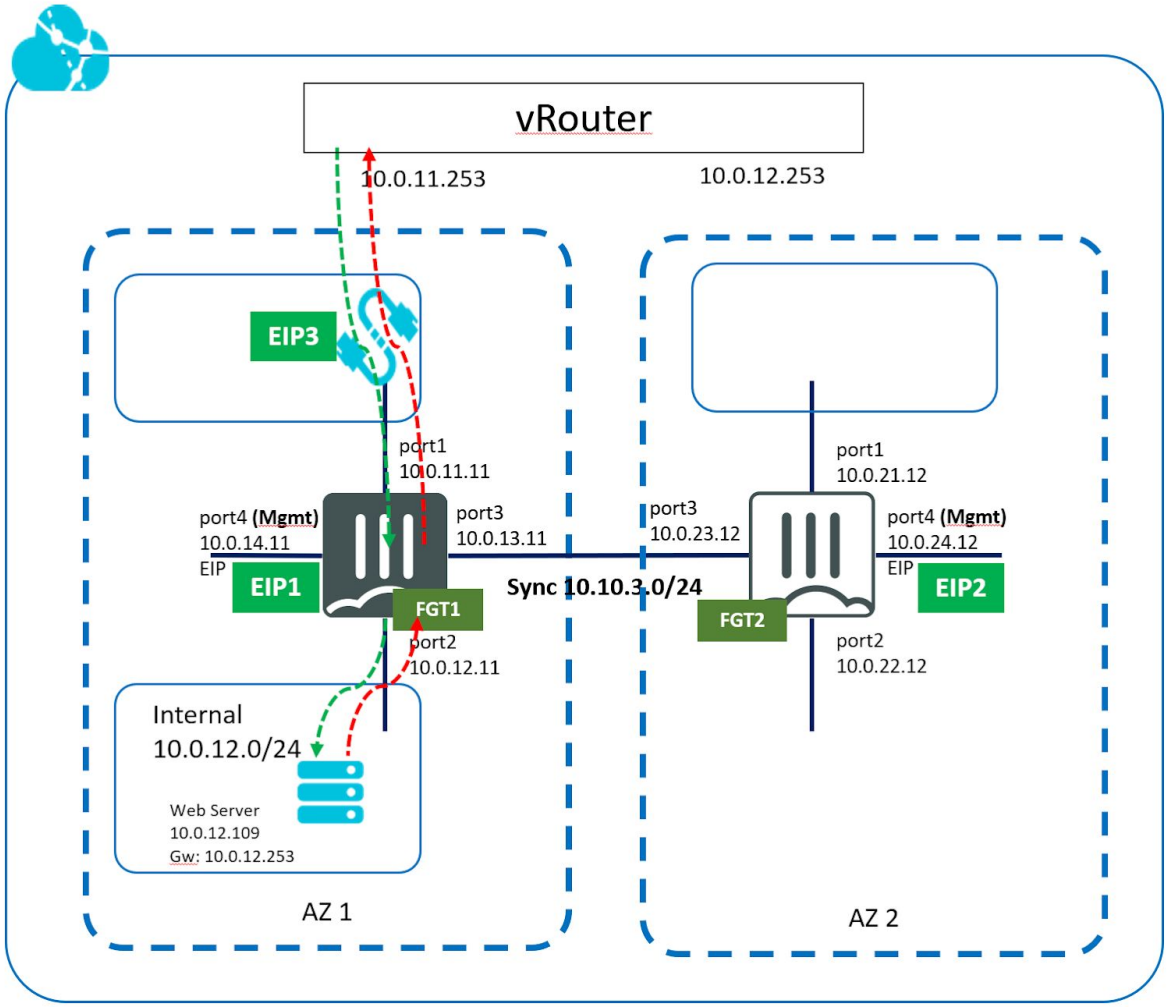
Step by Step guide for deploy and config fortigate A-P HA cross AZ zone

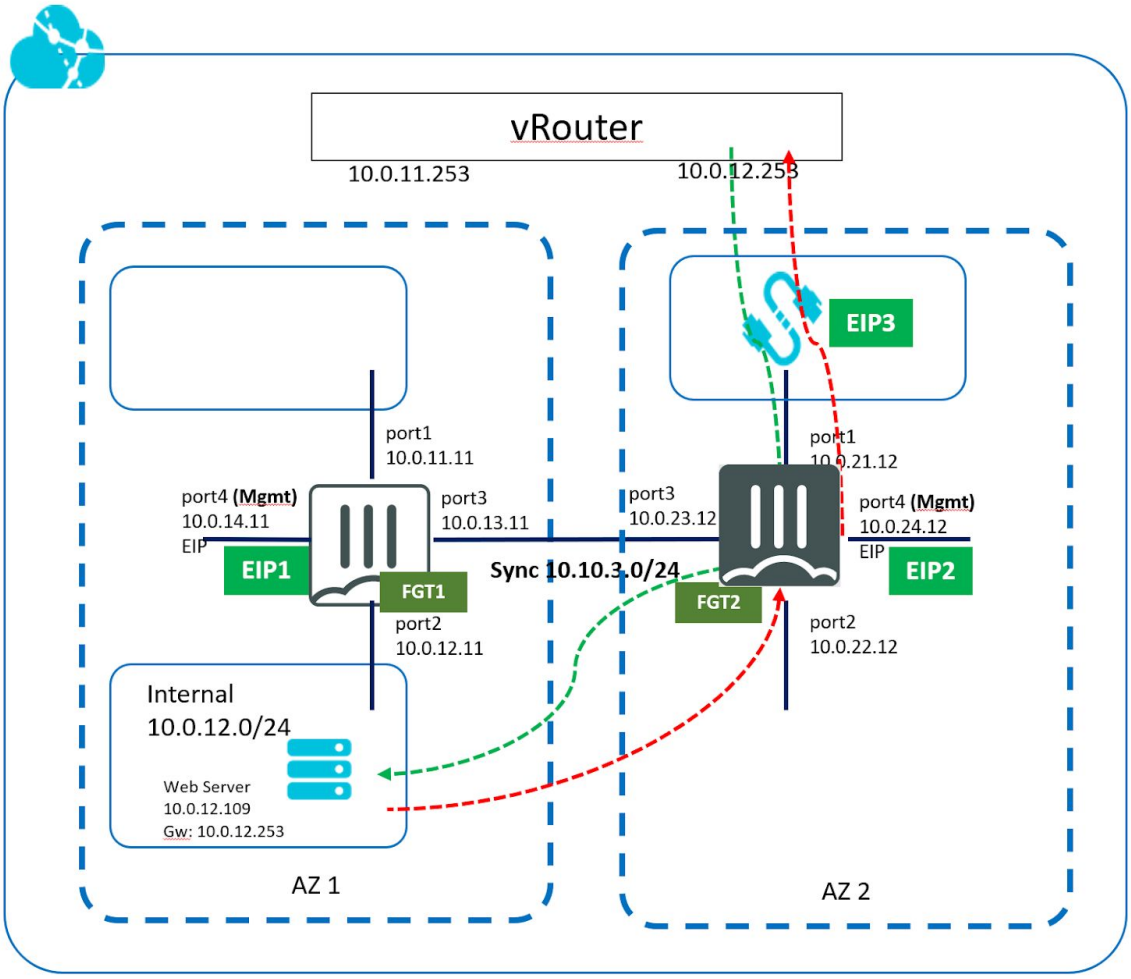
Diagram



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

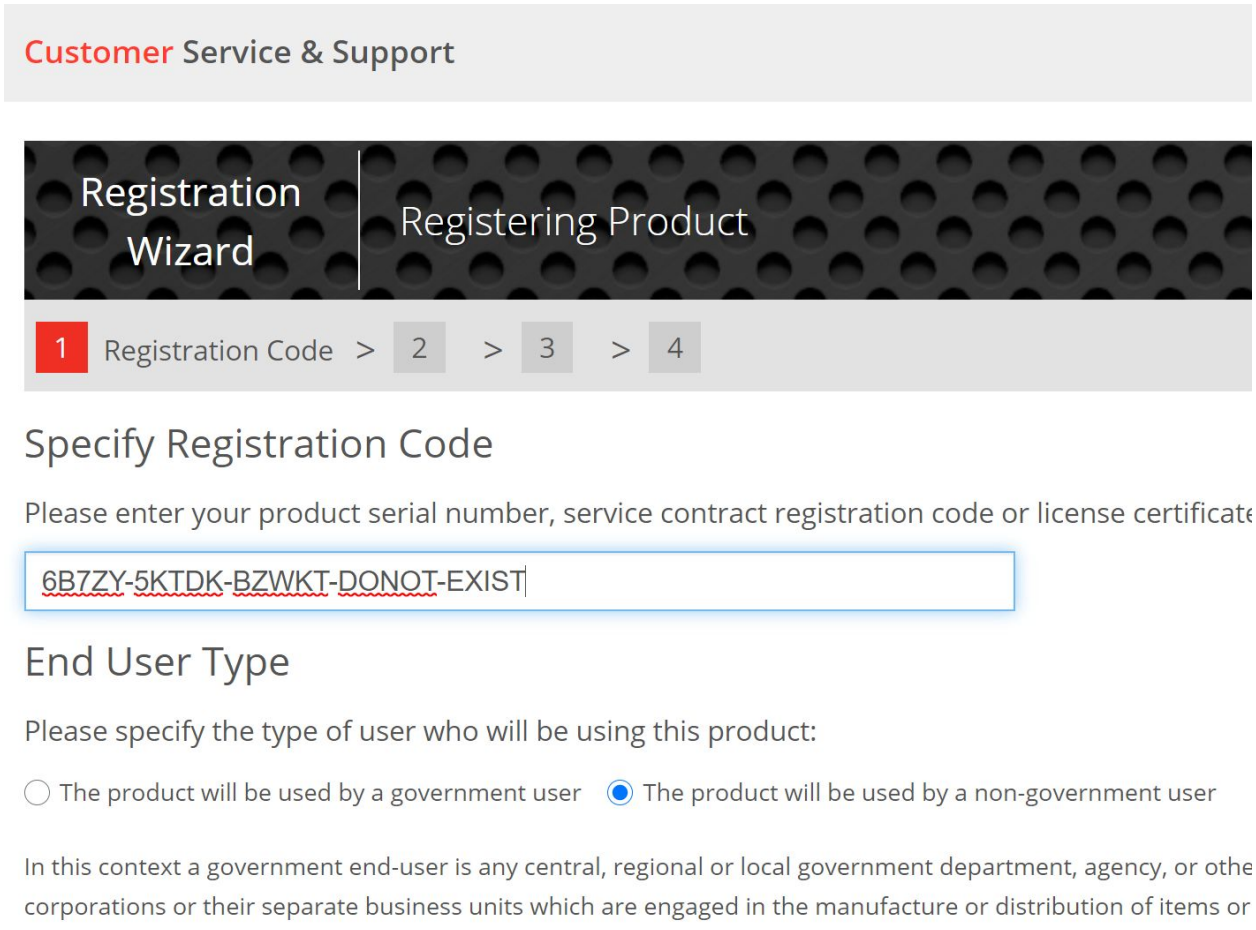
Reference Document

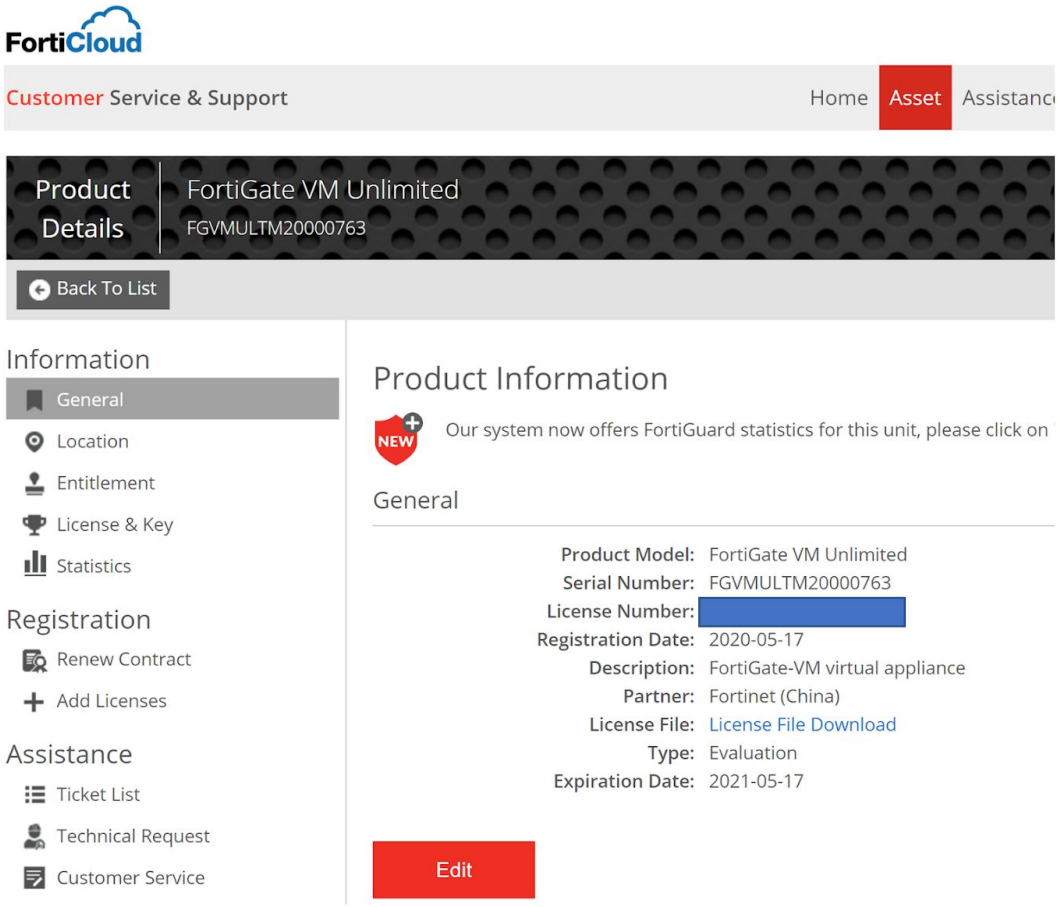
https://docs.fortinet.com/vm/alicloud/fortigate/6.4/alicloud-cookbook/6.4.0/967820/deploying-fortigate-vm-ha-on-alicloud-between-availability-zones

License

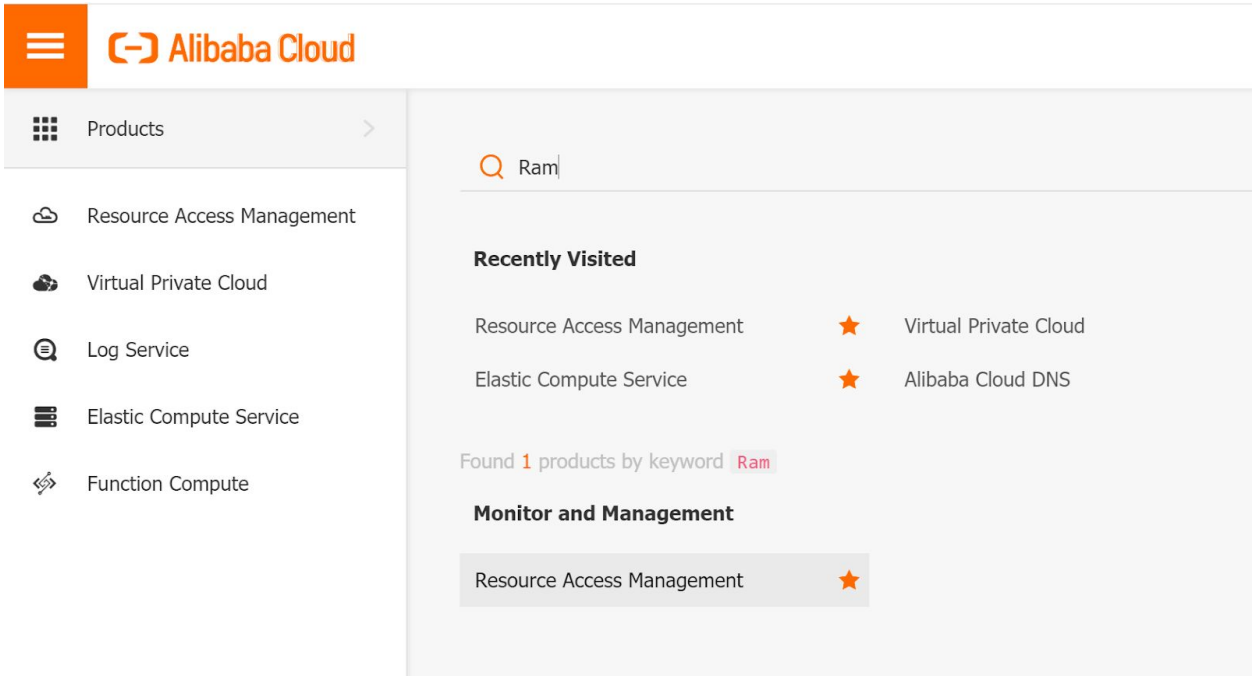
Two Fortigate BYOL License. and active your BYOL license

at support.fortinet.com to Register your license , and download license file.

