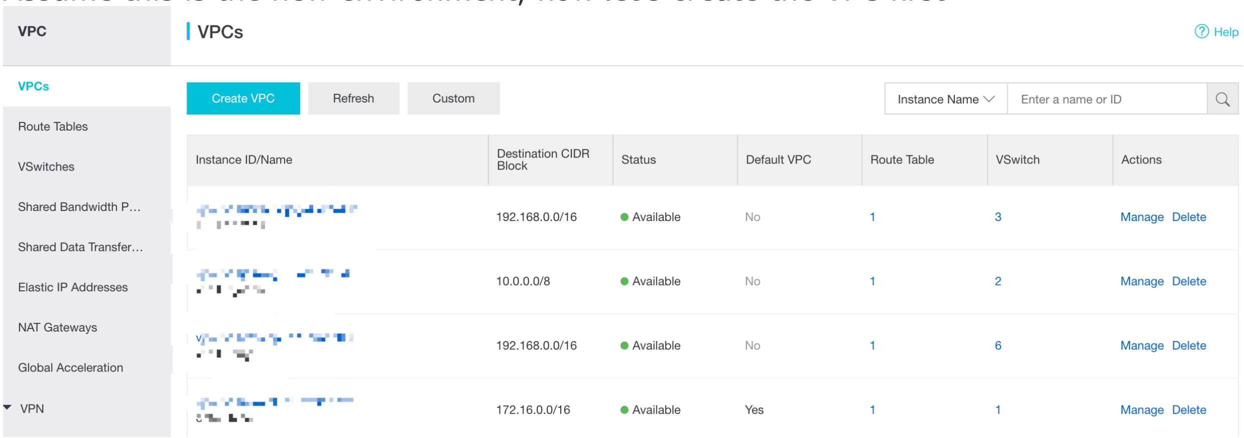
FortiGate-Aliyun

Deployment Guide

Table of Contents

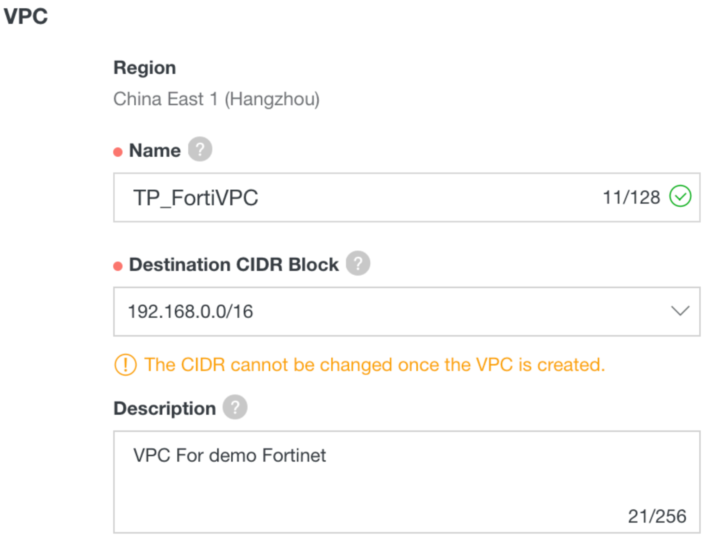
Setup Virtual Private Cloud (VPC)

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



Instance ID/Name	Destination CIDR Block	Status	Default VPC	Route Table	VSwitch	Actions
[redacted]	192.168.0.0/16	● Available	No	1	3	Manage Delete
[redacted]	10.0.0.0/8	● Available	No	1	2	Manage Delete
[redacted]	192.168.0.0/16	● Available	No	1	6	Manage Delete
[redacted]	172.16.0.0/16	● Available	Yes	1	1	Manage Delete

2. The VPC named TP_FortiVPC



VPC

Region
China East 1 (Hangzhou)

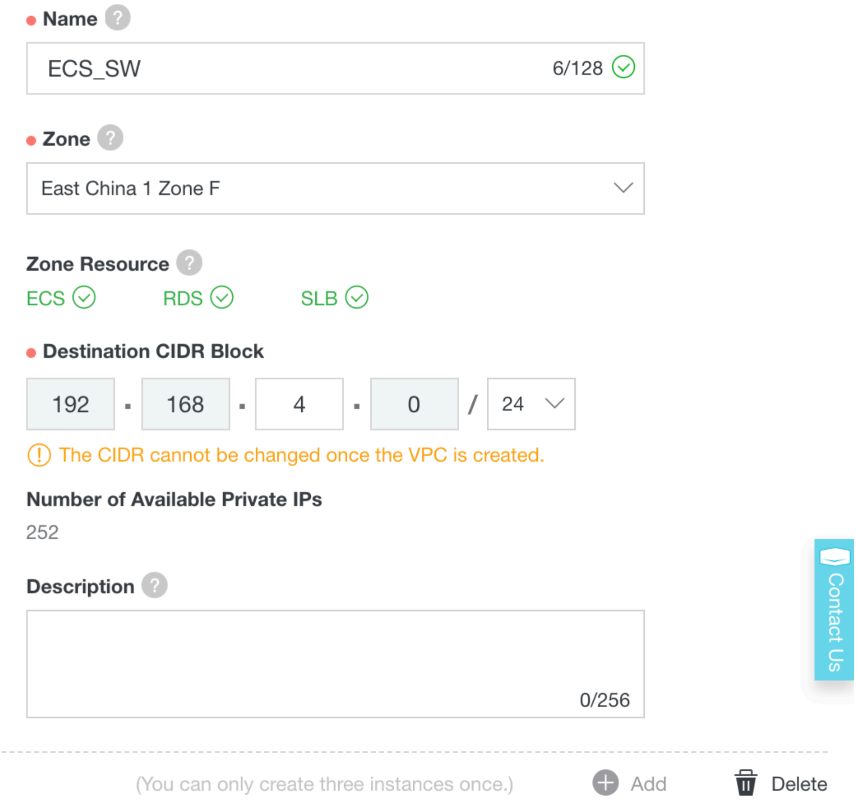
● **Name**
TP_FortiVPC 11/128

● **Destination CIDR Block**
192.168.0.0/16

The CIDR cannot be changed once the VPC is created.

Description
VPC For demo Fortinet 21/256

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



● Name ?

ECS_SW 6/128 ✓

● Zone ?

East China 1 Zone F

Zone Resource ?

ECS ✓ RDS ✓ SLB ✓

● Destination CIDR Block

192 . 168 . 4 . 0 / 24

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

Number of Available Private IPs

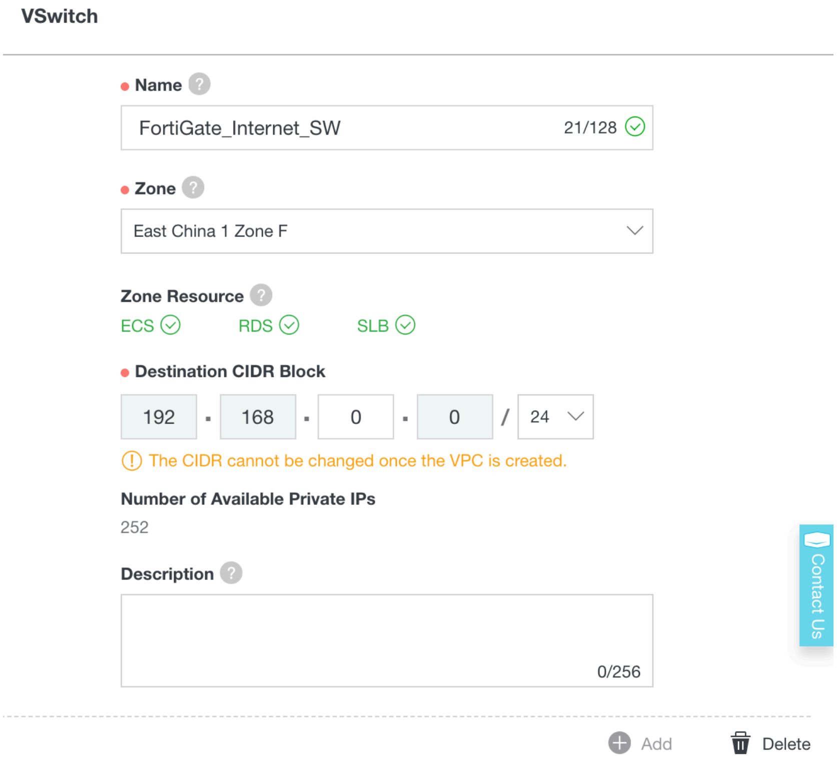
252

Description ?

0/256

(You can only create three instances once.)

4. And this is the VSwitch for keeping the FortiGate VM Inbound/Outbound interface



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.

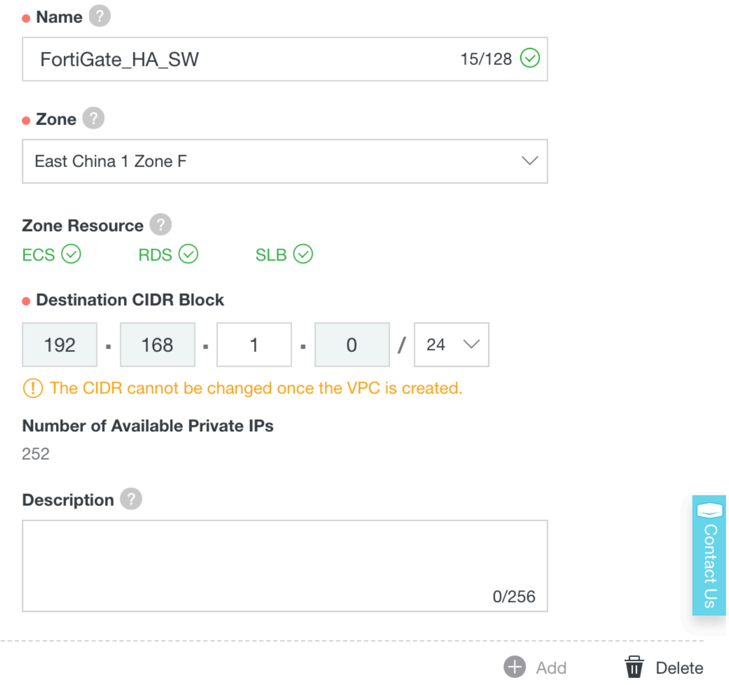
Number of Available Private IPs

252

Description ?

0/256

5. And this is the VSwitch for keeping the FortiGate VM HA interface



● Name ?

FortiGate_HA_SW 15/128 ✓

● Zone ?

East China 1 Zone F

Zone Resource ?

ECS ✓ RDS ✓ SLB ✓

● Destination CIDR Block

192 . 168 . 1 . 0 / 24

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

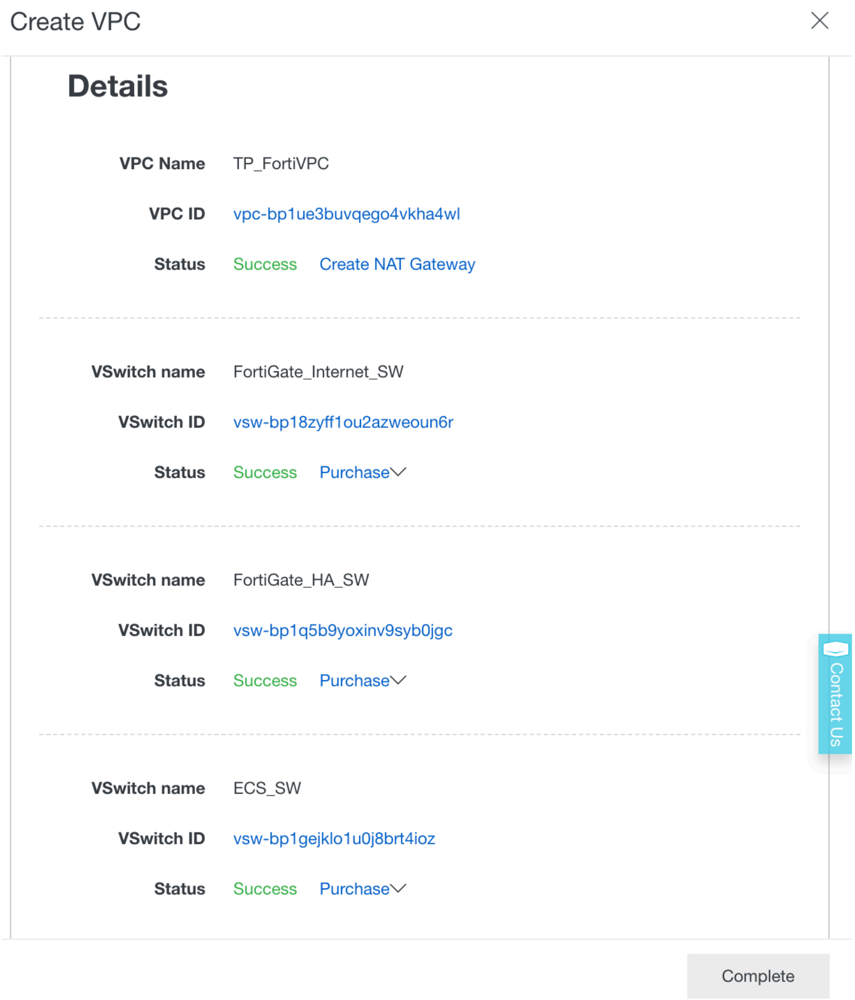
Number of Available Private IPs

252

Description ?

0/256

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



Create VPC

Details

VPC Name TP_FortiVPC

VPC ID vpc-bp1ue3buvqego4vkha4wl

Status Success Create NAT Gateway

VSwitch name FortiGate_Internet_SW

VSwitch ID vsw-bp18zyff1ou2azweoun6r

Status Success Purchase

VSwitch name FortiGate_HA_SW

VSwitch ID vsw-bp1q5b9yoxinv9syb0jgc

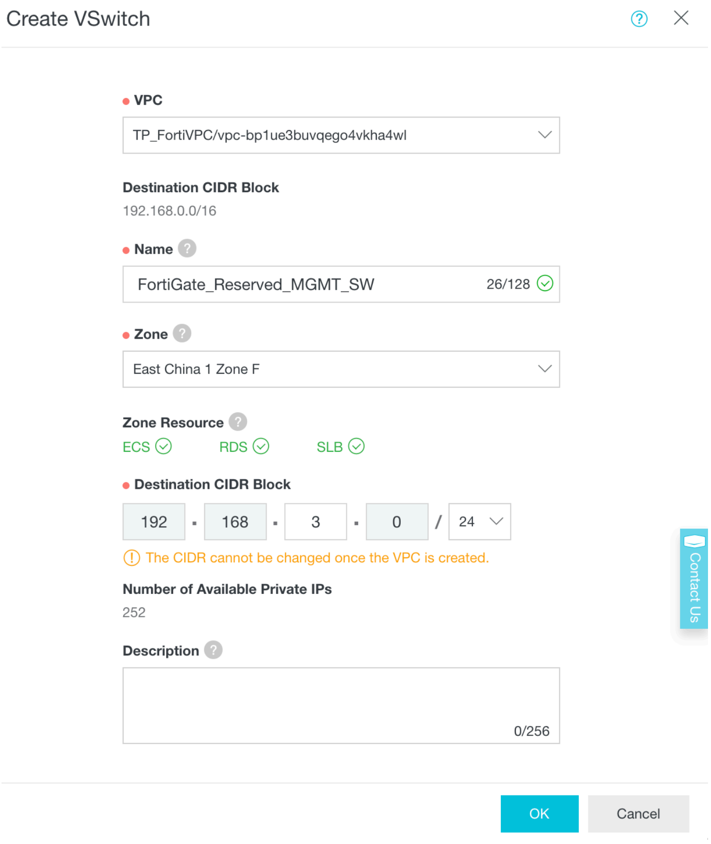
Status Success Purchase

VSwitch name ECS_SW

VSwitch ID vsw-bp1gejklo1u0j8brt4ioz

Status Success Purchase

7. (optional) Create one more VSwitch for 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

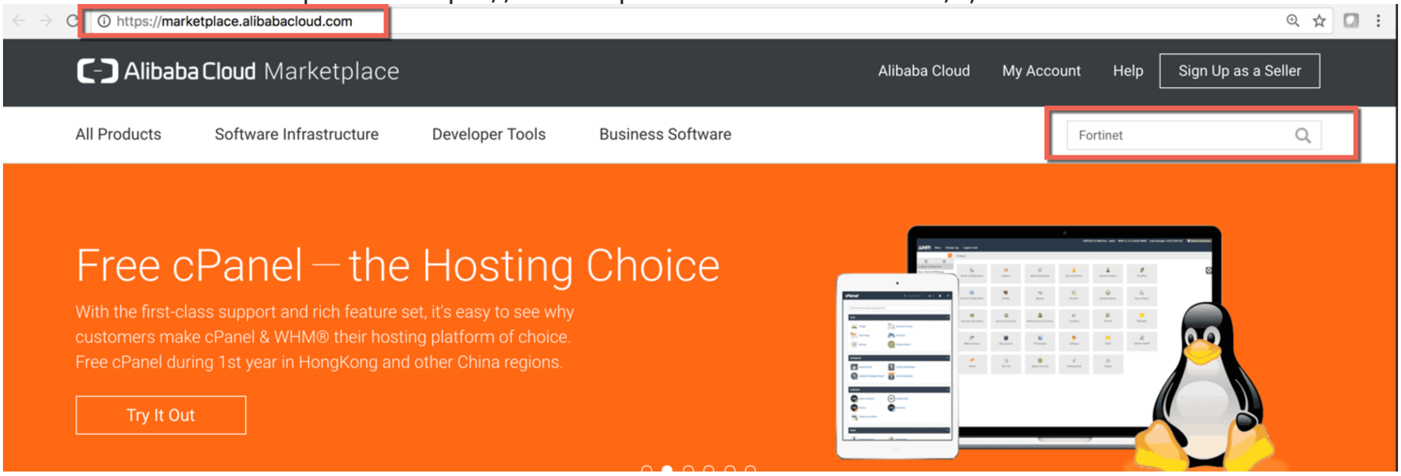
252

Description

0/256

Subscribe to the Fortinet VM in marketplace

8. Access to our marketplace : https://marketplace.alibabacloud.com/ , and search for Fortinet



https://marketplace.alibabacloud.com

Alibaba Cloud Marketplace

Alibaba Cloud | My Account | Help | Sign Up as a Seller

All Products | Software Infrastructure | Developer Tools | Business Software

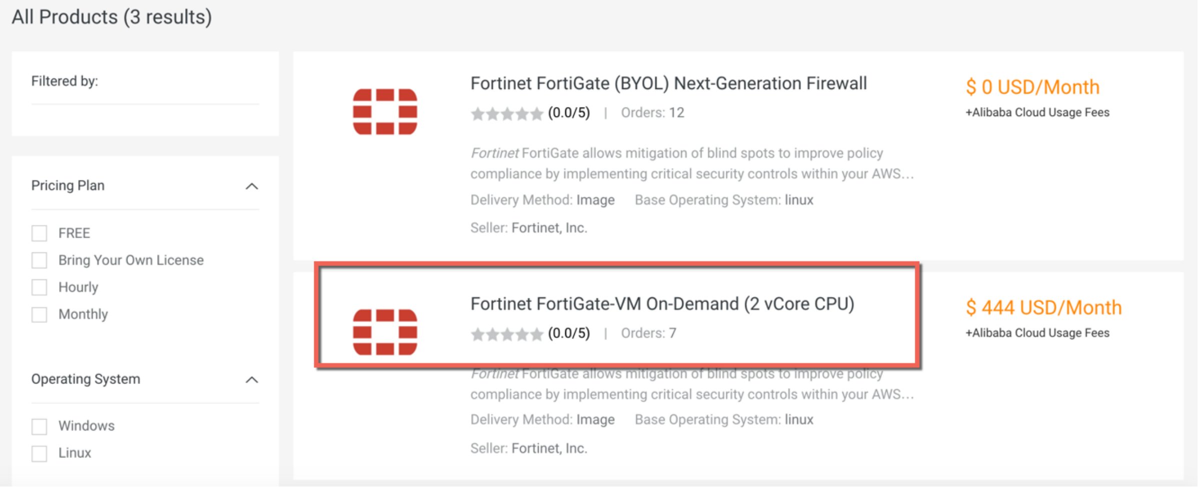
Fortinet

Free cPanel — the Hosting Choice

With the first-class support and rich feature set, it's easy to see why customers make cPanel & WHM® their hosting platform of choice. Free cPanel during 1st year in HongKong and other China regions.

Try It Out

9. If customer has their own FortiGate license they can choose the BYOL image, otherwise they can use On-Demand image offered



All Products (3 results)

Filtered by:

Pricing Plan

□ FREE
□ Bring Your Own License
□ Hourly
□ Monthly

Operating System

□ Windows
□ Linux

Fortinet FortiGate (BYOL) Next-Generation Firewall

(0.0/5) | Orders: 12

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

Delivery Method: Image Base Operating System: linux

Seller: Fortinet, Inc.

$ 0 USD/Month

+Alibaba Cloud Usage Fees

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

(0.0/5) | Orders: 7

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

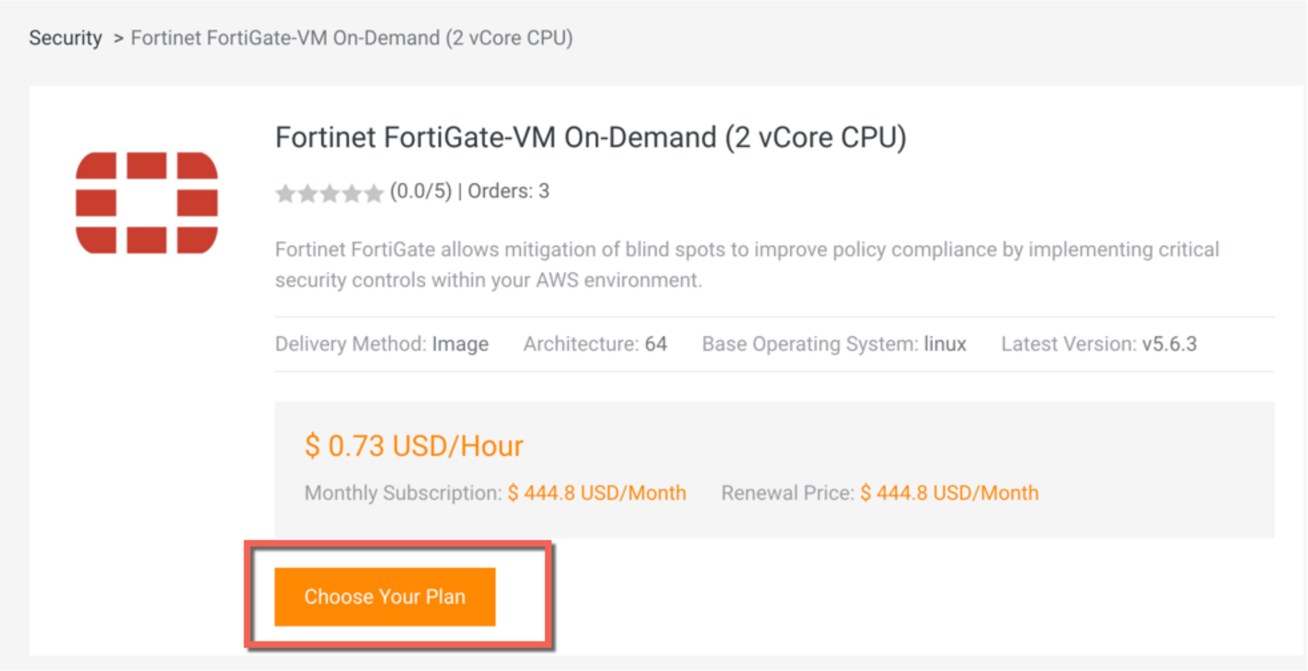
Delivery Method: Image Base Operating System: linux

Seller: Fortinet, Inc.

