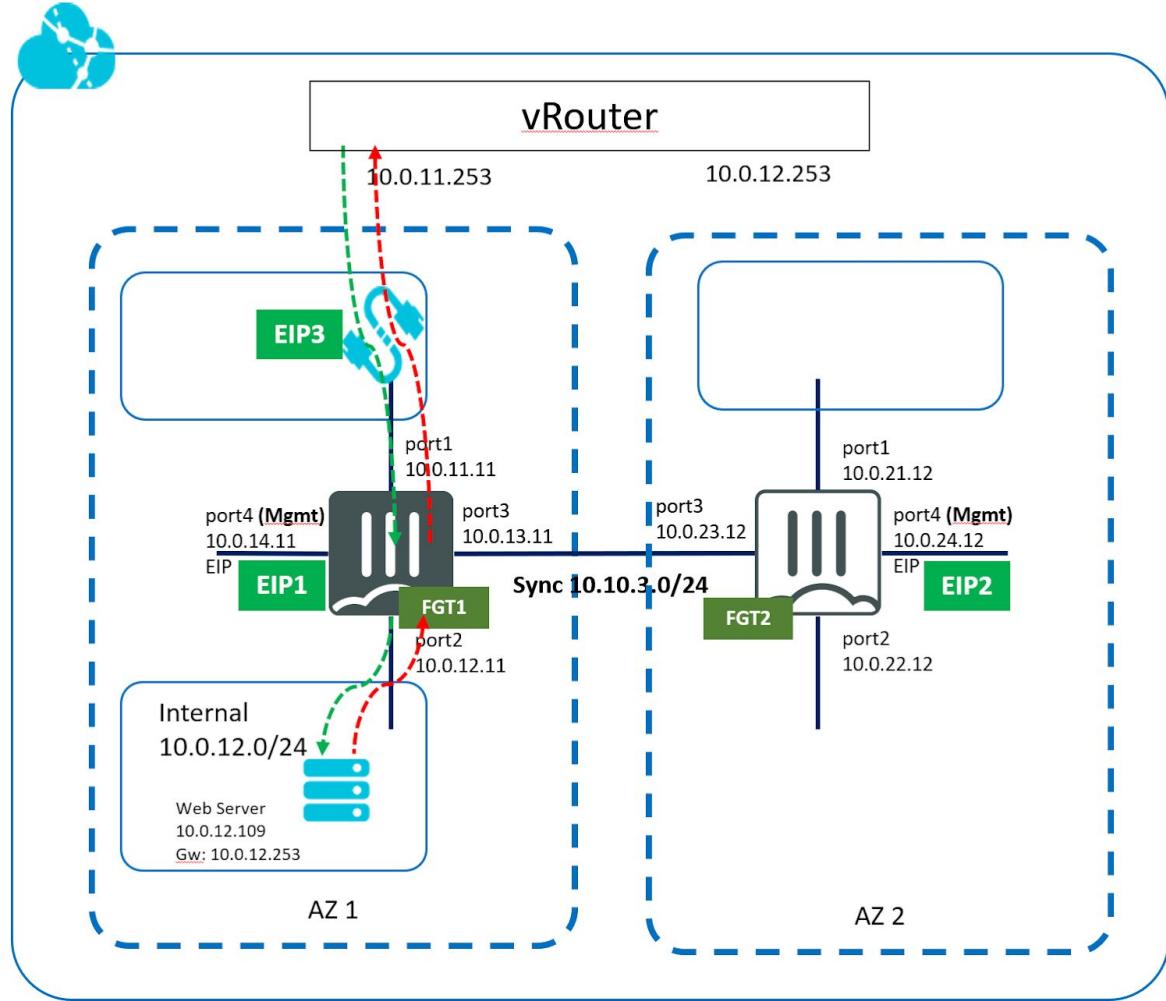


# Step by Step guide for deploy and config fortigate A-P HA cross AZ zone

<b>Diagram</b>	<b>3</b>
<b>Preparation</b>	<b>4</b>
Reference Document	4
License	4
Alicloud account or RAM account	6
Generate your Access/Secret Combination if you want to use terraform or aliyuncli to deploy/manage resources. for example. you can use terraform script to provision all resource by use	8
Find Fortigate image from aliyun market	9
plan your VPC, Region, Zone and instance type.	10
<b>Create alicloud resource</b>	<b>11</b>
create VPC	11
create switches.	11
create security-group	12
create fortigate instances	13
create ENI and EIP and associate with instances	16
create Custom Routing Table	20
create tag for instances FGT-1 and FGT-2	22
create RAM role and add RAM Policy	24
<b>Config Fortigate</b>	<b>28</b>
install the license.	28
config interface and static routing	29
config HA	36
exclude static-route sync	38
create firewall policy for egress traffic	40
create policy for ingress traffic	41
create policy for ingress traffic cross zone.	44
<b>Verify HA</b>	<b>47</b>
verify the HA result on both fortigate	47
create web-a workload VM for testing.	47
use cloud dashboard console to access web-a VM	47
start web server on web-a VM	48

verify the web server can be accessed from the internet.	49
verify egress traffic	50
check Failover interrupt time	51
<b>Verify the Changes due to Failover</b>	<b>54</b>
Master and Slave Role change	54
EIP3 moving	55
VPC custom routing table update	55
<b>Terraform code for automating the deployment</b>	<b>56</b>
if you want to use terraform instead GUI to deploy the resource. clone the code below	56
<a href="https://github.com/yagosys/fortigate_aliyun/tree/master/AP-CrossZone">https://github.com/yagosys/fortigate_aliyun/tree/master/AP-CrossZone</a>	56
<b>optional</b>	<b>56</b>
Connect Fortigate to FortiManager Cloud	56
obtain FortiManager Cloud license.	56
Setup FortiGate	57
config fortimanager	58

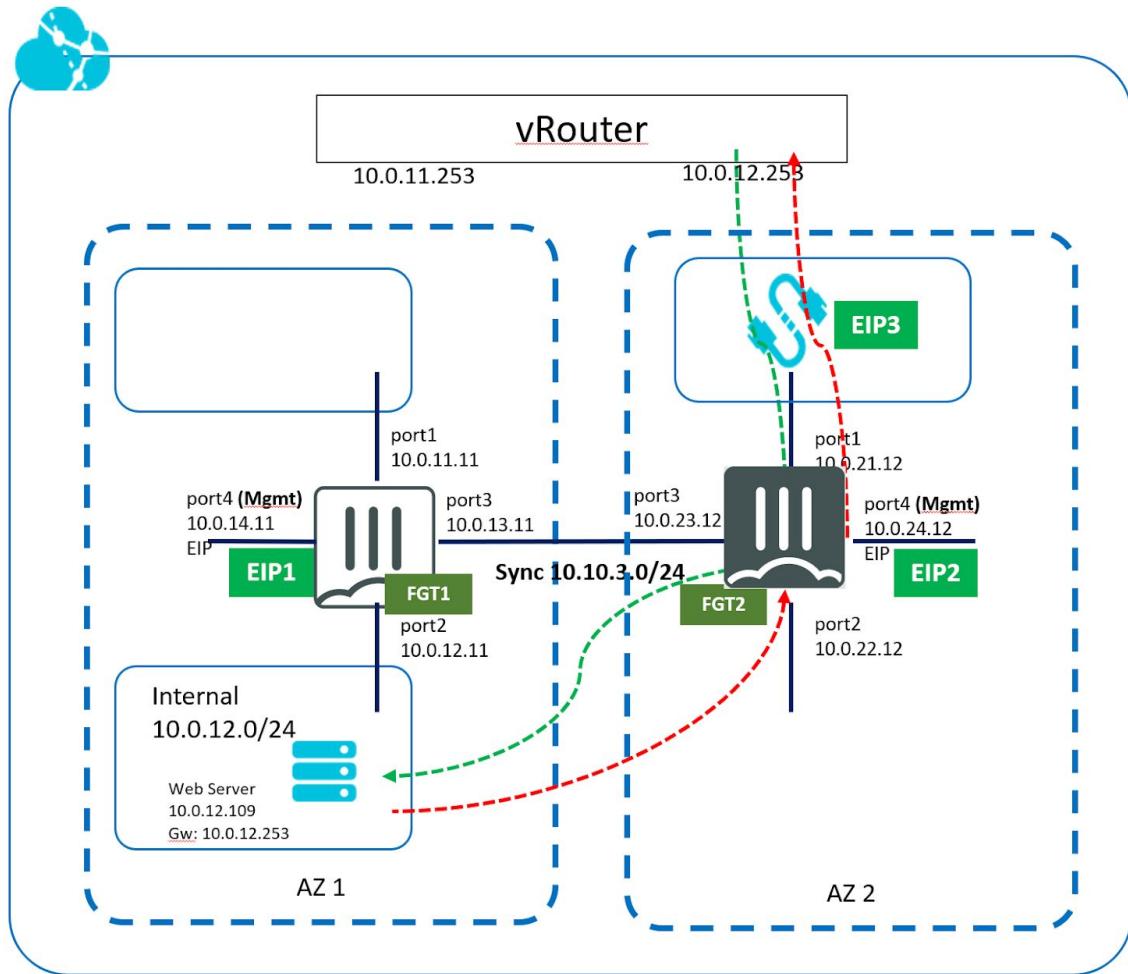
## Diagram



Two FGT are in different AZ zones but single Region. left FGT1 is Master as it is configured with high priority , FGT2 is slave( passive) and not forwarding any client traffic .

Two FGT is in HA Cluster with unicast heartbeat messages via port3. For whatever reason, if Heartbeat messages is not received from peer, FGT will assume master role, and associated itself with EIP3 and change VPC default route to 10.0.22.12 for vswitch internal to new Master.

a Web Server with IP (10.0.12.109) represents protected traffic in AZ1. when FGT2 becomes master, web server will use FGT2 for traffic in/out.



## Preparation

Here is a list of items needed

## Reference Document

<https://docs.fortinet.com/vm/alicloud/fortigate/6.4/alicloud-cookbook/6.4.0/967820/deploying-fortigate-vm-ha-on-alicloud-between-availability-zones>

## License

Two Fortigate BYOL License. and active your BYOL license

at [support.fortinet.com](http://support.fortinet.com) to Register your license , and download license file.

## Customer Service & Support



### Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate

6B7ZY-5KTDK-BZWKT-DONOT-EXIST

### End User Type

Please specify the type of user who will be using this product:

- The product will be used by a government user    The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other corporations or their separate business units which are engaged in the manufacture or distribution of items or



Customer Service & Support

Home Asset Assistance

Product Details

FortiGate VM Unlimited  
FGVMULTM20000763

Back To List

Information

- General
- Location
- Entitlement
- License & Key
- Statistics

Registration

- Renew Contract
- Add Licenses

Assistance

- Ticket List
- Technical Request
- Customer Service

Product Information



Our system now offers FortiGuard statistics for this unit, please click on

General

Product Model: FortiGate VM Unlimited  
Serial Number: FGVMULTM20000763  
License Number: REDACTED  
Registration Date: 2020-05-17  
Description: FortiGate-VM virtual appliance  
Partner: Fortinet (China)  
License File: [License File Download](#)  
Type: Evaluation  
Expiration Date: 2021-05-17

Edit

Alicloud account or RAM account

The screenshot shows the Alibaba Cloud homepage. On the left, there's a sidebar with a 'Products' section containing links to Resource Access Management, Virtual Private Cloud, Log Service, Elastic Compute Service, and Function Compute. A search bar at the top right contains the text 'Ram'. Below the search bar, a 'Recently Visited' section lists Resource Access Management, Virtual Private Cloud, Elastic Compute Service, and Alibaba Cloud DNS, each with a star icon. A message indicates 'Found 1 products by keyword Ram'. Under the heading 'Monitor and Management', there's a highlighted box for 'Resource Access Management' with a star icon.