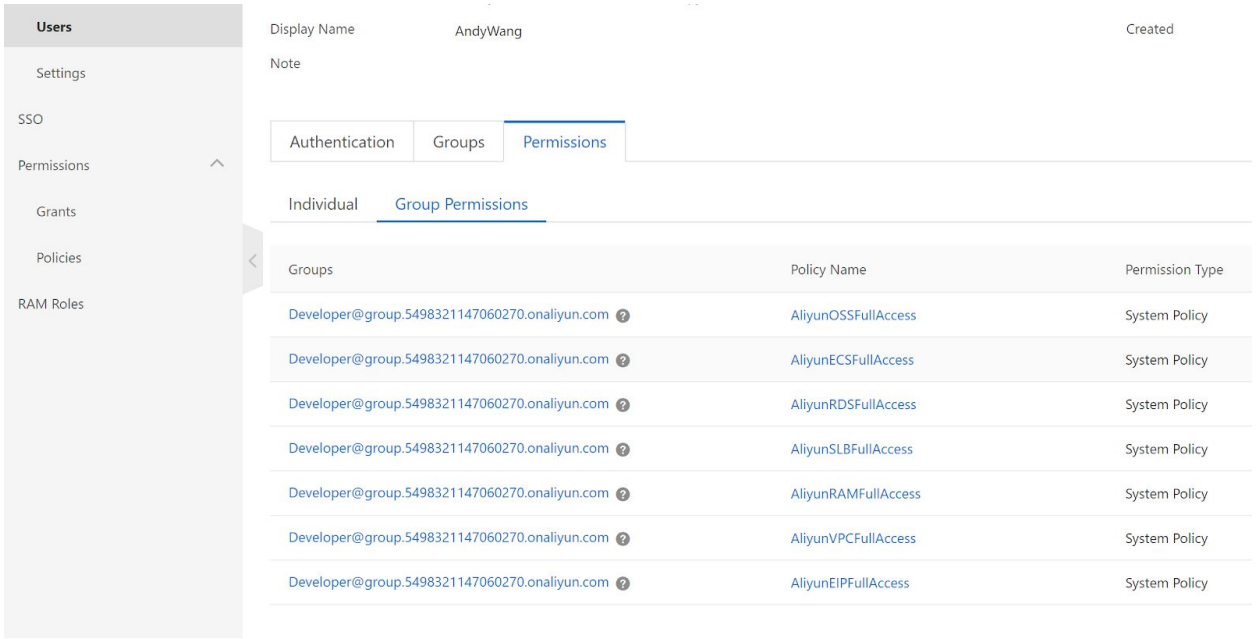


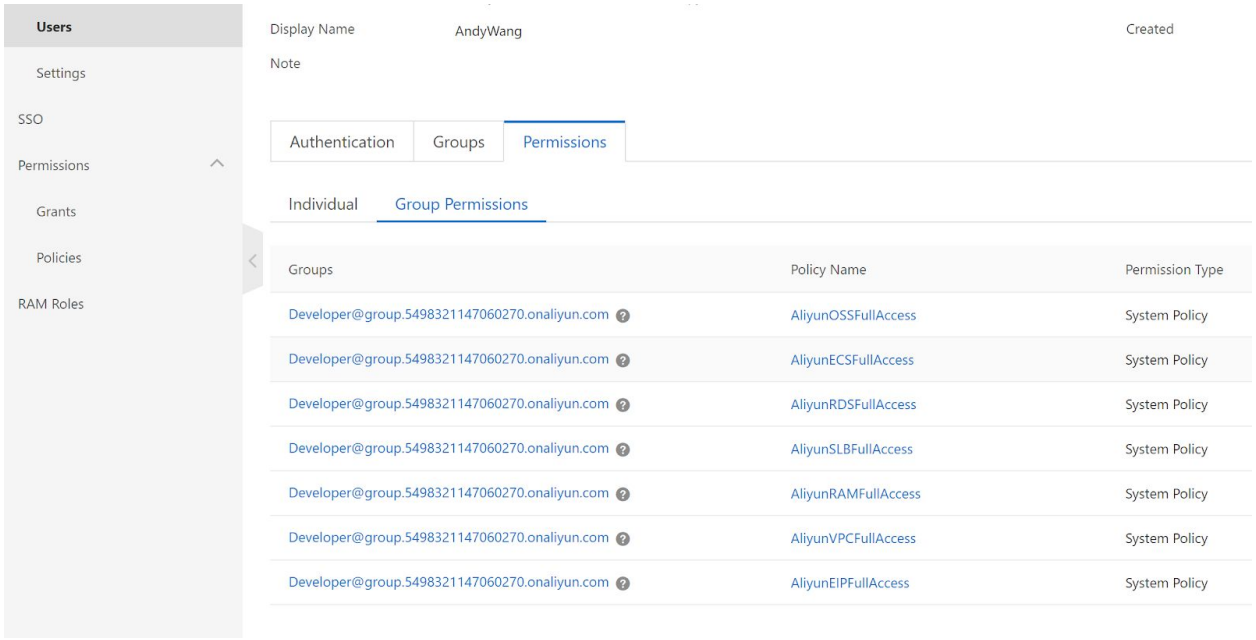


Alicloud account or RAM account



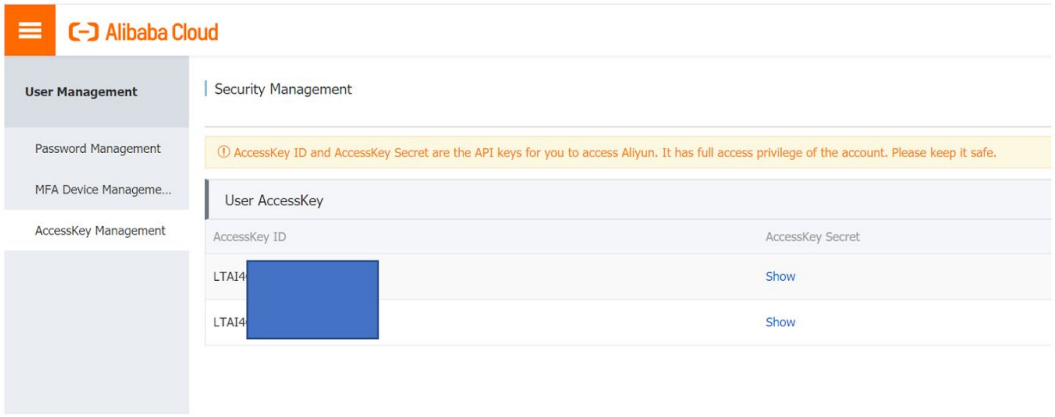
You shall have at least AliyunVPCFullAccess, AliyunECSFullAccess, AliyunRAMFullAccess, AliyunEIPFullAccess privilege.





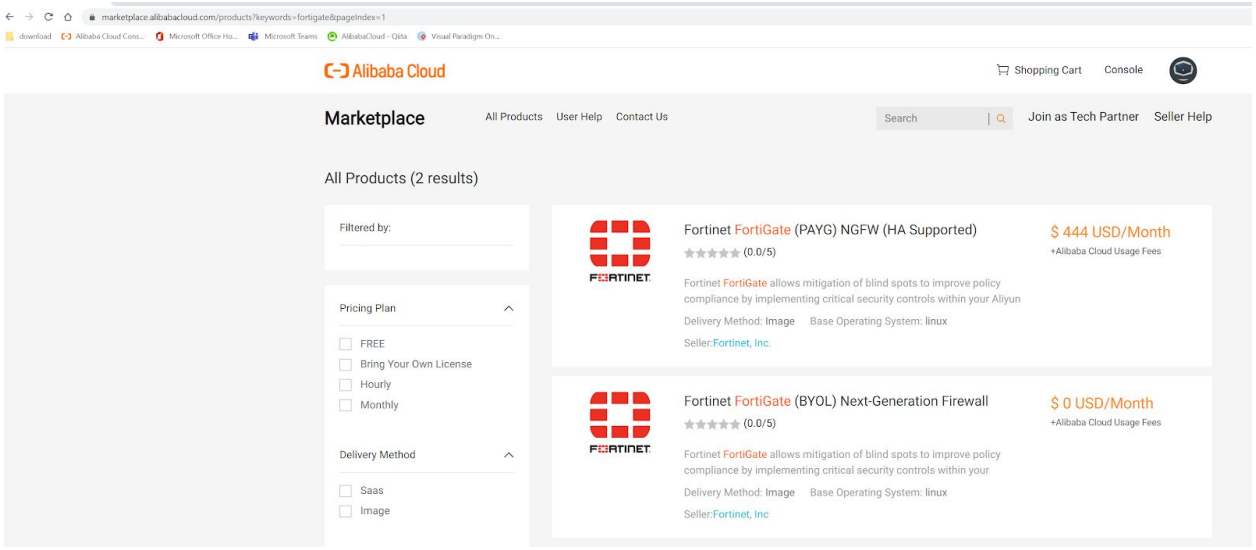
Generate your Access/Secret Combination if you want to use terraform or aliyuncli to deploy/manage resources. for example. you can use terraform script to provision all resource by use

https://github.com/yagosys/fortigate_aliyun/tree/master/AP-CrossZone. you can also just use Aliyun GUI to deploy the resource.