$ 444 USD/Month

+Alibaba Cloud Usage Fees

10. Click "Choose Your Plan" to continue



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

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

☆☆☆☆☆ (0.0/5) | Orders: 3

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

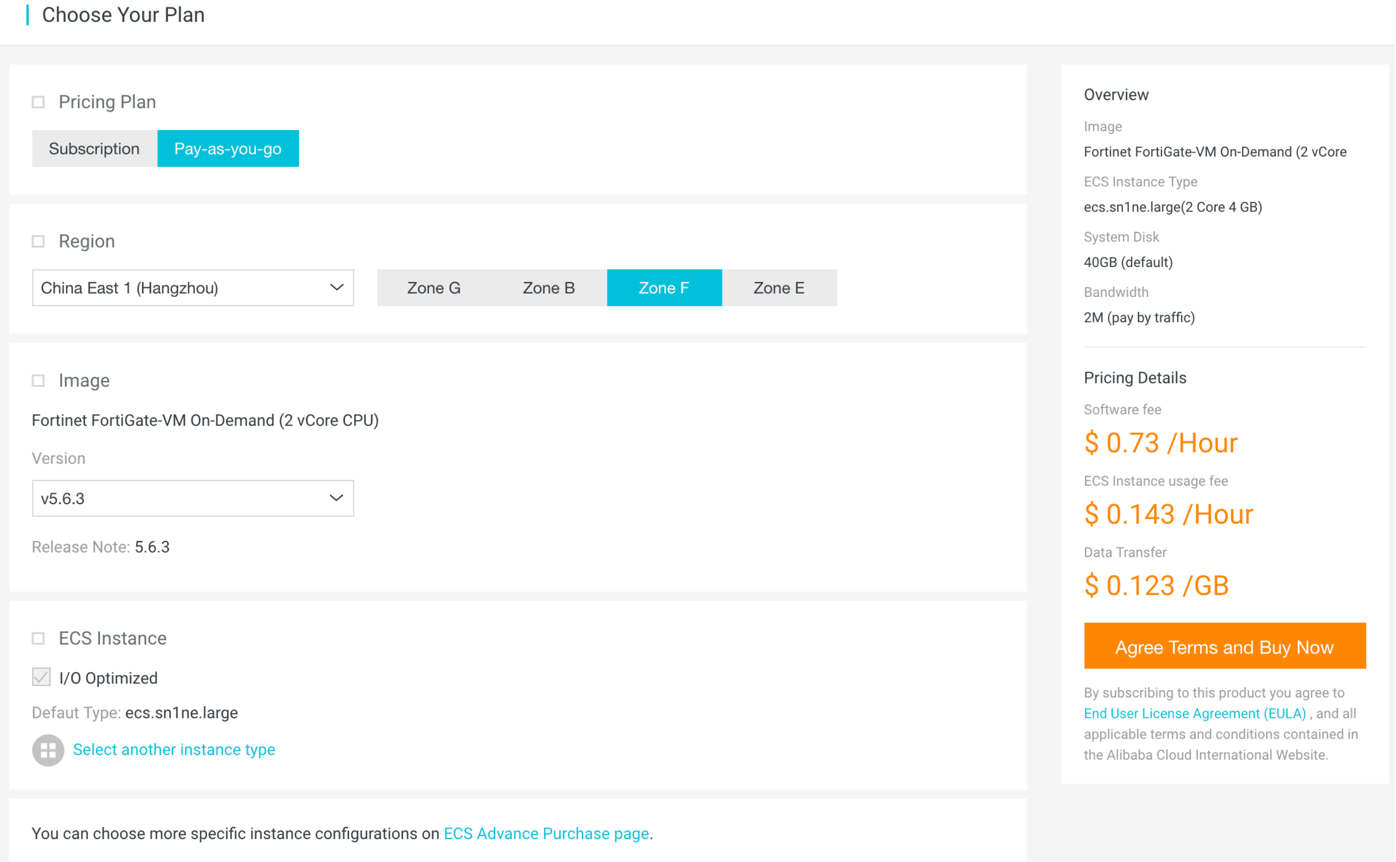
Delivery Method: Image Architecture: 64 Base Operating System: linux Latest Version: v5.6.3

$ 0.73 USD/Hour

Monthly Subscription: $ 444.8 USD/Month Renewal Price: $ 444.8 USD/Month

Choose Your Plan

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



Choose Your Plan

□ Pricing Plan

Subscription | Pay-as-you-go

□ Region

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

□ Image

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

Version

v5.6.3

Release Note: 5.6.3

□ ECS Instance

☑ I/O Optimized

Defaut Type: ecs.sn1ne.large

Select another instance type

You can choose more specific instance configurations on ECS Advance Purchase page.

Overview

Image

Fortinet FortiGate-VM On-Demand (2 vCore

ECS Instance Type

ecs.sn1ne.large(2 Core 4 GB)

System Disk

40GB (default)

Bandwidth

2M (pay by traffic)

Pricing Details

Software fee

$ 0.73 /Hour

ECS Instance usage fee

$ 0.143 /Hour

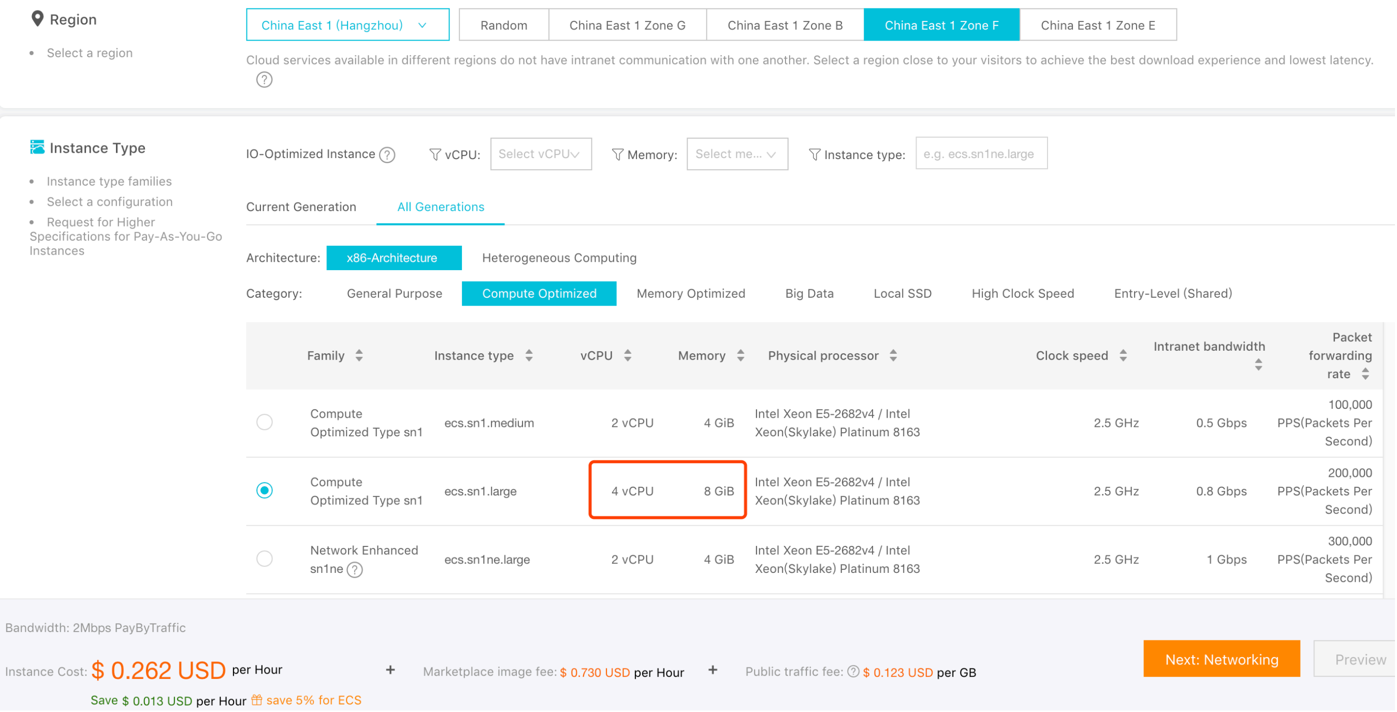
Data Transfer

$ 0.123 /GB

Agree Terms and Buy Now

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

12. Click 4 vCPU ECS type to launch the FortiGate instance (*4 vCPU ECS can support maximum 3 NIC, 2 vCPU can support 2 NIC, so if you need FortiGate reserved management interface, please select 4 vCPU ECS type.*)



Region
- Select a region

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

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

Instance Type
- Instance type families
- Select a configuration
- Request for Higher Specifications for Pay-As-You-Go Instances

IO-Optimized Instance ⓘ vCPU: Select vCPU Memory: Select me... Instance type: e.g. ecs.sn1ne.large

Current Generation | All Generations

Architecture: x86-Architecture | Heterogeneous Computing

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

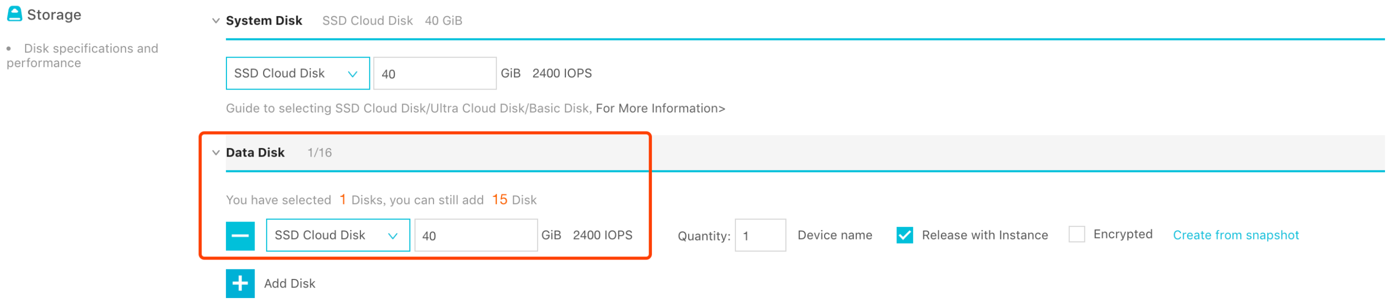
	Family	Instance type	vCPU	Memory	Physical processor	Clock speed	Intranet bandwidth	Packet forwarding rate
○	Compute Optimized Type sn1	ecs.sn1.medium	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps	100,000 PPS(Packets Per Second)
●	Compute Optimized Type sn1	ecs.sn1.large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

Bandwidth: 2Mbps PayByTraffic

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

Save $ 0.013 USD per Hour save 5% for ECS

13. Add a data disk for the Log (Suggest to use SSD for better performance)



Storage
- Disk specifications and performance

System Disk SSD Cloud Disk 40 GiB

SSD Cloud Disk | 40 | GiB 2400 IOPS

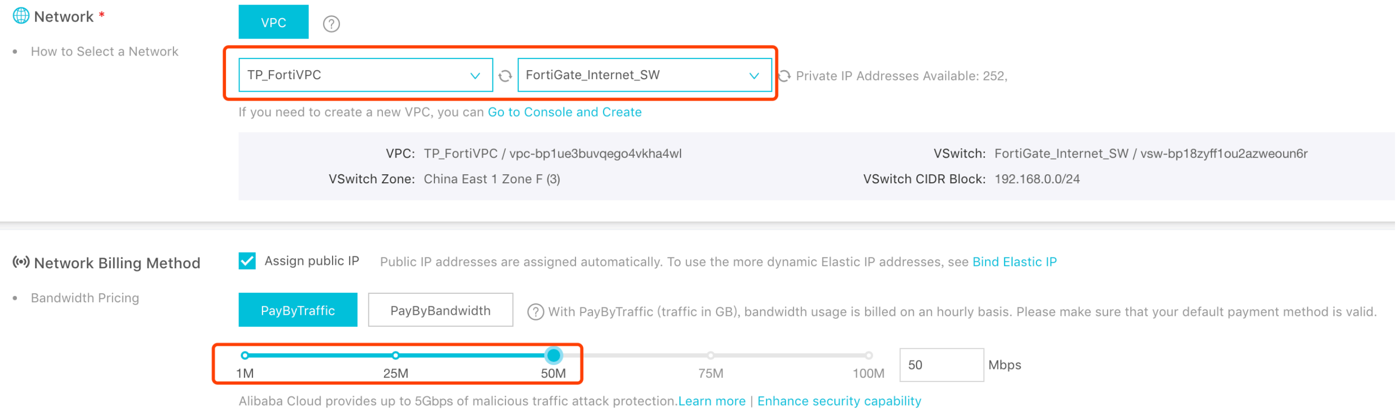
Guide to selecting SSD Cloud Disk/Ultra Cloud Disk/Basic Disk, For More Information>

Data Disk 1/16

You have selected 1 Disks, you can still add 15 Disk

SSD Cloud Disk | 40 | GiB 2400 IOPS Quantity: 1 Device name ☑ Release with Instance ☐ Encrypted Create from snapshot

14. Choose the TP_FortiVPC and FortiGate_internet_SW in Network section, also assign the Public IP to the image, this NIC will be port1 on FortiGate_VM, the default ENI.



Network *
- How to Select a Network

VPC ⓘ

TP_FortiVPC | FortiGate_Internet_SW | Private IP Addresses Available: 252,

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

VPC: TP_FortiVPC / vpc-bp1ue3buvqego4vkha4wl VSwitch: FortiGate_Internet_SW / vsw-bp18zyff1ou2azweoun6r

VSwitch Zone: China East 1 Zone F (3) VSwitch CIDR Block: 192.168.0.0/24

Network Billing Method
- Bandwidth Pricing

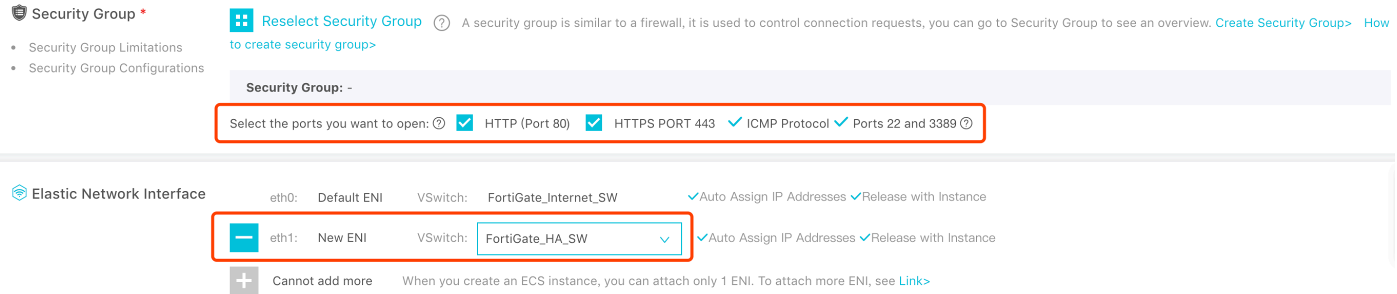
☑ Assign public IP Public IP addresses are assigned automatically. To use the more dynamic Elastic IP addresses, see Bind Elastic IP

PayByTraffic | PayByBandwidth ⓘ With PayByTraffic (traffic in GB), bandwidth usage is billed on an hourly basis. Please make sure that your default payment method is valid.

50 Mbps

Alibaba Cloud provides up to 5Gbps of malicious traffic attack protection.Learn more | Enhance security capability

15. Leave HTTPS/ICMP/SSH ports open to allow connect, and add one more ENI which is on 'FortiGate_HA_SW', this ENI will be port2 on FortiGate.



Security Group *

- Security Group Limitations
- Security Group Configurations

Reselect Security Group ⓘ A security group is similar to a firewall, it is used to control connection requests, you can go to Security Group to see an overview. Create Security Group> How to create security group>

Security Group: -

Select the ports you want to open: ⓘ ☑ HTTP (Port 80) ☑ HTTPS PORT 443 ✓ ICMP Protocol ✓ Ports 22 and 3389 ⓘ

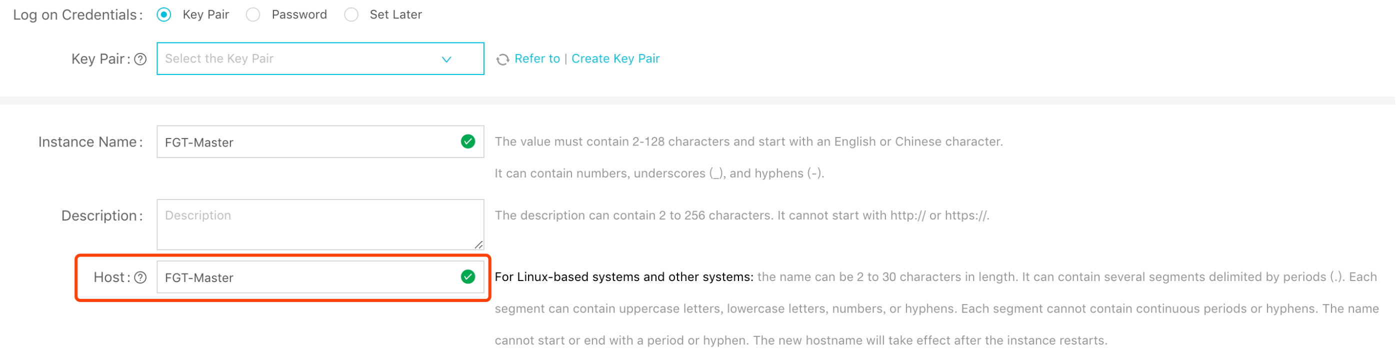
Elastic Network Interface

eth0: Default ENI VSwitch: FortiGate_Internet_SW ✓Auto Assign IP Addresses ✓Release with Instance

eth1: New ENI VSwitch: FortiGate_HA_SW ✓Auto Assign IP Addresses ✓Release with Instance

Cannot add more When you create an ECS instance, you can attach only 1 ENI. To attach more ENI, see Link>

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



Log on Credentials: ● Key Pair ○ Password ○ Set Later

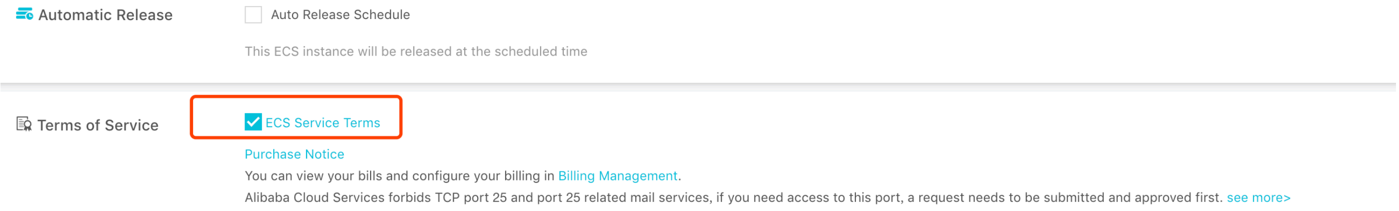
Key Pair: ⓘ Select the Key Pair Refer to | Create Key Pair

Instance Name: FGT-Master The value must contain 2-128 characters and start with an English or Chinese character. It can contain numbers, underscores (_), and hyphens (-).

Description: Description The description can contain 2 to 256 characters. It cannot start with http:// or https://.

Host: ⓘ FGT-Master For Linux-based systems and other systems: the name can be 2 to 30 characters in length. It can contain several segments delimited by periods (.). Each segment can contain uppercase letters, lowercase letters, numbers, or hyphens. Each segment cannot contain continuous periods or hyphens. The name cannot start or end with a period or hyphen. The new hostname will take effect after the instance restarts.

17. Click 'ECS Service Terms'



Automatic Release ☐ Auto Release Schedule

This ECS instance will be released at the scheduled time

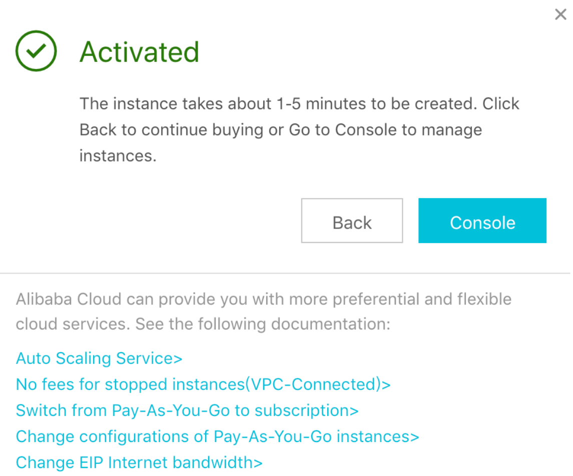
Terms of Service ☑ ECS Service Terms

Purchase Notice

You can view your bills and configure your billing in Billing Management.

Alibaba Cloud Services forbids TCP port 25 and port 25 related mail services, if you need access to this port, a request needs to be submitted and approved first. see more>

18. Click Console and back to the ECS instance list



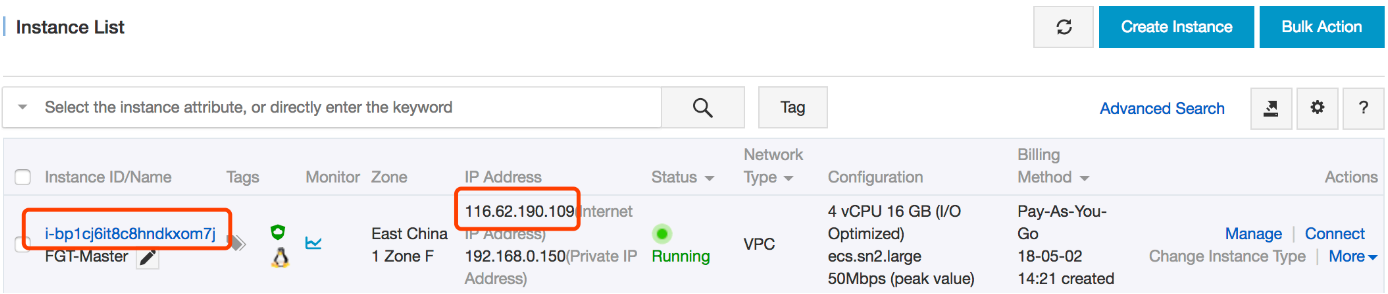
Activated

The instance takes about 1-5 minutes to be created. Click Back to continue buying or Go to Console to manage instances.

