 71 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.
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 76 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.

<table>
<thead>
<tr>
<th>Placeholder</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{SYNC_INTERFACE}</td>
<td>Text</td>
<td>The interface for FortiGate-VMs to synchronize information. All characters must be lowercase.</td>
</tr>
<tr>
<td>{CALLBACK_URL}</td>
<td>URL</td>
<td>The endpoint URL to interact with the Auto Scaling handler script. Automatically generated during the Terraform deployment.</td>
</tr>
<tr>
<td>{PSK_SECRET}</td>
<td>Text</td>
<td>The Pre-Shared key used in FortiOS. Randomly generated during the Terraform deployment.</td>
</tr>
</tbody>
</table>

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

- incoming request
- trusted source?
  - Yes
  - master exists?
    - Yes
    - Master healthy?
      - No
      - Can I hold master election?
        - No
        - elect new master
        - update new master in db
        - am I a new instance?
        - Yes
        - master IP same as mine?
          - No
          - am I new instance?
            - No
            - Response to heartbeat
            - Response with master config
          - Yes
          - Response with slave config
        - Yes
      - No
    - No
    - am I a new instance?
      - Yes
      - mark instance healthy
      - remove instance
      - add instance to monitor
      - update new master in db
      - wall
        - No
        - anyone's holding master election?
          - No
          - am I a new instance?
            - Yes
            - master IP same as mine?
              - No
              - am I new instance?
                - No
                - Response to heartbeat
                - Response with master config
              - Yes
              - Response with slave config
            - Yes
            - Response to heartbeat (with master IP)
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.
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.
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**.

7. (Optional) set the key pair.
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
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 -l
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:

```json
{
    "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": "xxxxxxxxxxxxxxxxx",
        "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:

```fortios
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 xxxxxxxxxxxxxxxxxxx
next
end
config vpn ipsec phase2-interface
  edit "AliCloudVPN"
    set phasename "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
```
VPN for FortiGate-VM on AliCloud

```
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
```

2. If the IPsec tunnel does not appear automatically, run the `diagnose vpn tunnel up AliCloudVPN` command.

3. 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:

```bash
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 d9d4ae911a51b0b/de39f4ac9defcf18
direction: initiator
status: established 1087-1078s ago = 9110ms
proposal: aes128-sha1
key: 9bf9b58431949e77-a0c21ded48368db1
```
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:

![Network Topology Diagram]

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:

```fortigate
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:

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

3. Configure IPsec VPN:

```fortigate
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-mlc aes256-mlc 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"
VPN for FortiGate-VM on AliCloud

```fortios
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:

   ```fortios
   config system interface
eedit "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
   ```
VPN for FortiGate-VM on AliCloud

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 xxxxxxxx
        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-ad33-41e96b656da
        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 e086b2b9-833c-51e9-3aaf-49e3cd4c5c70
        set srcintf "to_local"
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:

```bash
FGT-194-Levell # 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
```

2. Show the local FortiGate tunnel status:

```bash
FGT-194-Levell # diagnose vpn tunnel list
```

```bash
list all ipsec tunnel in vd 0
```

---

FortiOS 6.4 AliCloud Cookbook
Fortinet Technologies Inc.
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
[0x10]=create_dev frag/rfc accept_traffic=1
proxy_id_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=2000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxy_id=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 961323608e0f02c11ce4cc393cd79293
    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:

```bash
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 20/30/30 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
[0x10]=create_dev frag/rfc accept_traffic=1
proxy_id_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

---

FortiOS 6.4 AliCloud Cookbook
Fortinet Technologies Inc.
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=0 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
cenc: spi=8427ce41 esp=aes key=16 961323608ef02c111ce4cc393cd79293
ah=sha1 key=20 9cffabaa0163df6a92e1917efa333148b58ff9da
dec:pkts/bytes=3402/204120, enc:pkts/bytes=3402/435456
## Change log

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-03-31</td>
<td>Initial release.</td>
</tr>
<tr>
<td>2020-05-05</td>
<td>Updated Registering and downloading a license on page 9.</td>
</tr>
<tr>
<td>2020-05-13</td>
<td>Added Migrating a FortiGate-VM instance between license types on page 9.</td>
</tr>
<tr>
<td></td>
<td>Updated Order types on page 7.</td>
</tr>
</tbody>
</table>