Find Fortigate image from aliyun market

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



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 '.Available
Zones.AvailableZone[] | "\(.AvailableResources.AvailableResource[].SupportedResources.SupportedResource[].Value) \(.ZoneId)"'
"ecs.c5.2xlarge ap-northeast-1b"
```

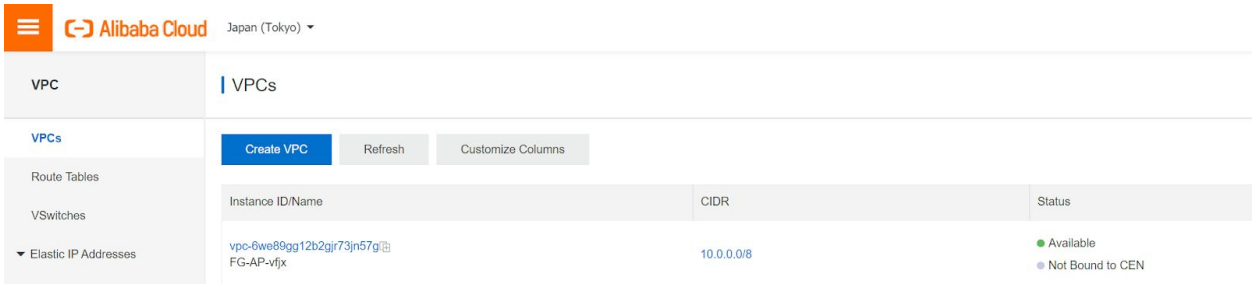
above you will find this instance type is only available in zone ap-northeast-1b.

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.

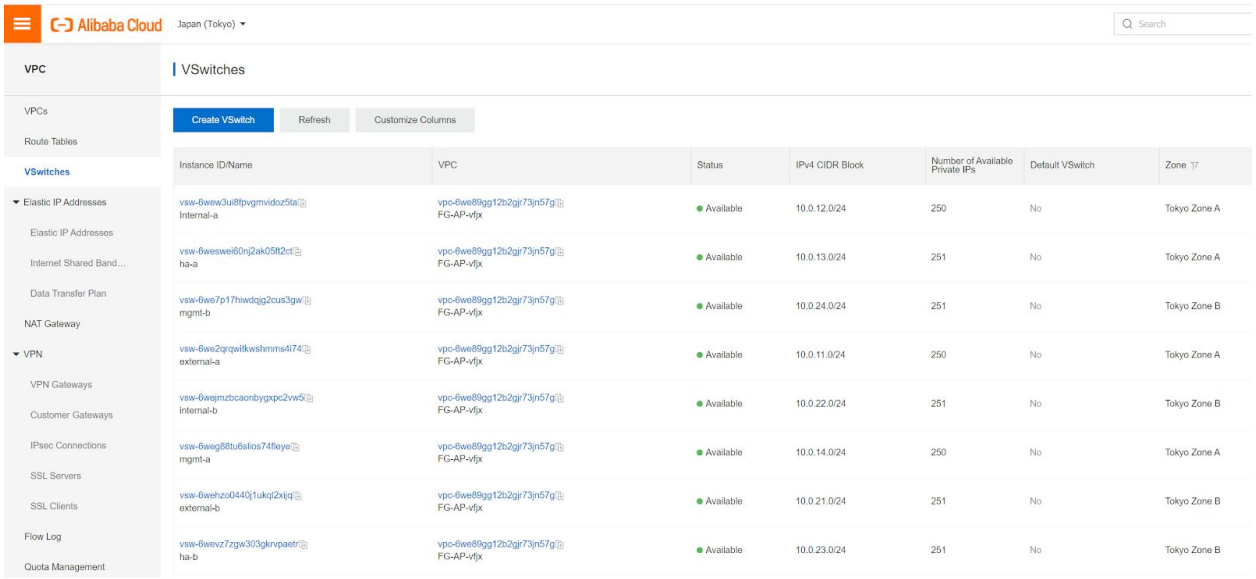
Create alicloud resource

create VPC



create switches.

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

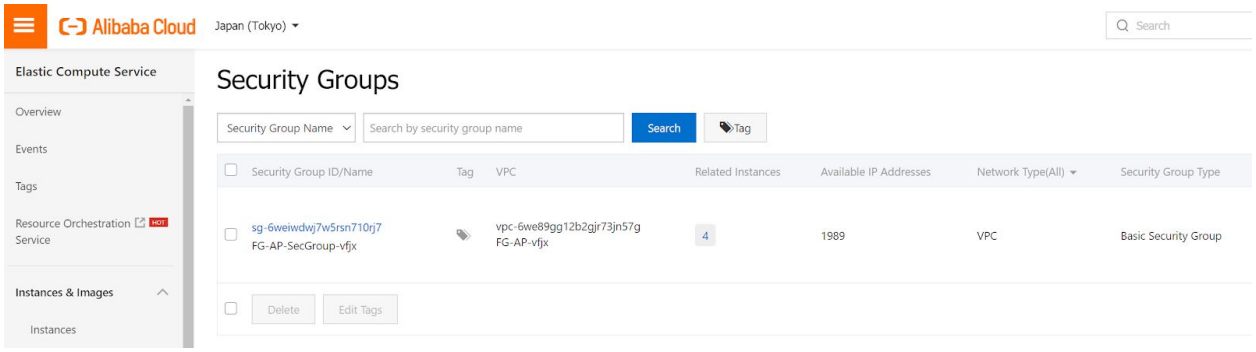


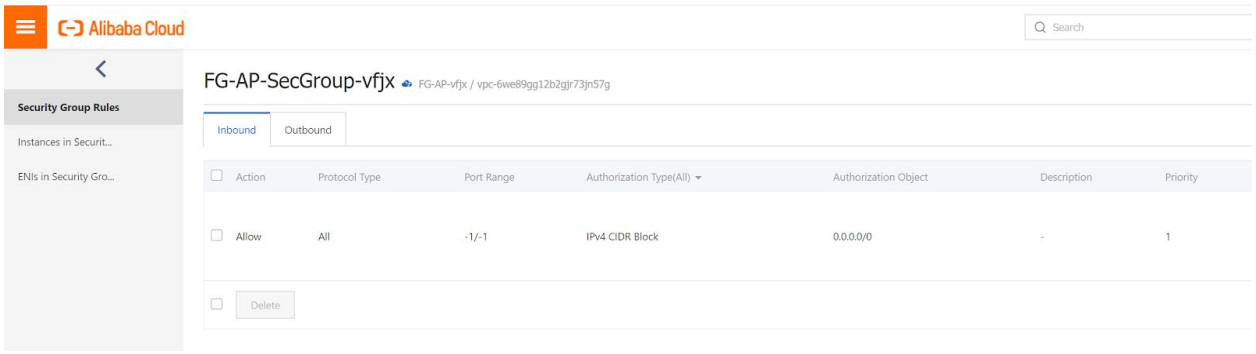
The switch named “externa” is for internet facing. “internal” is for protected traffic, “ha” is for clustering traffic. “mgmt” is for fortigate traffic that access aliyun metadata service(acs). the

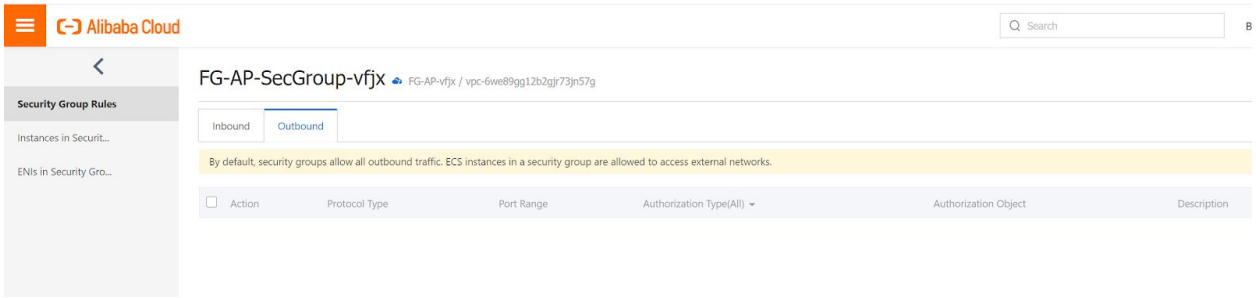
communication between vswitch in different zones has to go through vrouter according to the associated routing table.

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.

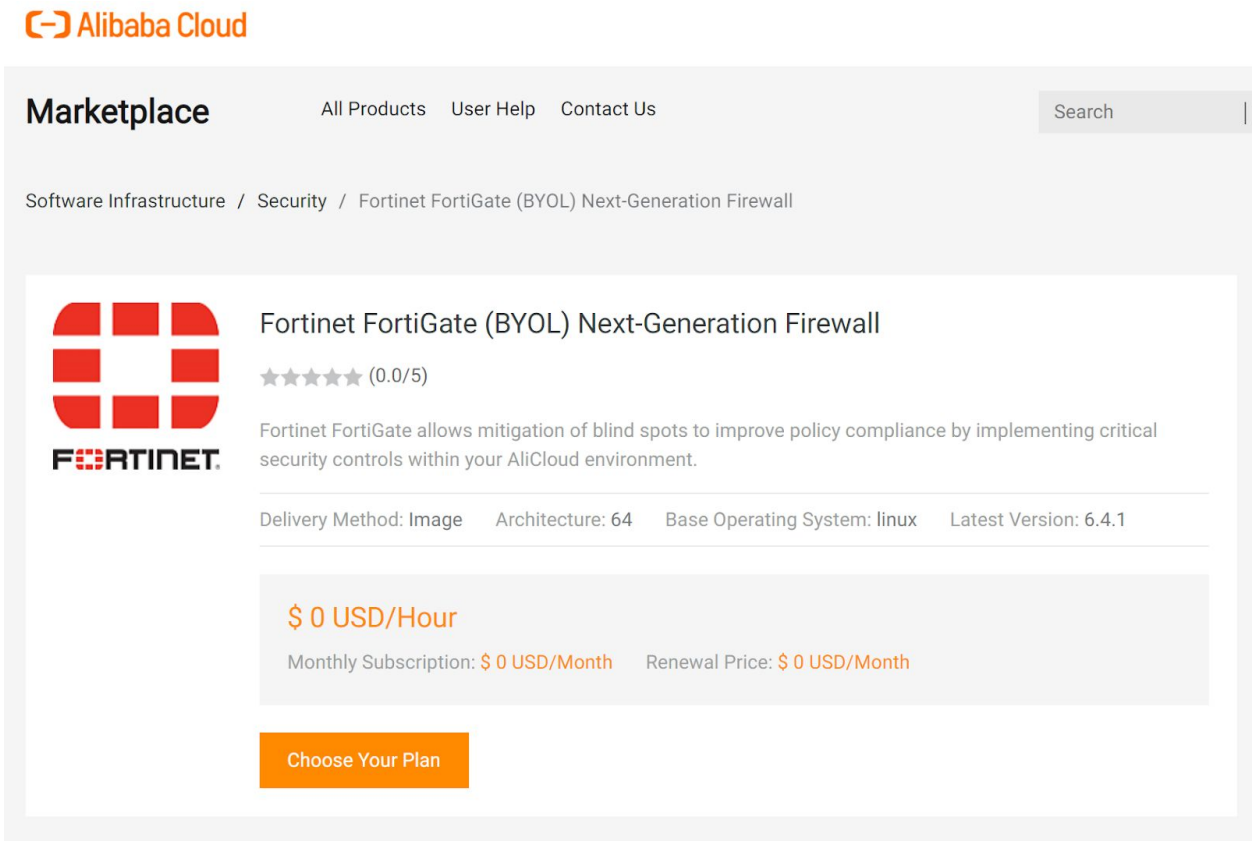




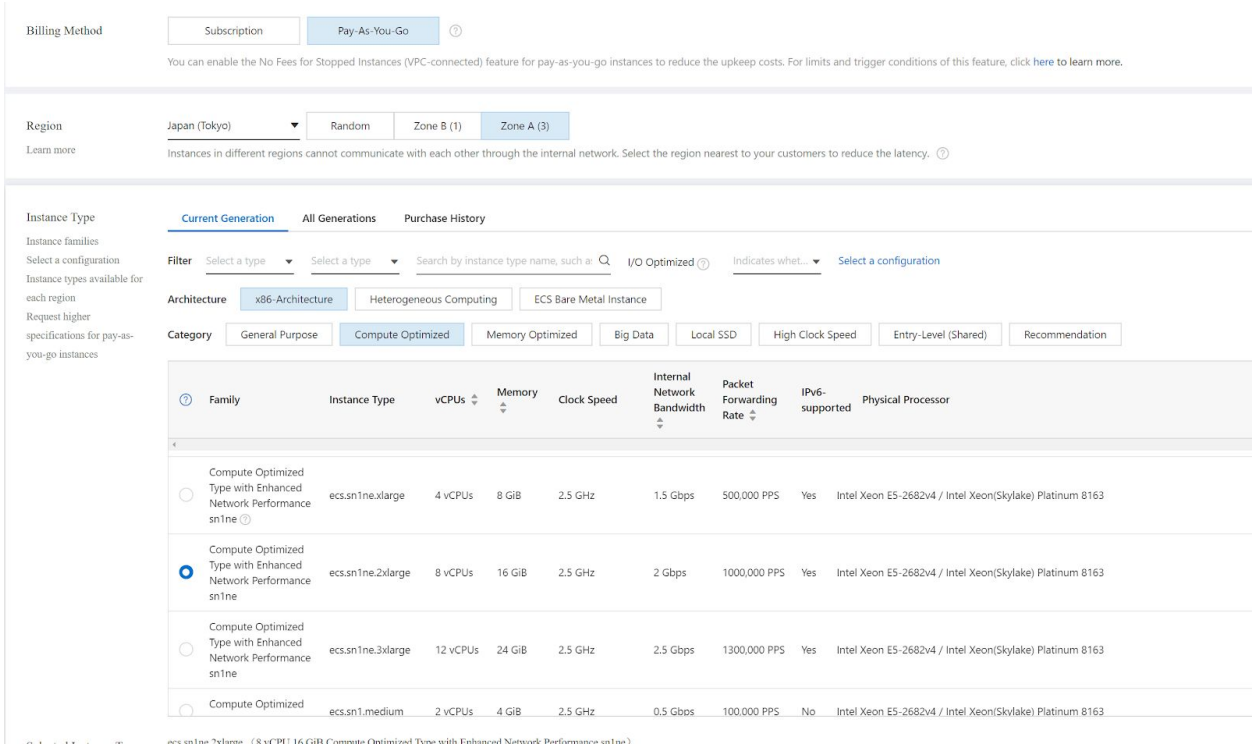


To simplify the installation , here I allow all protocols while the installation. after that. we can refine the policy to more restricted rules. no need to config outbound rules.
Later on, we will need to associate SecurityGroup with ENI and instances.

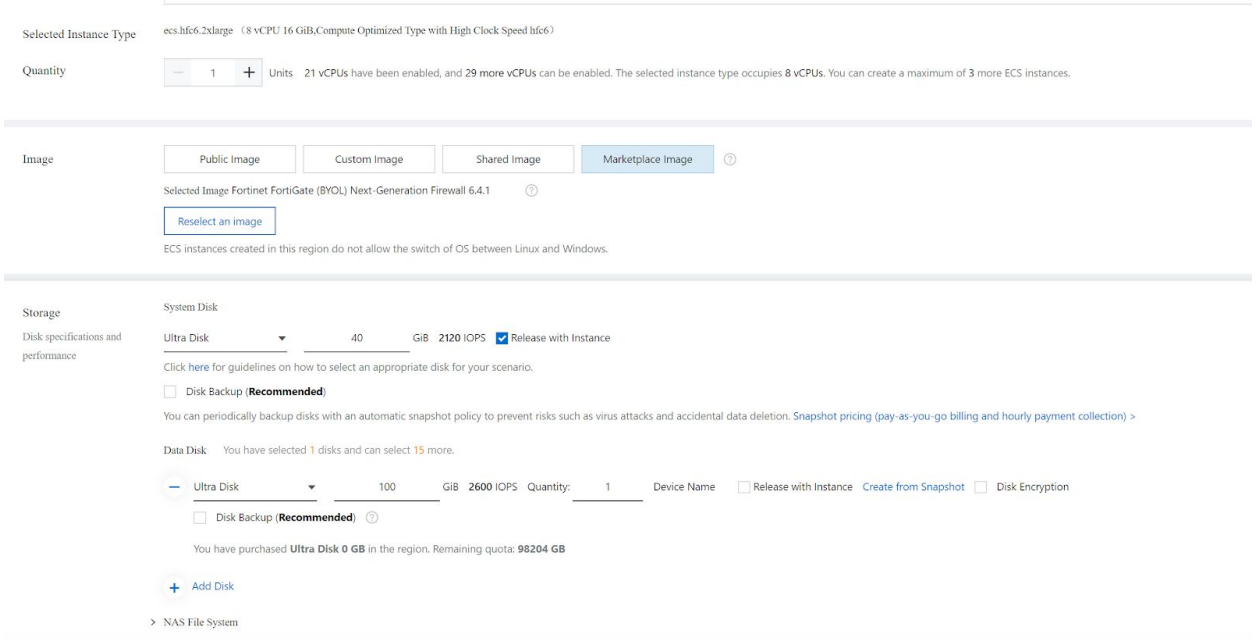
create fortigate instances

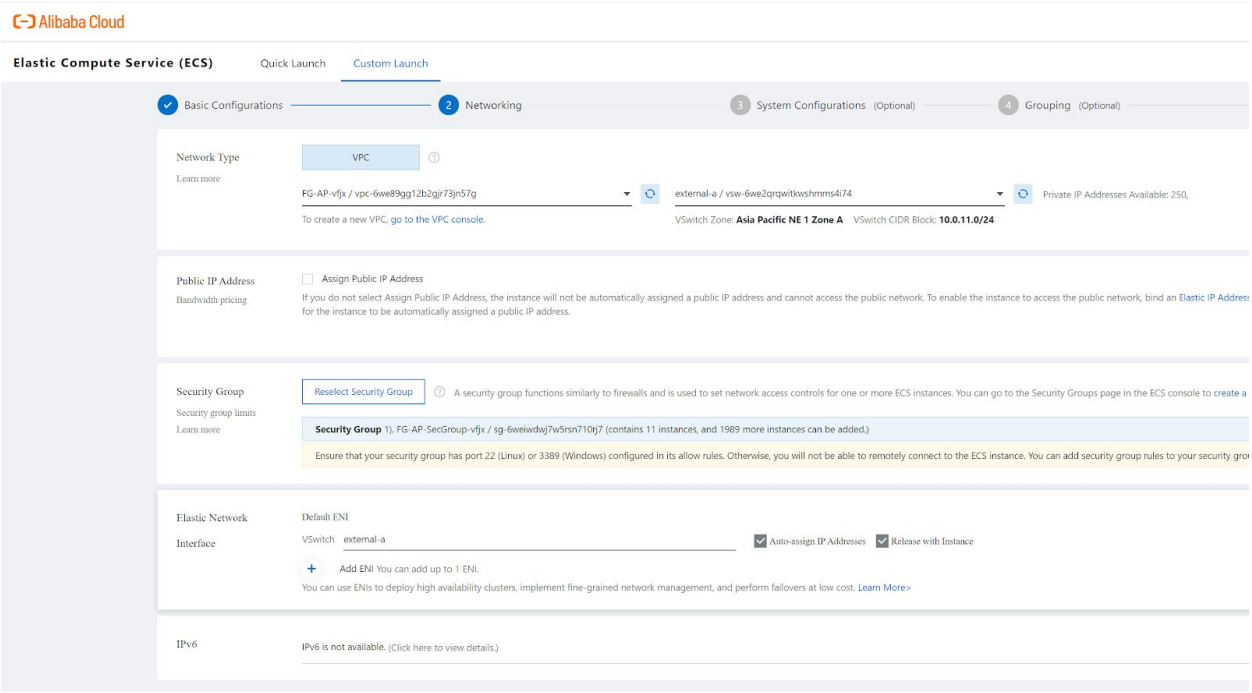


click choose your plan , we can choose either Pay-As-you-go or subscription billing method for aliyun instance. if you want to try a few days. you might want to choose pay-as-you-go.

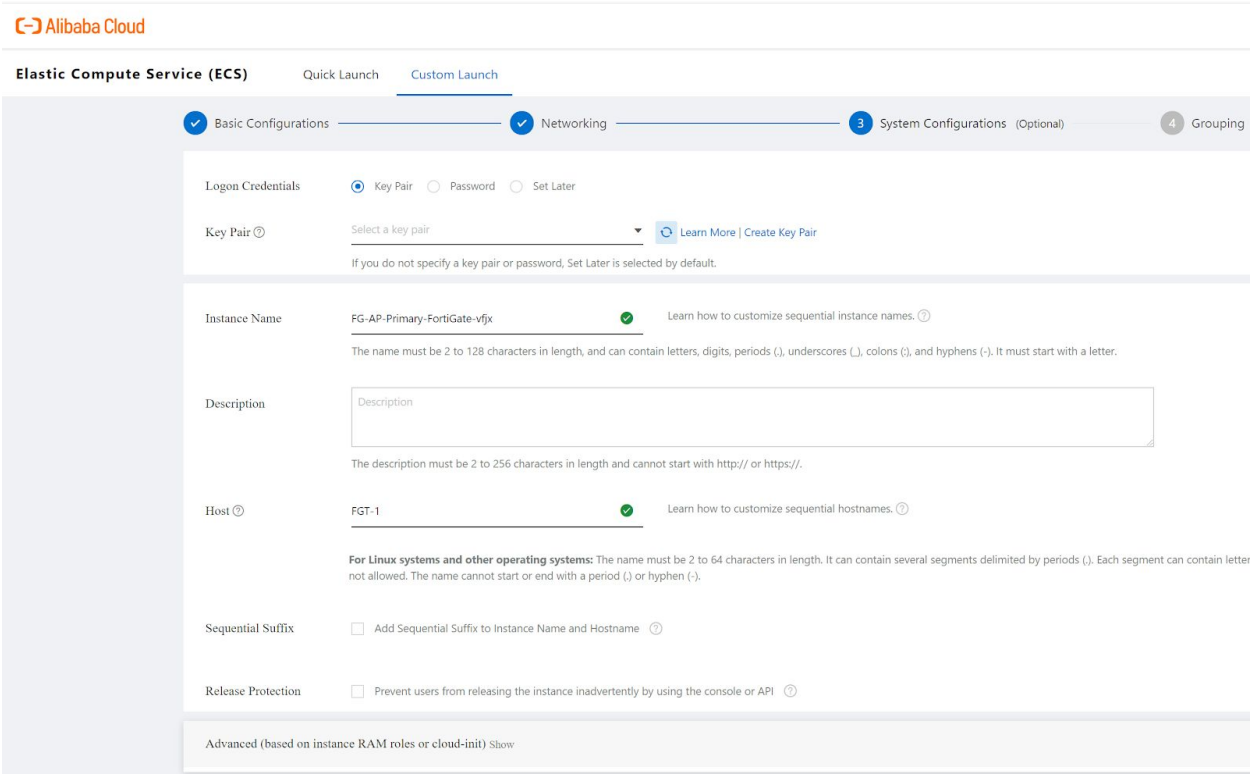


select Region, Zone, “compute Optimized” category. Images will be automatically selected. add Data Disk if you want to log to a local disk. we here select zone A for fortigate-Primary. the instance type use “ecs.sn1ne.2xlarge)

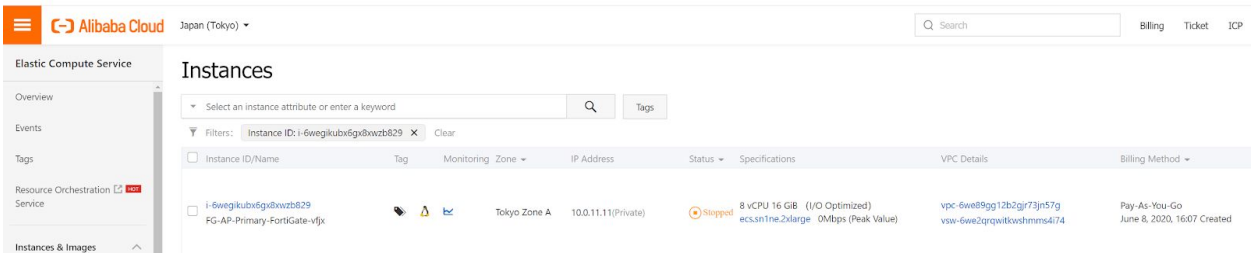




select VPC , external-a switch, as we want Fortigate Primary IP bound to external switch , so it will get an IP address from 10.0.11.0/24 CIDR block. we do not need to check “Assign Public IP address” as later on , we will create an EIP and bind to fortigate primary interface. select the Security group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



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.



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,Vswtich,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: **Up to 9 private IP addresses can be assigned to this ENI.**

(●) Not set ( ) Auto ( ) Manual

* Security Group: Select a security group

Name	ID
FG-AP-SecGroup-vfj...	sg-6weiwdwj7w5rsn710rj7

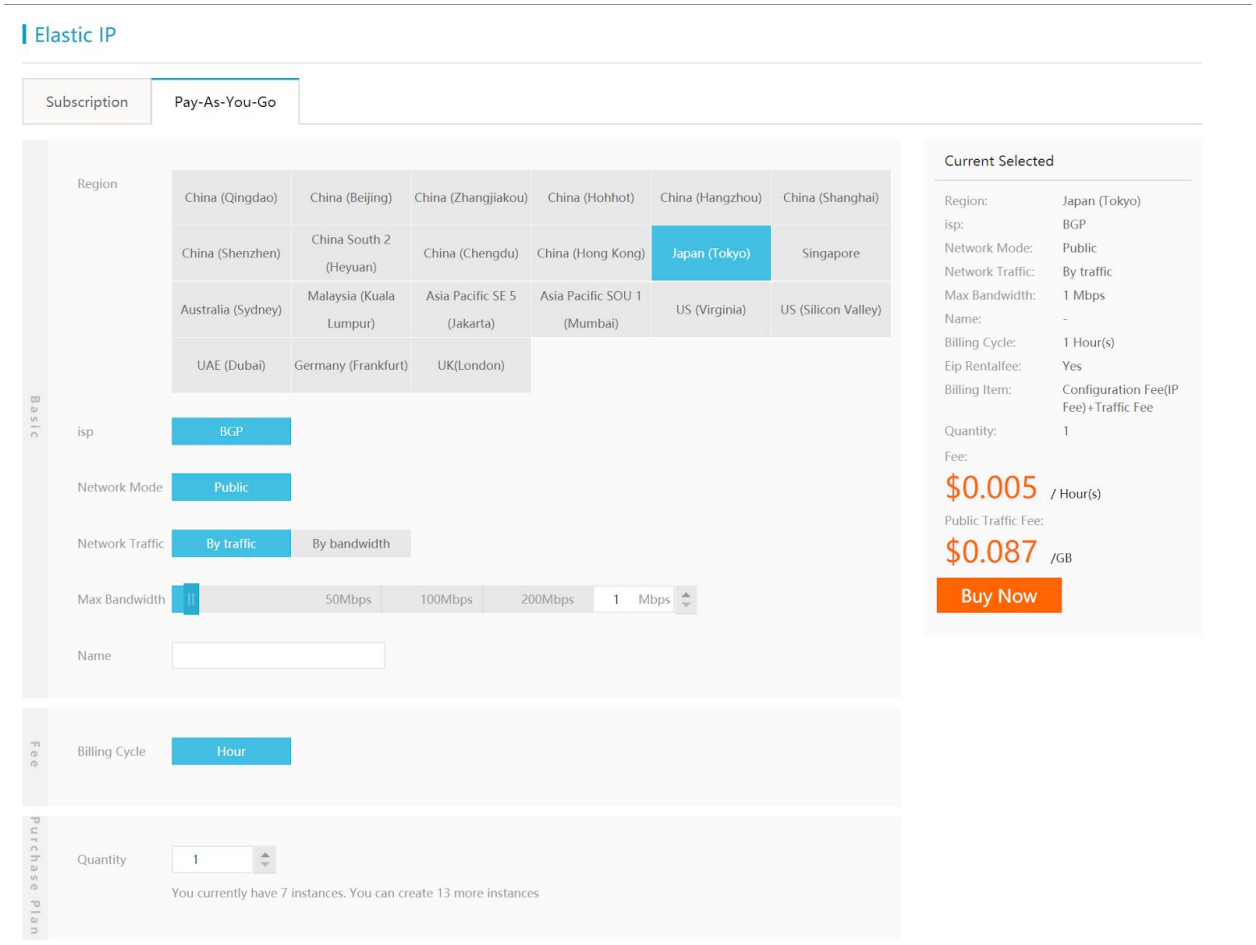
Description:

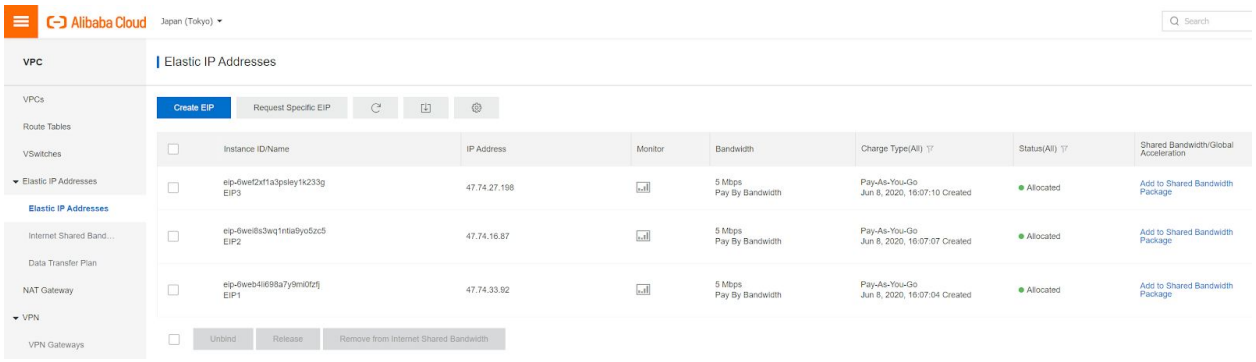
It must be 2 to 256 characters in length and cannot start with http:// or https://.

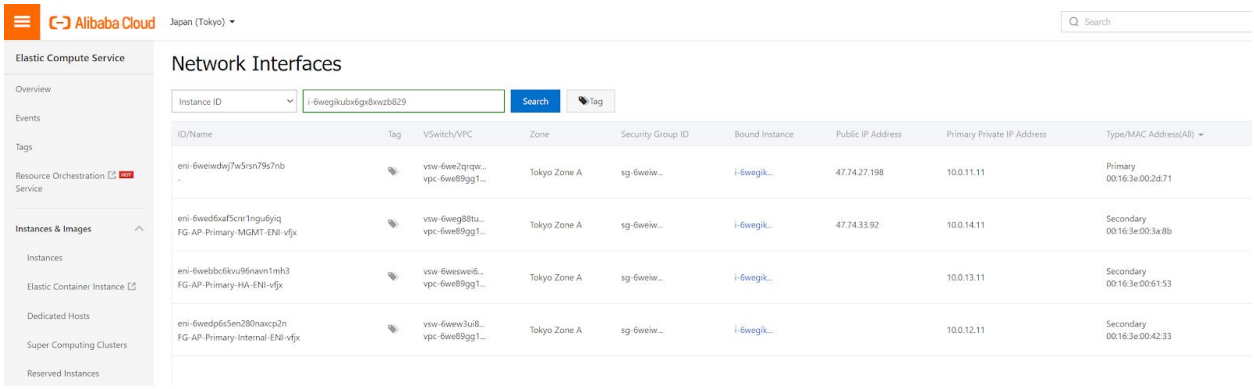
Tag: Select a tag key | Enter or select a tag value.

OK Cancel

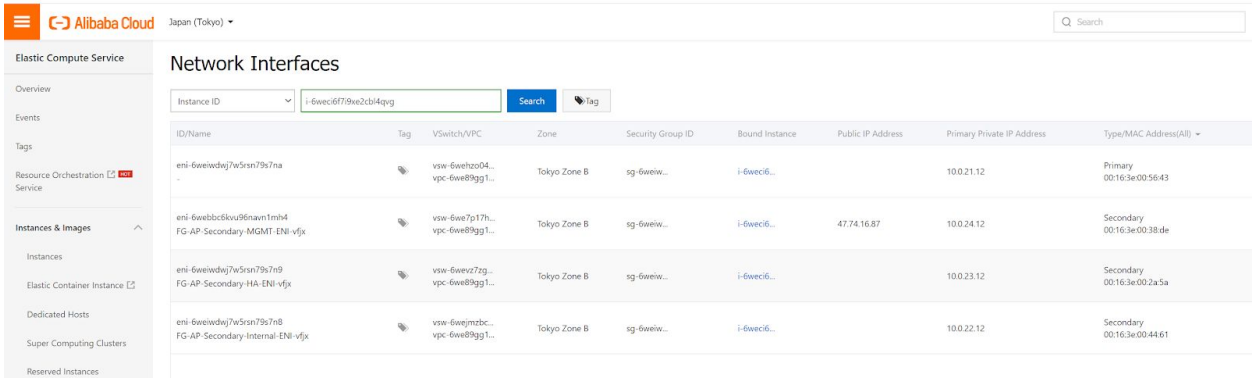
then you will need to create EIP, and Bind EIP to ENI, finally you shall see the result below.







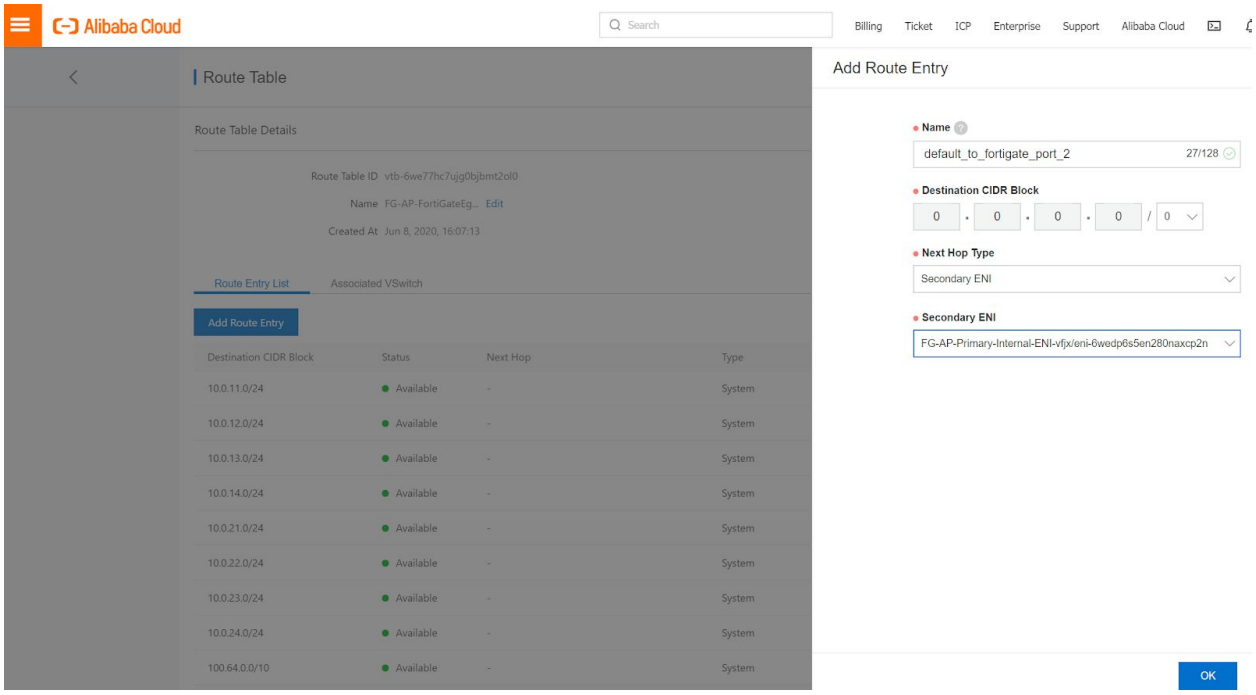