Alibaba Cloud can provide you with more preferential and flexible cloud services. See the following documentation:

Auto Scaling Service>
No fees for stopped instances(VPC-Connected)>
Switch from Pay-As-You-Go to subscription>
Change configurations of Pay-As-You-Go instances>
Change EIP Internet bandwidth>

19. You will see the VM created, mark down the Public IP and the instance ID (this will be FortiGate default password) and you will use later



Instance List

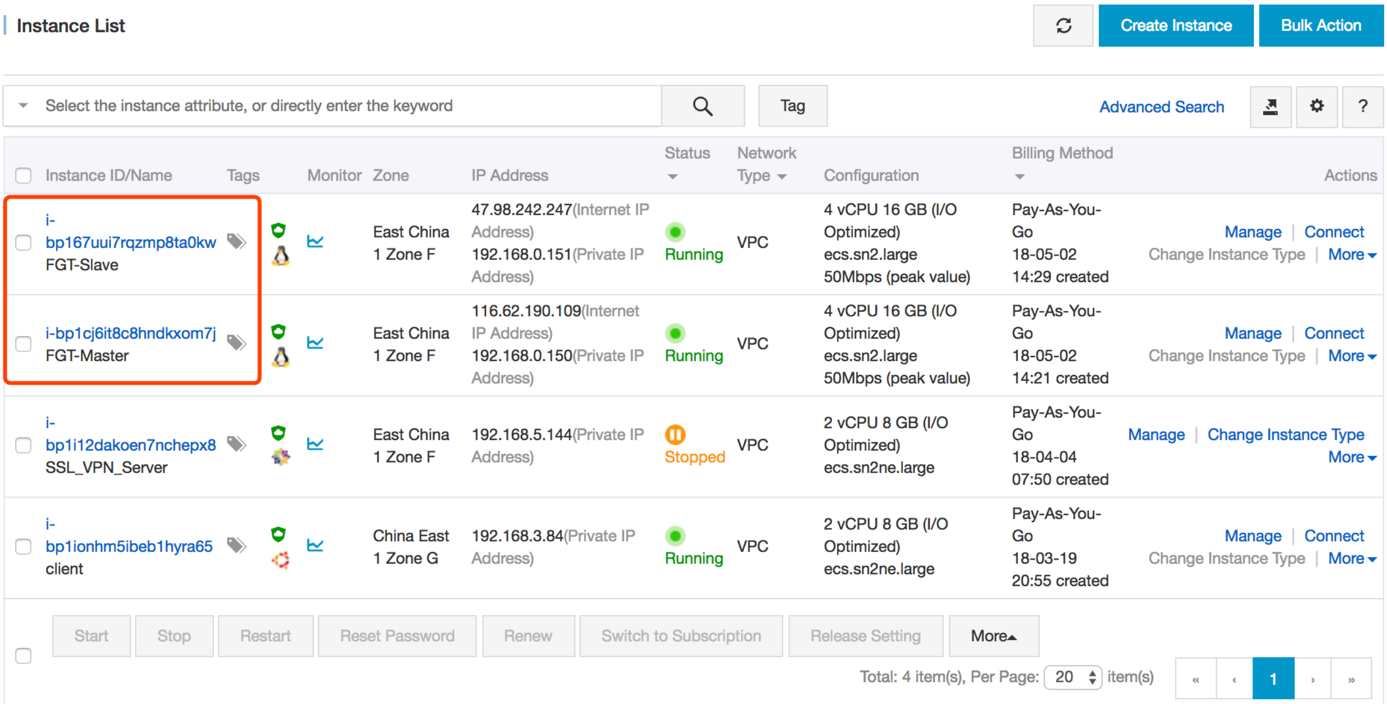
Create Instance | Bulk Action

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

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

i-bp1cj6it8c8hndkxom7j
FGT-Master
			East China 1 Zone F	116.62.190.109(Internet IP Address)
				192.168.0.150(Private IP Address)
					Running	VPC	4 vCPU 16 GB (I/O Optimized)
							ecs.sn2.large
							50Mbps (peak value)
								Pay-As-You-Go
								18-05-02 14:21 created
									Manage | Connect
									Change Instance Type | More

20. Please repeat step 7-17 to create one more FortiGate instance, which name is FGT-Slave.



Instance List

Create Instance | Bulk Action

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

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

i-bp167uui7rqzmp8ta0kw
FGT-Slave
			East China 1 Zone F	47.98.242.247(Internet IP Address)
				192.168.0.151(Private IP Address)
					Running	VPC	4 vCPU 16 GB (I/O Optimized)
							ecs.sn2.large
							50Mbps (peak value)
								Pay-As-You-Go
								18-05-02 14:29 created
									Manage | Connect
									Change Instance Type | More

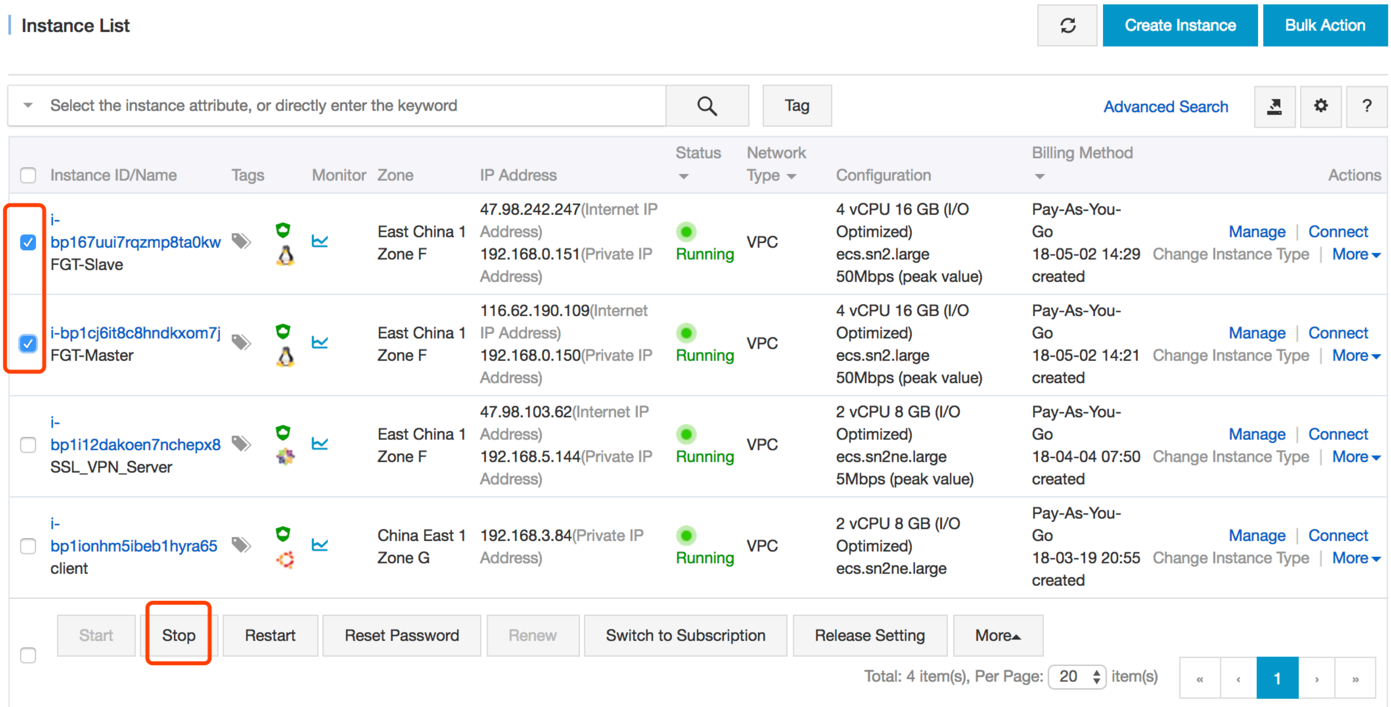
i-bp1cj6it8c8hndkxom7j
FGT-Master
			East China 1 Zone F	116.62.190.109(Internet IP Address)
				192.168.0.150(Private IP Address)
					Running	VPC	4 vCPU 16 GB (I/O Optimized)
							ecs.sn2.large
							50Mbps (peak value)
								Pay-As-You-Go
								18-05-02 14:21 created
									Manage | Connect
									Change Instance Type | More

i-bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	192.168.5.144(Private IP Address)	Stopped	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-04-04 07:50 created	Manage | Change Instance Type More
i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage | Connect Change Instance Type | More

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

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

21. (Optional) Stop those two FortiGate instances



Instance List

Create Instance | Bulk Action

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

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

☑	i-bp167uui7rqzmp8ta0kw
	FGT-Slave
				East China 1 Zone F	47.98.242.247(Internet IP Address)
					192.168.0.151(Private IP Address)
						Running	VPC	4 vCPU 16 GB (I/O Optimized)
								ecs.sn2.large
								50Mbps (peak value)
									Pay-As-You-Go
									18-05-02 14:29 created
										Manage | Connect
										Change Instance Type | More

☑	i-bp1cj6it8c8hndkxom7j
	FGT-Master
				East China 1 Zone F	116.62.190.109(Internet IP Address)
					192.168.0.150(Private IP Address)
						Running	VPC	4 vCPU 16 GB (I/O Optimized)
								ecs.sn2.large
								50Mbps (peak value)
									Pay-As-You-Go
									18-05-02 14:21 created
										Manage | Connect
										Change Instance Type | More

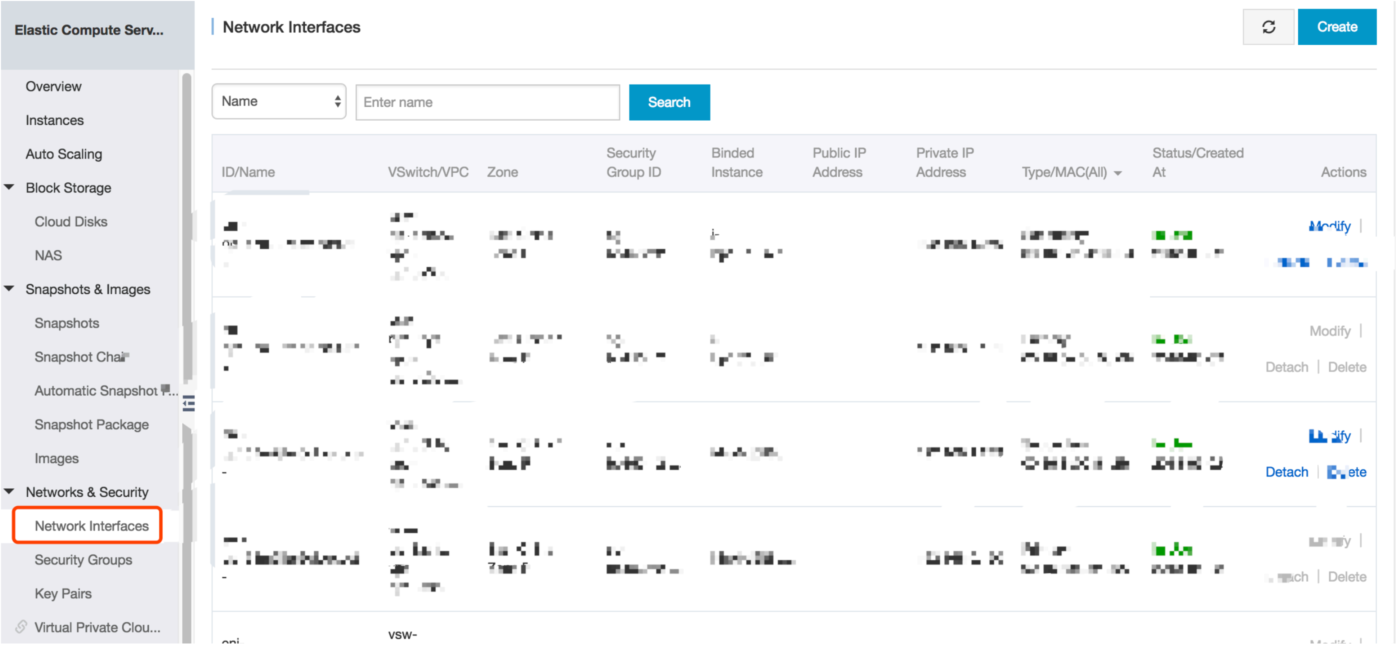
□	i-bp1i12dakoen7nchepx8
	SSL_VPN_Server
				East China 1 Zone F	47.98.103.62(Internet IP Address)
					192.168.5.144(Private IP Address)
						Running	VPC	2 vCPU 8 GB (I/O Optimized)
								ecs.sn2ne.large
								5Mbps (peak value)
									Pay-As-You-Go
									18-04-04 07:50 created
										Manage | Connect
										Change Instance Type | More

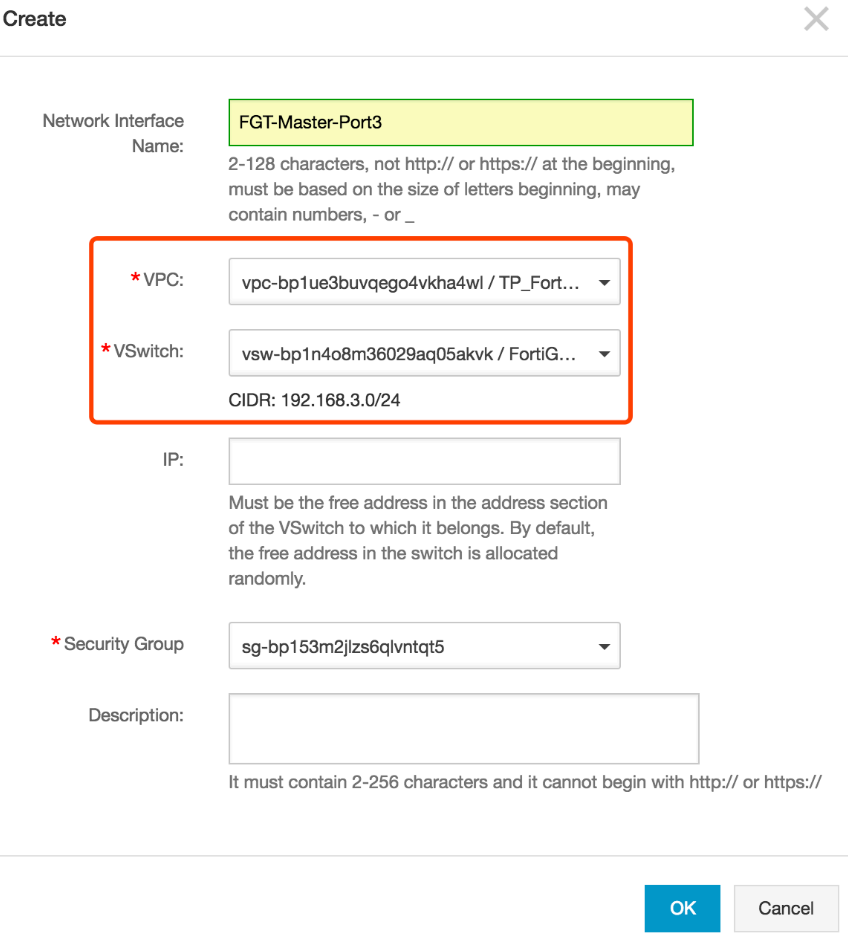
□	i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage | Connect Change Instance Type | More

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

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

22. (Optional) Go to 'Networks Interfaces' page to create two ENI, and then attach the ENI on each FortiGate instance.





Create

Network Interface Name: FGT-Master-Port3

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

*VPC: vpc-bp1ue3buvqego4vkha4wl / TP_Fort...

*VSwitch: vsw-bp1n4o8m36029aq05akvk / FortiG...

CIDR: 192.168.3.0/24

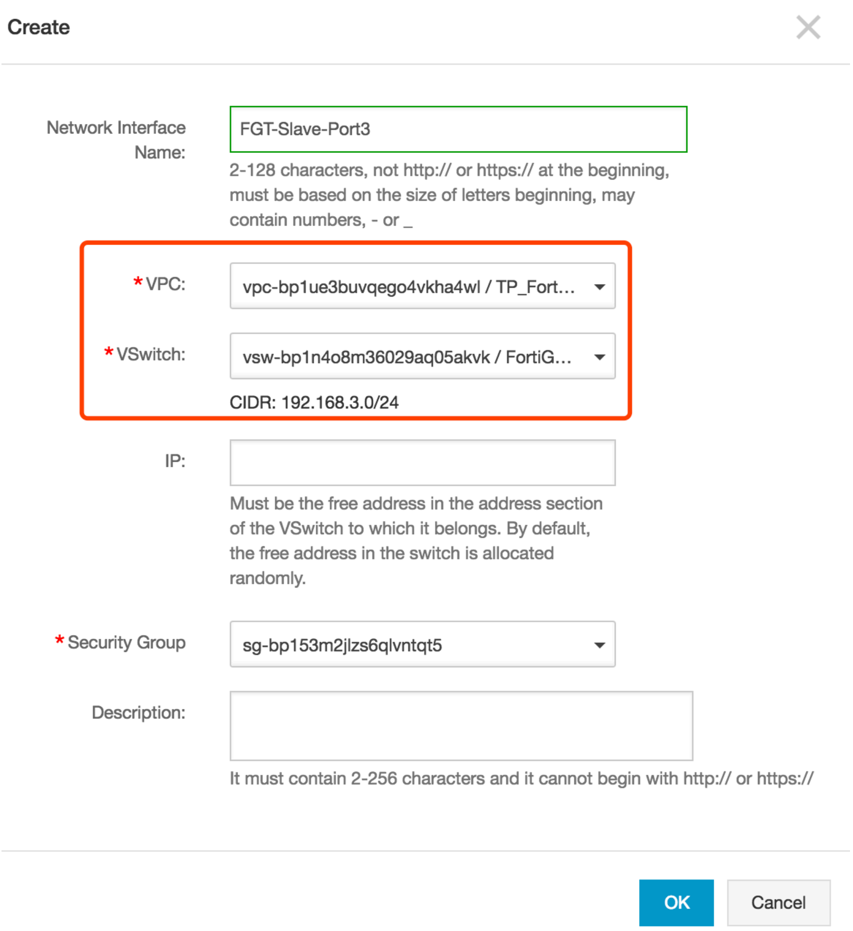
IP:

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

*Security Group: sg-bp153m2jlzs6qlvntqt5

Description:

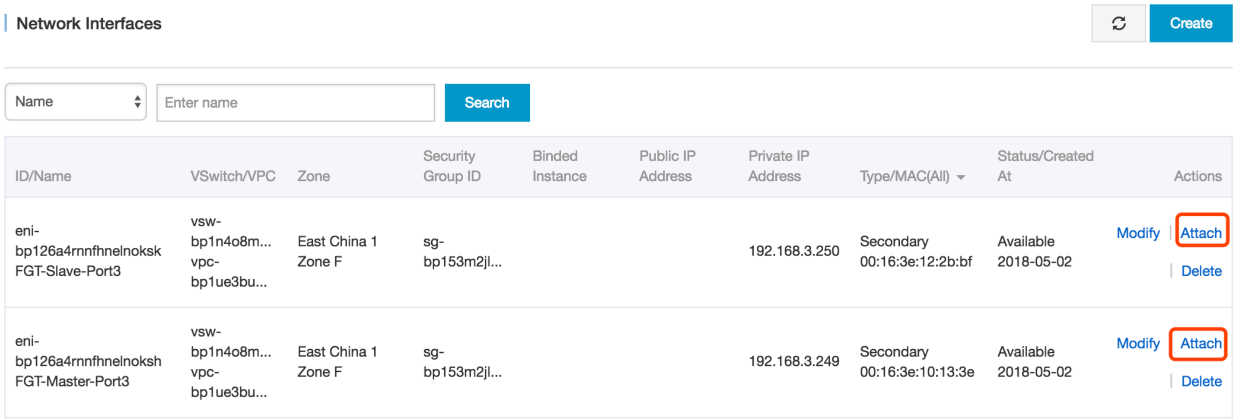
It must contain 2-256 characters and it cannot begin with http:// or https://



Create

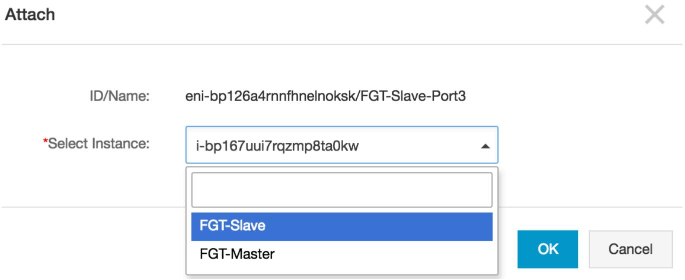
Network Interface Name:	FGT-Slave-Port3 2-128 characters, not http:// or https:// at the beginning, must be based on the size of letters beginning, may contain numbers, - or _
*VPC:	vpc-bp1ue3buvqego4vkha4wl / TP_Fort…
*VSwitch:	vsw-bp1n4o8m36029aq05akvk / FortiG… CIDR: 192.168.3.0/24
IP:	Must be the free address in the address section of the VSwitch to which it belongs. By default, the free address in the switch is allocated randomly.
*Security Group	sg-bp153m2jlzs6qlvntqt5
Description:	It must contain 2-256 characters and it cannot begin with http:// or https://

23.(Optional) Attach those two new ENI to two FortiGate.