You shall have at least AliyunVPCFullAccess, AliyunECSFullAccess, AliyunRAMFullAccess, AliyunEIPFullAccess privilege.

The screenshot shows the 'Users' page in the Alibaba Cloud RAM console. The user 'AndyWang' is selected. The 'Permissions' tab is active, showing 'Group Permissions' for the 'Groups' section. The table lists seven groups, each associated with a specific policy name and permission type. All entries are 'System Policy'.

Groups	Policy Name	Permission Type
Developer@group.5498321147060270.onaliyun.com	AliyunOSSFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunECSFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunRDSFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunSLBFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunRAMFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunVPCFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunEIPFullAccess	System Policy

Groups	Policy Name	Permission Type
Developer@group.5498321147060270.onaliyun.com	AliyunOSSFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunECSFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunRDSFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunSLBFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunRAMFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunVPCFullAccess	System Policy
Developer@group.5498321147060270.onaliyun.com	AliyunEIPFullAccess	System Policy

Generate your Access/Secret Combination if you want to use terraform or aliyuncli to deploy/manage resources. for example. you can use terraform script to provision all resource by use

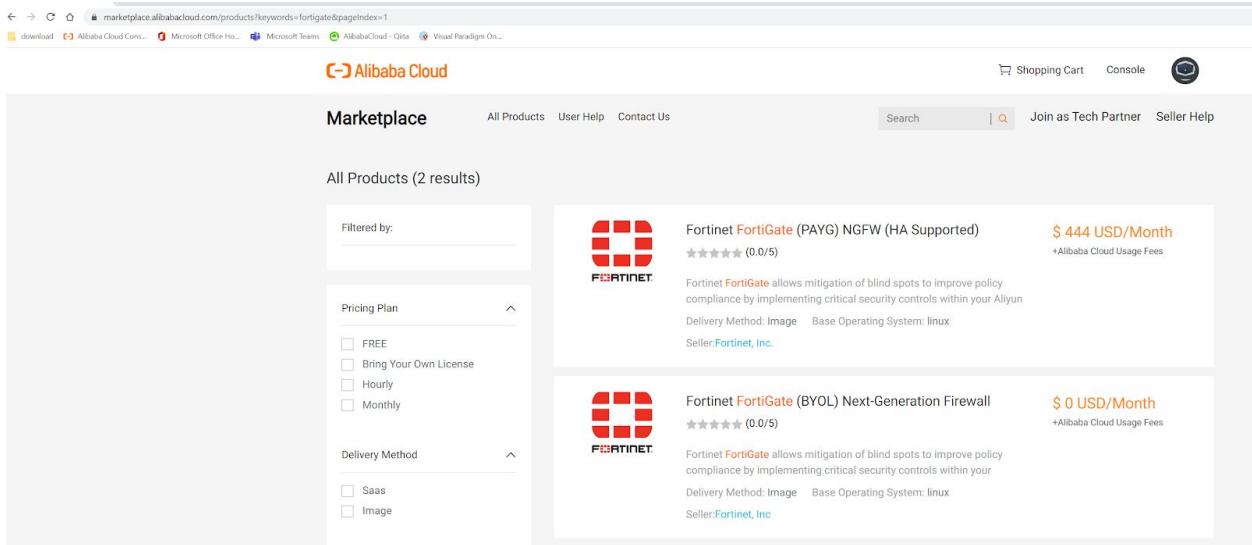
[https://github.com/yagosys/fortigate\\_aliyun/tree/master/AP-CrossZone](https://github.com/yagosys/fortigate_aliyun/tree/master/AP-CrossZone). you can also just use Aliyun GUI to deploy the resource.

① AccessKey ID and AccessKey Secret are the API keys for you to access Aliyun. It has full access privilege of the account. Please keep it safe.

User AccessKey	
AccessKey ID	AccessKey Secret
LTAI4... (redacted)	Show
LTAI4... (redacted)	Show

## Find Fortigate image from aliyun market

visit <https://marketplace.alibabacloud.com/> to locate fortigate images.



The screenshot shows the Alibaba Cloud Marketplace interface. At the top, there's a navigation bar with links for 'All Products', 'User Help', and 'Contact Us'. Below that is a search bar with the placeholder 'Search' and a magnifying glass icon. To the right of the search bar are buttons for 'Join as Tech Partner' and 'Seller Help'. The main content area displays a search result for 'All Products (2 results)'. On the left, there are two filter panels: 'Pricing Plan' (with options for FREE, Bring Your Own License, Hourly, Monthly) and 'Delivery Method' (with options for SaaS and Image). The main list contains two items, both from 'Fortinet, Inc.': 1. 'Fortinet FortiGate (PAYG) NGFW (HA Supported)' - Priced at \$444 USD/Month, it has a 0.0/5 rating. 2. 'Fortinet FortiGate (BYOL) Next-Generation Firewall' - Priced at \$0 USD/Month, it also has a 0.0/5 rating. Both items mention 'Alibaba Cloud Usage Fees' and specify 'Delivery Method: Image' and 'Base Operating System: linux'.

write down the region id and image id if you use terraform or cli to provision resource.

Image ID corresponding to each region

Image version: 6.4.1 ▾

Region	Image ID
China North 3 (Zhangjiakou)	m-8vb2p24tqw8l3ad5h3ln
China North 5 (Huhehaote)	m-hp3b6l40myz2w8wxajs4
East China 1	m-bp11lr0e89k9gnzrtwni
East China 2	m-uf62xgazjqodsnr0vnyd
South China 1	m-wz9g4zldn8zybdicq30g
cn-hongkong	m-j6cbretxym0yidwzk1hs
Asia Pacific SE 1 (Singapore)	m-t4ncpi4wp6eaotewxgbg
US East 1 (Virginia)	m-0xi24i6ur13zom03k0c3
Asia Pacific NE 1 (Tokyo)	m-6wegu0mh7x20iat6dhph
US West 1 (Silicon Valley)	m-rj9268ldc0zg0lk1t7ba

aliyun does not always have the same computer instance in different AZ zones. so you have to check which AZ zone has the computer instance type you needed. if you use GUI. you can use GUI to select the AZ zone, but if you use CLI or terraform, you need to find the AZ zone for the InstanceType.

you can also use aliyun cli to get region id and also the availability zone for the required instance type. to run fortigate A-P , you will need an instance that able to support at least 4 NICs.

```
vagrant@vagrant:~$ aliyun ecs DescribeAvailableResource --DestinationResource InstanceType --IoOptimized --InstanceType ecs.c5.2xlarge | jq '.AvailableZones.AvailableZone[] | "\(.AvailableResources.AvailableResource[].SupportedResources.SupportedResource[].Value) \(.ZoneId)"'
"ecs.c5.2xlarge ap-northeast-1b"
```

above you will find this instance type is only available in zone ap-northeast-1b.

plan your VPC, Region, Zone and instance type.

Plan your VPC CIDR , you will need 1 VPC, 1 Region, two zones, and computing optimized instances which support 4NICs.

# Create alicloud resource

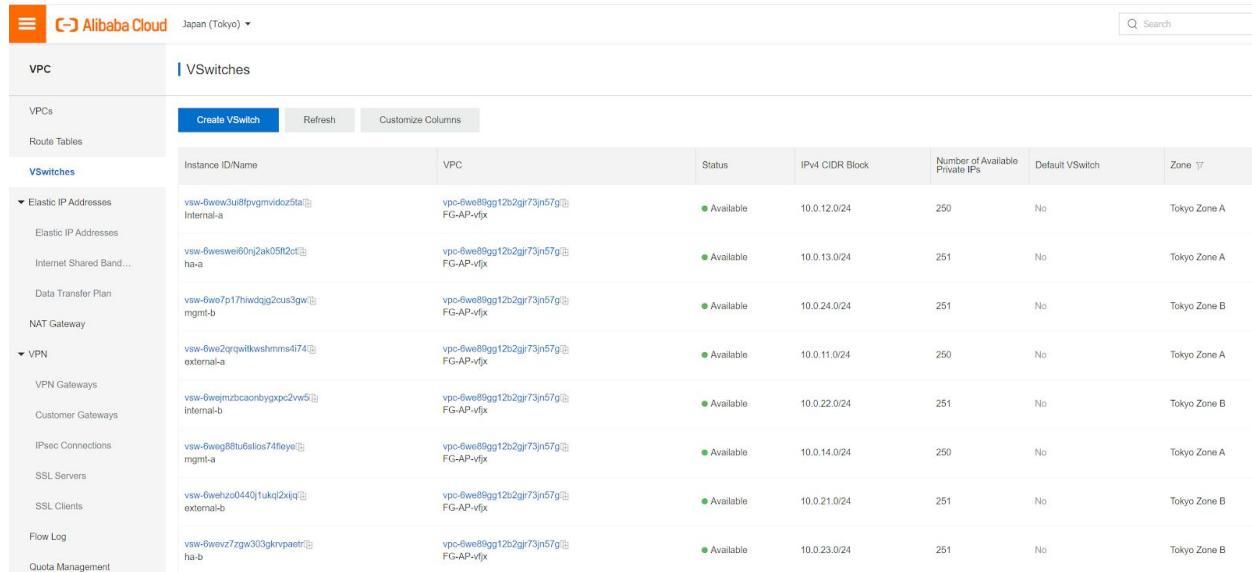
## create VPC



The screenshot shows the Alibaba Cloud VPC management interface. The top navigation bar includes the Alibaba Cloud logo and the region "Japan (Tokyo)". The main area has tabs for "VPC" and "VP Cs". The "VP Cs" tab is selected, showing a table with columns: "Instance ID/Name", "CIDR", and "Status". A single row is listed: "vpc-6we89gg12b2gr73jn57g" with CIDR "10.0.0.0/8" and status "Available". On the left sidebar, there are links for "Route Tables", "VSwitches", and "Elastic IP Addresses".

## create switches.

4 switches in Tokyo Zone A , 4 Switches in Tokyo Zone B. assign vswitch CIDR block by following the [cookbook](#) .



The screenshot shows the Alibaba Cloud VSwitch management interface. The top navigation bar includes the Alibaba Cloud logo and the region "Japan (Tokyo)". The main area has tabs for "VPC" and "VSswitches". The "VSswitches" tab is selected, showing a table with columns: "Instance ID/Name", "VPC", "Status", "IPv4 CIDR Block", "Number of Available Private IPs", "Default VSswitch", and "Zone". There are two sections of data: "Elastic IP Addresses" and "VPN". Under "Elastic IP Addresses", there are two entries: "Internal-a" and "ha-a". Under "VPN", there are two entries: "external-a" and "internal-b". Each entry shows its instance ID, the VPC it belongs to (e.g., "vpc-6we89gg12b2gr73jn57g"), its status ("Available"), its CIDR block (e.g., "10.0.12.0/24" or "10.0.13.0/24"), the number of available private IPs (e.g., "250" or "251"), and its zone ("Tokyo Zone A" or "Tokyo Zone B").