above you see that FGT-1 in zone A is associated with 4 ENIs. The first one in the list is the one created by default with instances. which is associated with EIP3 . The other 3 ENIs are additional ENI which are marked as type “Secondary”. The first “Secondary” ENI is associated with EIP1.



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

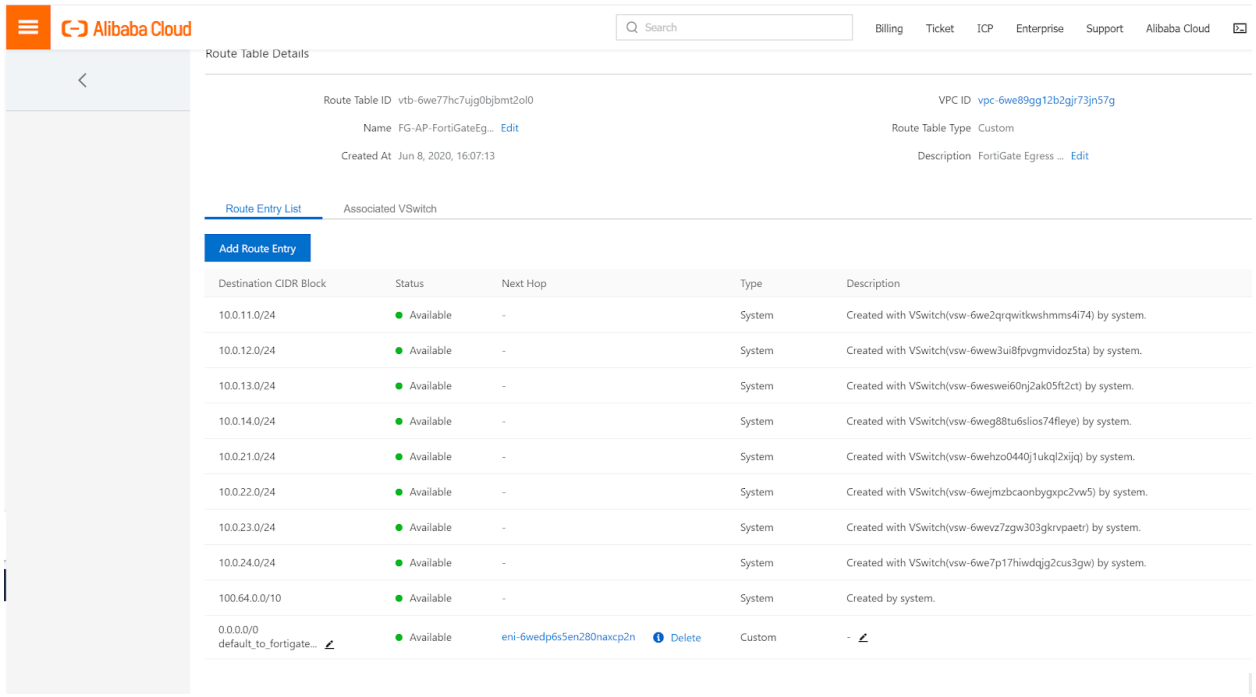
create Custom Routing Table

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 Foritgate instead go directly to vrouter. inside Fortigate, we have a default router point to aliyun vRouter for traffic leave VPC router to internet or aliyun CEN.



here we added a default route “Deafult_to_fortigate_port_2” . point to instance primary fortigate secondary ENI.

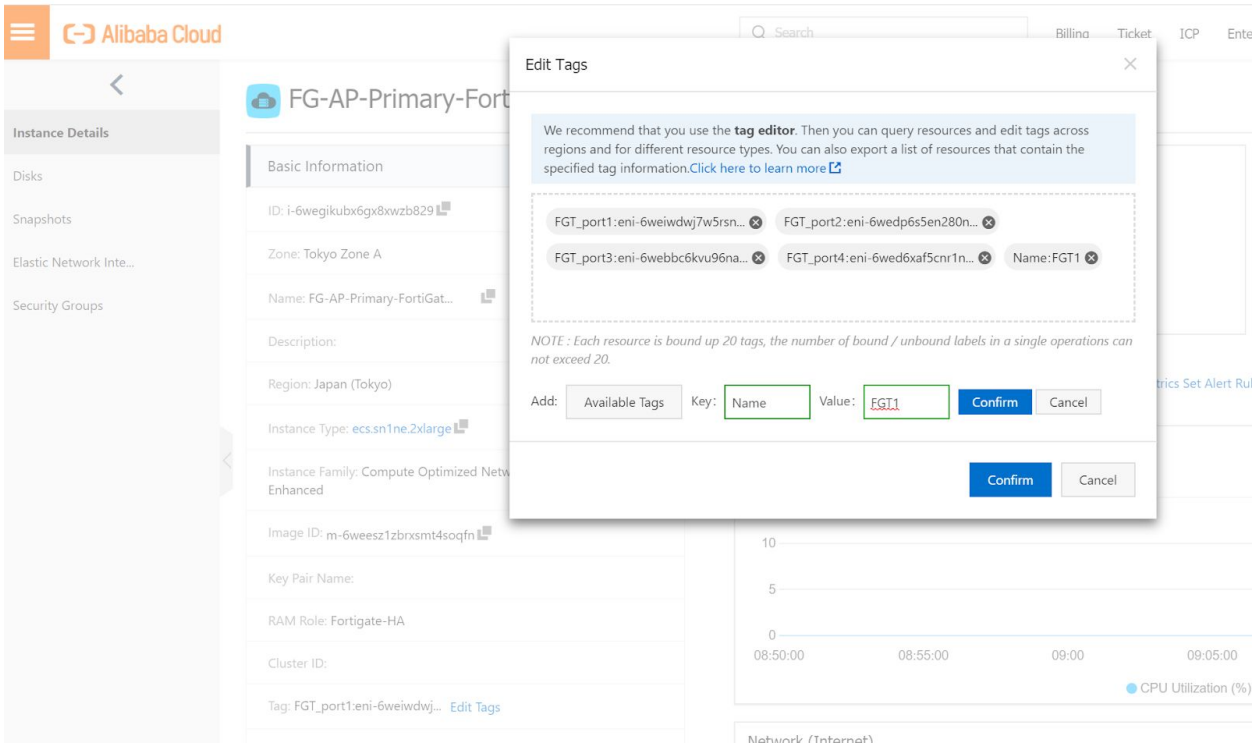
this custom routing table will also be automatically associated with vswitch named “internal-a”. and this vswitch “internal-a” will also be unassociated from the system routing table.

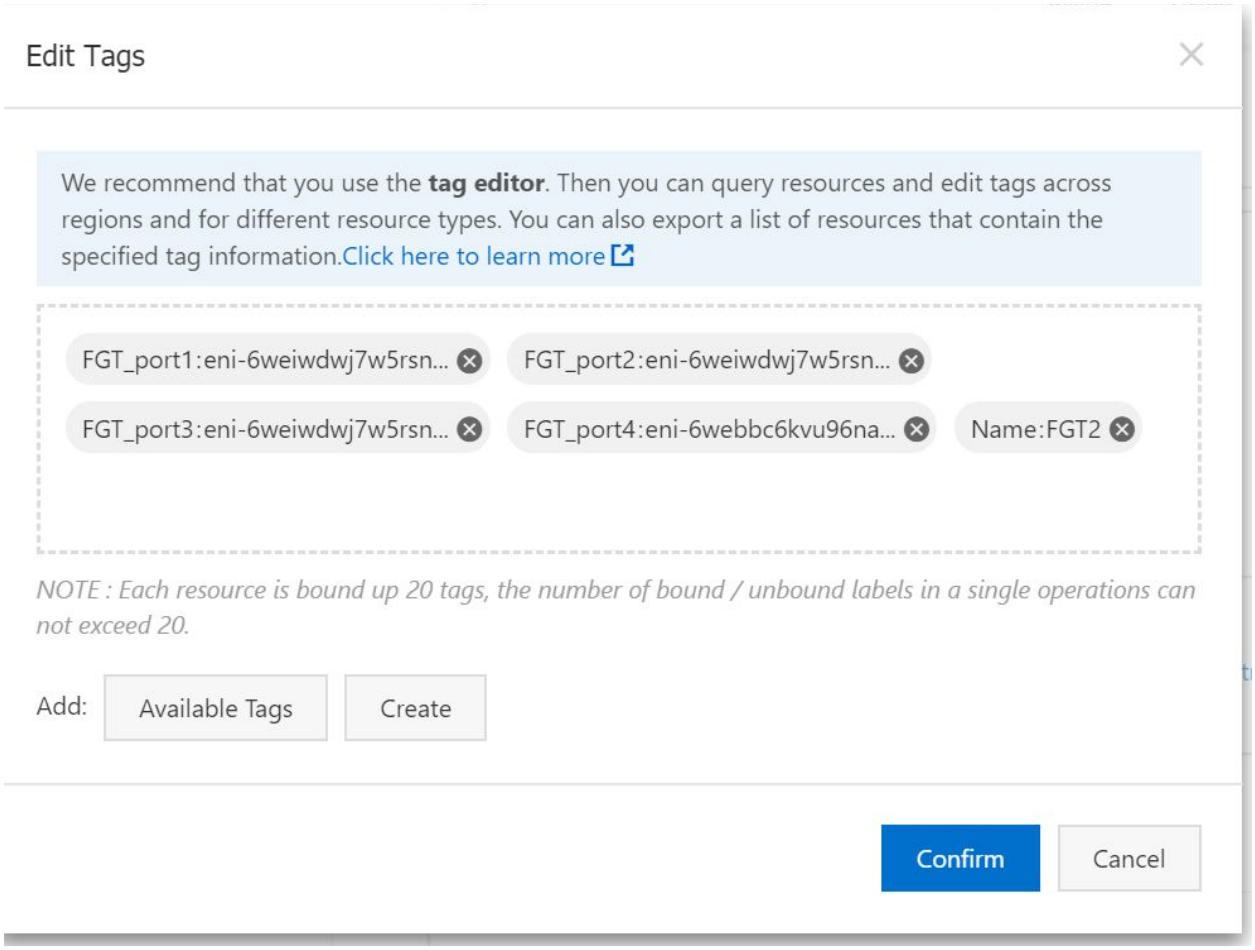


you will see the routing table above.

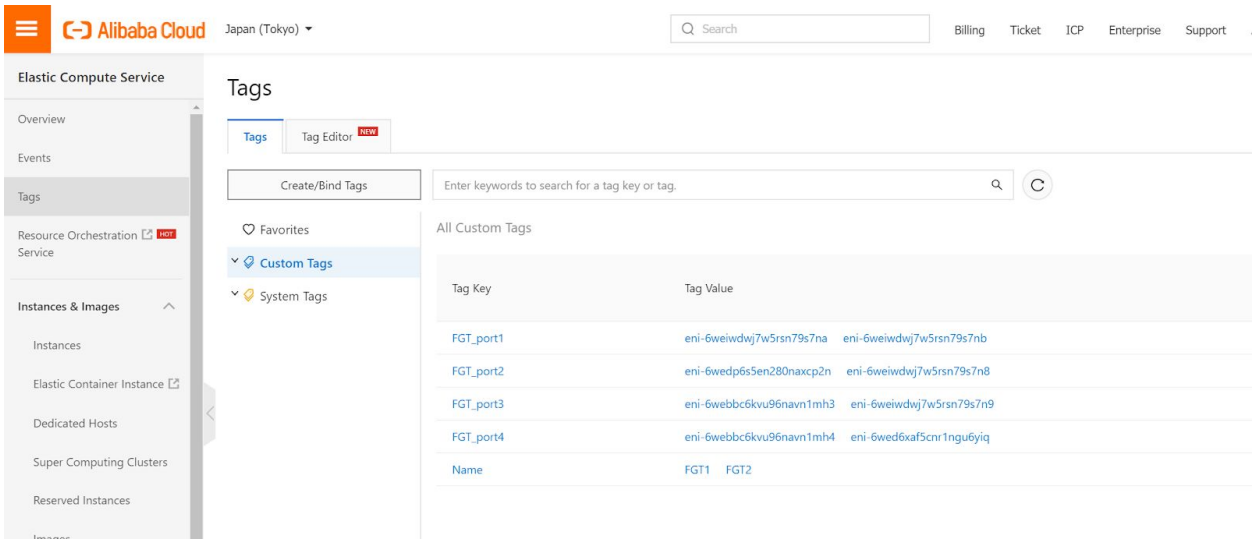
create tag for instances FGT-1 and FGT-2

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



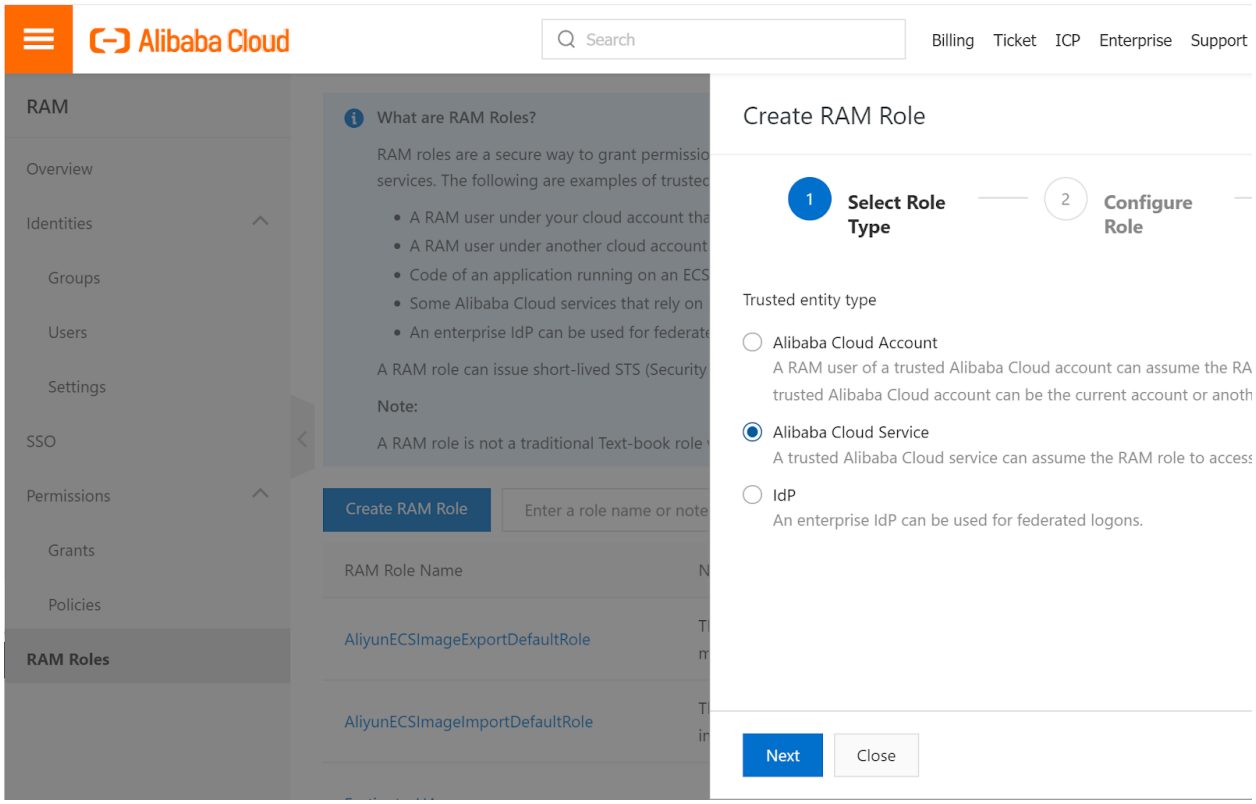


finally. you shall see all tags like below.



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.,



Create RAM Role

Select Type of Trusted Entity

Alibaba Cloud Service

Role Type

(•) Normal Service Role ( ) Service Linked Role

* RAM Role Name

Fortigate-HA

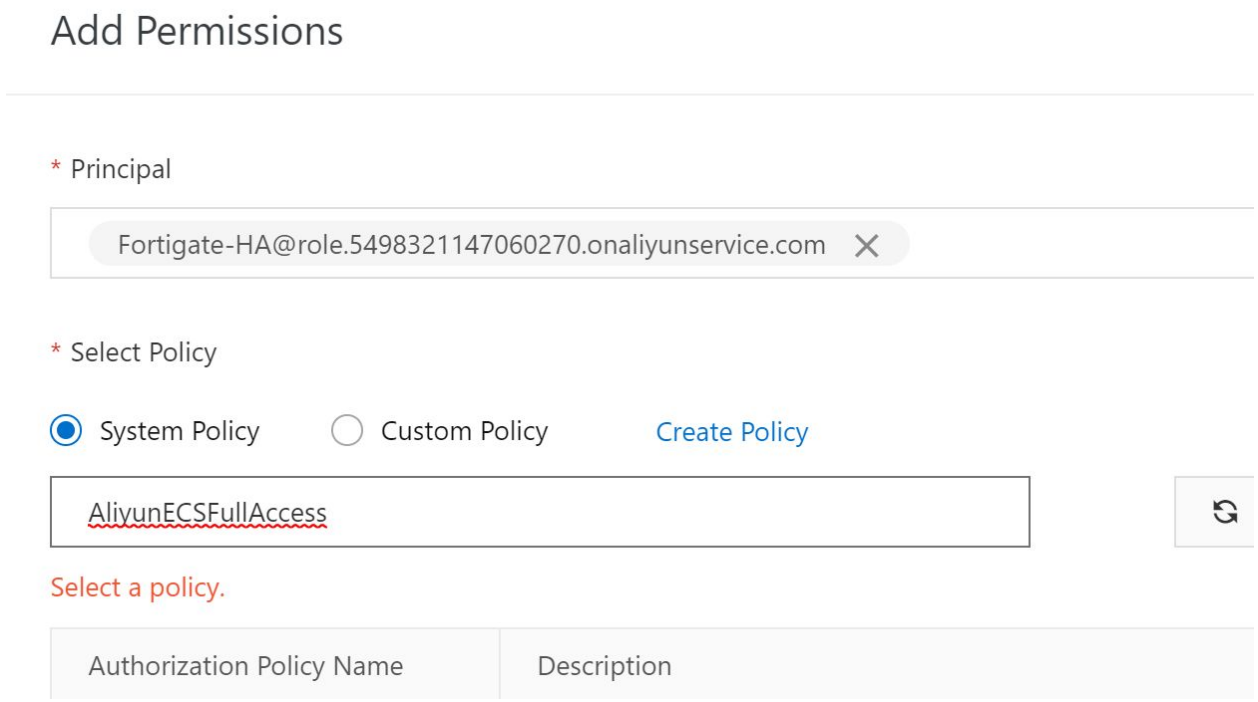
The name can contain a maximum of 64 characters, only English letters, numbers, and hyphens (-) are accepted.

Note

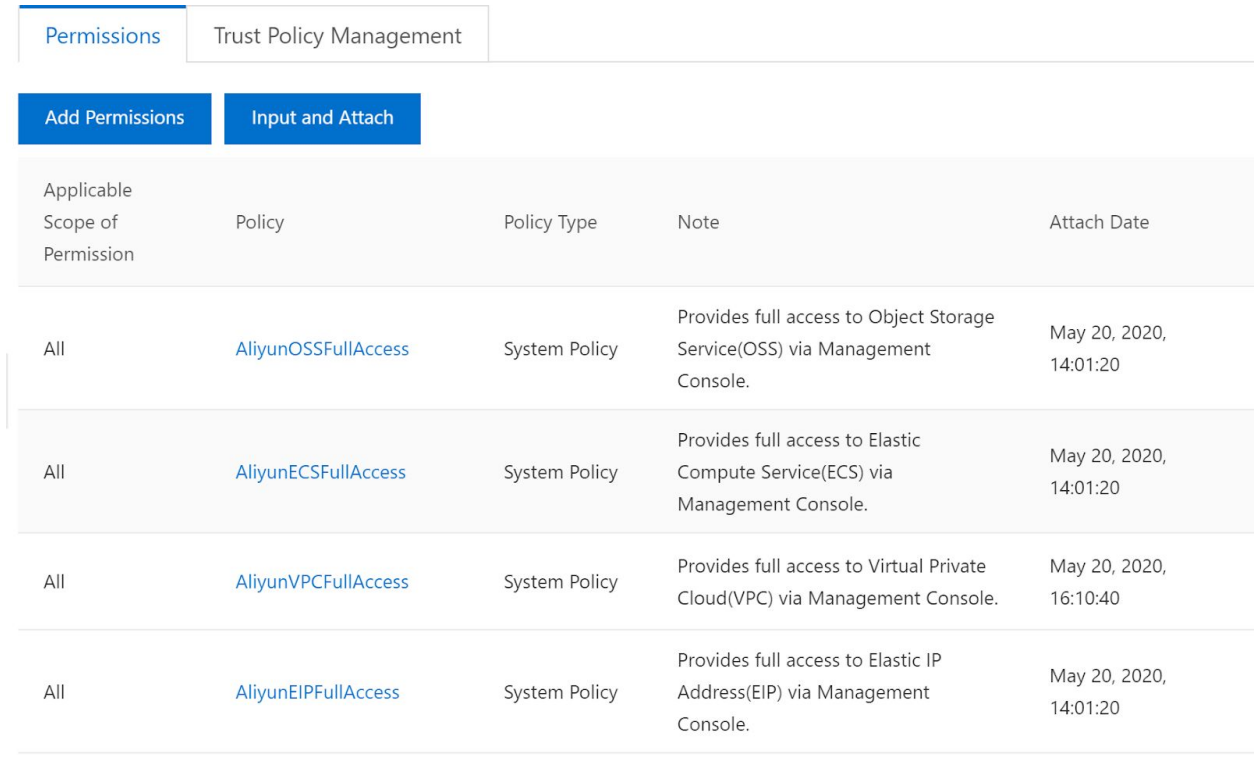
* Select Trusted Service

Elastic Compute Service

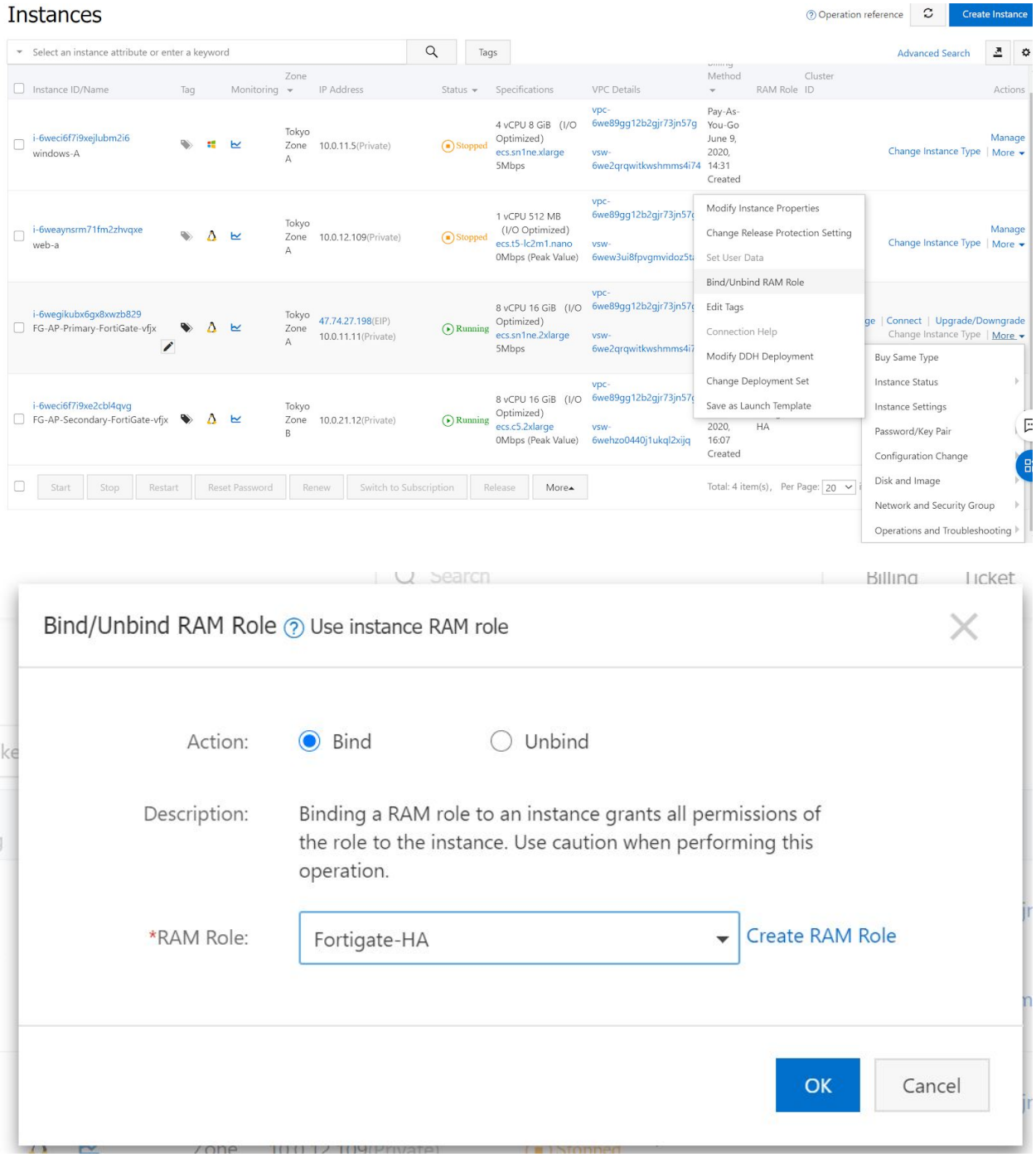
Back | OK | Close



Add AliyunECSFUllAccess,AliyunVPCFullAccess,AliyunEIPFullAccess .



then bind RAM rule to two Fortigate instances.

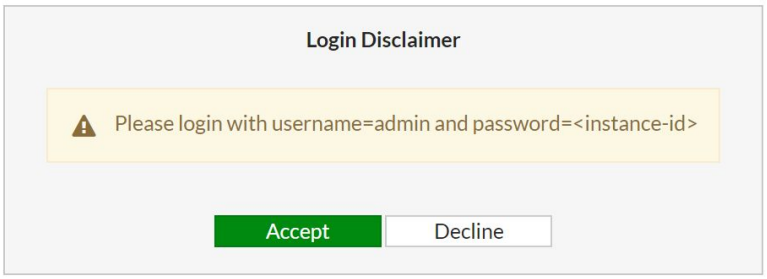


do the same for FGT2 in zone.

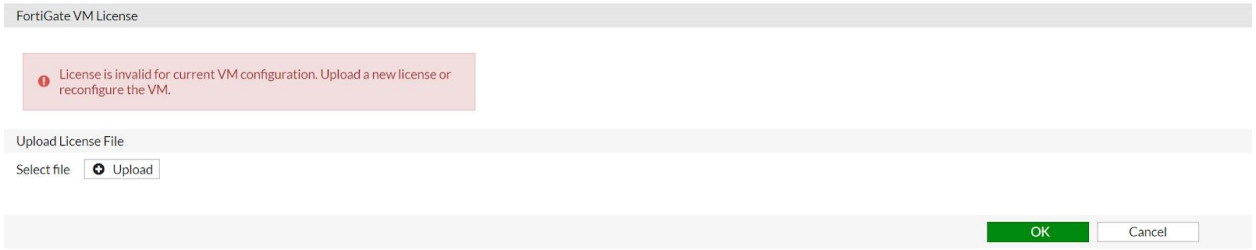
We shall complete an alicloud cloud setup and launch the fortigate instance in both zone A and zone B. Configuring the custom routing table added a default route point to fortigate.
now move to setup fortigate

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.

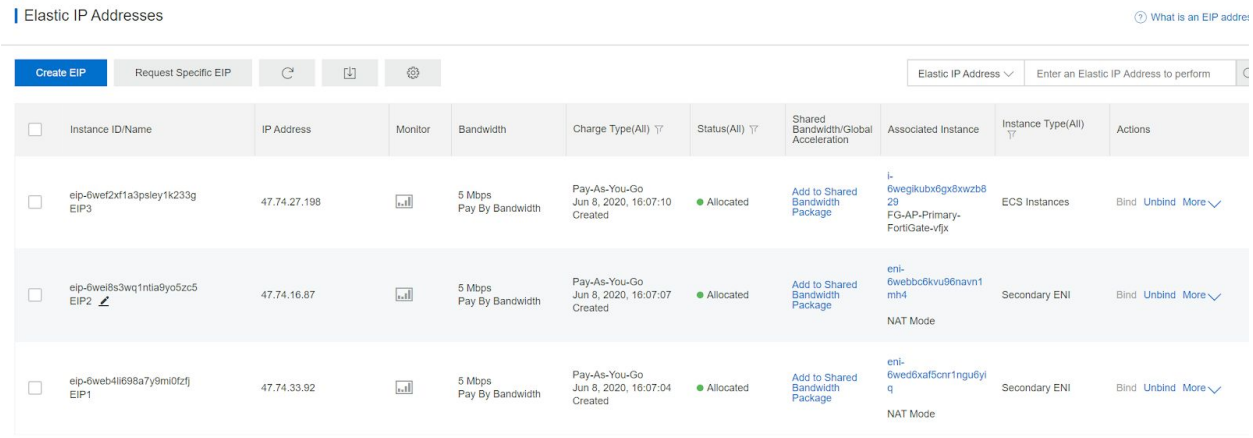


install the license.



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.



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.

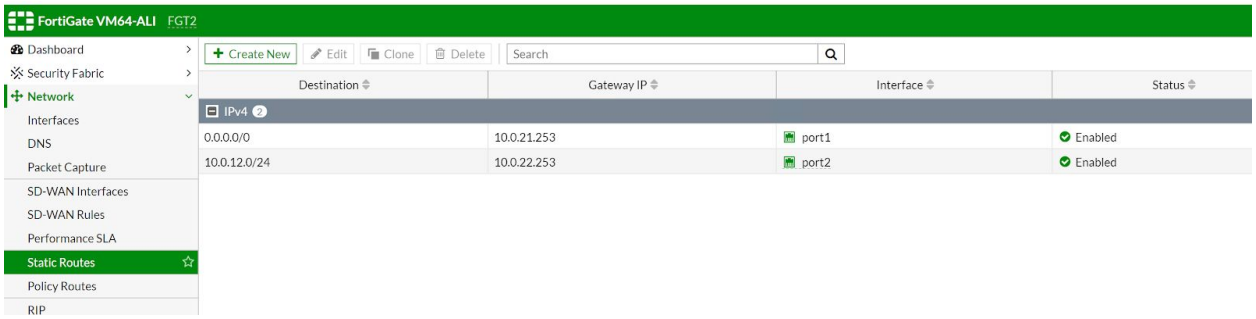
config interface and static routing

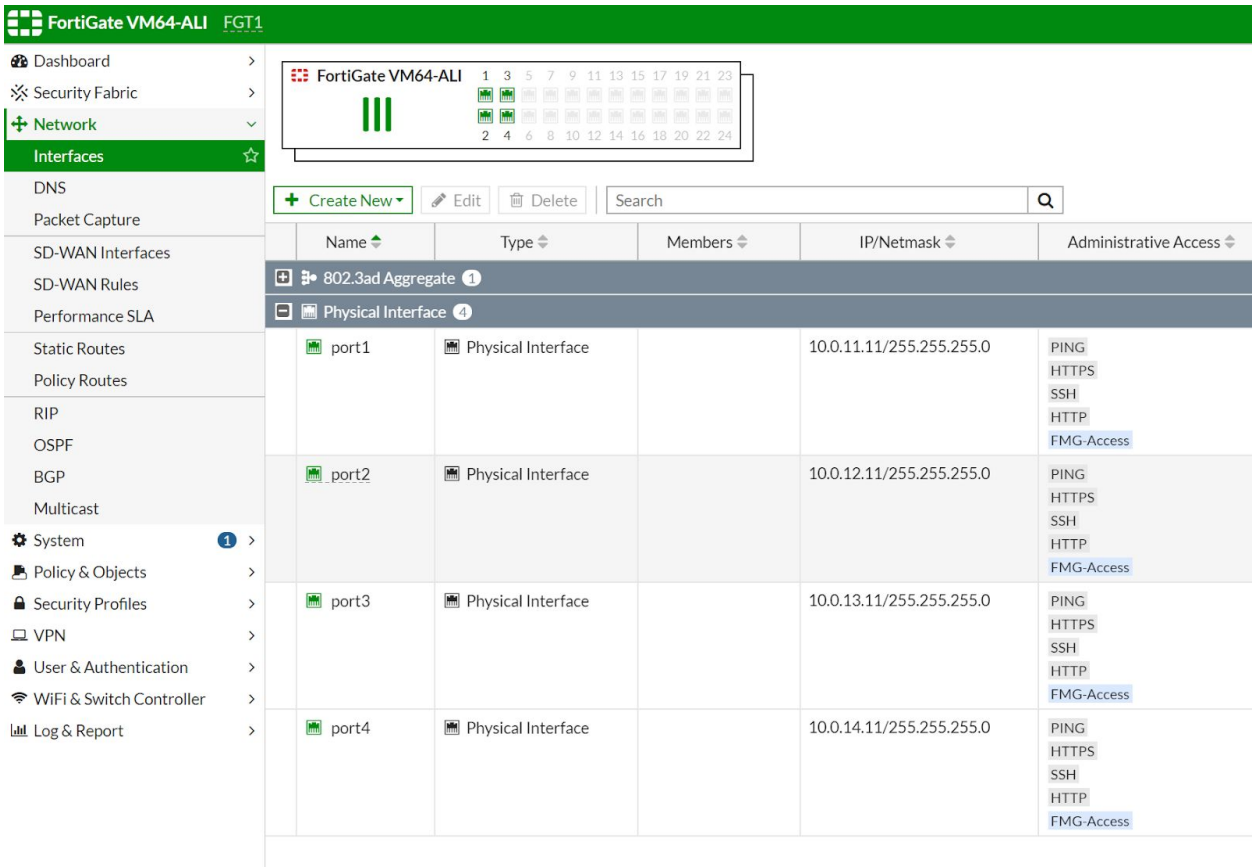
you can config fortigate by following the cookbook. basically you will have to config

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.

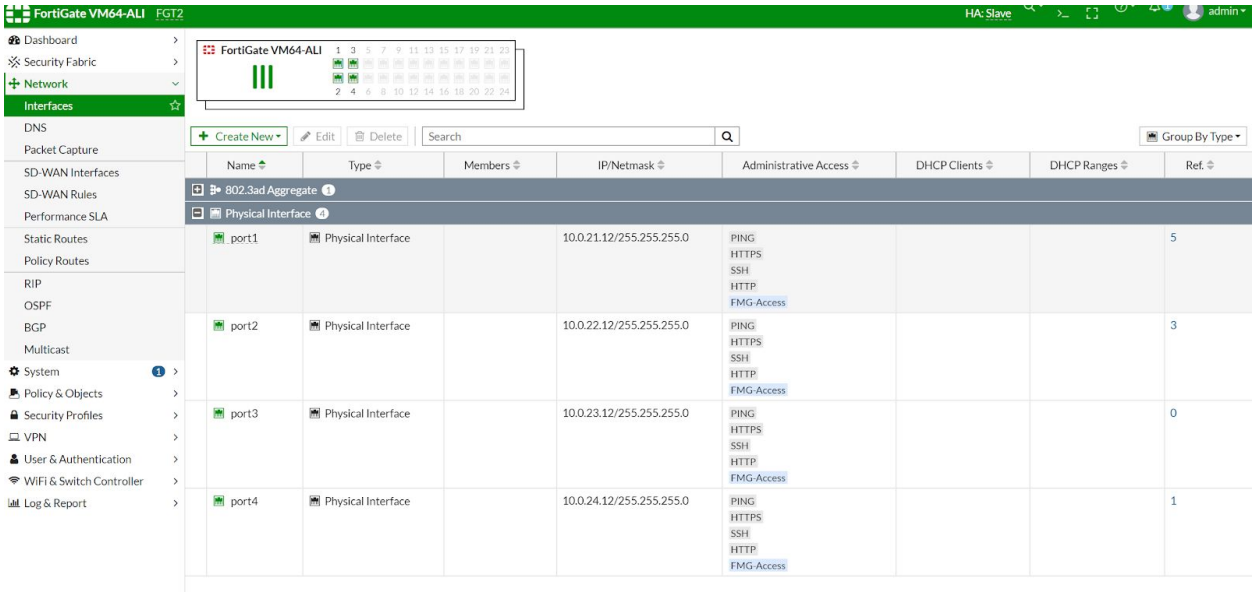
   on FGT2 , config a static route to 10.0.12.0/24 with exit port2 is required. this is needed after the switch over happens. web-a server in zone-A will talk to FGT2 in zone B. Config this route will let FGT2 send traffic back to web-a in ZoneA directly via port2.
   if you do not have any workload in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





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



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.

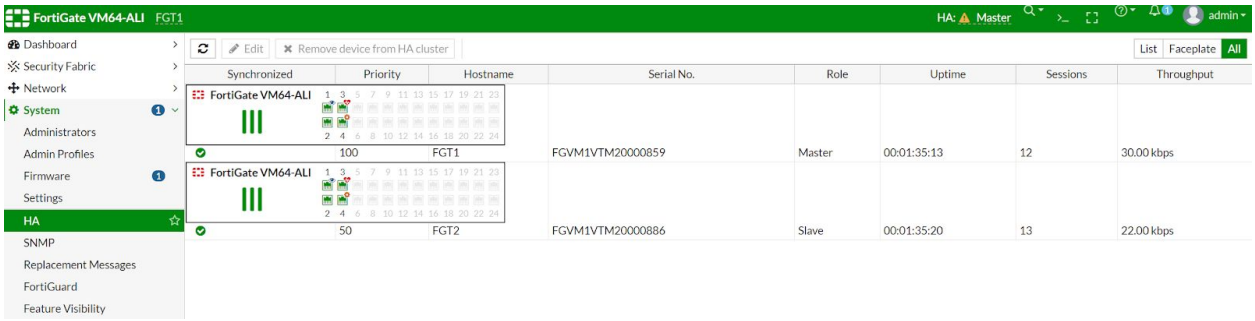
```
FGT1 #  config system ha