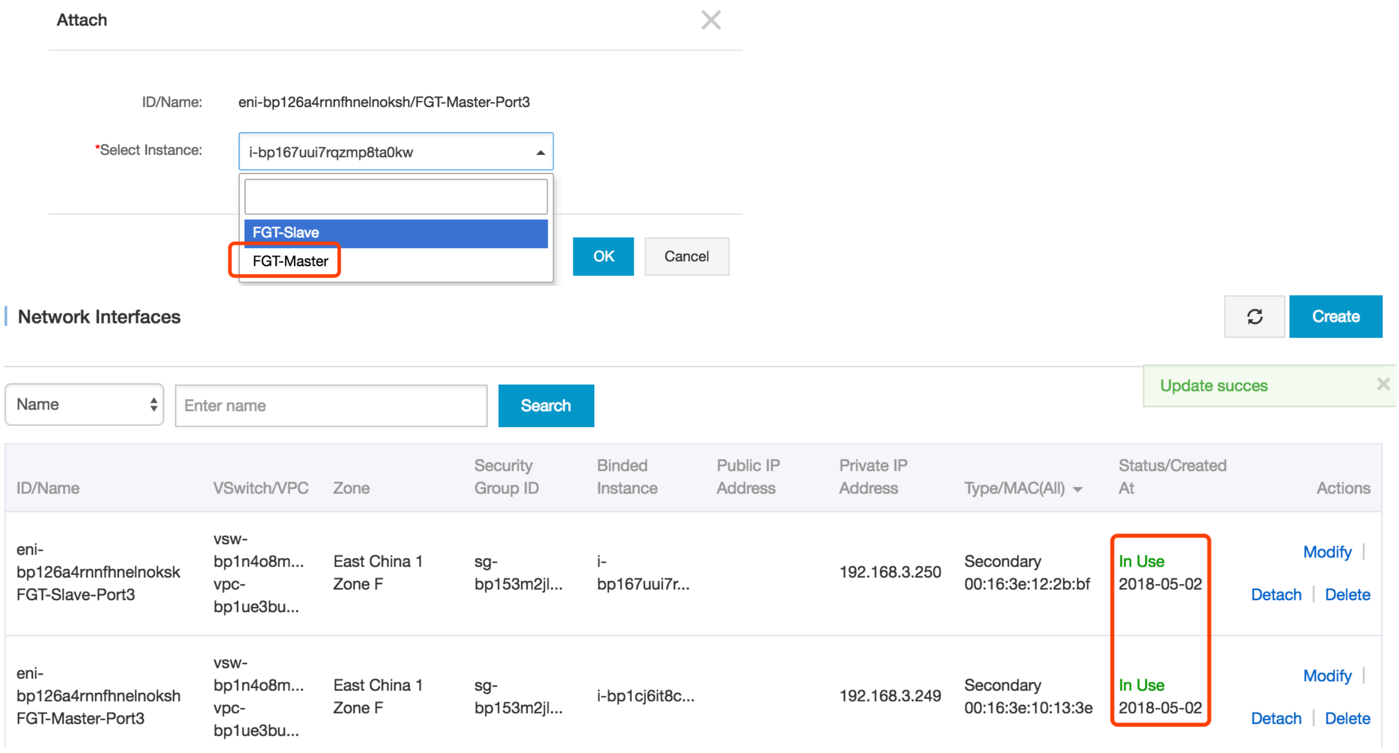
Network Interfaces

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



Attach

ID/Name:	eni-bp126a4rnnfhnelnoksk/FGT-Slave-Port3
*Select Instance:	i-bp167uui7rqzmp8ta0kw



Attach

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

*Select Instance: i-bp167uui7rqzmp8ta0kw

FGT-Slave

FGT-Master

OK Cancel

Network Interfaces

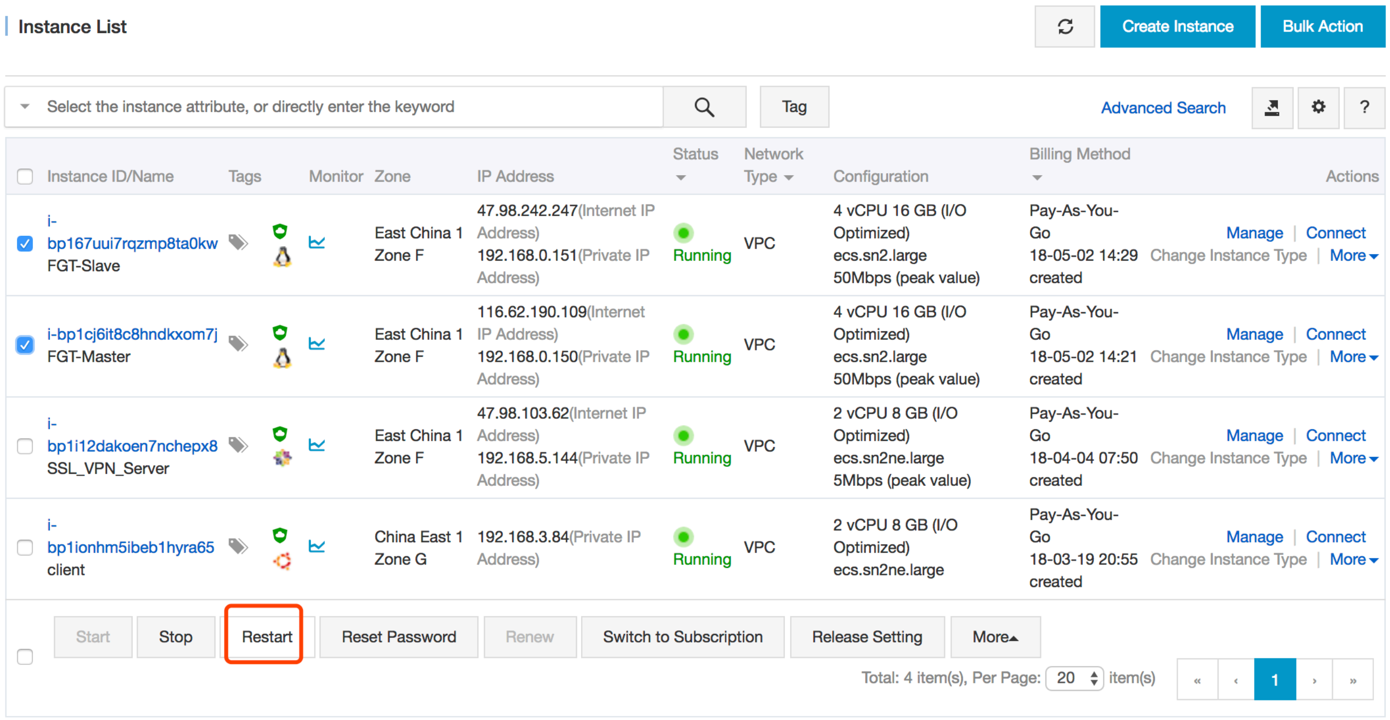
Create

Name Enter name Search

Update succes

ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-bp126a4rnnfhnelnoksk FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp167uui7r...		192.168.3.250	Secondary 00:16:3e:12:2b:bf	In Use 2018-05-02	Modify | Detach | Delete
eni-bp126a4rnnfhnelnoksh FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp1cj6it8c...		192.168.3.249	Secondary 00:16:3e:10:13:3e	In Use 2018-05-02	Modify | Detach | Delete

24.(Optional) Restart two FortiGate instance



Instance List

Create Instance Bulk Action

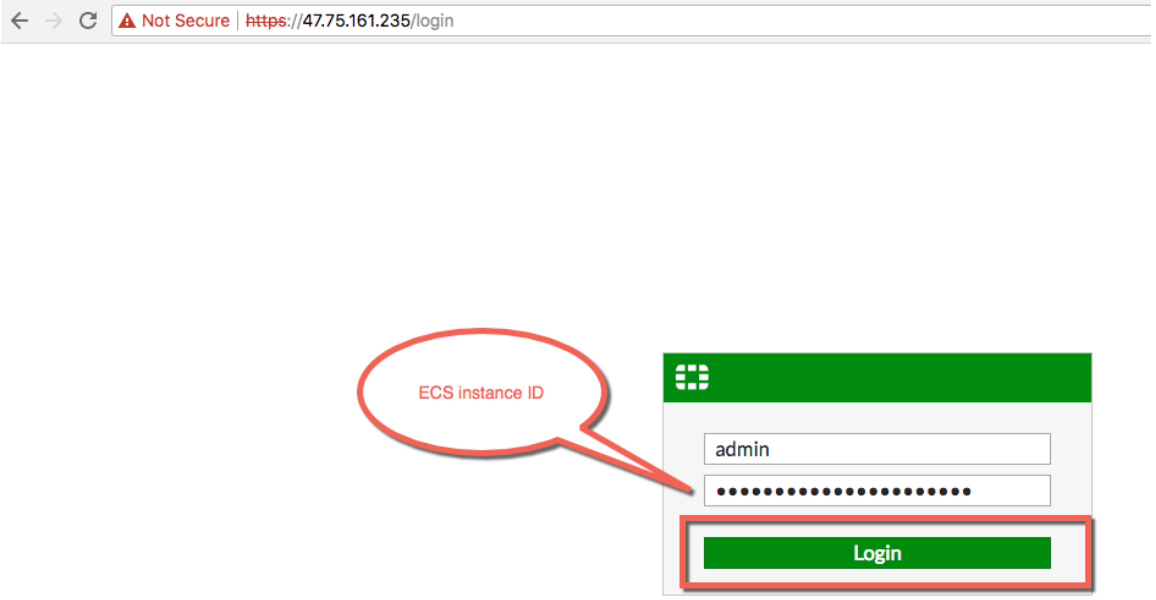
Select the instance attribute, or directly enter the keyword Tag Advanced Search

☐	Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
☑	i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247(Internet IP Address) 192.168.0.151(Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	Manage | Connect Change Instance Type | More
☑	i-bp1cj6it8c8hndkxom7j FGT-Master			East China 1 Zone F	116.62.190.109(Internet IP Address) 192.168.0.150(Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage | Connect Change Instance Type | More
☐	i-bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	47.98.103.62(Internet IP Address) 192.168.5.144(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large 5Mbps (peak value)	Pay-As-You-Go 18-04-04 07:50 created	Manage | Connect Change Instance Type | More
☐	i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84(Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage | Connect Change Instance Type | More

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

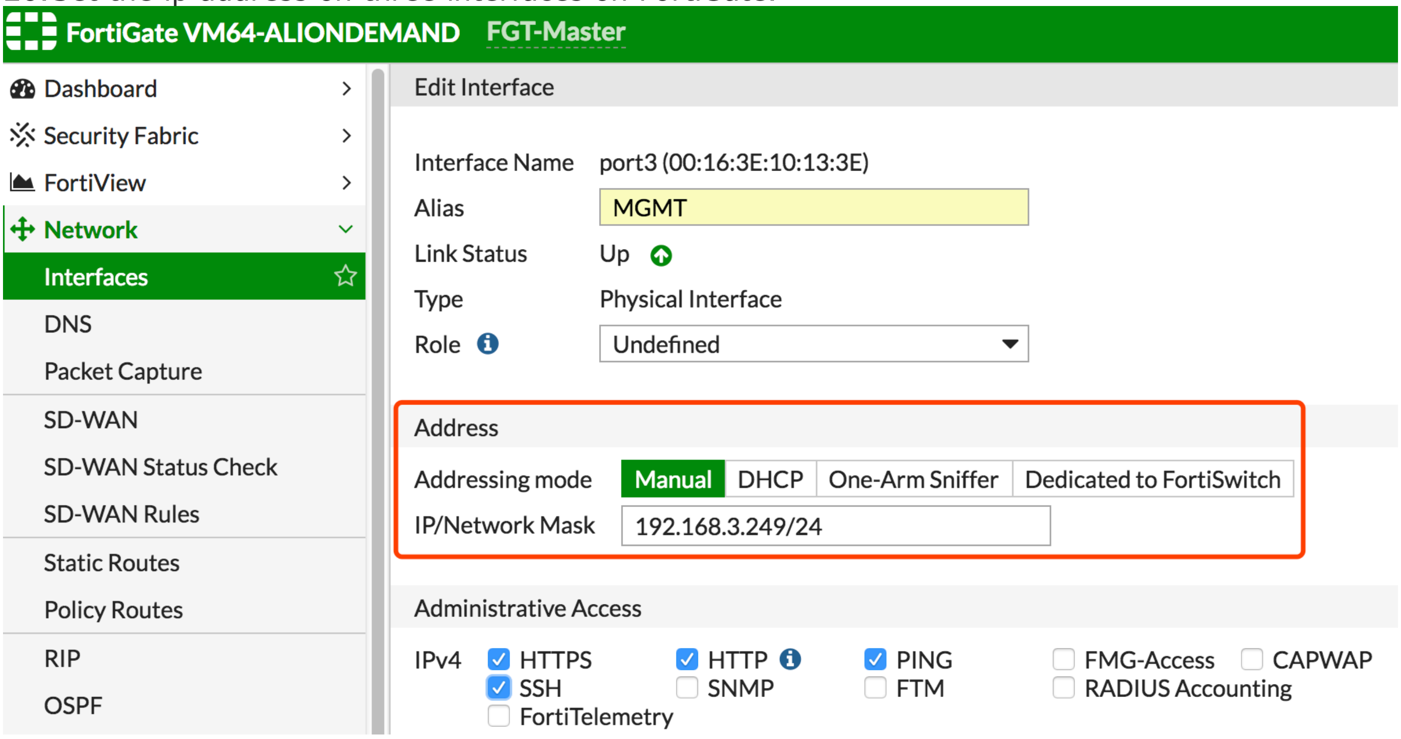
Total: 4 item(s), Per Page: 20 item(s) « ‹ 1 › »

25. Then we will be able to reach the Fortinet Web GUI by user admin/<***instanceid***>



⚠ Not Secure | https://47.75.161.235/login

26. Set the ip address on three interfaces on FortiGate.



Edit Interface

Interface Name port3 (00:16:3E:10:13:3E)

Alias MGMT

Link Status Up

Type Physical Interface

Role Undefined

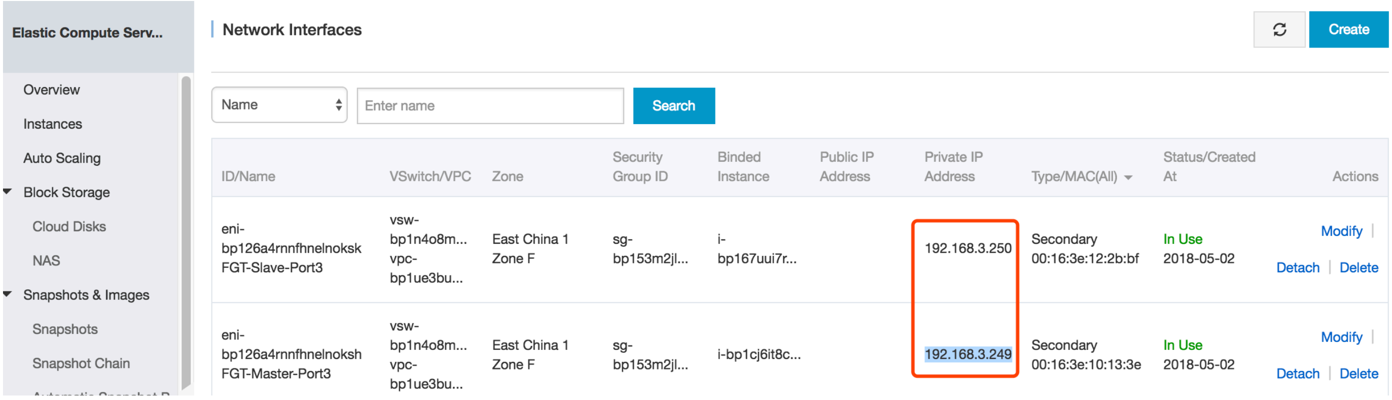
Address

Addressing mode [✓ Manual] DHCP One-Arm Sniffer Dedicated to FortiSwitch

IP/Network Mask 192.168.3.249/24

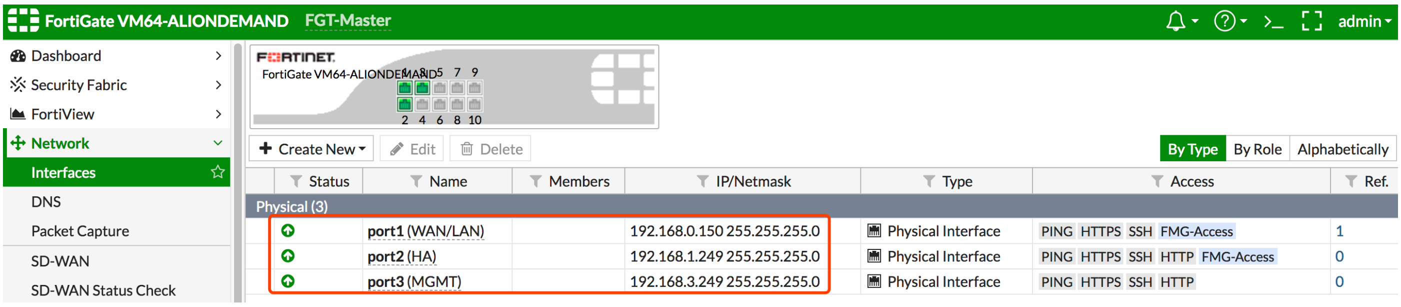
Administrative Access

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



Network Interfaces

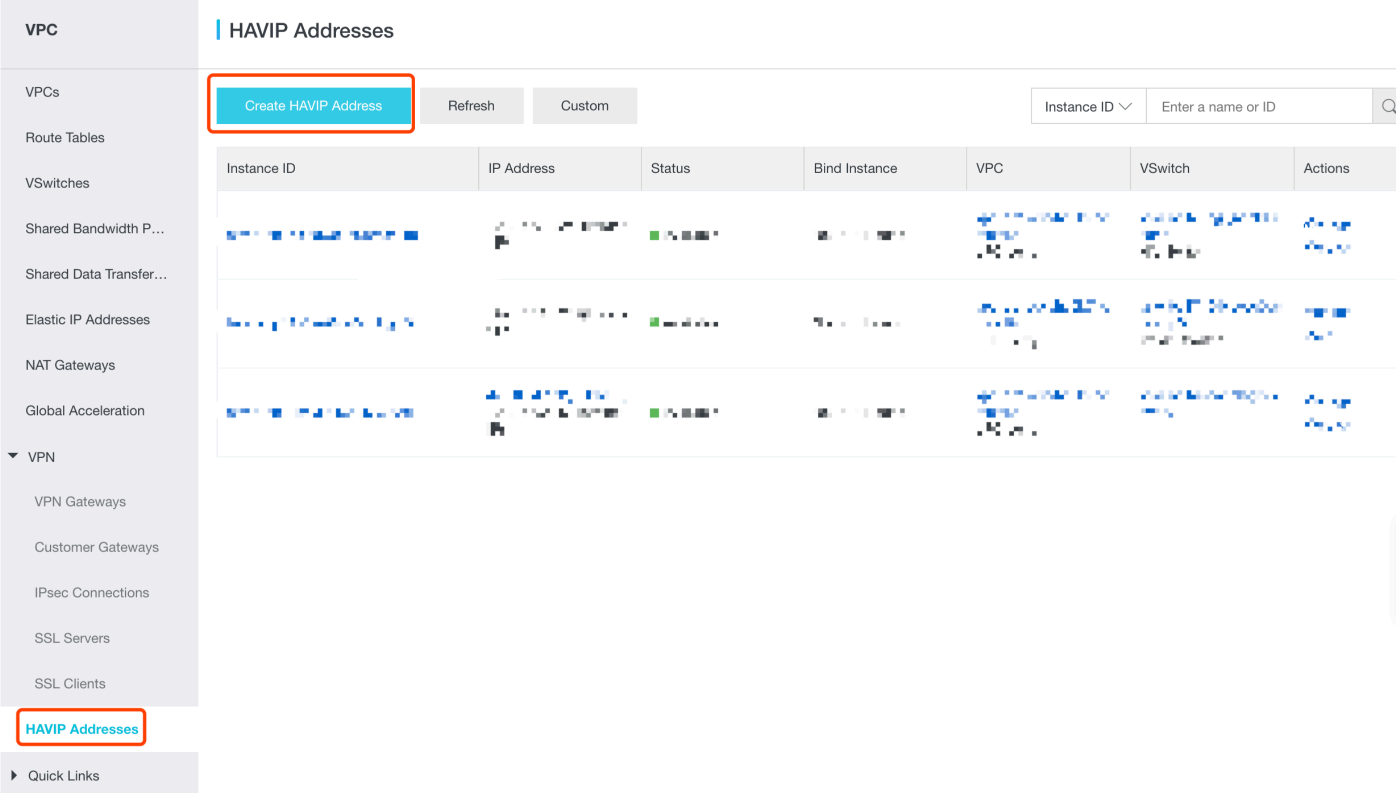
ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-bp126a4rnnfhnelnoksk FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp167uui7r...		192.168.3.250	Secondary 00:16:3e:12:2b:bf	In Use 2018-05-02	Modify | Detach | Delete
eni-bp126a4rnnfhnelnoksh FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp1cj6it8c...		192.168.3.249	Secondary 00:16:3e:10:13:3e	In Use 2018-05-02	Modify | Detach | Delete

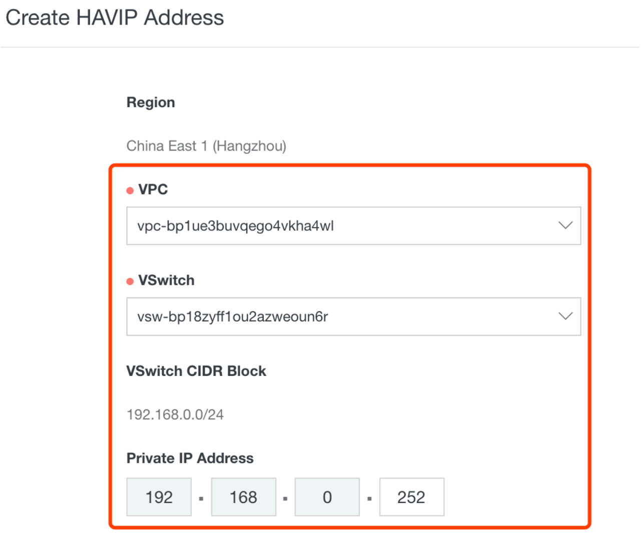


Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (3)						
●	port1 (WAN/LAN)		192.168.0.150 255.255.255.0	Physical Interface	PING HTTPS SSH FMG-Access	1
●	port2 (HA)		192.168.1.249 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
●	port3 (MGMT)		192.168.3.249 255.255.255.0	Physical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

Setting up the HAVIP on Aliyun Web Console

27. Create a new HAVIP address, select the VPC and FortiGate Port1 VSwitch, and set the HAVIP address.





Create HAVIP Address

Region

China East 1 (Hangzhou)

● VPC

vpc-bp1ue3buvqego4vkha4wl

● VSwitch

vsw-bp18zyff1ou2azweoun6r

VSwitch CIDR Block

192.168.0.0/24

Private IP Address

192 . 168 . 0 . 252

28.Set the HA configuration on FortiGate via VNC console on Aliyun Webgui, or via SSH.

FortiGate-Master:

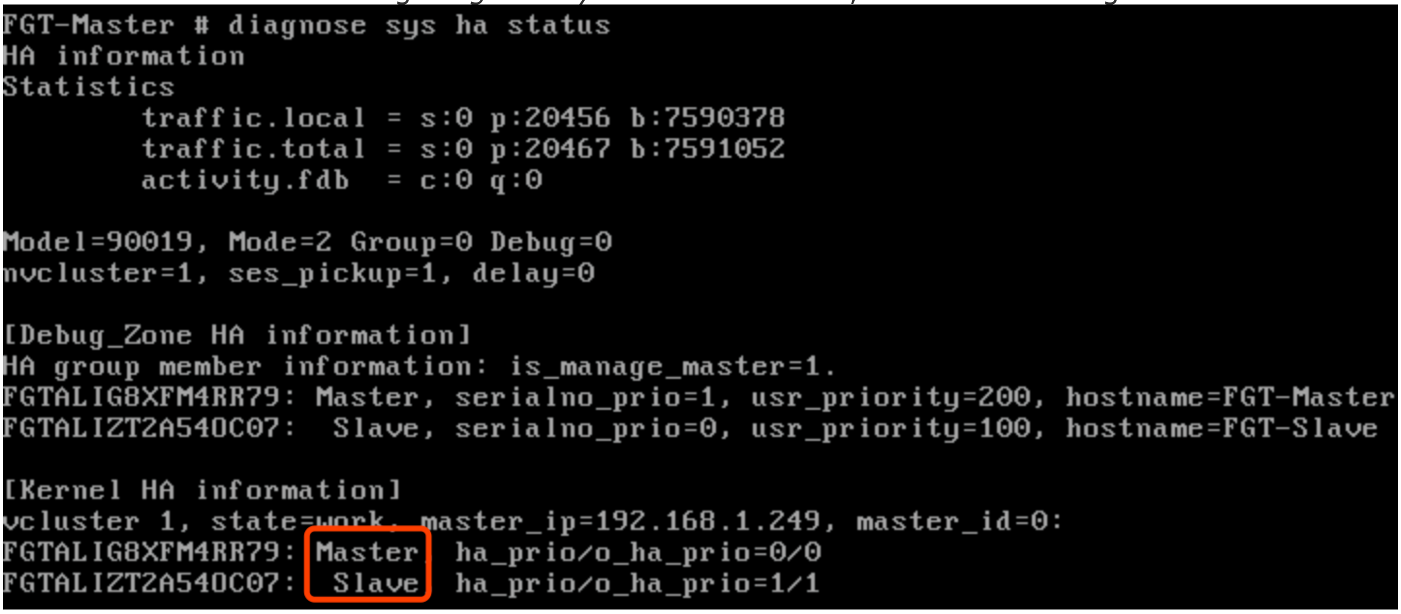
```
config system ha
    set group-name "ha"
    set mode a-p
    set hbdev "port2" 0
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interface
          edit 1
                    set interface "port3"
                    set gateway 192.168.3.253 --- gateway on vswitch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

FortiGate-Slave:

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

Then reboot two FortiGate.

Check the status of HA using '*diagnose sys ha status*' in CLI, it shows following:



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

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

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

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

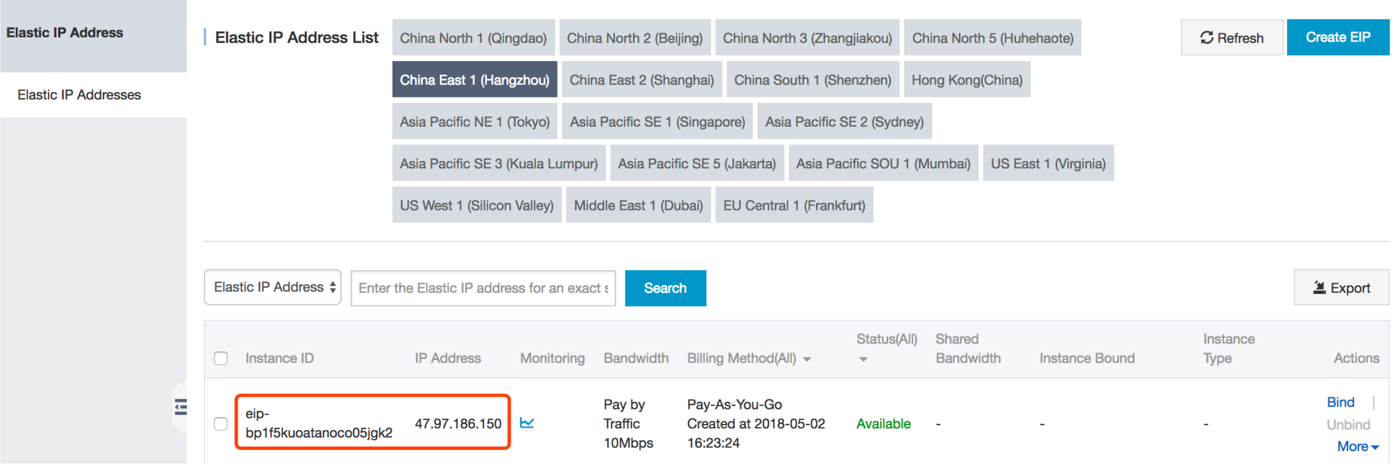
29. Set the HAVIP address to *port1 secondary ip address on two FortiGate*.

On both FGT-Master and FGT-Slave:

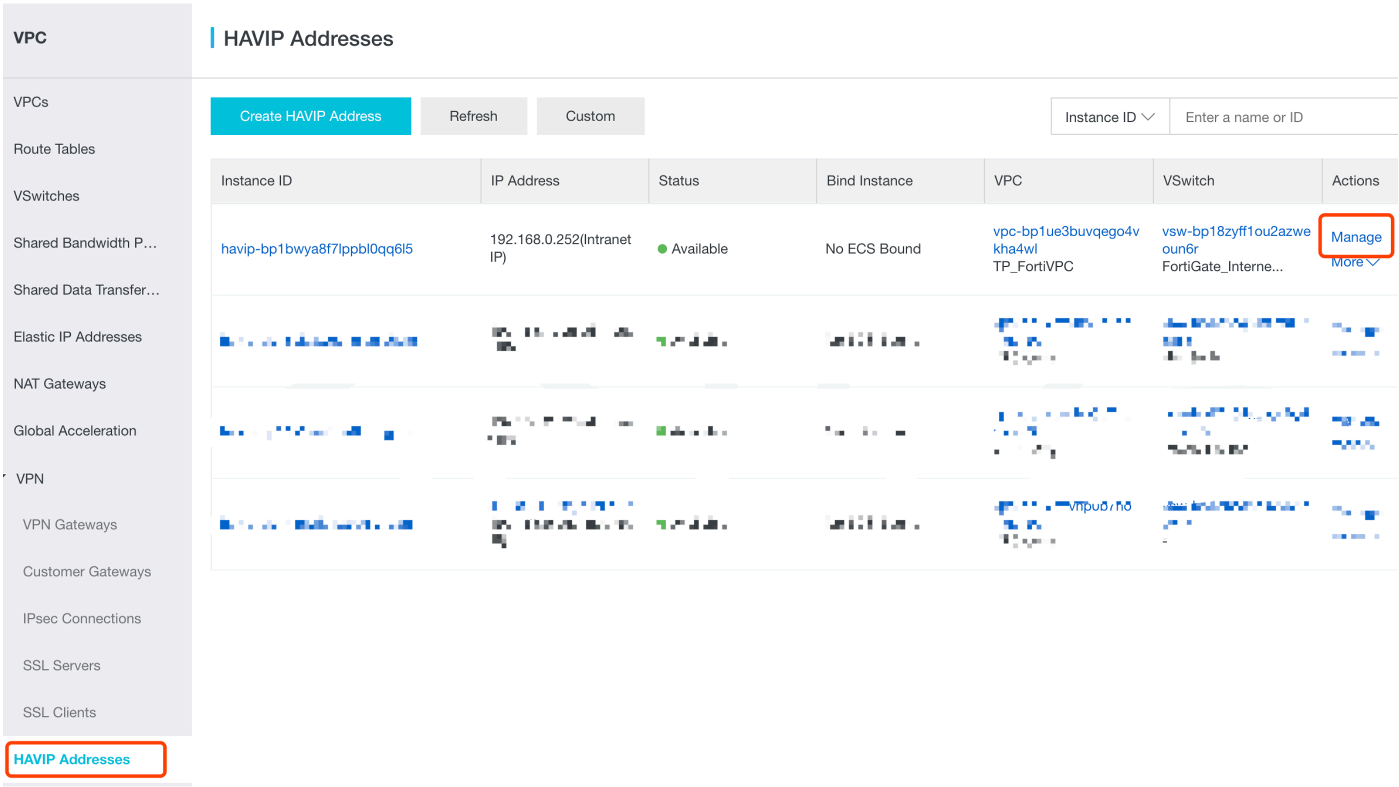
```
config system interface
    edit "port1"
        set secondary-IP enable
        config secondaryip
            edit 1
                set ip 192.168.0.252 255.255.255.0 --- this ip address should be same with HAVIP address
                set allowaccess ping https ssh
            next
        end
    next
end
```

30. Bind 'Elastic IP' and two FortiGate ECS to HAVIP

Create a new EIP

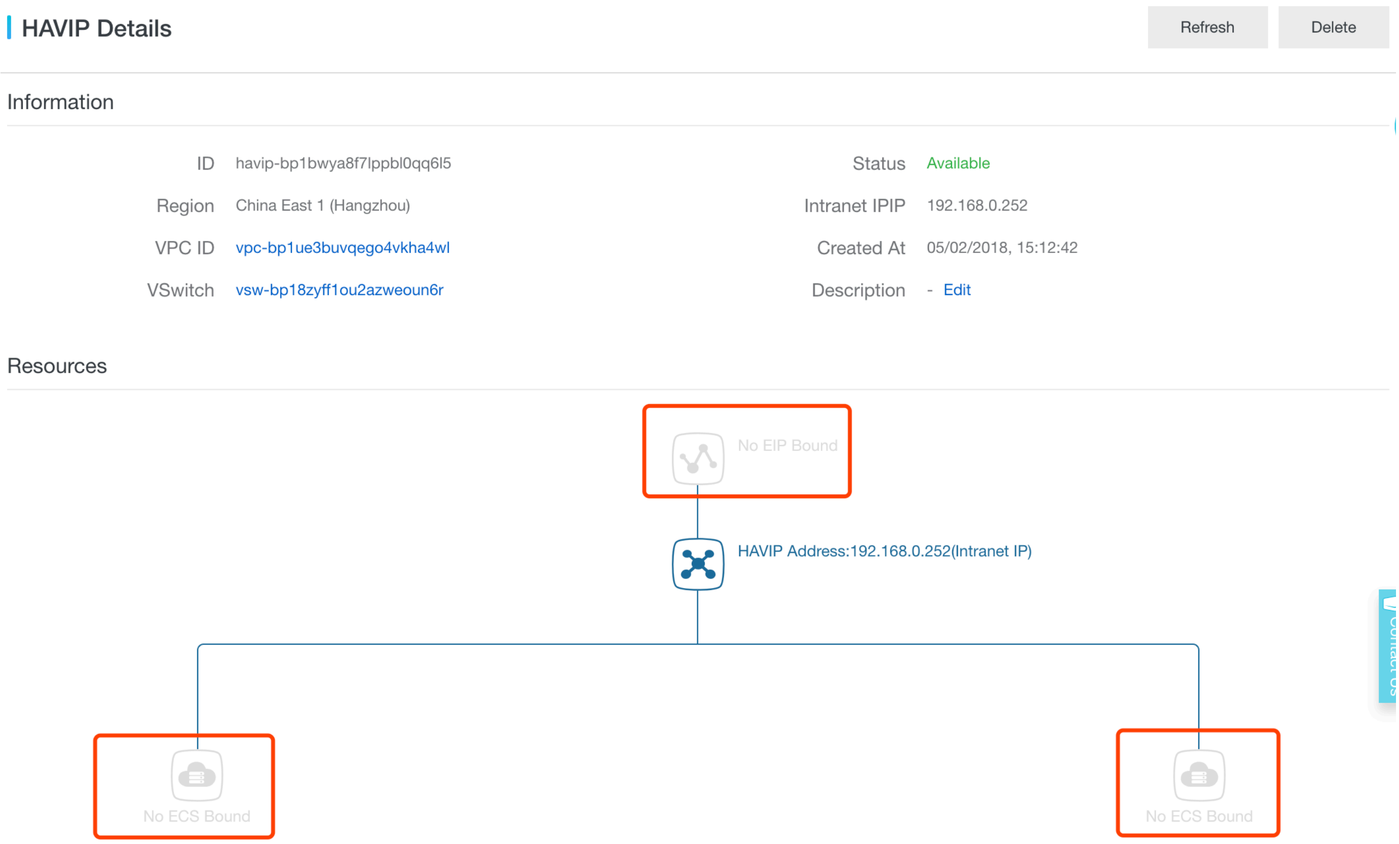


□	Instance ID	IP Address	Monitoring	Bandwidth	Billing Method(All)	Status(All)	Shared Bandwidth	Instance Bound	Instance Type	Actions
□	eip-bp1f5kuoatanoco05jgk2	47.97.186.150		Pay by Traffic 10Mbps	Pay-As-You-Go Created at 2018-05-02 16:23:24	Available	-	-	-	Bind | Unbind More



HAVIP Addresses

Instance ID	IP Address	Status	Bind Instance	VPC	VSwitch	Actions
havip-bp1bwya8f7lppbl0qq6l5	192.168.0.252(Intranet IP)	● Available	No ECS Bound	vpc-bp1ue3buvqego4vkha4wl TP_FortiVPC	vsw-bp18zyff1ou2azweoun6r FortiGate_Interne...	Manage More
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]



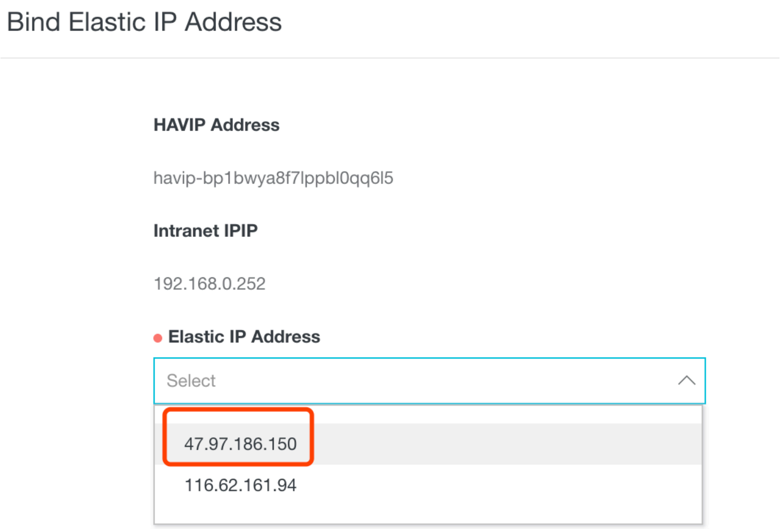
HAVIP Details

Information

ID	havip-bp1bwya8f7lppbl0qq6l5	Status	Available
Region	China East 1 (Hangzhou)	Intranet IPIP	192.168.0.252
VPC ID	vpc-bp1ue3buvqego4vkha4wl	Created At	05/02/2018, 15:12:42
VSwitch	vsw-bp18zyff1ou2azweoun6r	Description	- Edit

Resources

Bind EIP to HAVIP,



Bind Elastic IP Address

HAVIP Address

havip-bp1bwya8f7lppbl0qq6l5

Intranet IPIP

192.168.0.252

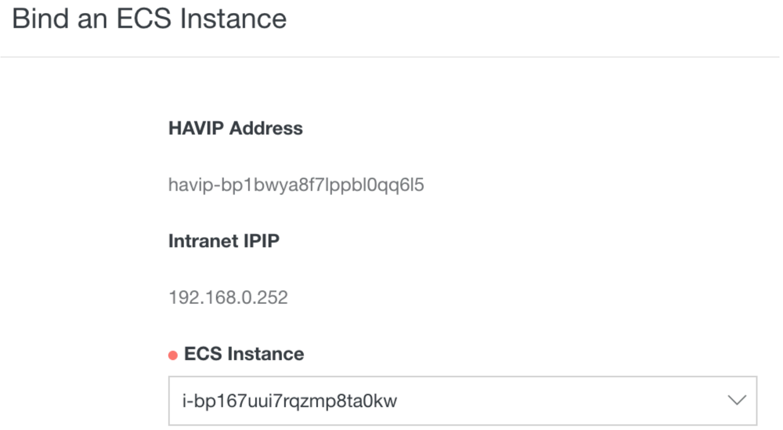
● Elastic IP Address

Select

47.97.186.150

116.62.161.94

Bind two FortiGate to HAVIP,



Bind an ECS Instance

HAVIP Address

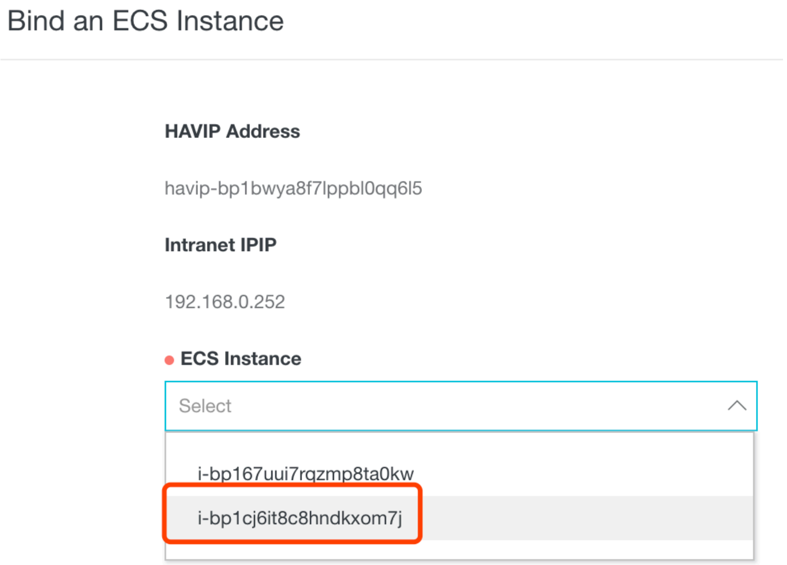
havip-bp1bwya8f7lppbl0qq6l5

Intranet IPIP

192.168.0.252

● ECS Instance

i-bp167uui7rqzmp8ta0kw



Bind an ECS Instance

HAVIP Address

havip-bp1bwya8f7lppbl0qq6l5

Intranet IPIP

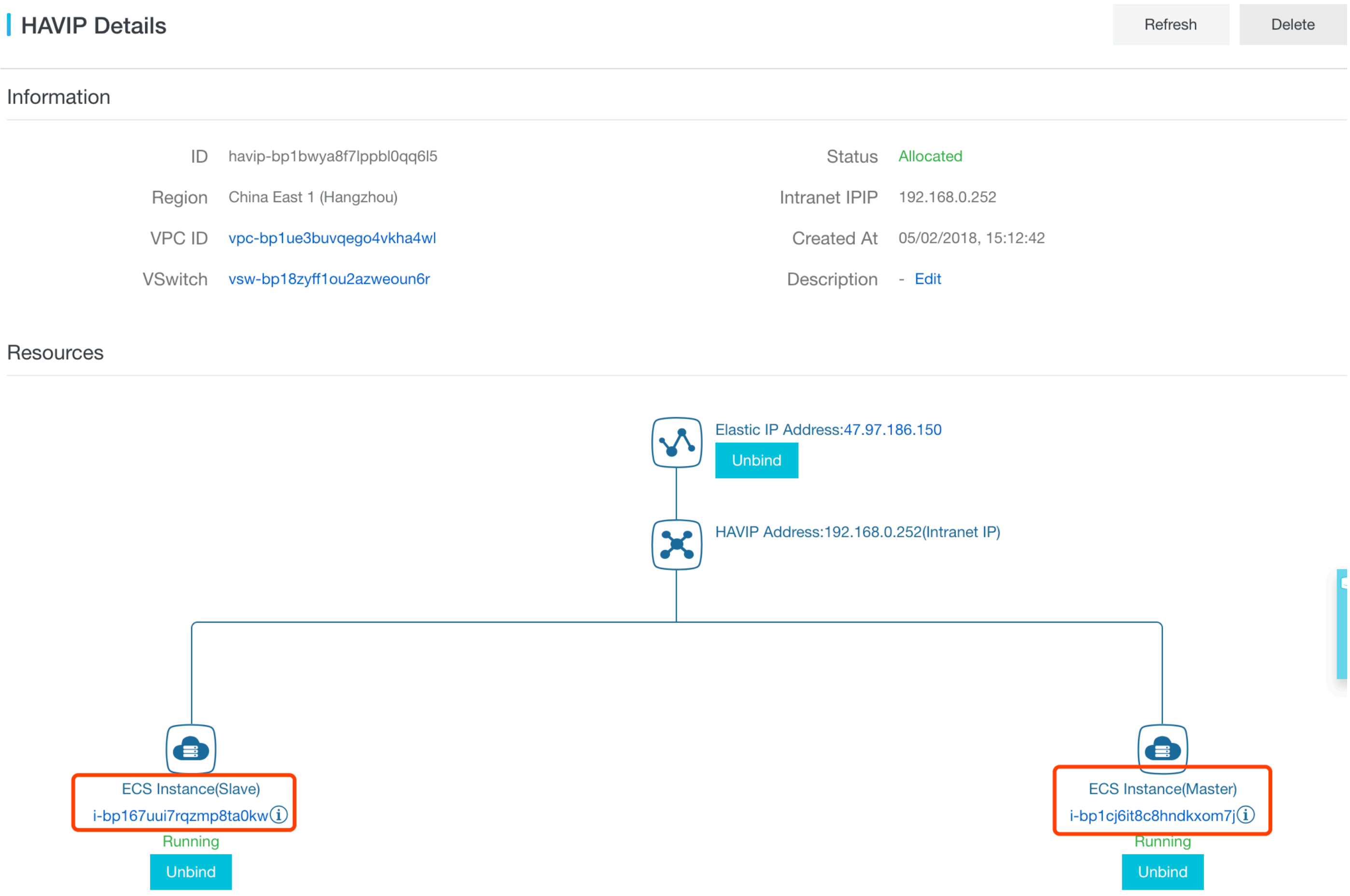
192.168.0.252

● ECS Instance

Select

i-bp167uui7rqzmp8ta0kw

i-bp1cj6it8c8hndkxom7j



HAVIP Details

Refresh Delete

Information

ID	havip-bp1bwya8f7lppbl0qq6l5	Status	Allocated
Region	China East 1 (Hangzhou)	Intranet IPIP	192.168.0.252
VPC ID	vpc-bp1ue3buvqego4vkha4wl	Created At	05/02/2018, 15:12:42
VSwitch	vsw-bp18zyff1ou2azweoun6r	Description	- Edit

Resources

Elastic IP Address:47.97.186.150

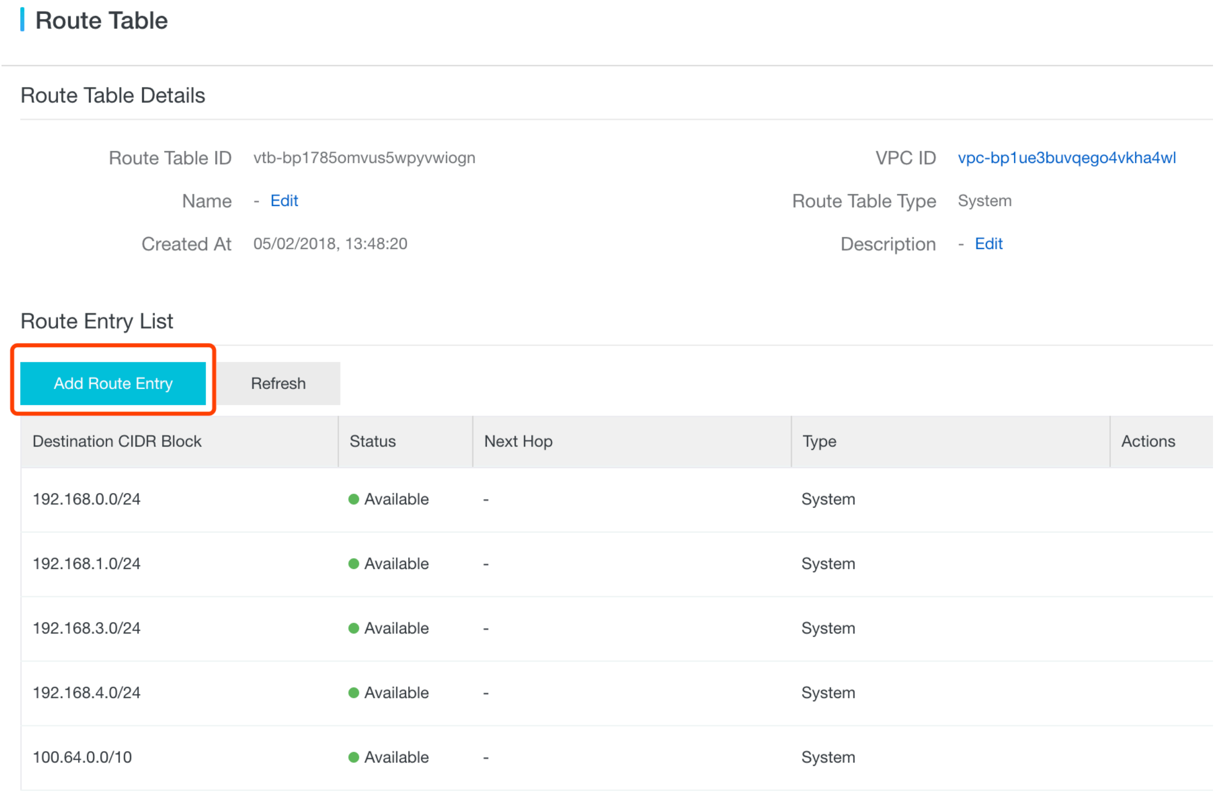
Unbind

HAVIP Address:192.168.0.252(Intranet IP)

ECS Instance(Slave)
i-bp167uui7rqzmp8ta0kw
Running
Unbind

ECS Instance(Master)
i-bp1cj6it8c8hndkxom7j
Running
Unbind

31. Also we need to add the route entry to FortiGate, this make sure all out-going traffic from ECS will go through Fortinet



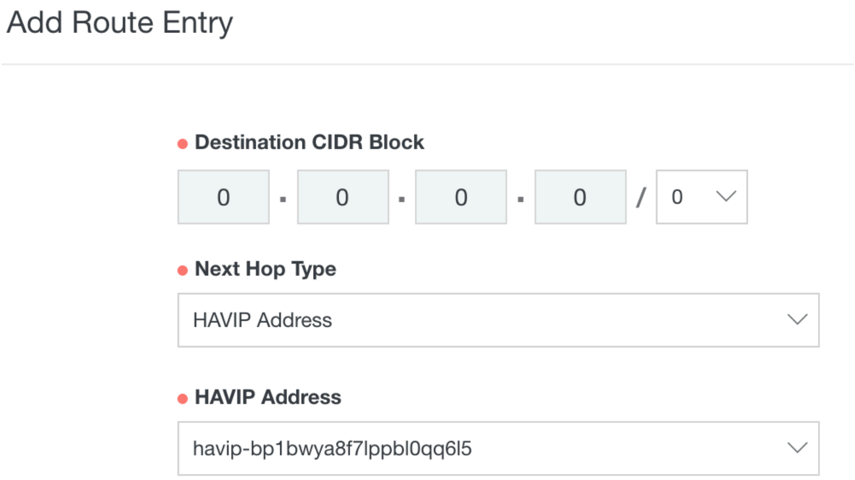
Route Table

Route Table Details

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

Route Entry List

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

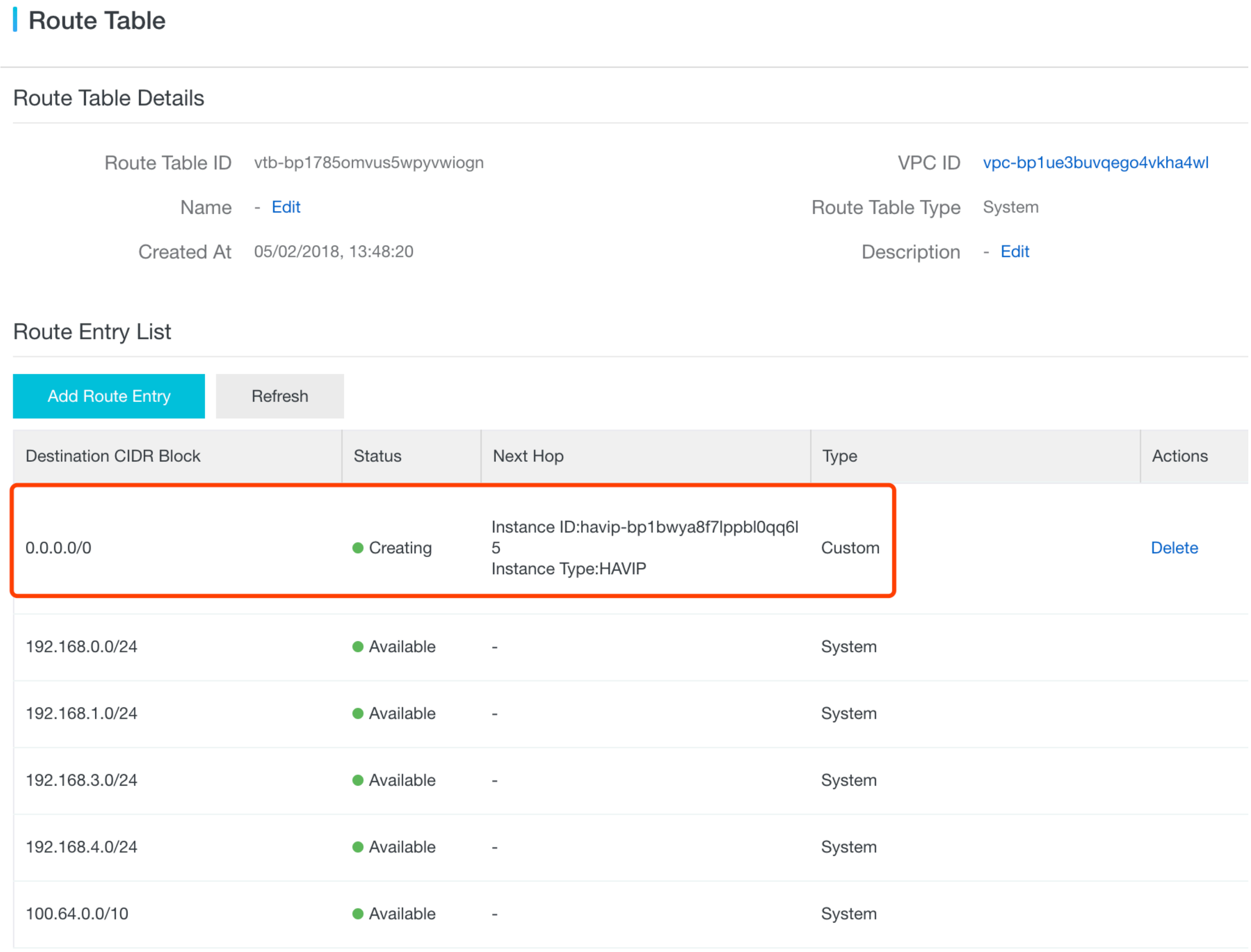


Add Route Entry

● Destination CIDR Block: 0 . 0 . 0 . 0 / 0

● Next Hop Type: HAVIP Address

● HAVIP Address: havip-bp1bwya8f7lppbl0qq6l5



Route Table

Route Table Details

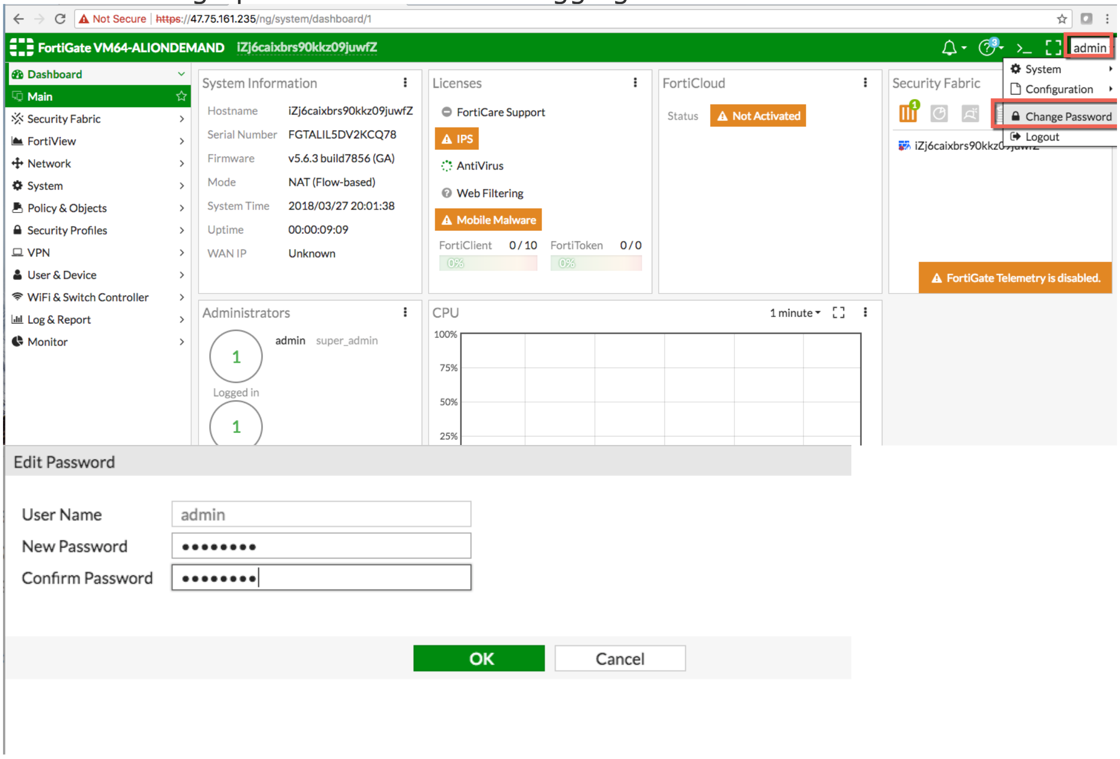
Route Table ID	vtb-bp1785omvus5wpyvwiogn	VPC ID	vpc-bp1ue3buvqego4vkha4wl
Name	- Edit	Route Table Type	System
Created At	05/02/2018, 13:48:20	Description	- Edit

Route Entry List

Destination CIDR Block	Status	Next Hop	Type	Actions
0.0.0.0/0	● Creating	Instance ID:havip-bp1bwya8f7lppbl0qq6l 5 Instance Type:HAVIP	Custom	Delete
192.168.0.0/24	● Available	-	System	
192.168.1.0/24	● Available	-	System	