The switch named “externa” is for internet facing. “internal” is for protected traffic, “ha” is for clustering traffic. “mgmt” is for fortigate traffic that access aliyun metadata service(acs). the

communication between vswitch in different zones has to go through vrouter according to the associated routing table.

## create security-group

The next step is we need to create a security-group and instance. go to aliyun ECS product to create those. as those are ECS related resource.

This screenshot shows the Alibaba Cloud Security Groups page. On the left, there's a sidebar with 'Elastic Compute Service' and 'Instances & Images' sections. The main area is titled 'Security Groups' with a search bar and a 'Search' button. A table lists one security group: 'sg-6weiwjdj7w5rsn710j7' (FG-AP-SecGroup-vfjx), which is associated with 'vpc-6we89gg12b2gjr73jn57g' (FG-AP-vfjx). The table includes columns for Security Group ID/Name, Tag, VPC, Related Instances, Available IP Addresses, Network Type(All), and Security Group Type (Basic Security Group). At the bottom, there are 'Delete' and 'Edit Tags' buttons.

This screenshot shows the 'Security Group Rules' page for the 'FG-AP-SecGroup-vfjx' group. It has tabs for 'Inbound' and 'Outbound'. The 'Outbound' tab is selected. A table lists a single rule: 'Allow All -/1 IPv4 CIDR Block 0.0.0.0/0 Priority 1'. There is a 'Delete' button at the bottom.

This screenshot is similar to the previous one but shows the 'Outbound' tab selected. A yellow banner at the top states: 'By default, security groups allow all outbound traffic. ECS instances in a security group are allowed to access external networks.' The table below shows the same single rule as the previous screenshot.

To simplify the installation , here I allow all protocols while the installation. after that. we can refine the policy to more restricted rules. no need to config outbound rules.  
Later on, we will need to associate SecurityGroup with ENI and instances.

create fortigate instances



## Marketplace

All Products User Help Contact Us

Search

Software Infrastructure / Security / Fortinet FortiGate (BYOL) Next-Generation Firewall



### Fortinet FortiGate (BYOL) Next-Generation Firewall

★★★★★ (0.0/5)

Fortinet FortiGate allows mitigation of blind spots to improve policy compliance by implementing critical security controls within your AliCloud environment.

Delivery Method: Image    Architecture: 64    Base Operating System: linux    Latest Version: 6.4.1

\$ 0 USD/Hour

Monthly Subscription: \$ 0 USD/Month    Renewal Price: \$ 0 USD/Month

Choose Your Plan

click choose your plan , we can choose either Pay-As-you-go or subscription billing method for aliyun instance. if you want to try a few days. you might want to choose pay-as-you-go.

Billing Method   ⓘ

You can enable the No Fees for Stopped Instances (VPC-connected) feature for pay-as-you-go instances to reduce the upkeep costs. For limits and trigger conditions of this feature, click [here](#) to learn more.

Region  ⓘ Random Zone B (1) Zone A (3)

Instances in different regions cannot communicate with each other through the internal network. Select the region nearest to your customers to reduce the latency. ⓘ

Instance Type  All Generations Purchase History

Filter Select a type Select a type Search by instance type name, such as: Q I/O Optimized ⓘ Indicates what... Select a configuration

Architecture x86-Architecture Heterogeneous Computing ECS Bare Metal Instance

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

Family	Instance Type	vCPUs	Memory	Clock Speed	Internal Network Bandwidth	Packet Forwarding Rate	IPv6-supported	Physical Processor
<input type="radio"/> Compute Optimized Type with Enhanced Network Performance sn1ne ⓘ	ecs.sn1ne.xlarge	4 vCPUs	8 GiB	2.5 GHz	1.5 Gbps	500,000 PPS	Yes	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163
<input checked="" type="radio"/> Compute Optimized Type with Enhanced Network Performance sn1ne ⓘ	ecs.sn1ne.2xlarge	8 vCPUs	16 GiB	2.5 GHz	2 Gbps	1000,000 PPS	Yes	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163
<input type="radio"/> Compute Optimized Type with Enhanced Network Performance sn1ne ⓘ	ecs.sn1ne.3xlarge	12 vCPUs	24 GiB	2.5 GHz	2.5 Gbps	1300,000 PPS	Yes	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163
<input type="radio"/> Compute Optimized	ecs.sn1.medium	2 vCPUs	4 GiB	2.5 GHz	0.5 Gbps	100,000 PPS	No	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163

See more details (8 vCPU 16 GiB Compute Optimized Type with Enhanced Network Performance sn1ne)

select Region, Zone, “compute Optimized” category. Images will be automatically selected. add Data Disk if you want to log to a local disk. we here select zone A for fortigate-Primary. the instance type use “ecs.sn1ne.2xlarge”

Selected Instance Type ecs.hfc6.2xlarge (8 vCPU 16 GiB,Compute Optimized Type with High Clock Speed hfc6)

Quantity    Units 21 vCPUs have been enabled, and 29 more vCPUs can be enabled. The selected instance type occupies 8 vCPUs. You can create a maximum of 3 more ECS instances.

Image     ⓘ

Selected Image Fortinet FortiGate (BYOL) Next-Generation Firewall 6.4.1 ⓘ

ECS instances created in this region do not allow the switch of OS between Linux and Windows.

Storage System Disk

Disk specifications and performance Ultra Disk 40 GiB 2120 IOPS  Release with Instance

Click [here](#) for guidelines on how to select an appropriate disk for your scenario.

Disk Backup (Recommended)

You can periodically backup disks with an automatic snapshot policy to prevent risks such as virus attacks and accidental data deletion. [Snapshot pricing \(pay-as-you-go billing and hourly payment collection\)](#) >

Data Disk You have selected 1 disks and can select 15 more.

Quantity: 1 Device Name  Release with Instance  Create from Snapshot  Disk Encryption

Disk Backup (Recommended) ⓘ

You have purchased Ultra Disk 0 GB in the region. Remaining quota: 98204 GB

> NAS File System

select VPC , external-a switch, as we want Fortigate Primary IP bound to external switch , so it will get an IP address from 10.0.11.0/24 CIDR block. we do not need to check “Assign Public IP address” as later on , we will create an EIP and bind to fortigate primary interface. select the Security group we just created. you will also noticed that an Default ENI will be created and attached to Vswitch external-A.



Elastic Compute Service (ECS) Quick Launch Custom Launch

Basic Configurations Networking System Configurations (Optional) Grouping

Logon Credentials Key Pair Password Set Later

Key Pair Select a key pair Learn More | Create Key Pair

If you do not specify a key pair or password, Set Later is selected by default.

Instance Name FG-AP-Primary-FortiGate-vfjx Learn how to customize sequential instance names.

The name must be 2 to 128 characters in length, and can contain letters, digits, periods (.), underscores (\_), colons (:), and hyphens (-). It must start with a letter.

Description Description

The description must be 2 to 256 characters in length and cannot start with http:// or https://.

Host FGT-1 Learn how to customize sequential hostnames.

For Linux systems and other operating systems: The name must be 2 to 64 characters in length. It can contain several segments delimited by periods (.). Each segment can contain letters not allowed. The name cannot start or end with a period (.) or hyphen (-).

Sequential Suffix Add Sequential Suffix to Instance Name and Hostname

Release Protection Prevent users from releasing the instance inadvertently by using the console or API

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

you do not need to choose a key pair, the default password for fortigate instance will be the instance ID. setup the instance Name and Host name. use default for rest configuration and access “Terms of Service” . you created Instances. do the same to create another fortigate instance in AZ B.

Alibaba Cloud Japan (Tokyo) Search Billing Ticket ICP

Elastic Compute Service Instances

Select an instance attribute or enter a keyword

Filters: Instance ID: i-6wregikubv6gx0wzb829 Clear

Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Specifications	VPC Details	Billing Method
i-6wregikubv6gx0wzb829 FG-AP-Primary-FortiGate-vfjx			Tokyo Zone A	10.0.11.11(Private)	Stopped	8 vCPU 16 GB (I/O Optimized) ecs.s1ne.2xlarge - 0Mbps (Peak Value)	vpc-6we89gg12b2gr73jn57g vsw-6we2qrqwtkwshmrns4l74	Pay-As-You-Go June 8, 2020, 16:07 Created

## create ENI and EIP and associate with instances

Next we will create additional ENI and EIP and associate with instances just created.

we will need to create 3 ENI for each fortigate in each Availability zone. total 6 ENI has to be created. and total 3 EIPs. EIP3 binds to FGT-1 primary interface, EIP1 binds to FGT-1 ENI3, EIP2 binds to FGT-2 ENI3.

you have to select VPC,Vswitch,SecurityGroup for that ENI, also you need to assign an Primary Private IP for the ENI. each ENI will be associated to the corresponding vswitch with an IP address belonging to that subnet.

## Create ENI [?](#) Create ENI



ENI Name	FG-AP-Primary-Internal-ENI-vfjx				
The name must be 2 to 128 characters in length and can contain letters, digits, hyphens (-), and underscores (_). It cannot start with http:// or https://. The name must start with a letter. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter and cannot start with http:// or https://.					
* VPC:	vpc-6we89gg12b2gjr73jn57g / FG-AP-vf...				
* VSwitch:	vsw-6wew3ui8fpvgmvidoz5ta / Internal...				
The available zone of the selected switch needs to be the same as the instance to be bound CIDR: 10.0.12.0/24 (ap-northeast-1a)					
Primary Private IP:	10.0.12.11				
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.					
Secondary Private IP Addresses:	<b>Up to 9 private IP addresses can be assigned to this ENI.</b> <input checked="" type="radio"/> Not set <input type="radio"/> Auto <input type="radio"/> Manual				
* Security Group	Select a security group				
<table border="1"><thead><tr><th>Name</th><th>ID</th></tr></thead><tbody><tr><td>FG-AP-SecGroup-vfj...</td><td>sg-6weiwdwj7w5rsn710rj7</td></tr></tbody></table>		Name	ID	FG-AP-SecGroup-vfj...	sg-6weiwdwj7w5rsn710rj7
Name	ID				
FG-AP-SecGroup-vfj...	sg-6weiwdwj7w5rsn710rj7				
Description:	It must be 2 to 256 characters in length and cannot start with http:// or https://.				
Tag:	Select a tag key	Enter or select a tag value.			
<b>OK</b> <b>Cancel</b>					

then you will need to create EIP, and Bind EIP to ENI, finally you shall see the result below.