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
```

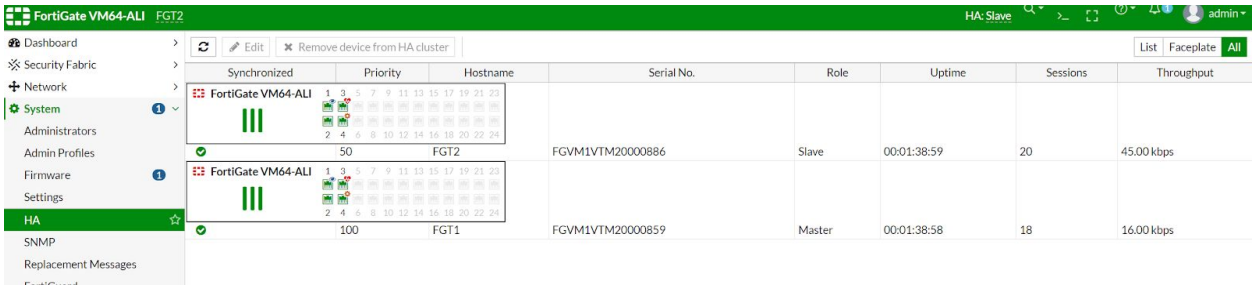
```
        next
    end
    set override disable
    set priority 100
    set monitor "port1"
    set unicast-hb enable
    set unicast-hb-peerip 10.0.23.12
end
```