192.168.3.0/24	● Available	-	System	
192.168.4.0/24	● Available	-	System	
100.64.0.0/10	● Available	-	System	

Start configuration of Fortinet Firewall

32. You can change password here after logging in



System Information

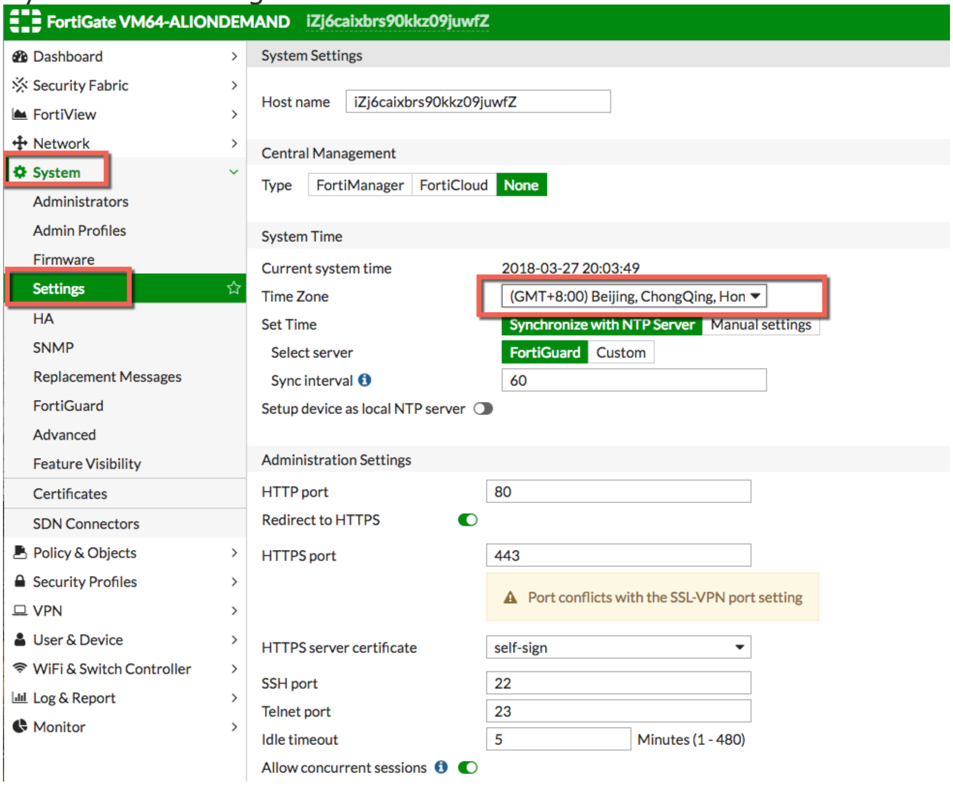
Hostname	iZj6caixbrs90kkz09juwfZ
Serial Number	FGTALIL5DV2KCQ78
Firmware	v5.6.3 build7856 (GA)
Mode	NAT (Flow-based)
System Time	2018/03/27 20:01:38
Uptime	00:00:09:09
WAN IP	Unknown

Edit Password

User Name	admin
New Password	••••••••
Confirm Password	••••••••

OK Cancel

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



System Settings

Host name: iZj6caixbrs90kkz09juwfZ

Central Management

Type: FortiManager | FortiCloud | **None**

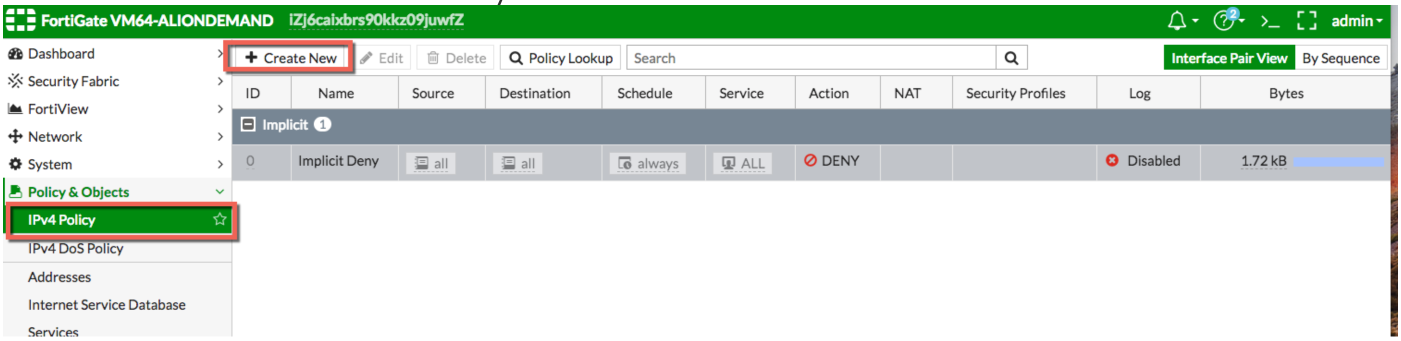
System Time

Current system time	2018-03-27 20:03:49
Time Zone	(GMT+8:00) Beijing, ChongQing, Hon
Set Time	**Synchronize with NTP Server** | Manual settings
Select server	**FortiGuard** | Custom
Sync interval	60
Setup device as local NTP server	○

Administration Settings

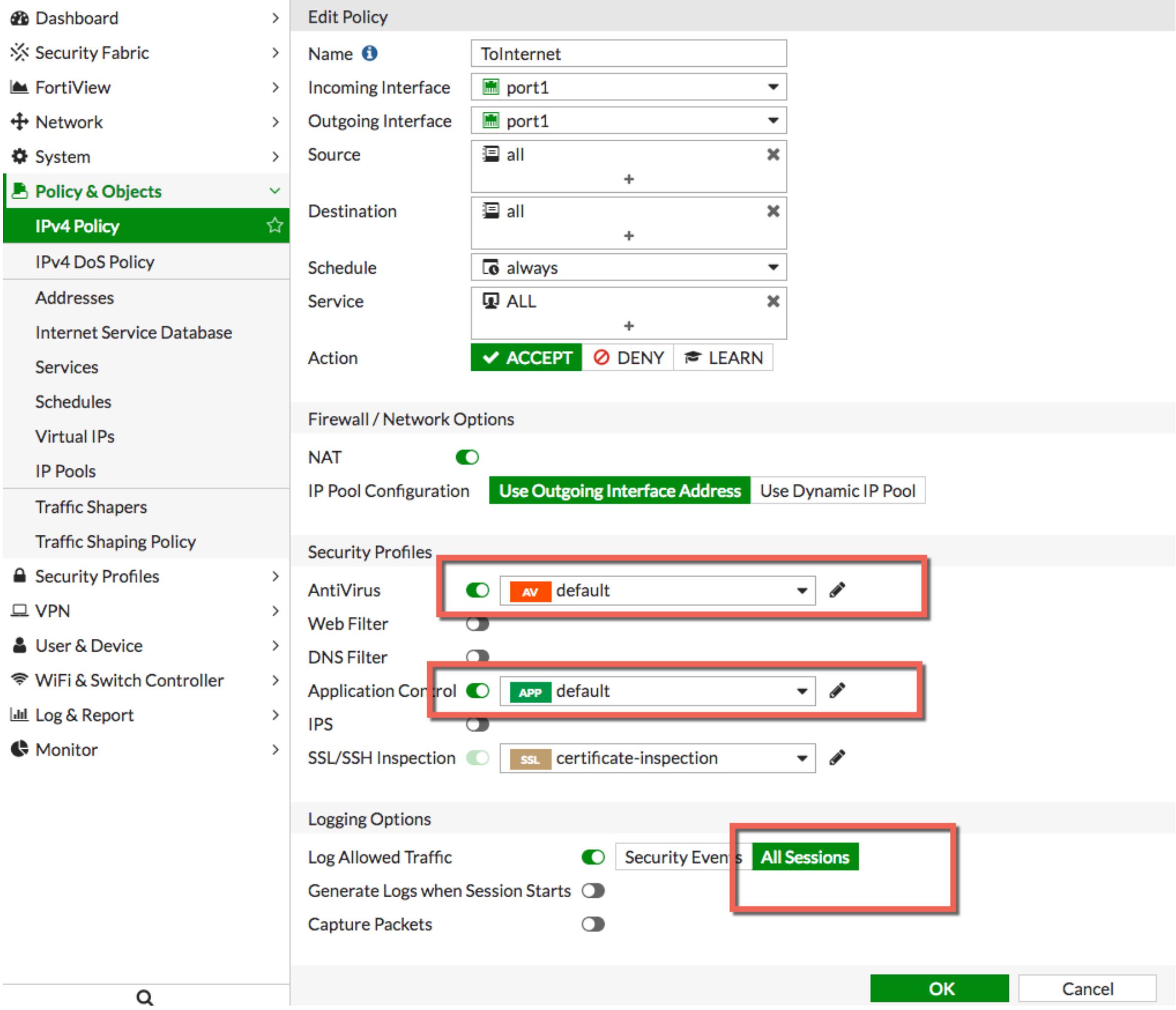
HTTP port	80
Redirect to HTTPS	●
HTTPS port	443
	Port conflicts with the SSL-VPN port setting
HTTPS server certificate	self-sign
SSH port	22
Telnet port	23
Idle timeout	5 Minutes (1 - 480)
Allow concurrent sessions	●

34. Now we need to add the IPv4 Policy for the outbound traffic



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Implicit 1										
0	Implicit Deny	all	all	always	ALL	⊘ DENY			Disabled	1.72 kB

35. Specific the following "ToInternet" policy, let's enabled the AntiVirus and Application Control here for Demo, also enabled All Sessions log too, then click "OK"



Edit Policy

Name: ToInternet

Incoming Interface: port1

Outgoing Interface: port1

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT | ⊘ DENY | LEARN

Firewall / Network Options

NAT: ●

IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles

AntiVirus: ● AV default

Web Filter: ○

DNS Filter: ○

Application Control: ● APP default

IPS: ○

SSL/SSH Inspection: ● SSL certificate-inspection

Logging Options

Log Allowed Traffic: ● Security Events [✓ All Sessions]

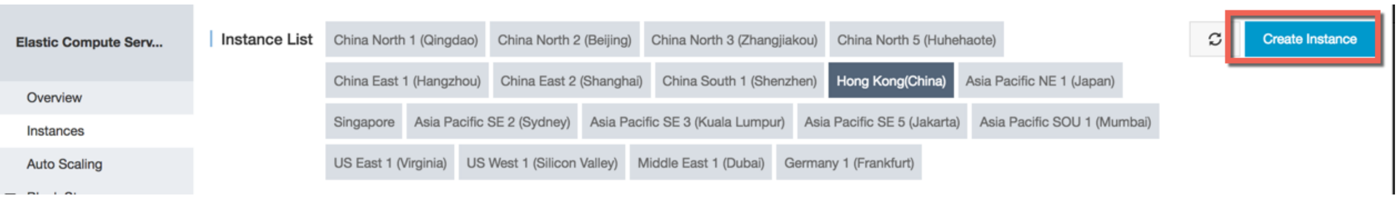
Generate Logs when Session Starts: ○

Capture Packets: ○

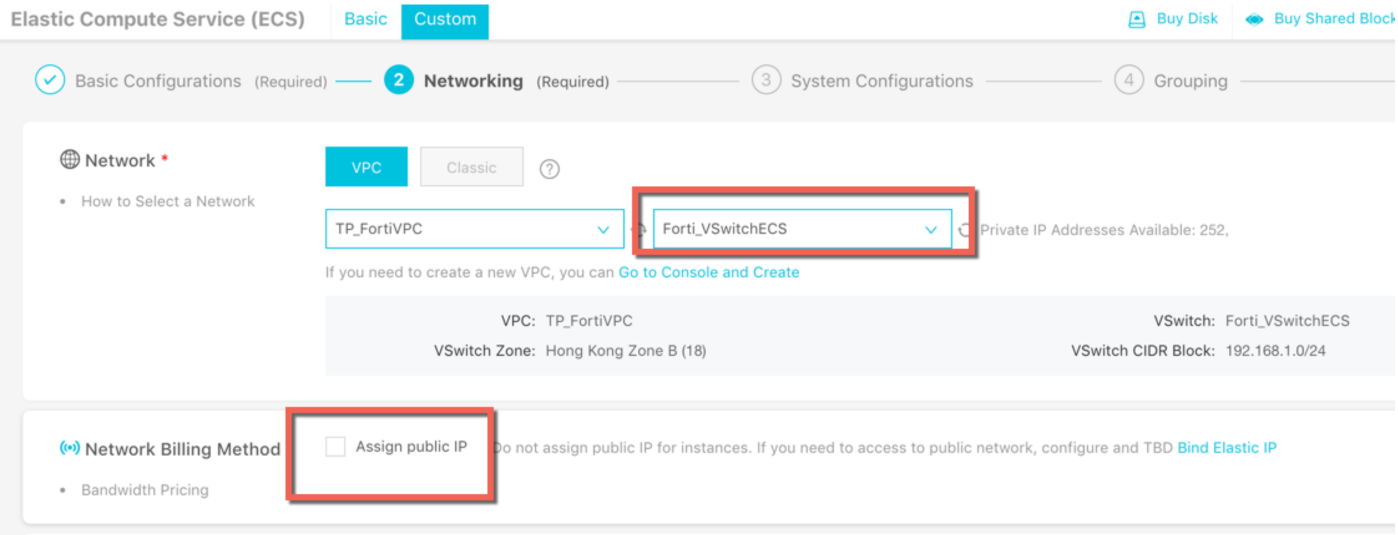
OK Cancel

Add ECS worker VMs for testing

36. Just create ECS as usual



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



VPC | Classic

TP_FortiVPC | Forti_VSwitchECS | Private IP Addresses Available: 252,

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

VPC: TP_FortiVPC

VSwitch: Forti_VSwitchECS

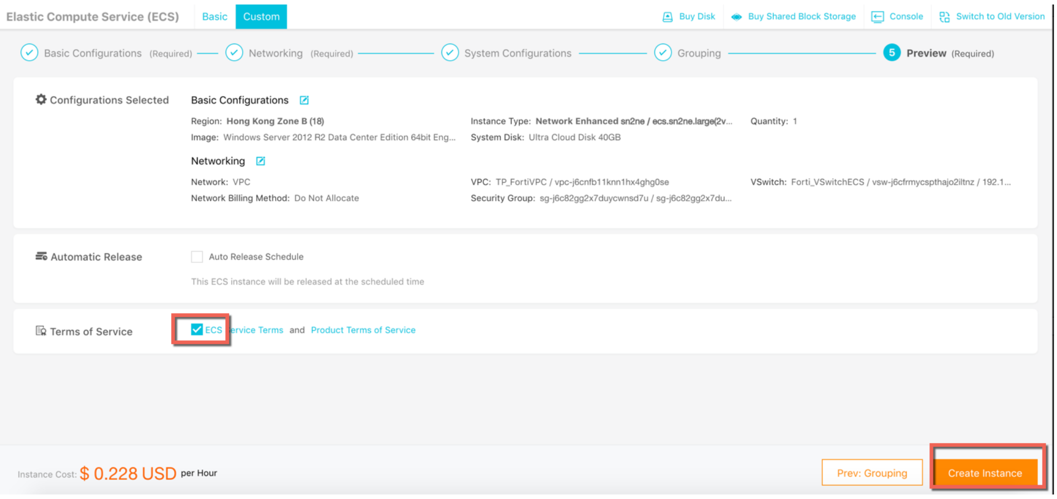
VSwitch Zone: Hong Kong Zone B (18)

VSwitch CIDR Block: 192.168.1.0/24

□ Assign public IP

Do not assign public IP for instances. If you need to access to public network, configure and TBD Bind Elastic IP

38. Confirm and create the instance



Configurations Selected

Basic Configurations

Region: Hong Kong Zone B (18)

Instance Type: Network Enhanced sn2ne / ecs.sn2ne.large(2v...

Quantity: 1

Image: Windows Server 2012 R2 Data Center Edition 64bit Eng...

System Disk: Ultra Cloud Disk 40GB

Networking

Network: VPC

VPC: TP_FortiVPC / vpc-j6cnfb11knn1hx4ghg0se

VSwitch: Forti_VSwitchECS / vsw-j6cfrmycspthajo2iltnz / 192.1...

Network Billing Method: Do Not Allocate

Security Group: sg-j6c82gg2x7duycwnsd7u / sg-j6c82gg2x7du...

Automatic Release

□ Auto Release Schedule

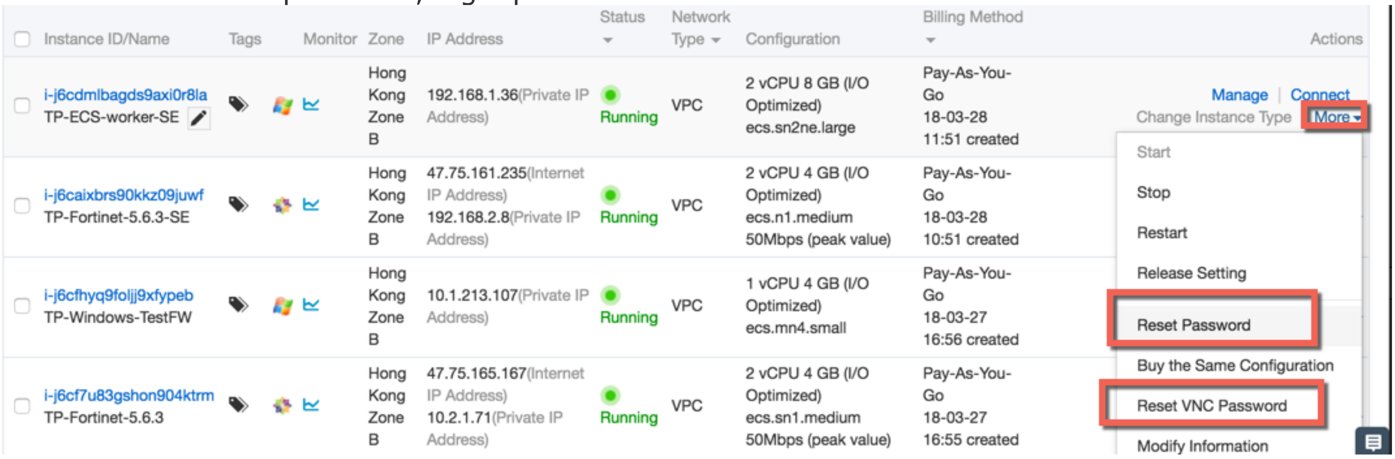
This ECS instance will be released at the scheduled time

Terms of Service

☑ ECS ervice Terms and Product Terms of Service

Instance Cost: $ 0.228 USD per Hour

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



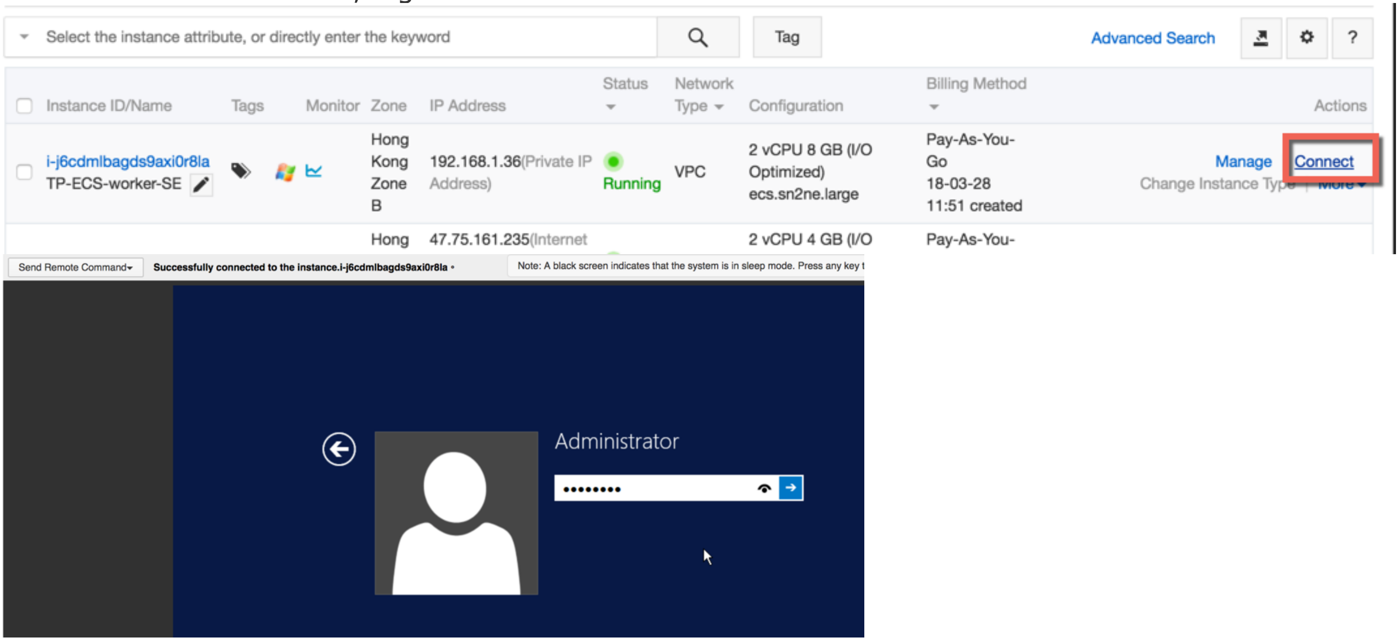
☐	Instance ID/Name	Tags	Monitor	Zone	IP Address	Status ▾	Network Type ▾	Configuration	Billing Method ▾	Actions
☐	i-j6cdmlbagds9axi0r8la TP-ECS-worker-SE			Hong Kong Zone B	192.168.1.36(Private IP Address)	● Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-28 11:51 created	Manage | Connect Change Instance Type | More ▾

☐	i-j6caixbrs90kkz09juwf
	TP-Fortinet-5.6.3-SE
				Hong Kong Zone B	47.75.161.235(Internet IP Address)
					192.168.2.8(Private IP Address)
						● Running	VPC	2 vCPU 4 GB (I/O Optimized)
								ecs.n1.medium
								50Mbps (peak value)
									Pay-As-You-Go
									18-03-28 10:51 created	

☐	i-j6cfhyq9foljj9xfypeb TP-Windows-TestFW			Hong Kong Zone B	10.1.213.107(Private IP Address)	● Running	VPC	1 vCPU 4 GB (I/O Optimized) ecs.mn4.small	Pay-As-You-Go 18-03-27 16:56 created	