### Elastic IP

	Subscription	Pay-As-You-Go	
Region	China (Qingdao) China (Beijing) China (Zhangjiakou) China (Hohhot) China (Hangzhou) China (Shanghai)	China (Shenzhen) China South 2 (Heyuan) China (Chengdu) China (Hong Kong) Japan (Tokyo) Singapore	Australia (Sydney) Malaysia (Kuala Lumpur) Asia Pacific SE 5 (Jakarta) Asia Pacific SOU 1 (Mumbai) US (Virginia) US (Silicon Valley)
isp	BGP		
Network Mode	Public		
Network Traffic	By traffic	By bandwidth	
Max Bandwidth	50Mbps 100Mbps 200Mbps 1 Mbps		
Name	<input type="text"/>		
Billing Cycle	Hour		
Quantity	<input type="text" value="1"/> <input type="button" value=""/>		
You currently have 7 instances. You can create 13 more instances			

**Current Selected**

Region:	Japan (Tokyo)
isp:	BGP
Network Mode:	Public
Network Traffic:	By traffic
Max Bandwidth:	1 Mbps
Name:	-
Billing Cycle:	1 Hour(s)
Eip Rentalfee:	Yes
Billing Item:	Configuration Fee(IP Fee)+Traffic Fee
Quantity:	1
Fee:	\$0.005 / Hour(s)
Public Traffic Fee:	\$0.087 /GB
<b>Buy Now</b>	

### Alibaba Cloud

Japan (Tokyo) ▾

VPC	Elastic IP Addresses						
VPCs	<input type="button" value="Create EIP"/>	<input type="button" value="Request Specific EIP"/>	<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>
Route Tables							
vSwitches							
▼ Elastic IP Addresses							
<b>Elastic IP Addresses</b>							
Internet Shared Band...	<input type="checkbox"/> eip-6wet2x1fa3psley1k233g EIP3	47.74.27.198	<input type="button" value=""/>	5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:10 Created	<input checked="" type="radio"/> Allocated	Add to Shared Bandwidth Package
Data Transfer Plan	<input type="checkbox"/> eip-6we083wq1ntua9y052c5 EIP2	47.74.16.87	<input type="button" value=""/>	5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:07 Created	<input checked="" type="radio"/> Allocated	Add to Shared Bandwidth Package
NAT Gateway	<input type="checkbox"/> eip-6web4l698a7y9m0t2j EIP1	47.74.33.92	<input type="button" value=""/>	5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:04 Created	<input checked="" type="radio"/> Allocated	Add to Shared Bandwidth Package
▼ VPN							
VPN Gateways							
	<input type="button" value="Unbind"/>	<input type="button" value="Release"/>	<input type="button" value="Remove from Internet Shared Bandwidth"/>				

The screenshot shows the Network Interfaces page for the Elastic Compute Service in Japan (Tokyo). The search bar contains 'i-6wegikubvfgd8xwzb529'. The table lists four network interfaces:

ID/Name	Tag	VSwitch/VPC	Zone	Security Group ID	Bound Instance	Public IP Address	Primary Private IP Address	Type/MAC Address(All)
eni-6weiwdj7w5sn79s7nb...		vsw-6wev2qrgw... vpc-6we89gq1...	Tokyo Zone A	sg-6weiw...	i-6wegik...	47.74.27.198	10.0.11.11	Primary 00:16:3e:00:2e:71
eni-6wed6xfaxf5cm1ngu6yiq...		vsw-6wev2q5tu... vpc-6we89gq1...	Tokyo Zone A	sg-6weiw...	i-6wegik...	47.74.33.92	10.0.14.11	Secondary 00:16:3e:00:3a:8b
eni-6weibc6kvu0fnanv1mh3...		vsw-6wev2q56... vpc-6we89gq1...	Tokyo Zone A	sg-6weiw...	i-6wegik...		10.0.13.11	Secondary 00:16:3e:00:61:53
eni-6wedp65en280nawcp2n...		vsw-6wev2u8... vpc-6we89gq1...	Tokyo Zone A	sg-6weiw...	i-6wegik...		10.0.12.11	Secondary 00:16:3e:00:42:33

above you see that FGT-1 in zone A is associated with 4 ENIs. The first one in the list is the one created by default with instances. which is associated with EIP3 . The other 3 ENIs are additional ENI which are marked as type "Secondary". The first "Secondary" ENI is associated with EIP1.

The screenshot shows the Network Interfaces page for the Elastic Compute Service in Japan (Tokyo). The search bar contains 'i-6wecc6f779xe2cb4qvg'. The table lists four network interfaces:

ID/Name	Tag	VSwitch/VPC	Zone	Security Group ID	Bound Instance	Public IP Address	Primary Private IP Address	Type/MAC Address(All)
eni-6weiwdj7w5sn79s7na...		vsw-6wev2o4... vpc-6we89gq1...	Tokyo Zone B	sg-6weiw...	i-6wecc6...		10.0.21.12	Primary 00:16:3e:00:56:43
eni-6webbc6kvu96nawv1mh4...		vsw-6wev271h... vpc-6we89gq1...	Tokyo Zone B	sg-6weiw...	i-6wecc6...	47.74.16.87	10.0.24.12	Secondary 00:16:3e:00:38:de
eni-6weiwdj7w5sn79s7n9...		vsw-6wev27zg... vpc-6we89gq1...	Tokyo Zone B	sg-6weiw...	i-6wecc6...		10.0.23.12	Secondary 00:16:3e:00:2a:5a
eni-6weiwdj7w5sn79s7n8...		vsw-6wejmzb... vpc-6we89gq1...	Tokyo Zone B	sg-6weiw...	i-6wecc6...		10.0.22.12	Secondary 00:16:3e:00:44:61

for FGT-2 in zone B, EIP2 is associated with MGMT ENI.

## create Custom Routing Table

By default. a system routing table is created for each VPC and associated with vswitch in this VPC. in our case. we want internal switch (internal-a) point all traffic towards fortigate instance in Zone A. so we have to create an custom route and create a rule entry to add a default router that point to FGT-1 first secondary ENI. by doing this. all the traffic from subnet (10.0.12.0/24) will be routed to fortigate instance secondary ENI. (which is fortigate Port 2). so the traffic will be handled by Fortigate instead go directly to vrouting. inside Fortigate, we have a default router point to aliyun vRouter for traffic leave VPC router to internet or aliyun CEN.

The screenshot shows the Route Table Details page. On the left, there's a table of existing route entries with columns for Destination CIDR Block, Status, Next Hop, and Type. Most entries have a status of 'Available' and type 'System'. One entry for '100.64.0.0/10' has a status of 'Unreachable'. On the right, a modal window titled 'Add Route Entry' is open, containing fields for Name (set to 'default\_to\_fortigate\_port\_2'), Destination CIDR Block (set to '0.0.0.0/0'), Next Hop Type (set to 'Secondary ENI'), and Secondary ENI (set to 'FG-AP-Primary-Internal-ENI-vfjx/eni-6wedp6s5en280naxcp2n'). A blue 'OK' button is at the bottom right of the modal.

here we added a default route “Deafult\_to\_fortigate\_port\_2” . point to instance primary fortigate secondary ENI.

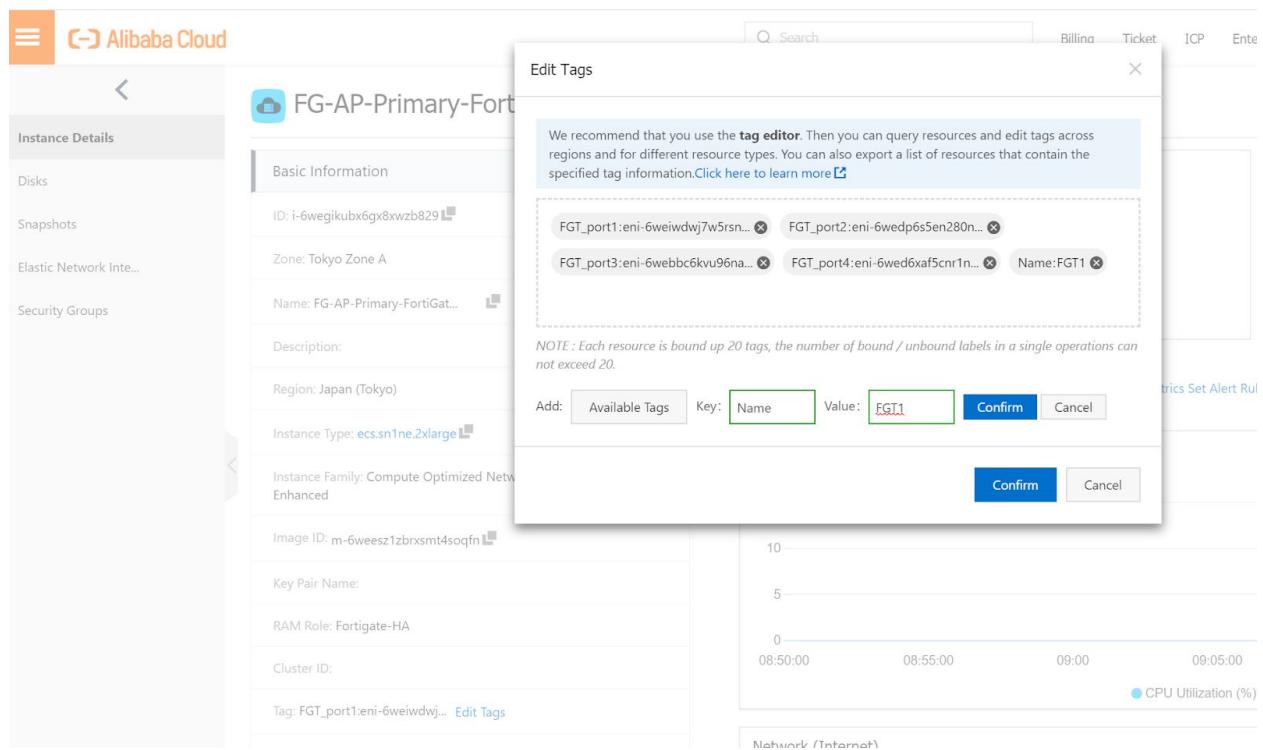
this custom routing table will also be automatically associated with vswitch named “internal-a”. and this vswitch “internal-a” will also be unassociated from the system routing table.

The screenshot shows the same Route Table Details page after the addition. The table now includes a new entry at the bottom for '0.0.0.0/0' with a status of 'Available', next hop 'eni-6wedp6s5en280naxcp2n', type 'Custom', and description '-'. The rest of the table remains the same, showing the previous 10 route entries.

you will see the routing table above.

## create tag for instances FGT-1 and FGT-2

This is needed for FGT to access alicloud metadata services. we create two tag with Name:FGT1 and Name:FGT2 respectively .



## Edit Tags

We recommend that you use the **tag editor**. Then you can query resources and edit tags across regions and for different resource types. You can also export a list of resources that contain the specified tag information.[Click here to learn more](#)

FGT\_port1:eni-6weiwdwj7w5rsn... X    FGT\_port2:eni-6weiwdwj7w5rsn... X  
FGT\_port3:eni-6weiwdwj7w5rsn... X    FGT\_port4:eni-6webbc6kvu96na... X    Name:FGT2 X

*NOTE : Each resource is bound up 20 tags, the number of bound / unbound labels in a single operations can not exceed 20.*

Add: Available Tags Create

Confirm

Cancel

finally. you shall see all tags like below.

The screenshot shows the Alibaba Cloud ECS Tags page. On the left, there's a sidebar with navigation links like Overview, Events, Tags (which is selected), Resource Orchestration, Instances & Images, Instances, Elastic Container Instance, Dedicated Hosts, Super Computing Clusters, and Reserved Instances. The main area has tabs for Tags and Tag Editor (NEW). Below that is a search bar and a table for managing tags. The table has columns for Tag Key and Tag Value. The data in the table is:

Tag Key	Tag Value
FGT_port1	eni-6weiwdwj7w5rsn79s7na eni-6weiwdwj7w5rsn79s7nb
FGT_port2	eni-6wedp65en280naxcp2n eni-6weiwdwj7w5rsn79s7n8
FGT_port3	eni-6webbc6kvu96navn1mh3 eni-6weiwdwj7w5rsn79s7n9
FGT_port4	eni-6webbc6kvu96navn1mh4 eni-6wed6xaf5cmr1ngu6yiq
Name	FGT1 FGT2

## create RAM role and add RAM Policy

for FGT1 to retrieve information from aliyun metadata services.