```
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.





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.

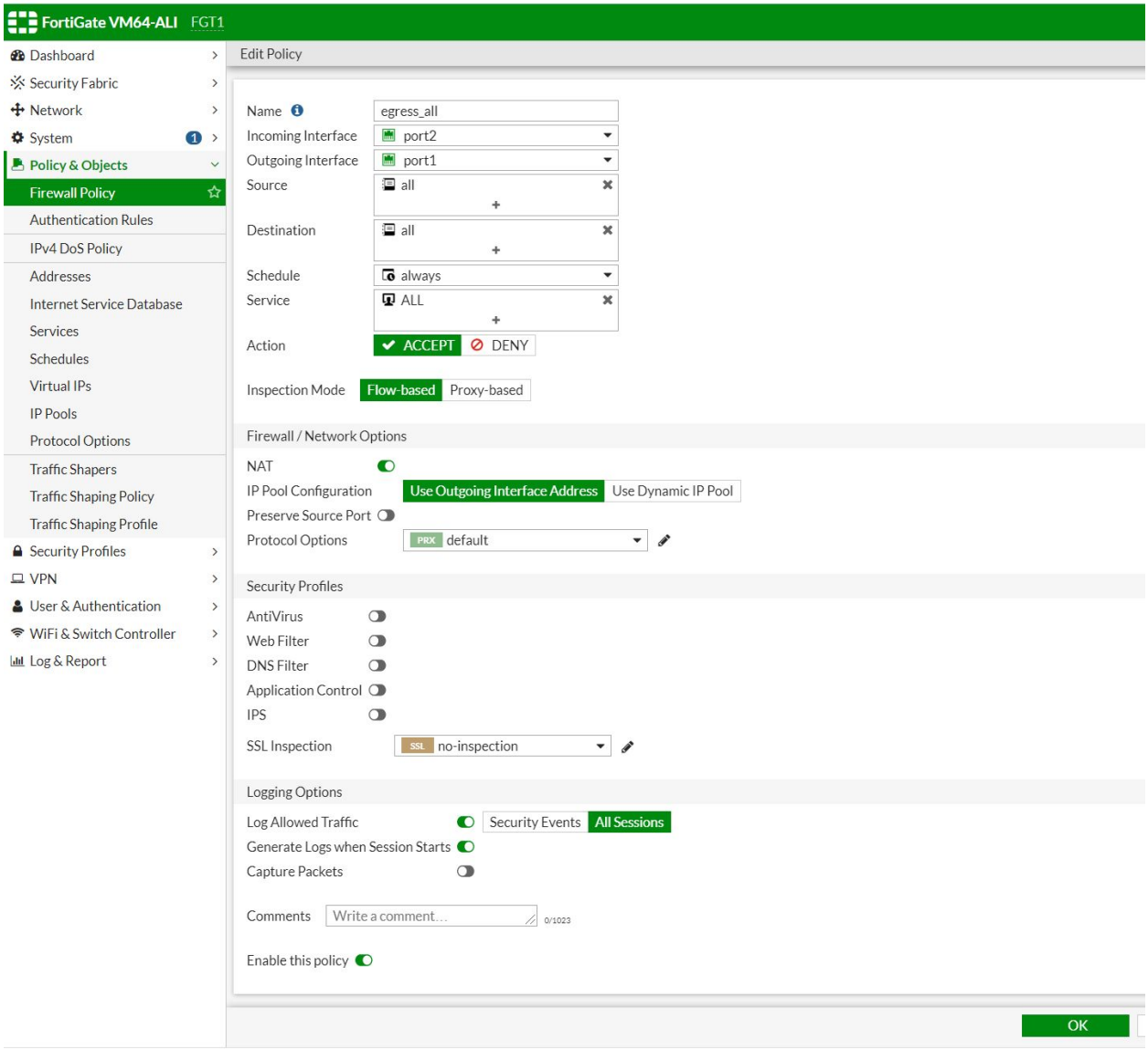
```
FGT1 # execute enter vsys_ha

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.

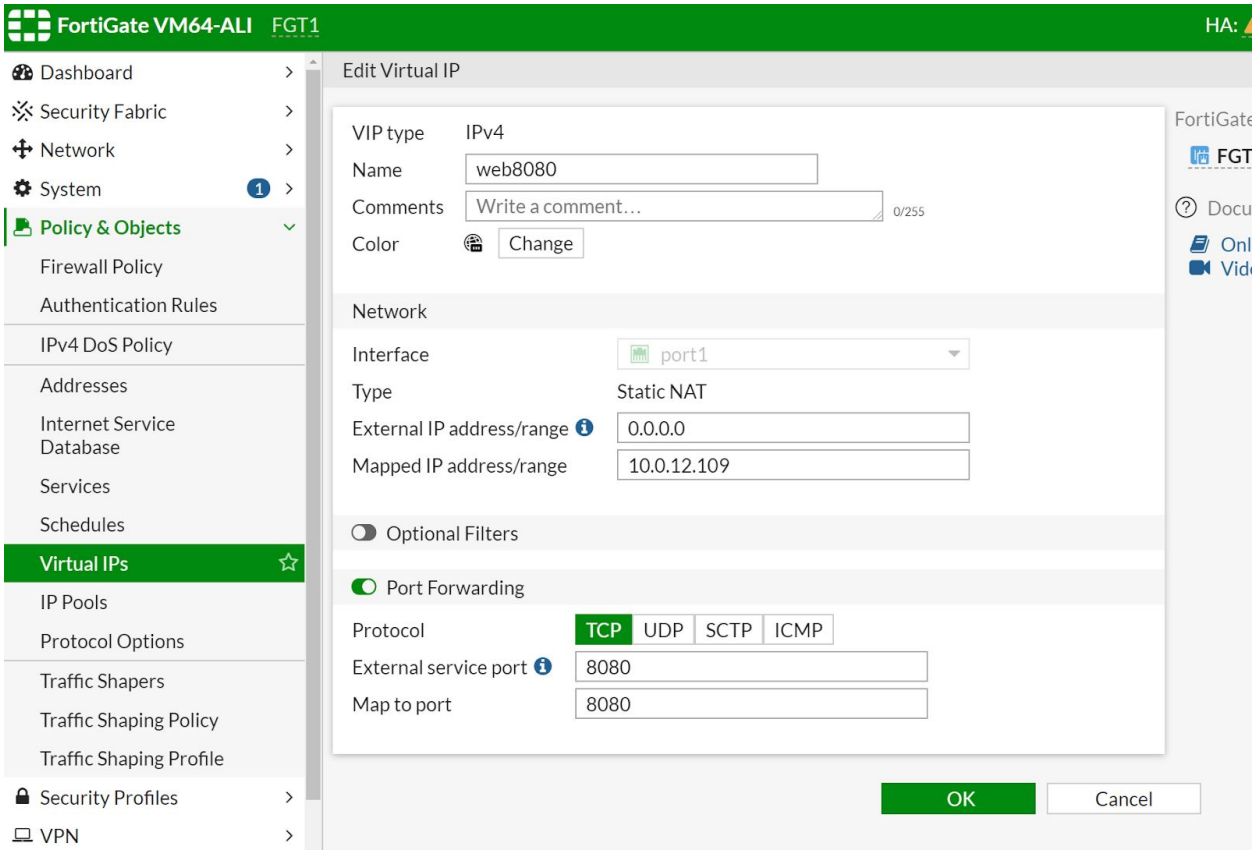
create firewall policy for egress traffic

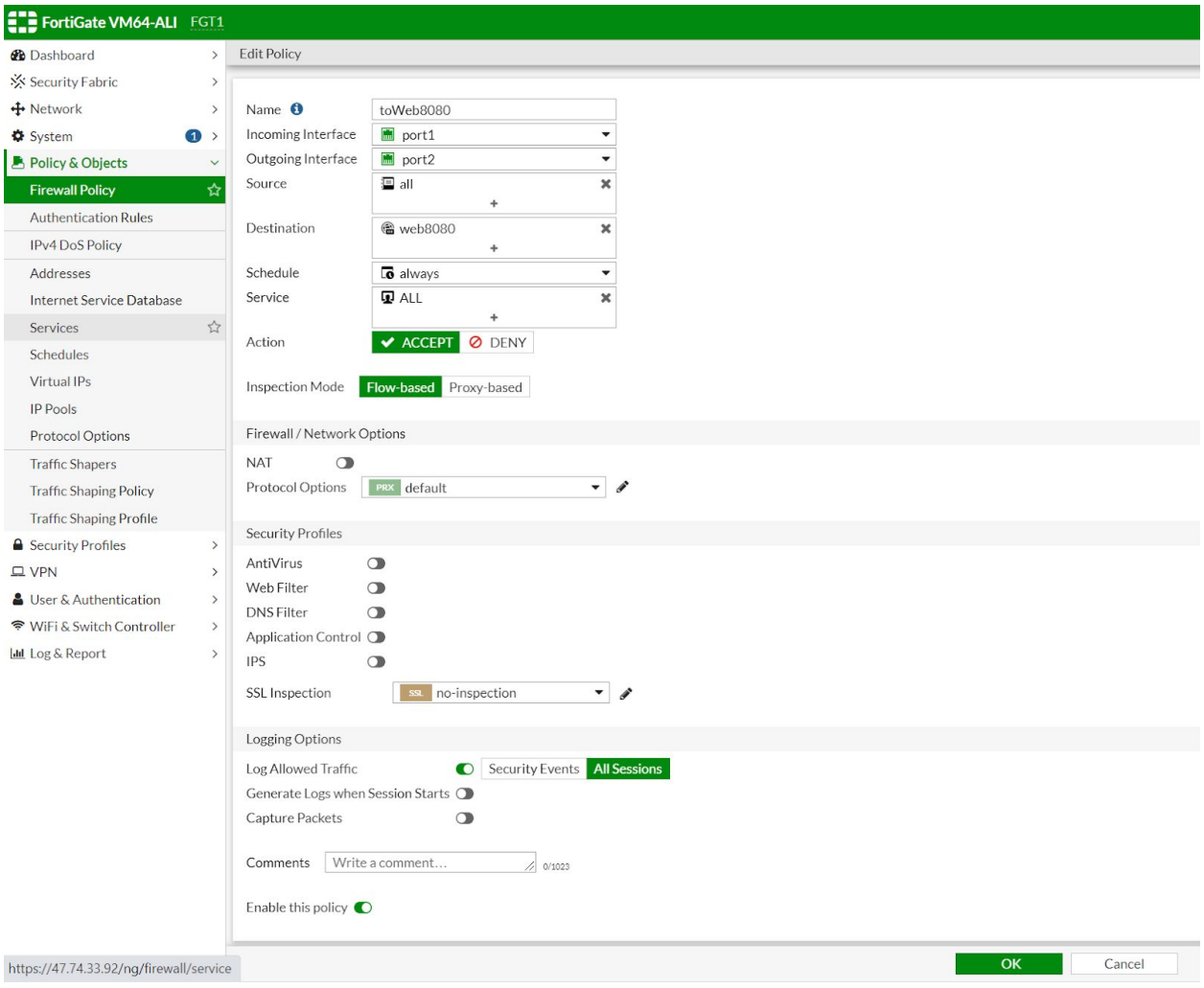


The traffic coming from port2 (attached to vswithinternal-A), exit from port1 (attached to vswitch external-A). port 1 is also the interface for the FGT-1 default route. we have to enable NAT. when traffic leaves port 1, the source IP of the VM will become the port1 interface's IP address which is 10.0.11.11.

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:
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
UDP
SCTP
ICMP
External service port
8080
Map to port
8080
OK
Cancel
FortiGate
FGT
Docu
Onl
Vid



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 uuid 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 uuid 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 #
```