☐	i-j6cf7u83gshon904ktrm
	TP-Fortinet-5.6.3
				Hong Kong Zone B	47.75.165.167(Internet IP Address)
					10.2.1.71(Private IP Address)
						● Running	VPC	2 vCPU 4 GB (I/O Optimized)
								ecs.sn1.medium
								50Mbps (peak value)
									Pay-As-You-Go
									18-03-27 16:55 created	

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



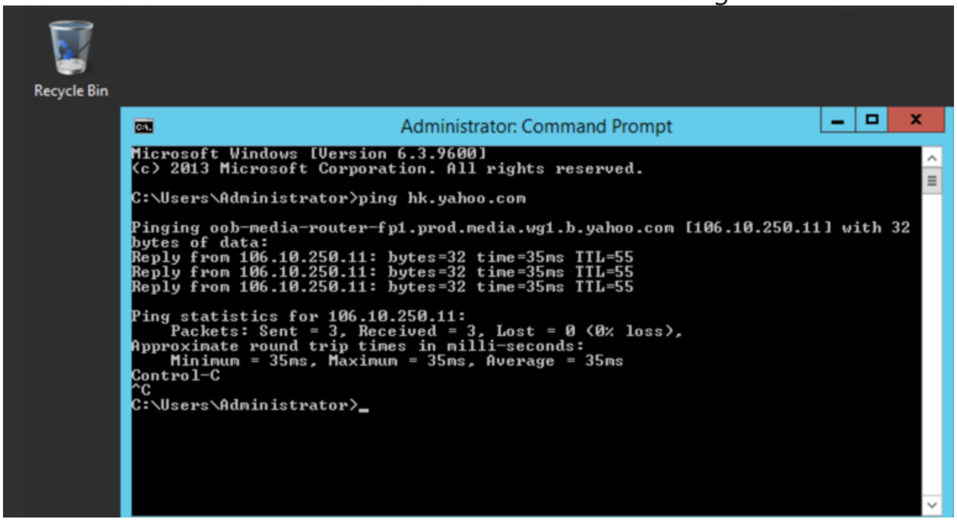
Select the instance attribute, or directly enter the keyword
Tag
Advanced Search
?

☐	Instance ID/Name	Tags	Monitor	Zone	IP Address	Status ▾	Network Type ▾	Configuration	Billing Method ▾	Actions
☐	i-j6cdmlbagds9axi0r8la TP-ECS-worker-SE			Hong Kong Zone B	192.168.1.36(Private IP Address)	● Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-28 11:51 created	Manage Connect Change Instance Type More ▾
				Hong	47.75.161.235(Internet			2 vCPU 4 GB (I/O	Pay-As-You-	

Successfully connected to the instance.i-j6cdmlbagds9axi0r8la ·

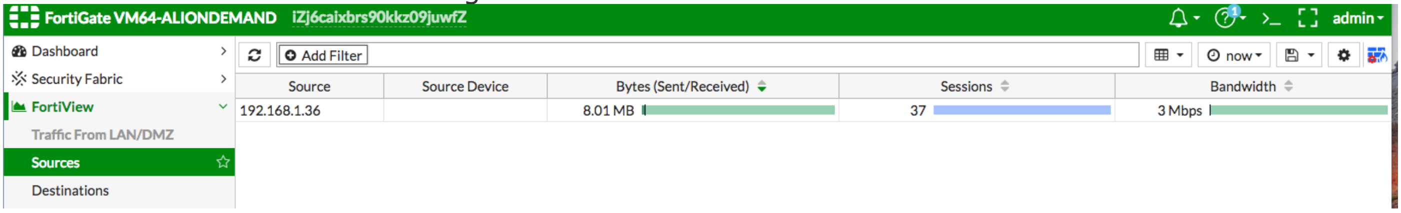
Note: A black screen indicates that the system is in sleep mode. Press any key t

41. You should find it is able to connect internet through the Fortinet

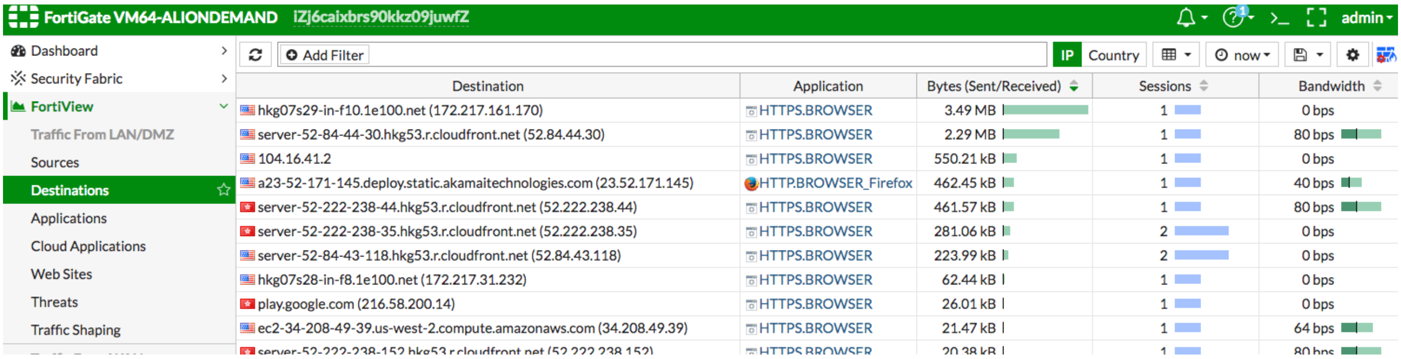


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

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

42. You should also find the detail log information in the Fortinet as well!



Source	Source Device	Bytes (Sent/Received)	Sessions	Bandwidth
192.168.1.36		8.01 MB	37	3 Mbps



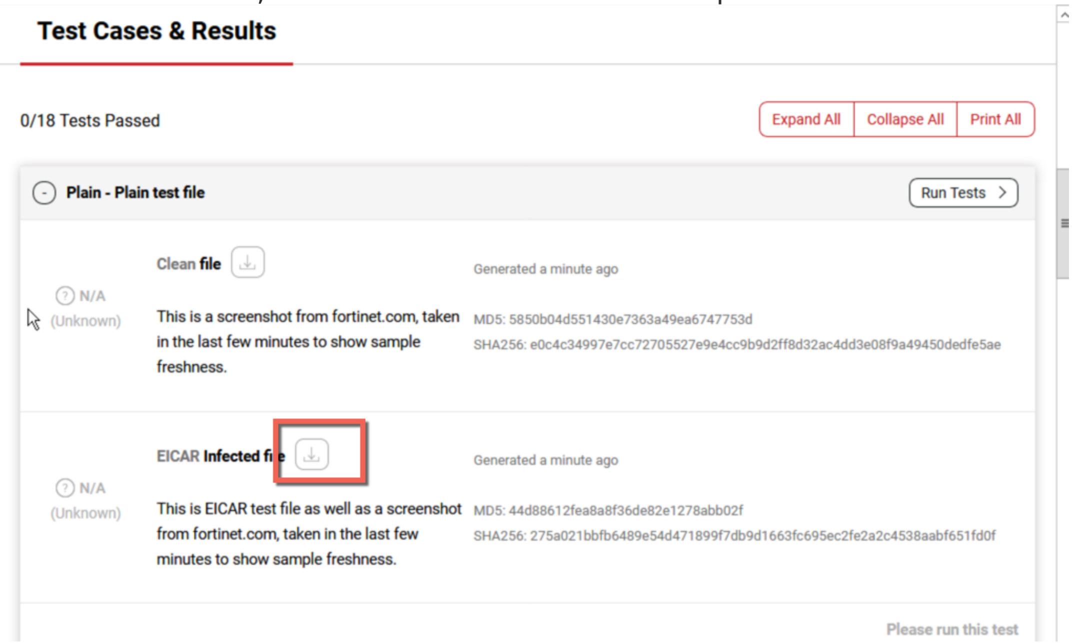
Destination	Application	Bytes (Sent/Received)	Sessions	Bandwidth
hkg07s29-in-f10.1e100.net (172.217.161.170)	HTTPS.BROWSER	3.49 MB	1	0 bps
server-52-84-44-30.hkg53.r.cloudfront.net (52.84.44.30)	HTTPS.BROWSER	2.29 MB	1	80 bps
104.16.41.2	HTTPS.BROWSER	550.21 kB	1	0 bps
a23-52-171-145.deploy.static.akamaitechnologies.com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

Verify the security capabilities of the Fortinet

Demonstrate the Anti-Virus feature

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

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



Test Cases & Results

0/18 Tests Passed

Plain - Plain test file

N/A (Unknown)

Clean file

This is a screenshot from fortinet.com, taken in the last few minutes to show sample freshness.

Generated a minute ago

MD5: 5850b04d551430e7363a49ea6747753d

SHA256: e0c4c34997e7cc72705527e9e4cc9b9d2ff8d32ac4dd3e08f9a49450dedfe5ae

N/A (Unknown)

EICAR Infected file

This is EICAR test file as well as a screenshot from fortinet.com, taken in the last few minutes to show sample freshness.

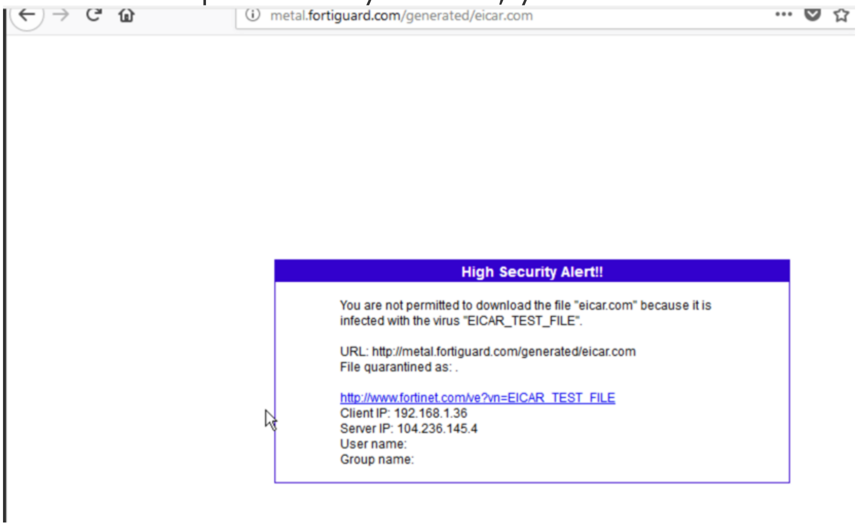
Generated a minute ago

MD5: 44d88612fea8a8f36de82e1278abb02f

SHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

Please run this test

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



metal.fortiguard.com/generated/eicar.com

High Security Alert!!

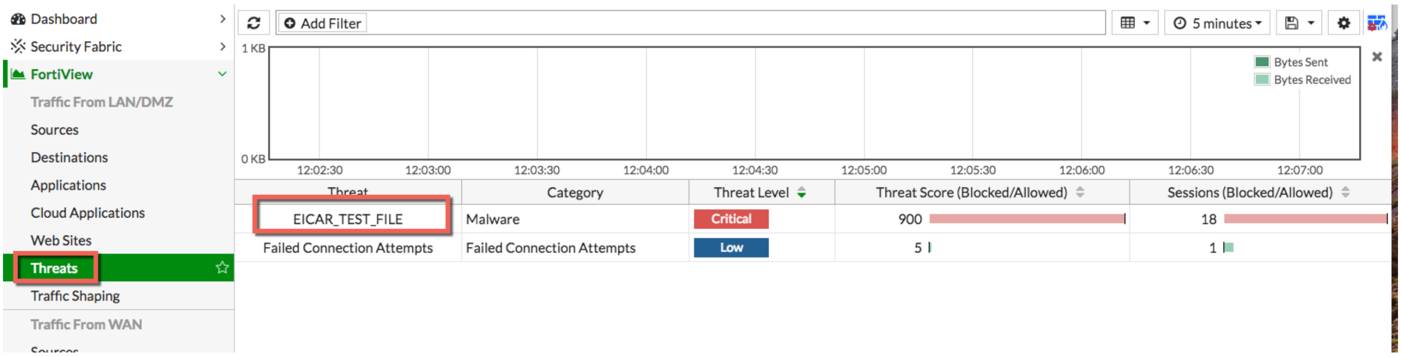
You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".

URL: http://metal.fortiguard.com/generated/eicar.com
File quarantined as: .

http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
Client IP: 192.168.1.36
Server IP: 104.236.145.4
User name:
Group name:

To have the best Anti-Virus scanning capabilities, make sure the anti-virus definition is up-to-update in Fortinet

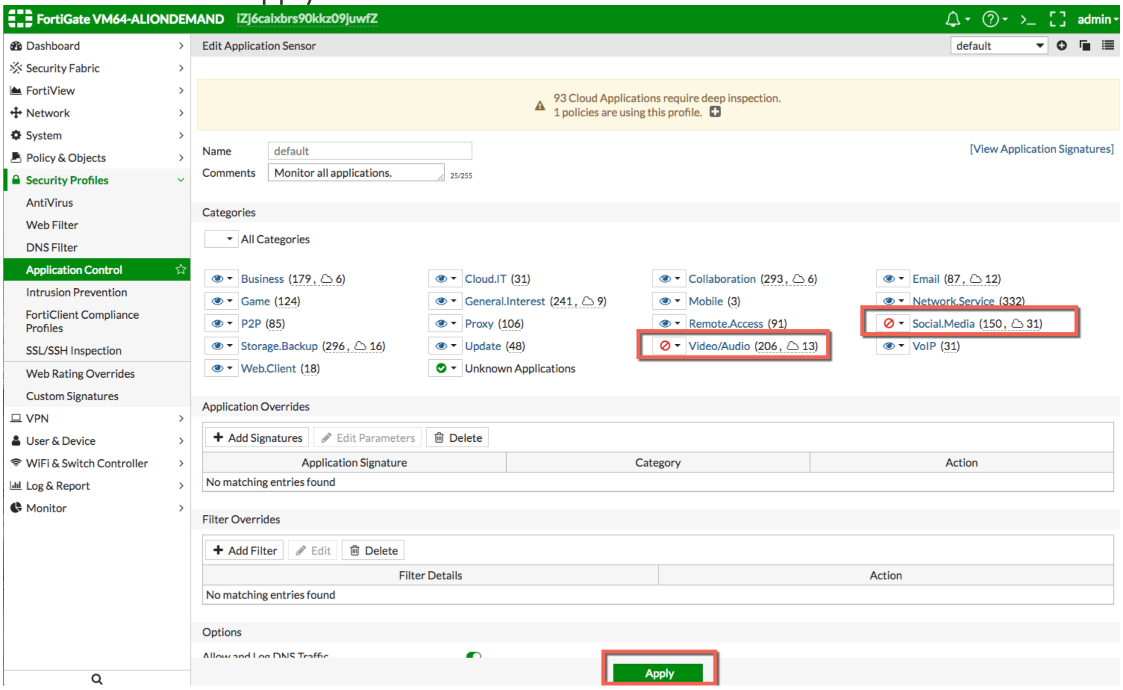
46. And we also can see the Threats in Fortinet console



Threat	Category	Threat Level	Threat Score (Blocked/Allowed)	Sessions (Blocked/Allowed)
EICAR_TEST_FILE	Malware	Critical	900	18
Failed Connection Attempts	Failed Connection Attempts	Low	5	1

Demonstrate the Application Control access feature

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



93 Cloud Applications require deep inspection.
1 policies are using this profile.

Name: default

Comments: Monitor all applications. 25/255

Categories

All Categories

Business (179, 6)
Game (124)
P2P (85)
Storage.Backup (296, 16)
Web.Client (18)
Cloud.IT (31)
General.Interest (241, 9)
Proxy (106)
Update (48)
✓ Unknown Applications
Collaboration (293, 6)
Mobile (3)
Remote.Access (91)
⊘ Video/Audio (206, 13)
Email (87, 12)
Network.Service (332)
⊘ Social.Media (150, 31)
VoIP (31)

Application Overrides

Application Signature	Category	Action
No matching entries found		

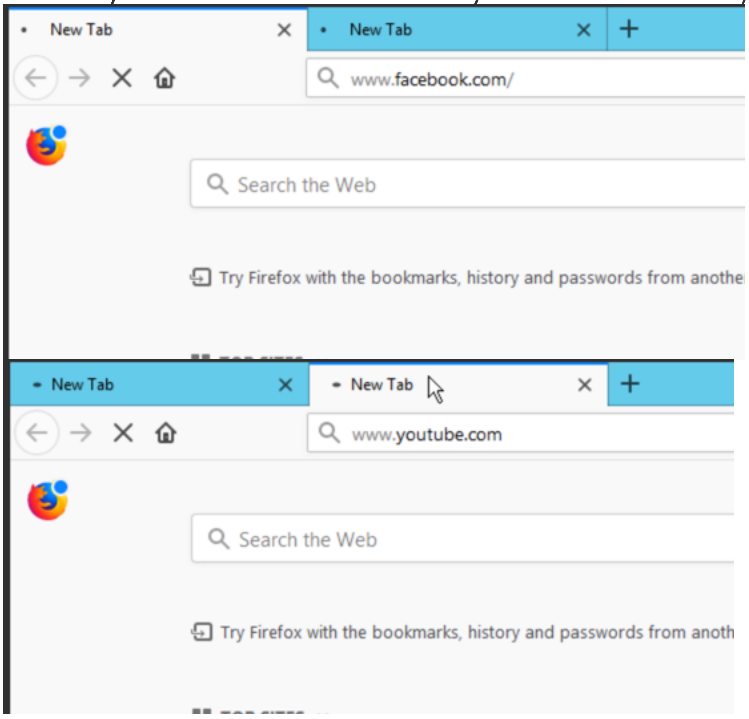
Filter Overrides

Filter Details	Action
No matching entries found	

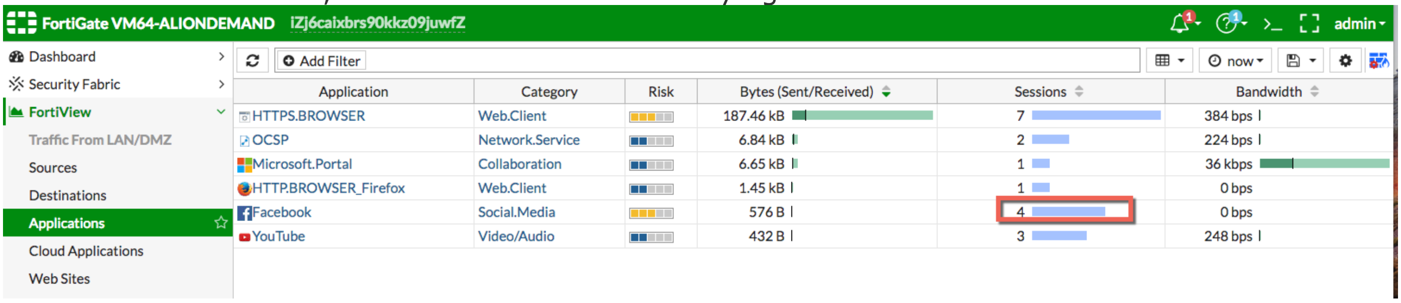