This is needed for failover to work. Fortigate need to know the EIP3 is associated with which Fortigate etc.,

The screenshot shows the Alibaba Cloud RAM service interface. On the left, there's a sidebar with options like Overview, Identities, Groups, Users, Settings, SSO, Permissions, Grants, Policies, and RAM Roles. The RAM Roles option is currently selected. The main area has a title 'Create RAM Role' with two tabs: 'Select Role Type' (selected) and 'Configure Role'. Below this, there's a section for 'Trusted entity type' with three options: 'Alibaba Cloud Account' (radio button), 'Alibaba Cloud Service' (radio button, selected), and 'IdP'. The 'Alibaba Cloud Service' option is described as allowing a trusted Alibaba Cloud service to assume the RAM role. There's also a note that a RAM role can issue short-lived STS (Security Token Service) tokens. A 'Create RAM Role' button is visible, along with a text input field for 'Enter a role name or note'. Two existing roles are listed: 'AliyunECSImageExportDefaultRole' and 'AliyunECSImageImportDefaultRole'. At the bottom right are 'Next' and 'Close' buttons.

## Create RAM Role

Select Type of Trusted Entity

Alibaba Cloud Service

Role Type

Normal Service Role  Service Linked Role

\* RAM Role Name

Fortigate-HA

The name can contain a maximum of 64 characters, only English letters, numbers, and hyphens (-) are accepted.

Note

[Empty note area]

\* Select Trusted Service

Elastic Compute Service

Back

OK

Close

## Add Permissions

\* Principal

Fortigate-HA@role.5498321147060270.onaliyunservice.com 

\* Select Policy

System Policy

Custom Policy

[Create Policy](#)

AliyunECSFullAccess



Select a policy.

Authorization Policy Name

Description

Add AliyunECSFullAccess,AliyunVPCFullAccess,AliyunEIPFullAccess .

Permissions

Trust Policy Management

Add Permissions

Input and Attach

Applicable

Scope of

Permission

Policy

Policy Type

Note

Attach Date

All

[AliyunOSSFullAccess](#)

System Policy

Provides full access to Object Storage Service(OSS) via Management Console.

May 20, 2020,  
14:01:20

All

[AliyunECSFullAccess](#)

System Policy

Provides full access to Elastic Compute Service(ECS) via Management Console.

May 20, 2020,  
14:01:20

All

[AliyunVPCFullAccess](#)

System Policy

Provides full access to Virtual Private Cloud(VPC) via Management Console.

May 20, 2020,  
16:10:40

All

[AliyunEIPFullAccess](#)

System Policy

Provides full access to Elastic IP Address(EIP) via Management Console.

May 20, 2020,  
14:01:20

then bind RAM rule to two Fortigate instances.

Instances

Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Specifications	VPC Details	Method	RAM Role	Cluster ID	Actions
i-6wec16f79xejlubm2i6 windows-A			Tokyo Zone A	10.0.11.5(Private)	Stopped	4 vCPU 8 GiB (I/O Optimized) ecs.s1ne.xlarge 5Mbps	vpc-6we89gg12b2gjr73jn57g	Pay-As-You-Go			Manage Change Instance Type   More ▾
i-6weaynsrm71fm2zhvqxe web-a			Tokyo Zone A	10.0.12.109(Private)	Stopped	1 vCPU 512 MB (I/O Optimized) ecs.t1c2m1.nano 0Mbps (Peak Value)	vpc-6we89gg12b2gjr73jn57g				Manage Change Instance Type   More ▾
i-6wegikubx6gx8xwzb829 FG-AP-Primary-FortiGate-vfjx			Tokyo Zone A	47.74.27.198(EIP) 10.0.11.11(Private)	Running	8 vCPU 16 GiB (I/O Optimized) ecs.s1ne.2xlarge 5Mbps	vpc-6we89gg12b2gjr73jn57g				ge   Connect   Upgrade/Downgrade Change Instance Type   More ▾
i-6wec16f79xe2cb4qvg FG-AP-Secondary-FortiGate-vfjx			Tokyo Zone B	10.0.21.12(Private)	Running	8 vCPU 16 GiB (I/O Optimized) ecs.c5.2xlarge 0Mbps (Peak Value)	vpc-6we89gg12b2gjr73jn57g				Buy Same Type Instance Status Instance Settings Password/Key Pair Configuration Change Disk and Image Network and Security Group Operations and Troubleshooting

Bind/Unbind RAM Role [? Use instance RAM role](#)

Action:  Bind  Unbind

Description: Binding a RAM role to an instance grants all permissions of the role to the instance. Use caution when performing this operation.

\*RAM Role:  [Create RAM Role](#)

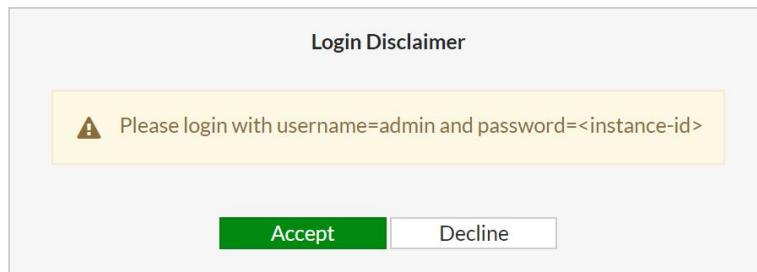
[OK](#) [Cancel](#)

do the same for FGT2 in zone.

We shall complete an alicloud cloud setup and launch the fortigate instance in both zone A and zone B. Configuring the custom routing table added a default route point to fortigate. now move to setup fortigate

## Config Fortigate

after starting the instance, login via EIP1 IP address to FGT1, EIP2 IP address to FGT2. change password following the instruction. by default. https port 443 is accessible.



install the license.



upload your license file ( FGVM1VTM20000859.lic) which is downloaded from support.fortinet.com.

after rebooting. you will be able to login into FGT1 and FGT2.

Elastic IP Addresses									
Create EIP		Request Specific EIP						Elastic IP Address	Enter an Elastic IP Address to perform
Instance ID/Name	IP Address	Monitor	Bandwidth	Charge Type(All) ▾	Status(All) ▾	Shared Bandwidth/Global Acceleration	Associated Instance	Instance Type(All) ▾	Actions
eip-6wef2xf1a3psley1k23g EIP3	47.74.27.198		5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:10 Created	Allocated	Add to Shared Bandwidth Package	6wegikubx6gx8xwzb8 29 FG-AP-Primary-FortiGate-vfjk	ECS Instances	Bind Unbind More ▾
eip-6wcl0s3wq1ntia9yo5zc5 EIP2	47.74.16.87		5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:07 Created	Allocated	Add to Shared Bandwidth Package	eni-6webbc6kvu96navn1 mth4 NAT Mode	Secondary ENI	Bind Unbind More ▾
eip-6web4l698a7y9mi0zfj EIP1	47.74.33.92		5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:04 Created	Allocated	Add to Shared Bandwidth Package	eni-6wed6xa5cnr1ngu6yl q NAT Mode	Secondary ENI	Bind Unbind More ▾

you will be asked to input default password which is instanceid and asked to change password. then you will be asked to import the license file you previously downloaded from support.fortinet.com . after that. fortigate will be rebooted. please be noticed the license may take up to 30 minutes to be active. so be patient for license to become active.

## config interface and static routing

you can config fortigate by following the cookbook. basically you will have to config

### 1. interface address and routing table.

the interface IP address has to match ENI ip addresses also the port number shall match the ENI numbers.

config default route for both fortigate, you can get the gateway ip address from port1 DHCP setup.

on FGT2 , config a static route to 10.0.12.0/24 with exit port2 is required. this is needed after the switch over happens. web-a server in zone-A will talk to FGT2 in zone B. Config this route will let FGT2 send traffic back to web-a in ZoneA directly via port2. if you do not have any workload in zone-B internal-B subnet. you do not need to config 10.0.22.0/24 on FGT1. but on FGT2. we need to config 10.0.12.0/24 . as web-A is on this subnet.

FortiGate VM64-ALI FGT1				
Network		IPv4		
Interfaces		Destination	Gateway IP	Interface
DNS		0.0.0.0	10.0.11.253	port1
Packet Capture		10.0.22.0/24	10.0.12.253	port2
SD-WAN Interfaces				Enabled
SD-WAN Rules				Enabled
Performance SLA				
Static Routes	★			
Policy Routes				
RIP				

FortiGate VM64-ALI FGT2				
Network		IPv4		
Interfaces		Destination	Gateway IP	Interface
DNS		0.0.0.0	10.0.21.253	port1
Packet Capture		10.0.12.0/24	10.0.22.253	port2
SD-WAN Interfaces				Enabled
SD-WAN Rules				Enabled
Performance SLA				
Static Routes	★			
Policy Routes				
RIP				

FortiGate VM64-ALI FGT1				
Network		Interfaces		
Interfaces	★			
DNS				
Packet Capture				
SD-WAN Interfaces				
SD-WAN Rules				
Performance SLA				
Static Routes				
Policy Routes				
RIP				
OSPF				
BGP				
Multicast				
System	1			
Policy & Objects				
Security Profiles				
VPN				
User & Authentication				
WiFi & Switch Controller				
Log & Report				

FortiGate VM64-ALI 1 3 5 7 9 11 13 15 17 19 21 23  
 2 4 6 8 10 12 14 16 18 20 22 24

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
Physical Interface 4				
port1	Physical Interface		10.0.11.11/255.255.255.0	PING HTTPS SSH HTTP FMG-Access
port2	Physical Interface		10.0.12.11/255.255.255.0	PING HTTPS SSH HTTP FMG-Access
port3	Physical Interface		10.0.13.11/255.255.255.0	PING HTTPS SSH HTTP FMG-Access
port4	Physical Interface		10.0.14.11/255.255.255.0	PING HTTPS SSH HTTP FMG-Access

by default, all interface are using DHCP to get ip address from vRouter,

port1 is instance-1 primary interface which is default ENI .  
 port2 is instance-1 is first secondary ENI and so on.  
 config static IP address instead DHCP . do same for both Fortigate