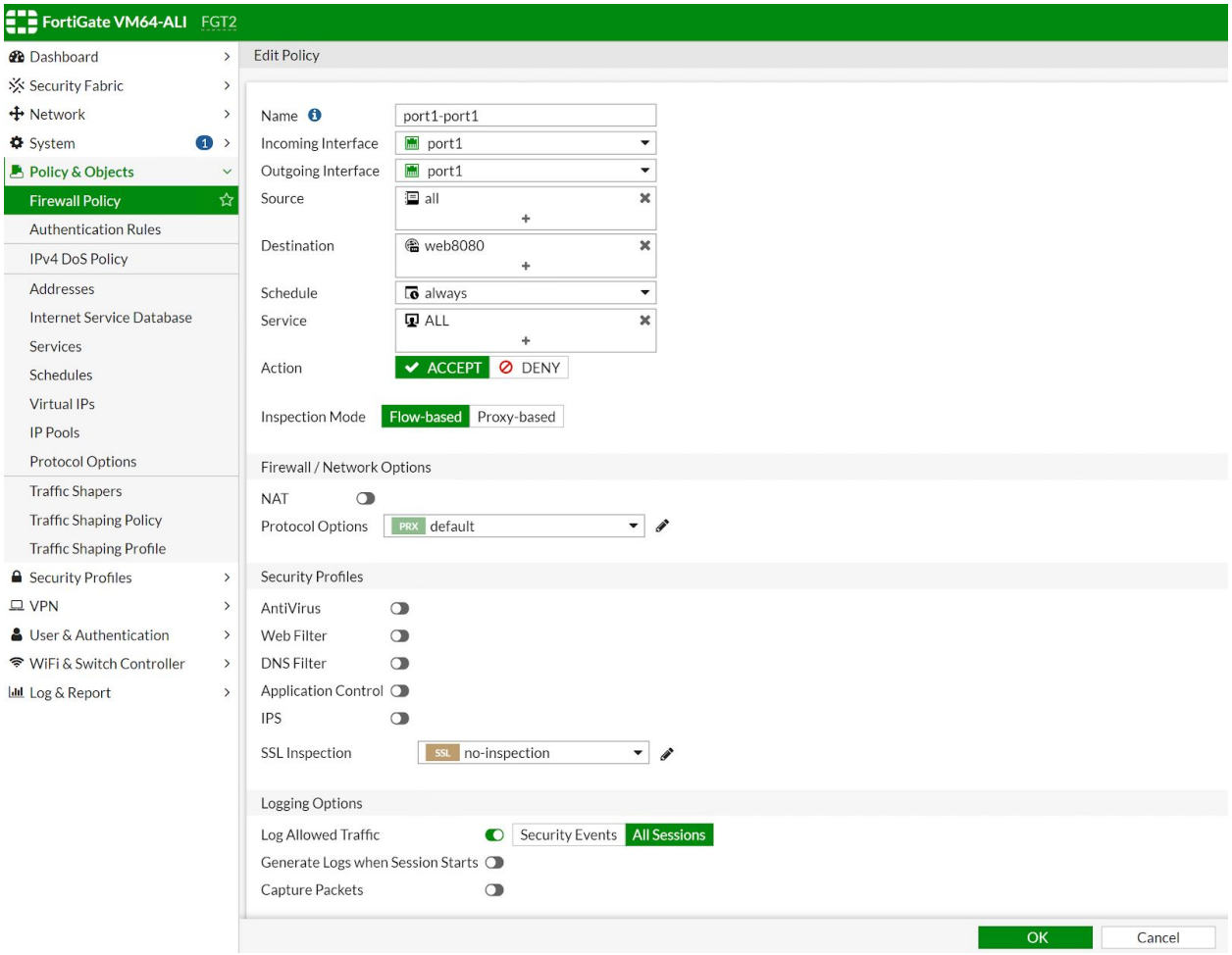
```
FGT1 # show firewall vip
config firewall vip
    edit "web8080"
        set uuid 8738a470-a981-51ea-0e12-933b08ae8835
        set extintf "port1"
        set portforward enable
        set mappedip "10.0.12.109"
        set extport 8080
        set mappedport 8080
    next
end

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. vrouter 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.