Options

Allow and Log DNS Traffic

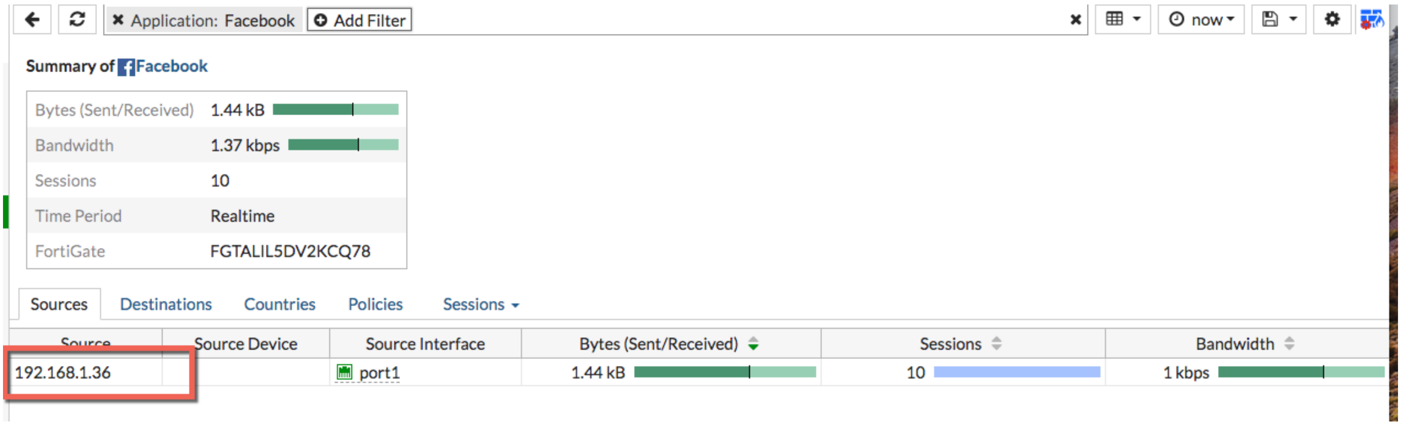
48. Then try to access facebook and youtube in the ECS, you will see they are not able to connect


New Tab
New Tab
www.facebook.com/
Search the Web
Try Firefox with the bookmarks, history and passwords from anothe
New Tab
New Tab
www.youtube.com
Search the Web
Try Firefox with the bookmarks, history and passwords from anoth

49. In the Fortinet console, we will see which clients trying to connect to facebook as well



Application	Category	Risk	Bytes (Sent/Received)	Sessions	Bandwidth
HTTPS.BROWSER	Web.Client		187.46 kB	7	384 bps
OCSP	Network.Service		6.84 kB	2	224 bps
Microsoft.Portal	Collaboration		6.65 kB	1	36 kbps
HTTP.BROWSER_Firefox	Web.Client		1.45 kB	1	0 bps
Facebook	Social.Media		576 B	4	0 bps
YouTube	Video/Audio		432 B	3	248 bps



Summary of Facebook

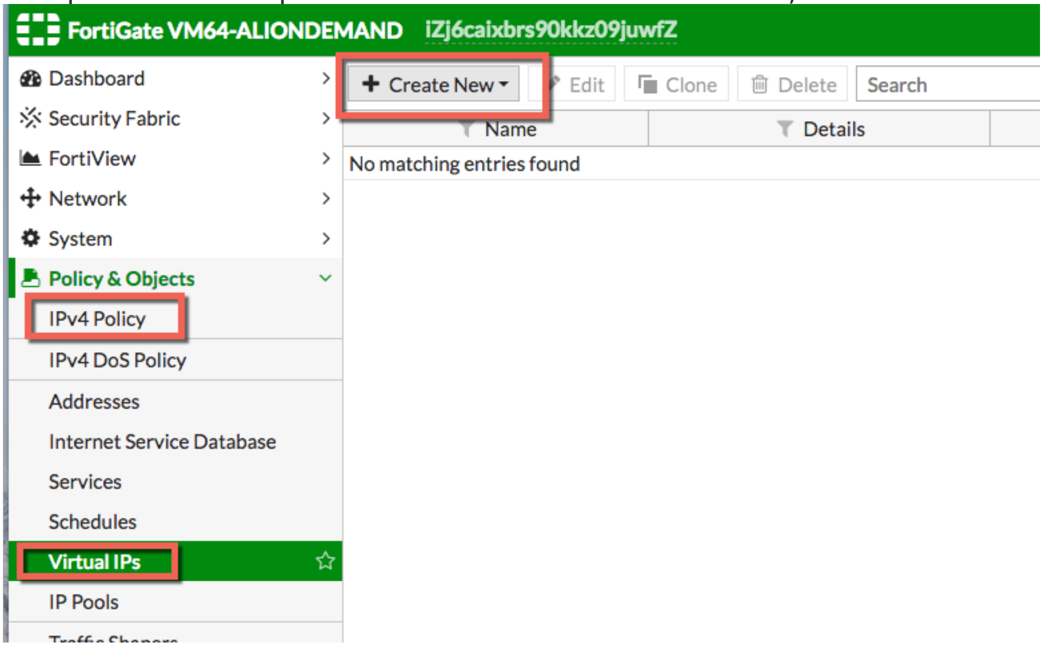
Bytes (Sent/Received)	1.44 kB
Bandwidth	1.37 kbps
Sessions	10
Time Period	Realtime
FortiGate	FGTALIL5DV2KCQ78

Source	Source Device	Source Interface	Bytes (Sent/Received)	Sessions	Bandwidth
192.168.1.36		port1	1.44 kB	10	1 kbps

Enable NAT inbound protection in Fortinet

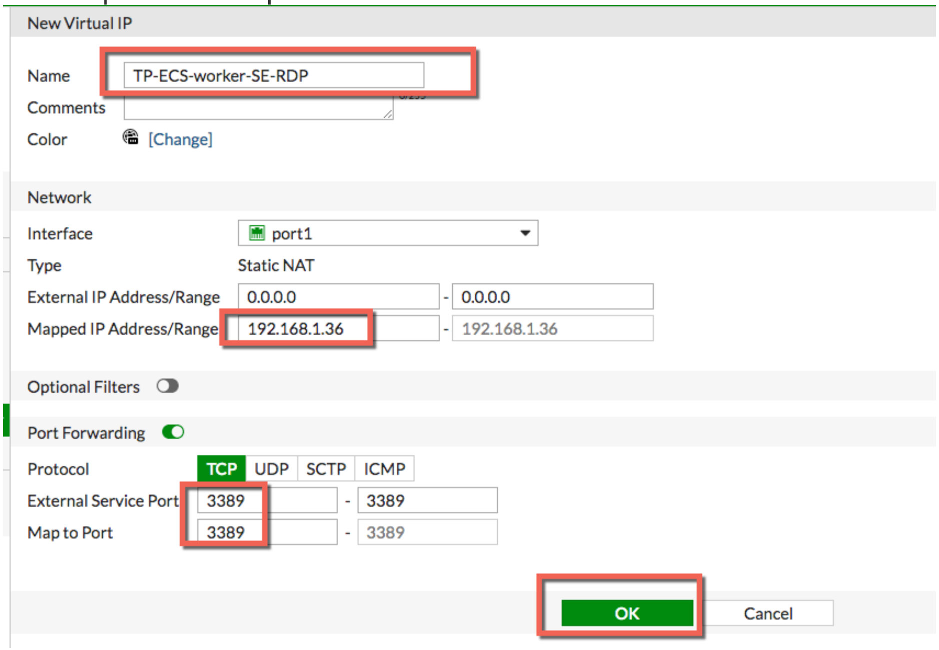
In this sample, I’ll try to enable the Fortinet to protect inbound RDP traffic, the same concept can be applied to HTTP/HTTPS and other services too, this is very useful because most customers want Fortinet to monitor both inbound and outbound traffic

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



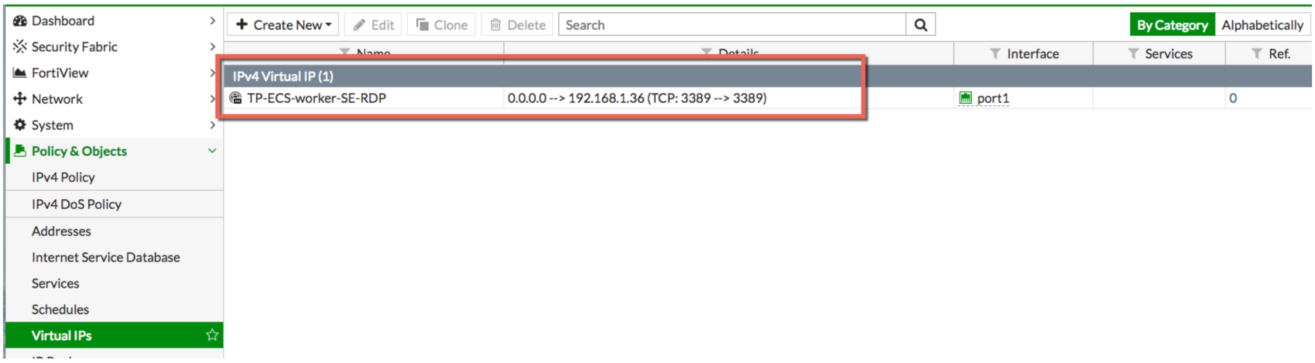
No matching entries found

51. We map the 3389 port of the Fortinet to the ECS 192.168.1.36



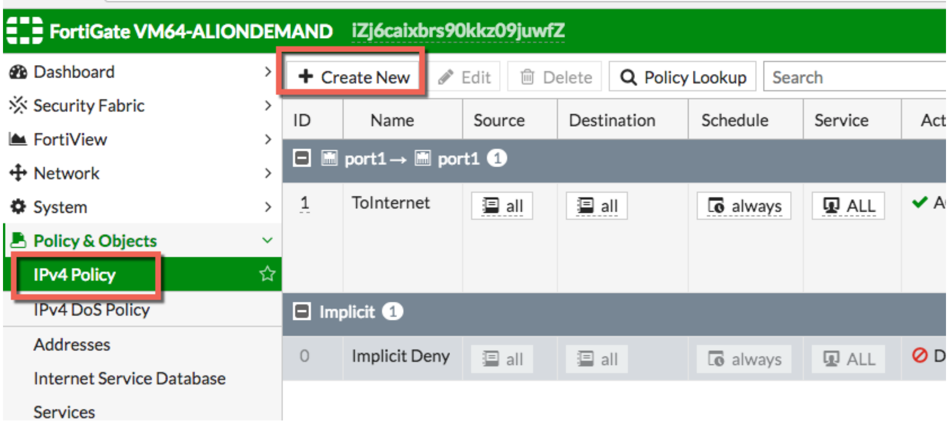
Name	TP-ECS-worker-SE-RDP
Comments	
Interface	port1
Type	Static NAT
External IP Address/Range	0.0.0.0 - 0.0.0.0
Mapped IP Address/Range	192.168.1.36 - 192.168.1.36
Protocol	TCP
External Service Port	3389 - 3389
Map to Port	3389 - 3389

52. Can see the Virtual IP there now



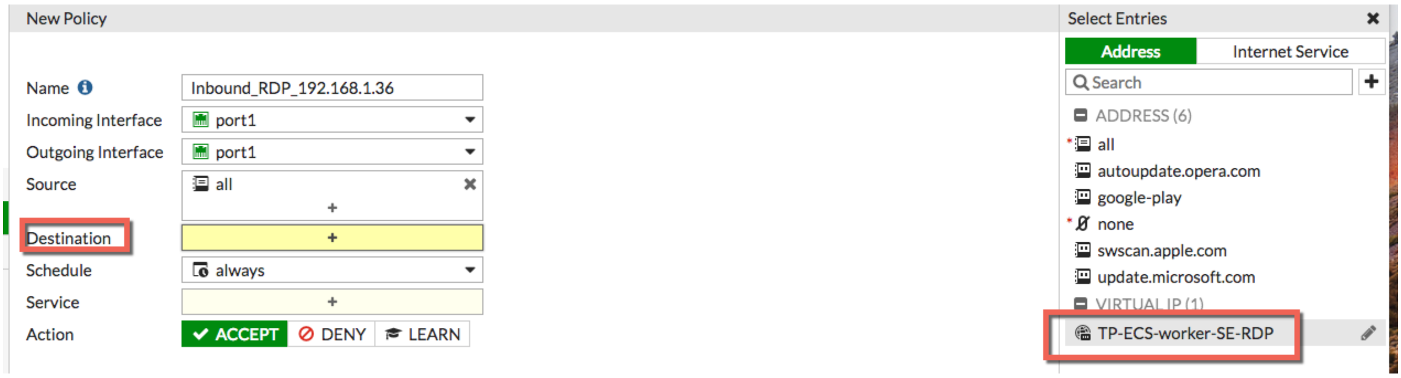
Name	Details	Interface	Services	Ref.
IPv4 Virtual IP (1)				
TP-ECS-worker-SE-RDP	0.0.0.0 --> 192.168.1.36 (TCP: 3389 --> 3389)	port1		0

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



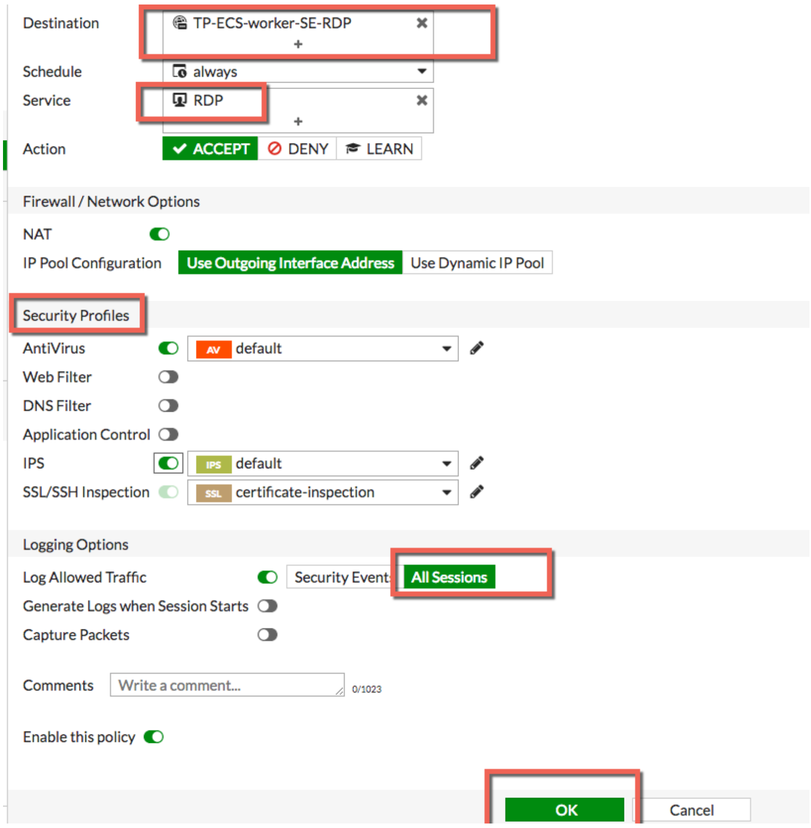
ID	Name	Source	Destination	Schedule	Service	Act
port1 → port1 1						
1	ToInternet	all	all	always	ALL	✓ A
Implicit 1						
0	Implicit Deny	all	all	always	ALL	⊘ D

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


New Policy

Name	Inbound_RDP_192.168.1.36
Incoming Interface	port1
Outgoing Interface	port1
Source	all
Destination	+
Schedule	always
Service	+
Action	✓ ACCEPT ⊘ DENY LEARN

55. Similarly, enable the security profiles you want, and then use All Sessions as Log allowed traffic for demo purpose.



Destination: TP-ECS-worker-SE-RDP

Schedule: always

Service: RDP

Action: ✓ ACCEPT | DENY | LEARN

Firewall / Network Options

NAT: ●

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

Security Profiles

AntiVirus: ● AV default

Web Filter: ○

DNS Filter: ○

Application Control: ○

IPS: ● IPS default

SSL/SSH Inspection: ● SSL certificate-inspection

Logging Options

Log Allowed Traffic: ● Security Events | All Sessions

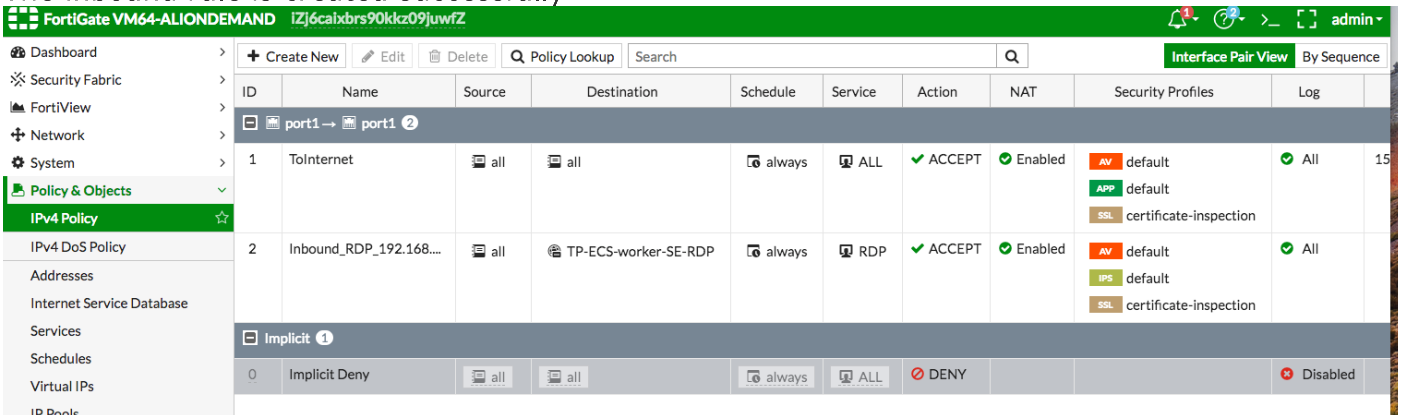
Generate Logs when Session Starts: ○

Capture Packets: ○

Comments: Write a comment... 0/1023

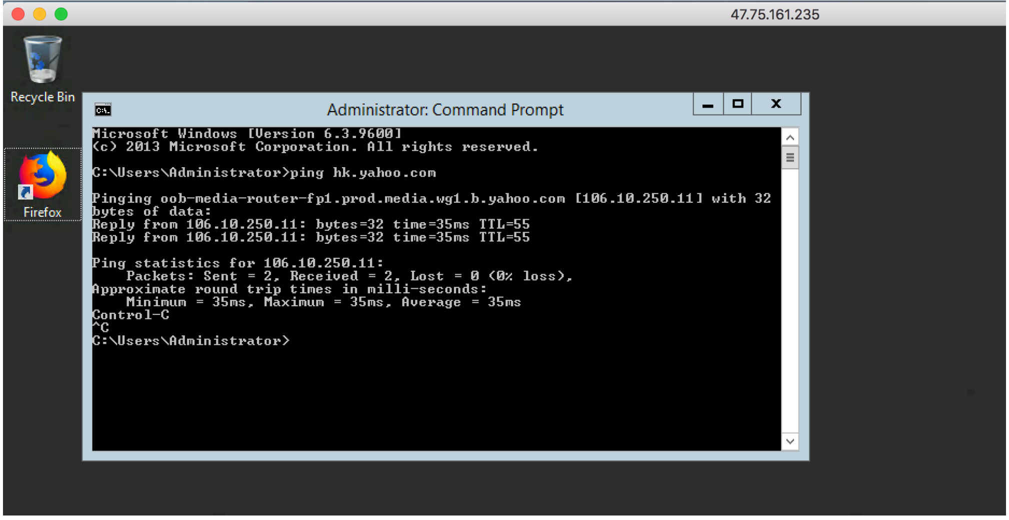
Enable this policy: ●

56. The inbound rule is created successfully



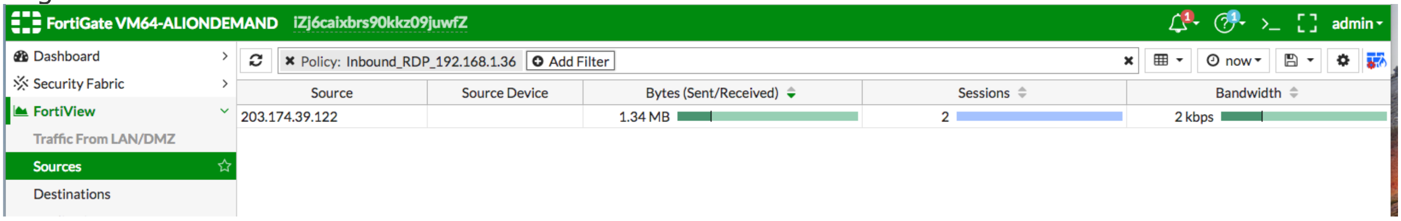
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	
port1 → port1 2										
1	ToInternet	all	all	always	ALL	✓ ACCEPT	✓ Enabled	AV default APP default SSL certificate-inspection	✓ All	15
2	Inbound_RDP_192.168....	all	TP-ECS-worker-SE-RDP	always	RDP	✓ ACCEPT	✓ Enabled	AV default IPS default SSL certificate-inspection	✓ All	
Implicit 1										
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	

57. And now you should be able to use the Fortinet Public IP address to RDP the ECS



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

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

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

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

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



Policy: Inbound_RDP_192.168.1.36

Source	Source Device	Bytes (Sent/Received)	Sessions	Bandwidth
203.174.39.122		1.34 MB	2	2 kbps

Conclusions

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