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate							
port1	Physical Interface		10.0.21.12/255.255.255.0	PING HTTPS SSH HTTP FMG-Access			5
port2	Physical Interface		10.0.22.12/255.255.255.0	PING HTTPS SSH HTTP FMG-Access			3
port3	Physical Interface		10.0.23.12/255.255.255.0	PING HTTPS SSH HTTP FMG-Access			0
port4	Physical Interface		10.0.24.12/255.255.255.0	PING HTTPS SSH HTTP FMG-Access			1

after configuration interface IP address and static route . you shall see configuration on two fortigate like this.

```
FGT1 (interface) # show
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.0.11.11 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
```

```
set ip 10.0.12.11 255.255.255.0

set allowaccess ping https ssh http fgfm

set type physical

set snmp-index 2

next

edit "port3"

set ip 10.0.13.11 255.255.255.0

set allowaccess ping https ssh http fgfm

set type physical

set snmp-index 3

next

edit "port4"

set ip 10.0.14.11 255.255.255.0

set allowaccess ping https ssh http fgfm

set type physical

set snmp-index 4

next

edit "ssl.root"

set vdom "root"

set type tunnel

set alias "SSL VPN interface"

set snmp-index 5

next

edit "fortilink"

set vdom "root"

set fortilink enable

set ip 169.254.1.1 255.255.255.0
```

```
set allowaccess ping fabric  
set type aggregate  
set lldp-reception enable  
set lldp-transmission enable  
set snmp-index 6  
  
next  
  
end  
  
  
FGT1 (interface) #
```

```
FGT2 (static) # show  
  
config router static  
  
edit 1  
  
set gateway 10.0.21.253  
set device "port1"  
  
next  
  
edit 2  
  
set dst 10.0.12.0 255.255.255.0  
set gateway 10.0.22.253  
  
set device "port2"  
  
next
```

```
FGT2 # config system interface
```

```
FGT2 (interface) # show

config system interface

edit "port1"

    set vdom "root"

    set ip 10.0.21.12 255.255.255.0

    set allowaccess ping https ssh http fgfm

    set type physical

    set snmp-index 1

next

edit "port2"

    set vdom "root"

    set ip 10.0.22.12 255.255.255.0

    set allowaccess ping https ssh http fgfm

    set type physical

    set snmp-index 2

next

edit "port3"

    set ip 10.0.23.12 255.255.255.0

    set allowaccess ping https ssh http fgfm

    set type physical

    set snmp-index 3

next

edit "port4"

    set ip 10.0.24.12 255.255.255.0

    set allowaccess ping https ssh http fgfm

    set type physical

    set snmp-index 4
```

```
next

edit "ssl.root"

    set vdom "root"

    set type tunnel

    set alias "SSL VPN interface"

    set snmp-index 5

next

edit "fortilink"

    set vdom "root"

    set fortilink enable

    set ip 169.254.1.1 255.255.255.0

    set allowaccess ping fabric

    set type aggregate

    set lldp-reception enable

    set lldp-transmission enable

    set snmp-index 6

next

end
```

```
FGT2 # config route static

FGT2 (static) # show

config router static

    edit 1

        set gateway 10.0.21.253
```

```
set device "port1"

next

edit 2

set dst 10.0.12.0 255.255.255.0

set gateway 10.0.22.253

set device "port2"

next

end
```

## config HA

the next step is to config HA setup.

```
FGT1 # config system ha

FGT1 (ha) # show

config system ha

set group-name "fgtha2"

set mode a-p

set hbdev "port3" 50

set session-pickup enable

set ha-mgmt-status enable

config ha-mgmt-interfaces

edit 1

set interface "port4"

set gateway 10.0.14.253
```

```
next

end

set override disable

set priority 100

set monitor "port1"

set unicast-hb enable

set unicast-hb-peerip 10.0.23.12

end
```

```
FGT2 # config system ha

FGT2 (ha) # show

config system ha

    set group-name "fgtha2"

    set mode a-p

    set hbdev "port3" 50

    set session-pickup enable

    set ha-mgmt-status enable

    config ha-mgmt-interfaces

        edit 1

            set interface "port4"

            set gateway 10.0.24.253

        next

    end

    set override disable

    set priority 50
```

```

set monitor "port1"

set unicast-hb enable

set unicast-hb-peerip 10.0.13.11

end

FGT2 (ha) #

```

after config HA. you shall see the two fortigate now in Cluster mode. Both two fortigate will be in-sync. The FGT1 has high priority. so it will become master. FGT2 will become a slave.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
FortiGate VM64-ALI 1 3 5 7 9 11 13 15 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24	100	FGT1	FGVM1VTM20000859	Master	00:01:35:13	12	30.00 kbps
FortiGate VM64-ALI 1 3 5 7 9 11 13 15 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24	50	FGT2	FGVM1VTM20000886	Slave	00:01:35:20	13	22.00 kbps

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
FortiGate VM64-ALI 1 3 5 7 9 11 13 15 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24	50	FGT2	FGVM1VTM20000886	Slave	00:01:38:59	20	45.00 kbps
FortiGate VM64-ALI 1 3 5 7 9 11 13 15 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24	100	FGT1	FGVM1VTM20000859	Master	00:01:38:58	18	16.00 kbps

take a look again at the routing table on FGT2. if you see the routing table is changed to 10.0.11.253. This means the configuration of the static route is also synced with FGT1. this is not expected, as FGT2 is default routing table shall point to 10.0.21.253. we can config to exclude sync static configuration. after that. static routing will NOT be synced.

exclude static-route sync

```
FGT1 # show system vdom-exception

config system vdom-exception

    edit 1

        set object router.static

    next

end

FGT1 # execute ha manage 0 admin

admin@10.0.23.12's password:

FGT2 # show system vdom-exception

config system vdom-exception

    edit 1

        set object router.static

    next

end
```

## TIPS

beware that when you will not be able to ping HA interface address from the root vdom (which is the default administrator domain). HA port is automatically moved to another administrator domain called (vsys\_ha) domain. In that domain you will be able to ping HA interface from FGT1 to FGT2, you can use “execute enter root” go back to root domain.

```
FGT1 # execute enter vsys_ha

current vdom=vsys_ha:2
```

```
FGT1 # execute ping 10.0.23.12

PING 10.0.23.12 (10.0.23.12): 56 data bytes

64 bytes from 10.0.23.12: icmp_seq=0 ttl=255 time=1.7 ms

--- 10.0.23.12 ping statistics ---

1 packets transmitted, 1 packets received, 0% packet loss

round-trip min/avg/max = 1.7/1.7/1.7 ms
```

Next step we will create a sample VM to test ingress and egress traffic goes through firewall fortigate.

we will launch a linux machine in vswitch internal-A. this switch shall be able to reach the internet through fortigate, and also we config a web service in this VM. allow from public access to this VM by configure policy on fortigate. from vm to access internet. we need to config a policy on fortigate to allow this traffic and do a SNAT. for ingress to this VM. we need to config a policy on fortigate for DNAT and config a VIP for this vm.

create firewall policy for egress traffic

The screenshot shows the FortiGate management interface for policy configuration. The left sidebar navigation includes: Dashboard, Security Fabric, Network, System (with a red notification dot), Policy & Objects (selected), Firewall Policy, Authentication Rules, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report.

The main 'Edit Policy' window displays the following settings:

- Name:** egress\_all
- Incoming Interface:** port2
- Outgoing Interface:** port1
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ✓ ACCEPT (highlighted)
- Inspection Mode:** Flow-based (selected)
- Firewall / Network Options:**
  - NAT:** Enabled (green switch)
  - IP Pool Configuration:** Use Outgoing Interface Address (selected)
  - Preserve Source Port:** Disabled (gray switch)
  - Protocol Options:** PRX default
- Security Profiles:**
  - AntiVirus: Off (gray switch)
  - Web Filter: Off (gray switch)
  - DNS Filter: Off (gray switch)
  - Application Control: Off (gray switch)
  - IPS: Off (gray switch)
- SSL Inspection:** SSL no-inspection
- Logging Options:**
  - Log Allowed Traffic: On (green switch)
  - Security Events: Selected
  - All Sessions: Selected (highlighted)
  - Generate Logs when Session Starts: On (green switch)
  - Capture Packets: Off (gray switch)
- Comments:** Write a comment... (disabled)
- Enable this policy:** On (green switch)

At the bottom right of the window is a large green 'OK' button.

The traffic coming from port2 (attached to vswitchinternal-A), exit from port1 (attached to vswitch external-A). port 1 is also the interface for the FGT-1 default route. we have to enable NAT. when traffic leaves port 1, the source IP of the VM will become the port1 interface's IP address which is 10.0.11.11.

## create policy for ingress traffic

For Ingress traffic, we need to create an VIP to represent VM and then create DIP to that VIP.

FortiGate VM64-ALI FGT1 HA: 1

Dashboard >

Security Fabric >

Network >

System > 1 >

**Policy & Objects**

- Firewall Policy
- Authentication Rules
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules

**Virtual IPs** ☆

- IP Pools
- Protocol Options
- Traffic Shapers
- Traffic Shaping Policy
- Traffic Shaping Profile

Security Profiles >

VPN >

Edit Virtual IP

VIP type: IPv4  
Name: web8080  
Comments: Write a comment... 0/255  
Color: Change

Network

Interface: port1  
Type: Static NAT  
External IP address/range: 0.0.0.0  
Mapped IP address/range: 10.0.12.109

Optional Filters

Port Forwarding

Protocol: TCP (selected) UDP SCTP ICMP  
External service port: 8080  
Map to port: 8080

OK Cancel

https://47.74.33.92/ng/firewall/service

**Edit Policy**

**Name:** toWeb8080

**Incoming Interface:** port1

**Outgoing Interface:** port2

**Source:** all

**Destination:** web8080

**Schedule:** always

**Service:** ALL

**Action:**  ACCEPT  DENY

**Inspection Mode:** Flow-based

**NAT:**

**Protocol Options:** PRX default

**Security Profiles:**

- AntiVirus:
- Web Filter:
- DNS Filter:
- Application Control:
- IPS:

**SSL Inspection:** no-inspection

**Logging Options:**

- Log Allowed Traffic:  Security Events  All Sessions
- Generate Logs when Session Starts:
- Capture Packets:

**Comments:** Write a comment... 0/1023

**Enable this policy:**

**Buttons:** OK, Cancel

incoming traffic will come from port 1 (external-a switch), and reach port 2 (internal-a switch). if the destination is web8080. fortigate will do a Destination NAT. replace the ip address of fortigate EIP3 (which is associated with master fortigate) to the VIP of VM which is 10.0.12.x).

Do not enable NAT. as here we do not need SNAT.  
you can also config vip and firewall policy in cli as shown below.

```
FGT1 # show firewall policy
config firewall policy
edit 1
    set name "egress_all"
    set uid bc9bf0e4-a96e-51ea-b3c5-5db8c110bcab
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set logtraffic-start enable
    set nat enable
next
edit 2
    set name "toWeb8080"
    set uid ac6ff84c-a981-51ea-1d36-05798c17d816
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "web8080"
    set action accept
    set schedule "always"
--More--
    set service "ALL"
set logtraffic all
next
end

FGT1 #
```

```
FGT1 # show firewall vip
config firewall vip
edit "web8080"
    set uuid 8738a470-a981-51ea-0e12-933b08ae8835
    set extintf "port1"
    set portforward enable
    set mappedip "10.0.12.109"
    set extport 8080
    set mappedport 8080
next
end

FGT1 #
```

Config will be sync to slave fortigate

create policy for ingress traffic cross zone.

the traffic between vswitch in different zones has to go through default router which via port 1.

After switching over , the incoming traffic from the internet will arrive port 1 on FGT-2, then it will then do A DNAT, translated to DIP address of web-a VM which is 10.0.11.209. then it will find a routing table to reach that address. which is in Zone -A. so it will again go back to port 1 to vrouter. vrouting will take that packet to web-A vm in zone-A. so we have to config a policy for incoming traffic that arrive on port 1 and exist on port 1.

FortiGate VM64-ALI FGT2

Dashboard >

Security Fabric >

Network >

System > 1 >

Policy & Objects >

**Firewall Policy** ☆

- Authentication Rules
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shapers
- Traffic Shaping Policy
- Traffic Shaping Profile
- Security Profiles >
- VPN >
- User & Authentication >
- WiFi & Switch Controller >
- Log & Report >

Name: port1-port1

Incoming Interface: port1

Outgoing Interface: port1

Source: all

Destination: web8080

Schedule: always

Service: ALL

Action:  ACCEPT  DENY

Inspection Mode: Flow-based  Proxy-based

NAT:

Protocol Options: PRX default

SSL Inspection: no-inspection

Logging Options:

- Log Allowed Traffic:  Security Events  All Sessions
- Generate Logs when Session Starts:
- Capture Packets:

OK Cancel

```
FGT2 # config firewall policy

FGT2 (policy) # edit 3

FGT2 (3) # show

config firewall policy

edit 3

    set name "port1-port1"

    set uuid 4bb3372a-adec-51ea-2fb1-7e5bbe37e5b
```

```

set srcintf "port1"

set dstintf "port1"

set srcaddr "all"

set dstaddr "web8080"

set action accept

set schedule "always"

set service "ALL"

set logtraffic all

next

end

FGT2 (3) #

```

if turn on packet trace for http client that access web-a 8080. you will see below logs

```

FGT2 # diagnose debug flow trace start 1
FGT2 # id=20085 trace_id=256 Func=print_pkt_detail line=5588 msg="vd-root:0 received a packet(proto=6, 115.204.228.209:51270->10.0.21.12:8080) from port1. flag [5], seq 2880903269, ack 0, win 64240"
1d=20085 trace_id=256 func=init_ip_session_common line=5754 msg="allocate a new session-80000aab"
1d=20085 trace_id=256 func=fw_pre_route_handler line=181 msg="VIP-10.0.12.109:8080, outdev-port1"
1d=20085 trace_id=256 func=_ip_session_run_tuple line=3409 msg="DNAT 10.0.21.12:8080->10.0.12.109:8080"
1d=20085 trace_id=256 func=fw_ip_route_input_common line=2598 msg="find a route: flag=00000000 fw=10.0.21.253 via port1"
1d=20085 trace_id=256 func=fw_forward_handler line=781 msg="Allowed by Policy-3: SNAT"
1d=20085 trace_id=256 func=_ip_session_run_tuple line=3395 msg="SNAT 115.204.228.209->10.0.21.12:51270"

```

wait until these function in-sync between master and slave. then you have done all the configuration.

## Verify HA

verify the HA result on both fortigate  
you can use EIP1 and EIP2 to remotely access fortigate

The screenshot shows the FortiGate Management interface for an HA cluster. It displays two FortiGate VM64-ALI units, FGT1 and FGT2, which are synchronized. FGT1 is the Master unit, and FGT2 is the Slave unit. Both units have an uptime of 00:02:36:43 and are handling 19 and 9 sessions respectively, with throughput of 23.00 kbps and 21.00 kbps. The interface includes a sidebar with System, HA, and other management options.

create web-a workload VM for testing.

create a linux WebServer VM in zone a called web-a to verify the HA .  
choose VPC and zone A internal-a switch. setup your username and password.

The screenshot shows the Alibaba Cloud ECS Instances page. It lists a single instance named "web-a" which is running in the Tokyo region, Zone A. The instance has 1 vCPU, 512 MB RAM, and is using the ecs.t5.lc1m1.nano 0Mbps (Peak Value) configuration. It was created on June 8, 2020, at 17:47. The instance is associated with a VPC (vpc-6we89gg12b2gj73jn57g), a subnet (vsw-6new3ui8fpvgmvidoz5ta), and a Pay-As-You-Go billing method. The Actions column includes links for Manage, Connect, Change Instance Type, and More.

use cloud dashboard console to access web-a VM

after starting this instance . you can access this web-a console via alicloud vnc console connect.

**Instances**

Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Specifications	VPC Details	Billing Method	RAM	Cluster ID	Actions
i-6weaynsrm71fm2zhvqxe web-a			Tokyo Zone A	10.0.12.109(Private)	Running	1 vCPU 512 MB (I/O Optimized) ecs.t1.lc2.m1.nano 0Mbps (Peak Value)	vpc- 6we89gg12b2gj73jn57g vsw- 6wew3ui8fpvgmvidcz5ta	Pay-As-You-Go			Manage   Connect Change Instance Type   More

```

Ubuntu 18.04.4 LTS web-a tty1

web-a login: root
Password:
Last login: Tue Jun  9 16:32:39 CST 2020 from 10.0.12.11 on pts/1
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-96-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Welcome to Alibaba Cloud Elastic Compute Service !
root@web-a:~# 

```

## start web server on web-a VM

then start web server. this web-a VM come with python installed. so we here just use python as web server for testing.



```
root@web-a:~# python -m SimpleHTTPServer 8080 &
[1] 961
root@web-a:~# Serving HTTP on 0.0.0.0 port 8080 ...
root@web-a:~# _
```

from your local PC. you can use a browser to curl to access this web server via FGT-1 EIP3 address. EIP3 is currently associated with FGT-1 as FGT-1 is master .

verify the web server can be accessed from the internet.



## Directory listing for /

- 
- [.bash\\_history](#)
  - [.bashrc](#)
  - [.cache/](#)
  - [.gnupg/](#)
  - [.pip/](#)
  - [.profile](#)
  - [.pydistutils.cfg](#)
  - [.ssh/](#)
  - [nohup.out](#)
-

on the FGT-1 log & Report menu. you can see access log.

```
root@web-a:~# python -m SimpleHTTPServer 8080 &
[1] 961
root@web-a:~# Serving HTTP on 0.0.0.0 port 8080 ...

root@web-a:~# 34.92.67.255 -- [13/Jun/2020 13:55:14] "GET / HTTP/1.1" 200 -
34.92.67.255 -- [13/Jun/2020 13:55:17] "GET /.ssh/ HTTP/1.1" 200 -
34.92.67.255 -- [13/Jun/2020 13:55:18] "GET /.ssh/authorized_keys HTTP/1.1" 200 -
115.204.228.209 -- [13/Jun/2020 14:00:18] "GET / HTTP/1.1" 200 -

root@web-a:~#
root@web-a:~#
root@web-a:~#
```

the web server will dump the access information.

The screenshot shows the FortiGate VM64-ALI interface with the 'Forward Traffic' log details expanded. The log table lists several entries, each with a timestamp, source IP, destination IP, and various metrics like bytes transferred. To the right of the table, detailed information is provided for the first entry:

General	
Date	2020/06/12
Time	23:00:30
Duration	12s
Session ID	751
Virtual Domain	root
NAT Translation	Destination
Source	
IP	115.204.228.209
Source Port	62446
Country/Region	China
Source Interface	port1
User	
Destination	
IP	10.0.11.11
NAT IP	10.0.12.109
Port	8080
Country/Region	Reserved
Destination Interface	port2
Application Control	
Application Name	
Category	unscanned
Risk	undefined
Protocol	6
Service	tcp/8080
Data	
Received Bytes	144 B
Received Packets	3
Sent Bytes	224 B
Sent Packets	5
Action	
Action	Accept: session close
Policy	toWeb8080 (2)
Policy	ac6ff84c-a981-51ea-1d36-05798c17d816

verify egress traffic

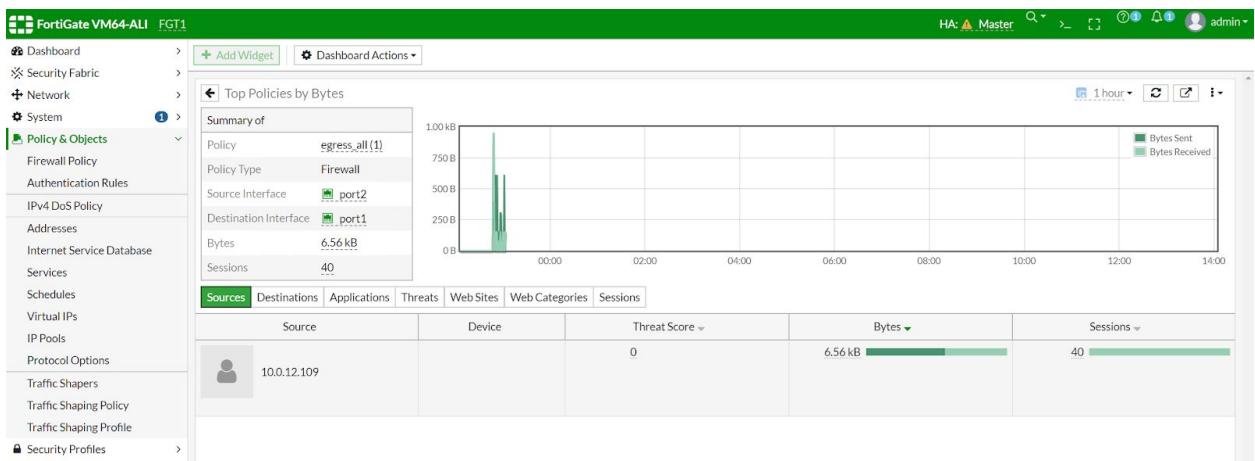
Let's now verify the egress traffic. the web-a shall able to access internet , we can use ping to verify that.

```

root@web-a:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=59 time=1.15 ms
^C
--- 1.1.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.156/1.156/1.156/0.000 ms
root@web-a:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=1.37 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.373/1.373/1.373/0.000 ms
root@web-a:~#

```

you can also show traffic logs from FGT-1.



check Failover interrupt time

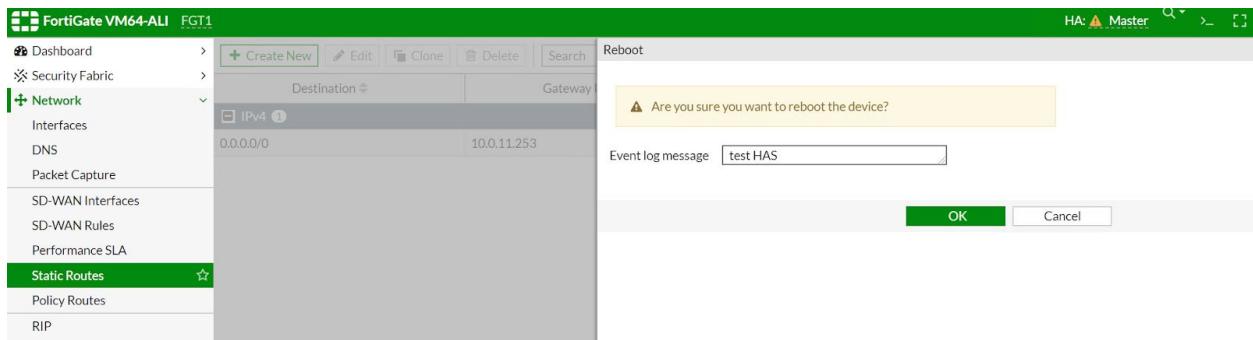
keep ping on web-a, and let's reboot FGT-1 to trigger a switchover. recorder the switch-over time and change of VPC routing table and EIP moving to new master.

1. start ping from web-a console.

```
64 bytes from 1.1.1.1: icmp_seq=53 ttl=59 time=1.14 ms
64 bytes from 1.1.1.1: icmp_seq=54 ttl=59 time=1.13 ms
64 bytes from 1.1.1.1: icmp_seq=55 ttl=59 time=1.15 ms
64 bytes from 1.1.1.1: icmp_seq=56 ttl=59 time=1.11 ms
64 bytes from 1.1.1.1: icmp_seq=57 ttl=59 time=1.13 ms
64 bytes from 1.1.1.1: icmp_seq=58 ttl=59 time=1.21 ms
64 bytes from 1.1.1.1: icmp_seq=59 ttl=59 time=1.13 ms
64 bytes from 1.1.1.1: icmp_seq=60 ttl=59 time=1.13 ms
64 bytes from 1.1.1.1: icmp_seq=61 ttl=59 time=1.13 ms
64 bytes from 1.1.1.1: icmp_seq=62 ttl=59 time=1.14 ms
64 bytes from 1.1.1.1: icmp_seq=63 ttl=59 time=1.13 ms
64 bytes from 1.1.1.1: icmp_seq=64 ttl=59 time=1.14 ms
```

2. reboot FGT-1 from FGT-1 menu

choose Restart FGT-1



ping will interrupt around 24 seconds.

← → ⌂ ⌂ 🔒 ecs-ap-northeast-1.console.aliyun.com/vnc/index.htm?spm=5176.2020520101.107.d515.1cda7d33

download Alibaba Cloud Co... Microsoft Office... Microsoft Teams AlibabaCloud - Qi... Visual Paradigm

Send Remote Call ▾ Successfully connected to the instance.i-6weaynsrm71fm2zhvqxe. Note:.

```
64 bytes from 8.8.8.8: icmp_seq=87 ttl=119 time=1.33 ms
64 bytes from 8.8.8.8: icmp_seq=88 ttl=119 time=1.34 ms
64 bytes from 8.8.8.8: icmp_seq=89 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=90 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=91 ttl=119 time=1.29 ms
64 bytes from 8.8.8.8: icmp_seq=92 ttl=119 time=1.30 ms
64 bytes from 8.8.8.8: icmp_seq=93 ttl=119 time=1.27 ms
64 bytes from 8.8.8.8: icmp_seq=94 ttl=119 time=1.29 ms
64 bytes from 8.8.8.8: icmp_seq=95 ttl=119 time=1.28 ms

64 bytes from 8.8.8.8: icmp_seq=96 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=97 ttl=119 time=1.28 ms

64 bytes from 8.8.8.8: icmp_seq=98 ttl=119 time=1.29 ms
64 bytes from 8.8.8.8: icmp_seq=99 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=100 ttl=119 time=1.27 ms
64 bytes from 8.8.8.8: icmp_seq=101 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=102 ttl=119 time=1.30 ms
64 bytes from 8.8.8.8: icmp_seq=103 ttl=119 time=1.31 ms
64 bytes from 8.8.8.8: icmp_seq=104 ttl=119 time=1.40 ms
64 bytes from 8.8.8.8: icmp_seq=105 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=106 ttl=119 time=1.29 ms
64 bytes from 8.8.8.8: icmp_seq=107 ttl=119 time=1.26 ms
64 bytes from 8.8.8.8: icmp_seq=108 ttl=119 time=1.29 ms
64 bytes from 8.8.8.8: icmp_seq=109 ttl=119 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=110 ttl=119 time=1.27 ms
64 bytes from 8.8.8.8: icmp_seq=111 ttl=119 time=1.27 ms
64 bytes from 8.8.8.8: icmp_seq=112 ttl=119 time=1.29 ms

64 bytes from 8.8.8.8: icmp_seq=136 ttl=119 time=3.67 ms
64 bytes from 8.8.8.8: icmp_seq=137 ttl=119 time=3.62 ms
64 bytes from 8.8.8.8: icmp_seq=138 ttl=119 time=3.64 ms
64 bytes from 8.8.8.8: icmp_seq=139 ttl=119 time=3.68 ms
64 bytes from 8.8.8.8: icmp_seq=140 ttl=119 time=3.68 ms
64 bytes from 8.8.8.8: icmp_seq=141 ttl=119 time=3.64 ms
64 bytes from 8.8.8.8: icmp_seq=142 ttl=119 time=3.61 ms
64 bytes from 8.8.8.8: icmp_seq=143 ttl=119 time=3.55 ms
64 bytes from 8.8.8.8: icmp_seq=144 ttl=119 time=3.60 ms
64 bytes from 8.8.8.8: icmp_seq=145 ttl=119 time=3.61 ms
64 bytes from 8.8.8.8: icmp_seq=146 ttl=119 time=3.60 ms
```

web service back to work at similar time interruption.

← → ⌂ ⌂ Not secure | fortigate.vitaomics.com:8080

download Alibaba Cloud Cons... Microsoft Office Ho... Microsoft Teams AlibabaC

## Directory listing for /

- [.bash\\_history](#)
- [.bashrc](#)
- [.cache/](#)
- [.gnupg/](#)
- [.pip/](#)
- [.profile](#)
- [.pydistutils.cfg](#)
- [.ssh/](#)
- [nohup.out](#)

## Verify the Changes due to Failover

Now let's take a look at the master slave change as well as the routing table and EIP3 moving.

### Master and Slave Role change

FGT-1 now becomes slave , FGT-2 becomes master.

The screenshot shows the HA status for two FortiGate units, FGT1 and FGT2. In the previous state, FGT1 was the Master and FGT2 was the Slave. After the failover, FGT2 has become the Master and FGT1 has become the Slave. The table below details the HA status:

Serial No.	Role	Uptime	Sessions
FGVM1VTM20000859	Slave	00:00:00:55	24
FGVM1VTM20000886	Master	00:00:06:30	60

The screenshot shows the FortiGate HA cluster management interface. On the left, a sidebar menu includes Dashboard, Security Fabric, Network, System (with 1 notification), HA (selected), SNMP, and Replacement Messages. The main area displays two FortiGate VM64-ALI instances in a grid. The top instance, FGT2, is the Master, with Serial No. FGVM1VTM20000886, Role Master, Uptime 00:00:07:13, and Sessions 62. The bottom instance, FGT1, is the Slave, with Serial No. FGVM1VTM20000859, Role Slave, Uptime 00:00:01:39, and Sessions 18. Both instances show a priority of 50 and a hostname of FG[1,2]. A legend indicates green for Synchronized and red for Unsynced.

## EIP3 moving

EIP3 is associated with the Secondary Fortigate instance which is FGT-2.

The screenshot shows the Alibaba Cloud VPC Elastic IP Addresses page. The left sidebar lists VPCs, Route Tables, VSwitches, and Elastic IP Addresses (selected). Under Elastic IP Addresses, it shows Internet Shared Bandwidth, Data Transfer Plan, and NAT Gateway options. The main table lists three Elastic IP Addresses:

	Instance ID/Name	IP Address	Monitor	Bandwidth	Charge Type	Status	Shared Bandwidth/Global Acceleration	Associated Instance	Instance Type
<input type="checkbox"/>	eip-6wei2xf1a3psley1k233g EIP3	47.74.27.198		5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:10 Created	Allocated	Add to Shared Bandwidth Package	eni-6webcif70xe2cb4qvq FG-AP-Secondary-FortiGate-vfjx	ECS Instances
<input type="checkbox"/>	eip-6wei8s3wq1ntla9yo5zc5 EIP2	47.74.16.87		5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:07 Created	Allocated	Add to Shared Bandwidth Package	eni-6webbc0kvu96navn1 mjh4 NAT Mode	Secondary ENI
<input type="checkbox"/>	eip-6web4li698a7y9ml0zfj EIP1	47.74.33.92		5 Mbps Pay By Bandwidth	Pay-As-You-Go Jun 8, 2020, 16:07:04 Created	Allocated	Add to Shared Bandwidth Package	eni-6wed6xaf5cnr1ngu6yl q NAT Mode	Secondary ENI

At the bottom, there are buttons for Unbind, Release, and Remove from Internet Shared Bandwidth.

## VPC custom routing table update

VPC custom routing table 0.0.0.0/0 now point to ENI which attached zone B internal-B switch

Route Table ID: vtb-6we77hc7ujg0bjbmt2oI0

Name: FG-AP-FortiGateEg... Edit

Created At: Jun 8, 2020, 16:07:13

VPC ID: vpc-6we89gg12b2gr73jn57g

Route Table Type: Custom

Description: FortiGate Egress ... Edit

Destination CIDR Block	Status	Next Hop	Type	Description
10.0.11.0/24	Available	-	System	Created with VSwitch(vsw-6we2qrqwikwshmmns4i74) by system.
10.0.12.0/24	Available	-	System	Created with VSwitch(vsw-6wev3ui8fpvgmvidoz5ta) by system.
10.0.13.0/24	Available	-	System	Created with VSwitch(vsw-6weswei60nj2ak05f2ct) by system.
10.0.14.0/24	Available	-	System	Created with VSwitch(vsw-6weg88tusilos74lleye) by system.
10.0.21.0/24	Available	-	System	Created with VSwitch(vsw-6wehzo0440j1ukql2xijg) by system.
10.0.22.0/24	Available	-	System	Created with VSwitch(vsw-6wejmzbcoonbygxpcc2vw5) by system.
10.0.23.0/24	Available	-	System	Created with Vswitch(vsw-6wevz7zgw303gkvpaet) by system.
10.0.24.0/24	Available	-	System	Created with Vswitch(vsw-6we7p17hiwdqjg2cus3gw) by system.
100.64.0.0/10	Available	-	System	Created by system.
0.0.0.0/0	Available	eni-6weiwdqj7w5rsn79s7n8	<span>Delete</span>	Custom

## Terraform code for automating the deployment

if you want to use terraform instead GUI to deploy the resource. clone the code below

[https://github.com/yagosys/fortigate\\_aliyun/tree/master/AP-CrossZone](https://github.com/yagosys/fortigate_aliyun/tree/master/AP-CrossZone)

optional

Connect Fortigate to FortiManager Cloud

obtain FortiManager Cloud license.

The screenshot shows the FortiCloud Customer Service & Support website at https://support.fortinet.com/Main.aspx. The main navigation bar includes Home, Asset, Assistance, and Download. A sidebar on the right provides links to various support and management tools under categories like SUPPORT AND SETTINGS, CLOUD MANAGEMENT, and CLOUD SERVICE.

## Setup FortiGate

The screenshot shows the FortiGate VM64-ALI FGT1 configuration interface at https://47.74.33.92/ng/fabric-connector. The left sidebar lists various configuration sections. The Fabric Connectors section is currently selected. The main panel displays Core Network Security and Other Fortinet Products. The FortiManager Cloud option is highlighted with a green border.

The screenshot shows the FortiGate UI with the URL <https://47.74.33.92/ng/fabric-connector/edit/fortimanager/FortiManager Cloud>. The left sidebar has sections like Dashboard, Security Fabric (Physical Topology, Logical Topology, Security Rating, Automation), and Fabric Connectors (External Connectors, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, Log & Report). The main content area is titled 'Edit Fabric Connector' under 'Other Fortinet Products'. It shows a FortiManager icon and settings for 'FortiManager Settings': Status (Enabled), Type (FortiManager Cloud selected), and Mode (Normal selected).

The screenshot shows the FortiGate CLI Console with the title 'CLI Console'. The user is in HA mode, Master. The command history shows:

```
FGT1 # config system central-management
FGT1 (central-management) # show
config system central-management
    set type fortimanager
    set fmg "fortimanager.forticloud.com"
end
FGT1 (central-management) #
```

config fortimanager

then go to fortimanager cloud to config fortimanager to authorize this fortigate.

The screenshot shows the FortiManager Cloud interface. At the top, there's a navigation bar with links for Device Manager, Device & Groups, Firmware, License, Provisioning Templates, Scripts, SD-WAN, Add Device, Device Group, Install Wizard, Tools, and Table View. The main area is titled "Managed Devices" and shows a table with the following data:

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
FGT1	Synchronized	FGT1	FortiGate 6.2.0.build1579 (GA)	FGT1	10.10.0.209	FortiGate-VM64-AU	

Below the table, there's a search bar with the placeholder "Search..." and a small icon, followed by a list item "FGT1".