```
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-2fb1-7e5bbbe37e5b
```

```
        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

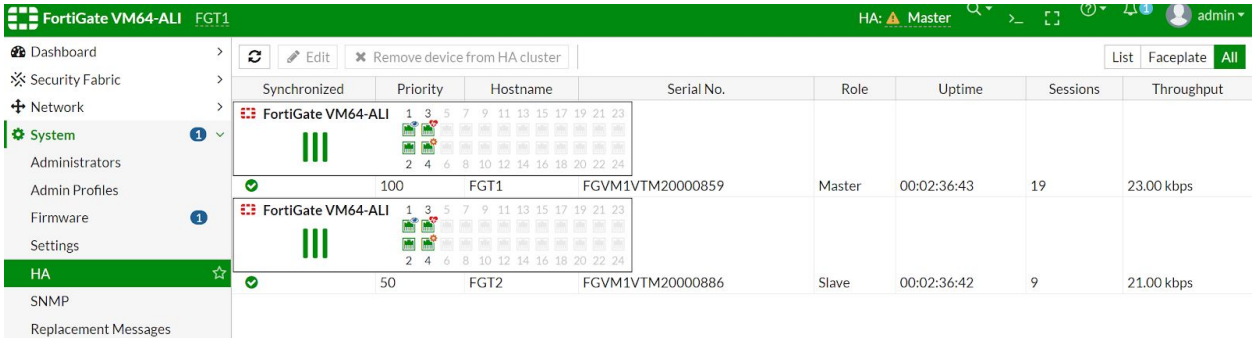
```
FGT2 # diagnose debug flow trace start 1

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 [S], seq 2880903269, ack 0, win 64240"
id=20085 trace_id=256 func=init_ip_session_common line=5754 msg="allocate a new session-00000aab"
id=20085 trace_id=256 func=fw_pre_route_handler line=181 msg="VIP-10.0.12.109:8080, outdev-port1"
id=20085 trace_id=256 func=__ip_session_run_tuple line=3409 msg="DNAT 10.0.21.12:8080->10.0.12.109:8080"
id=20085 trace_id=256 func=vf_ip_route_input_common line=2598 msg="find a route: flag=00000000 gw-10.0.21.253 via port1"
id=20085 trace_id=256 func=fw_forward_handler line=781 msg="Allowed by Policy-3: SNAT"
id=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

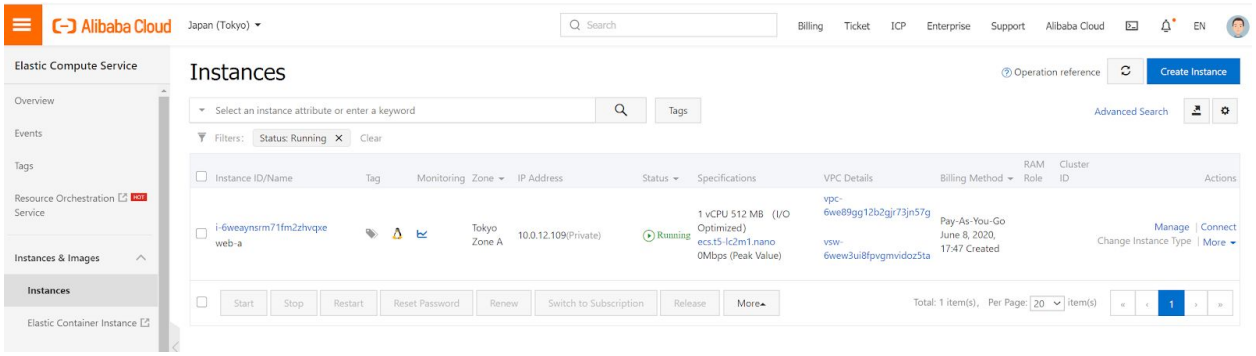
verify the HA result on both fortigate

you can use EIP1 and EIP2 to remotely access fortigate



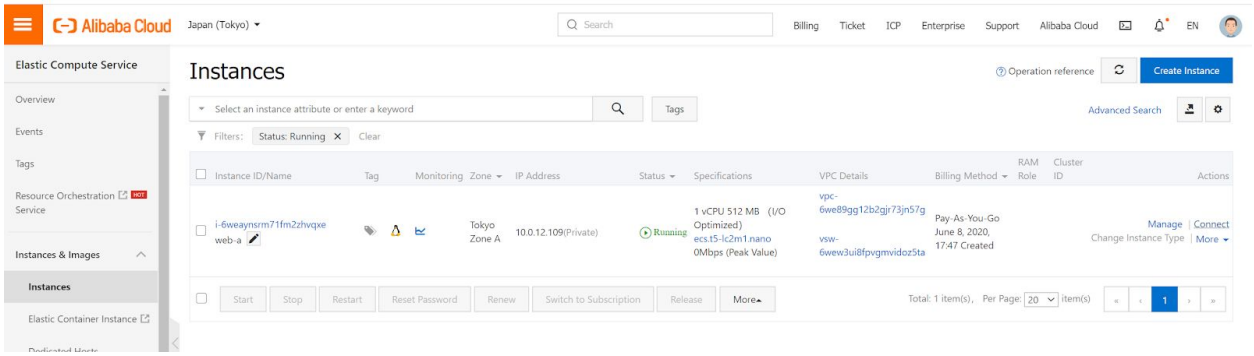
create web-a workload VM for testing.

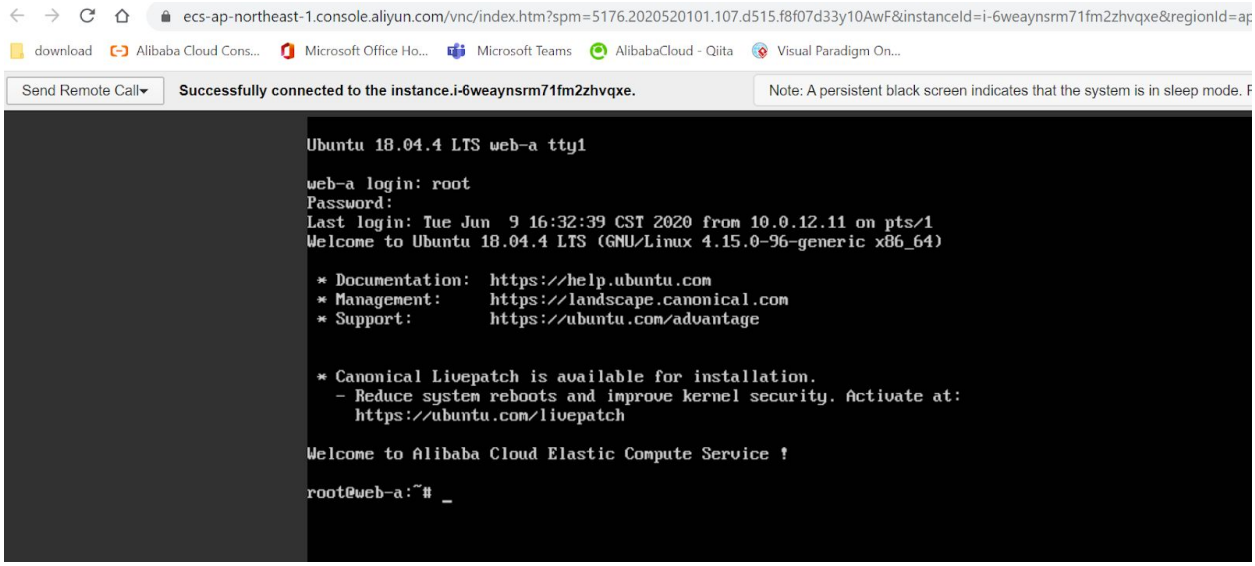
create a linux WebServer VM in zone a called web-a to verify the HA .
choose VPC and zone A internal-a switch. setup your username and password.



use cloud dashboard console to access web-a VM

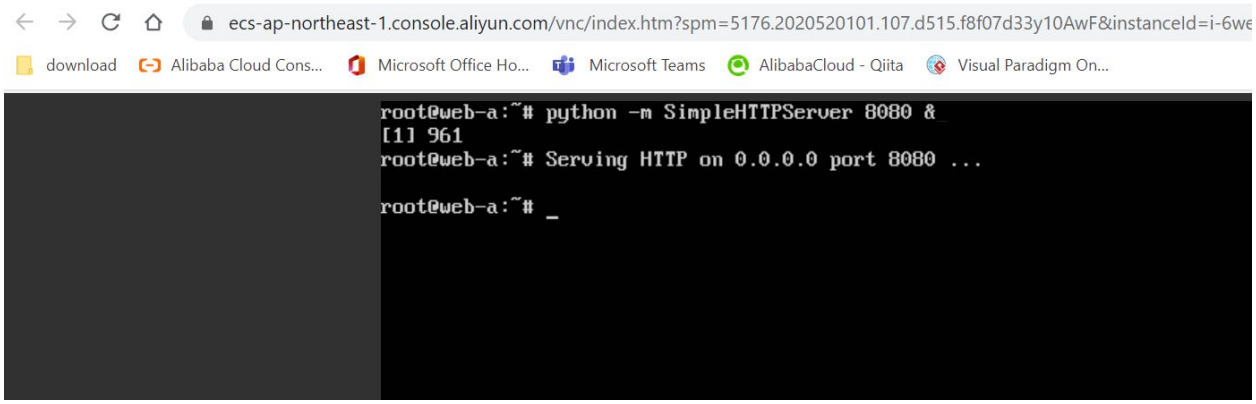
after starting this instance . you can access this web-a console via alicloud vnc console connect.





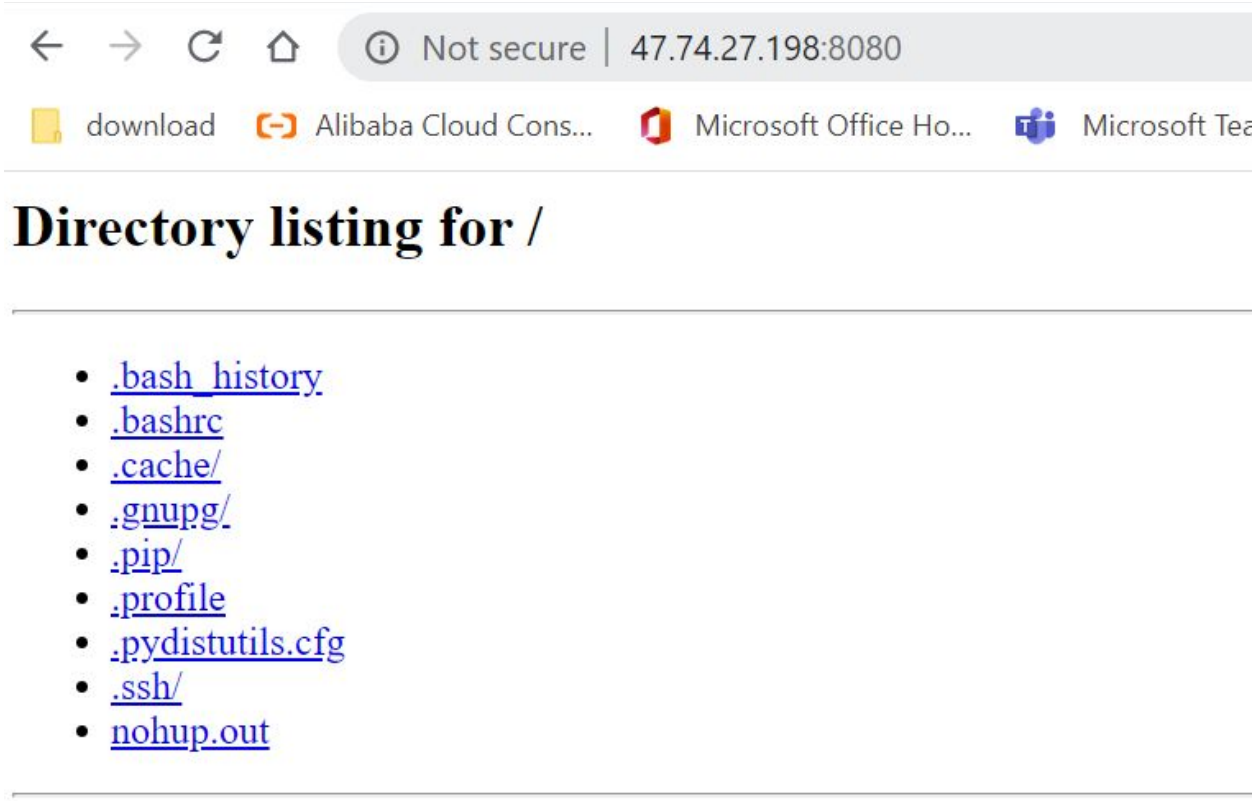
start web server on web-a VM

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



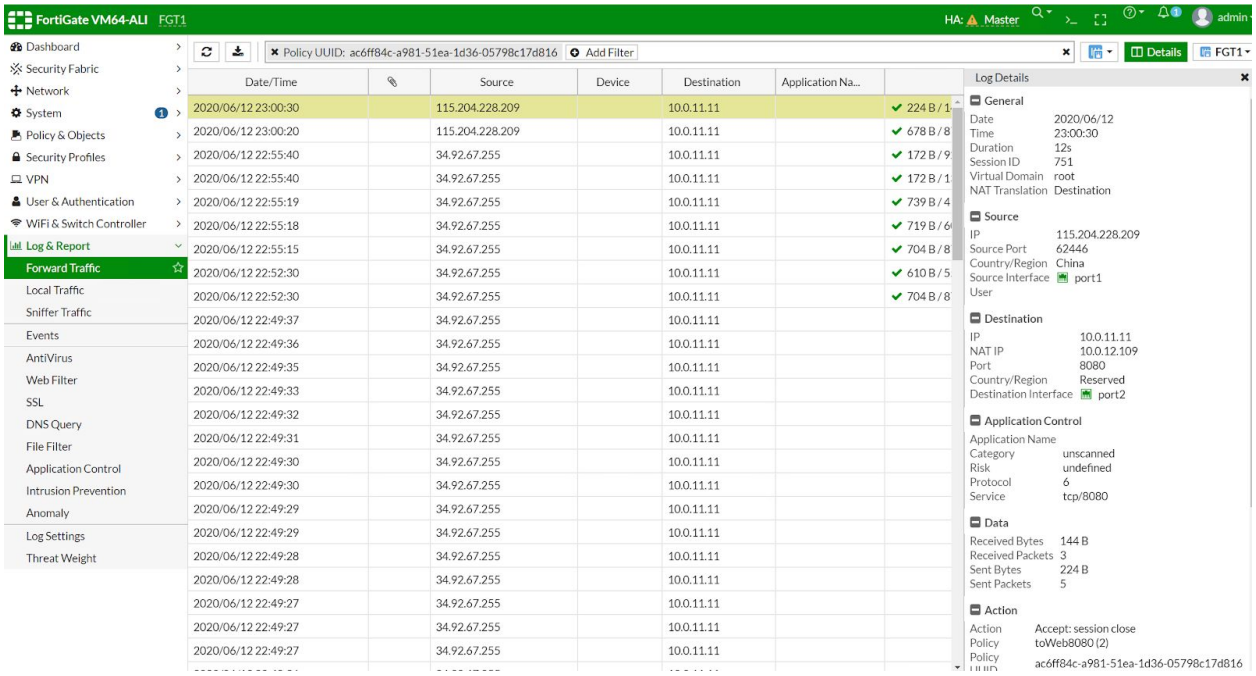
from your local PC. you can use a browser to curl to access this web server via FGT-1 EIP3 address. EIP3 is currently associated with FGT-1 as FGT-1 is master .

verify the web server can be accessed from the internet.



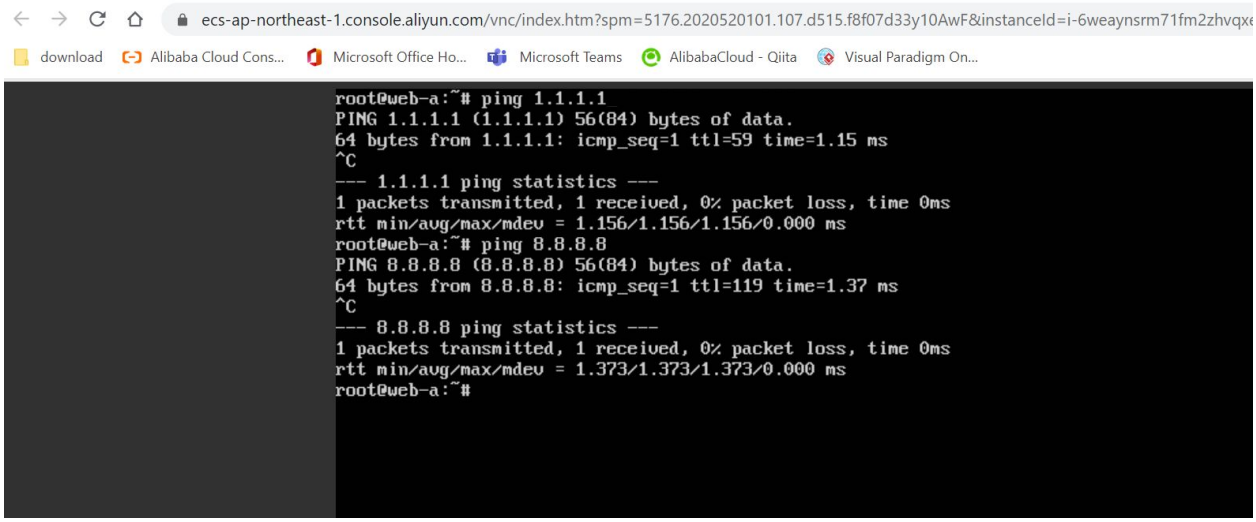
on the FGT-1 log & Report menu. you can see access log.

the web server will dump the access information.

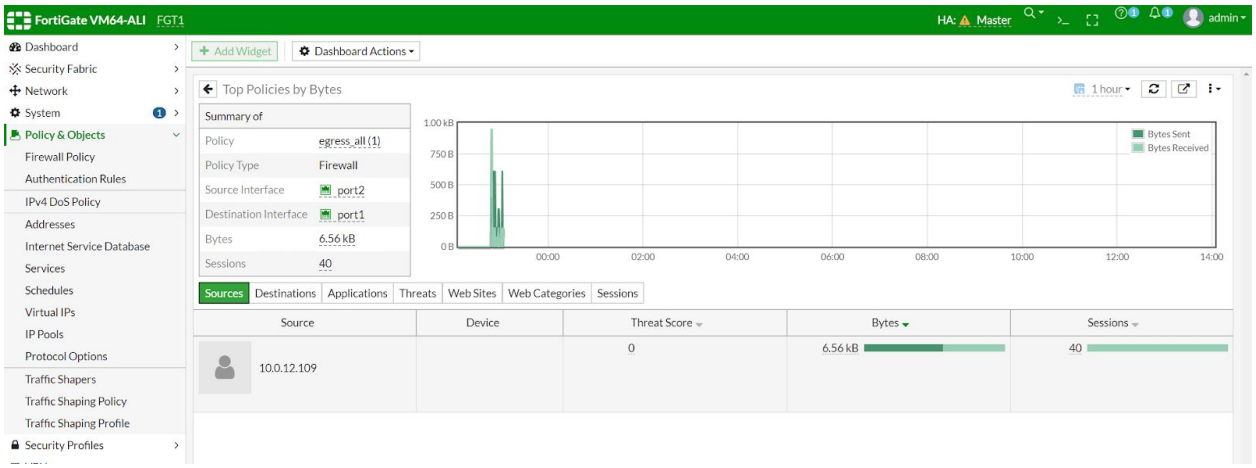


verify egress traffic

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



you can also show traffic logs from FGT-1.

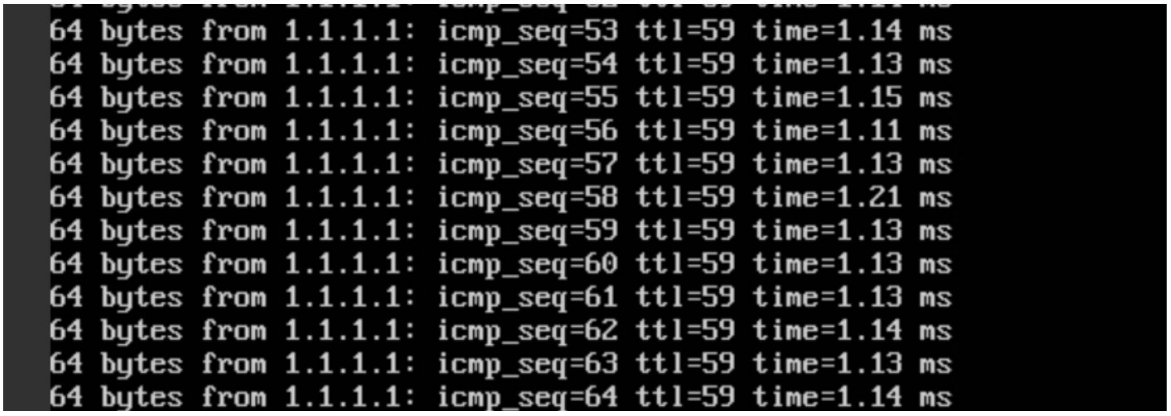


.

check Failover interrupt time

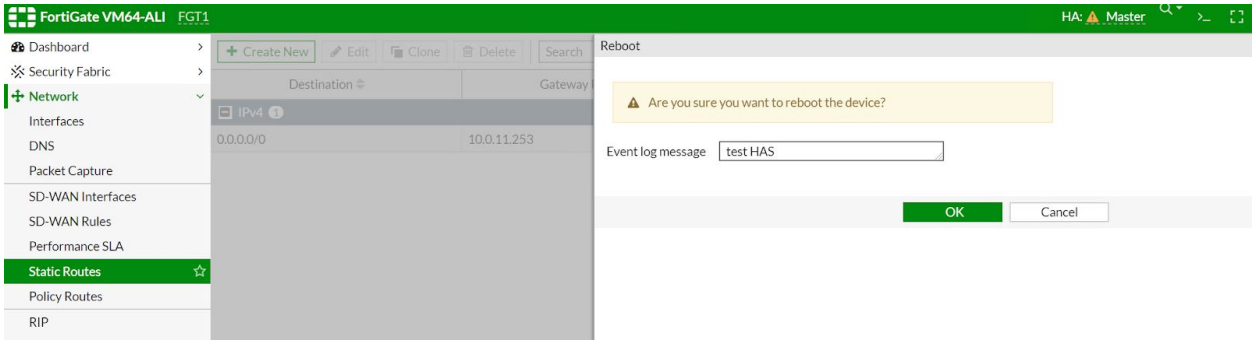
keep ping on web-a, and let's reboot FGT-1 to trigger a switchover. recorder the switch-over time and change of VPC routing table and EIP moving to new master.

1. start ping from web-a console.

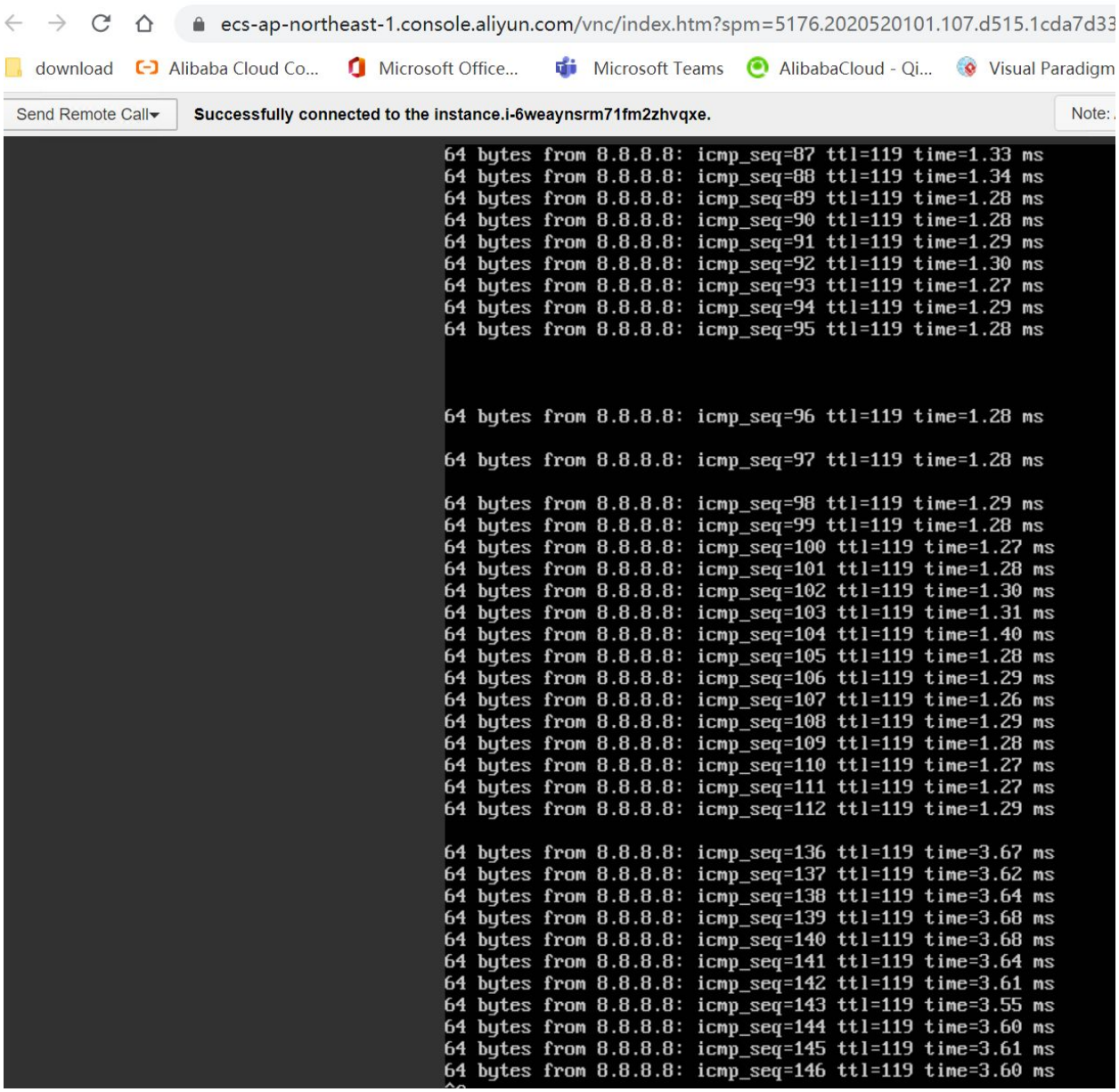


2. reboot FGT-1 from FGT-1 menu

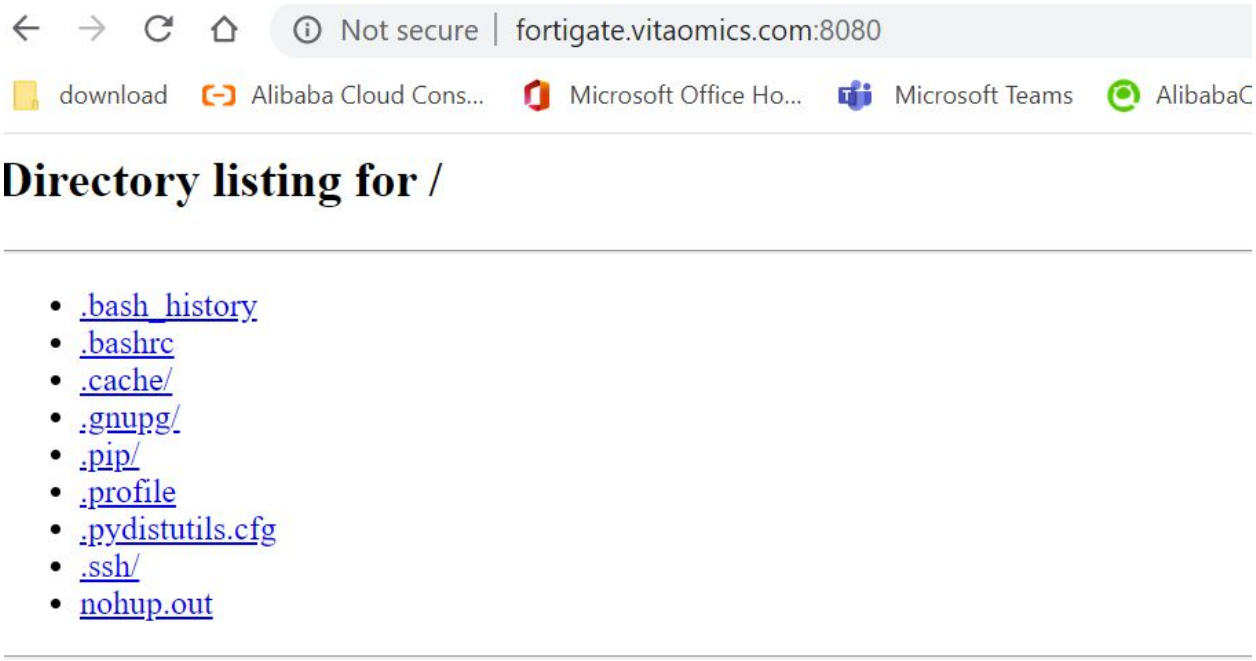
choose Restart FGT-1



ping will interrupt around 24 seconds.



web service back to work at similar time interruption.

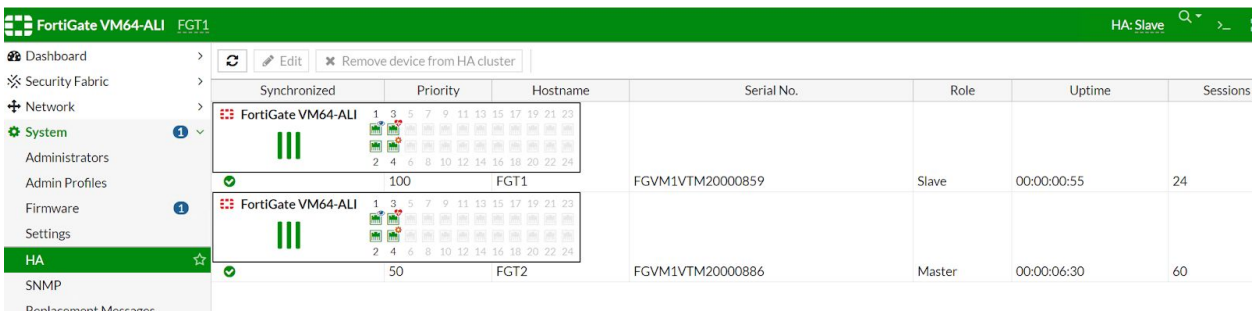


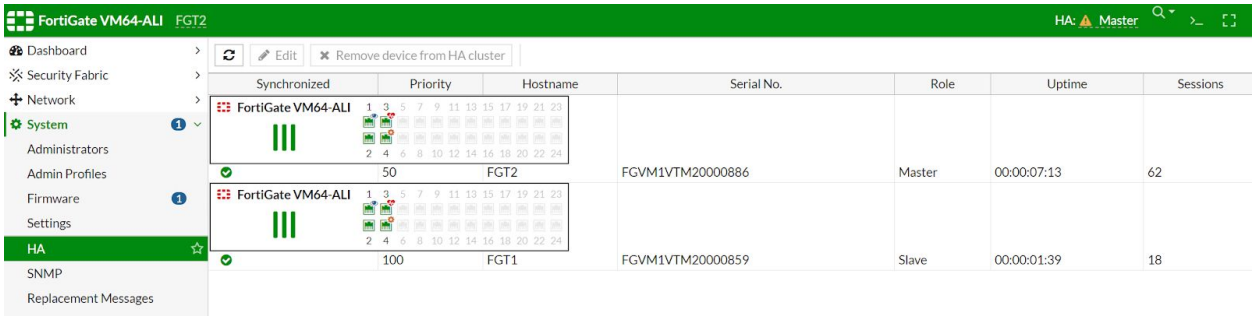
Verify the Changes due to Failover

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

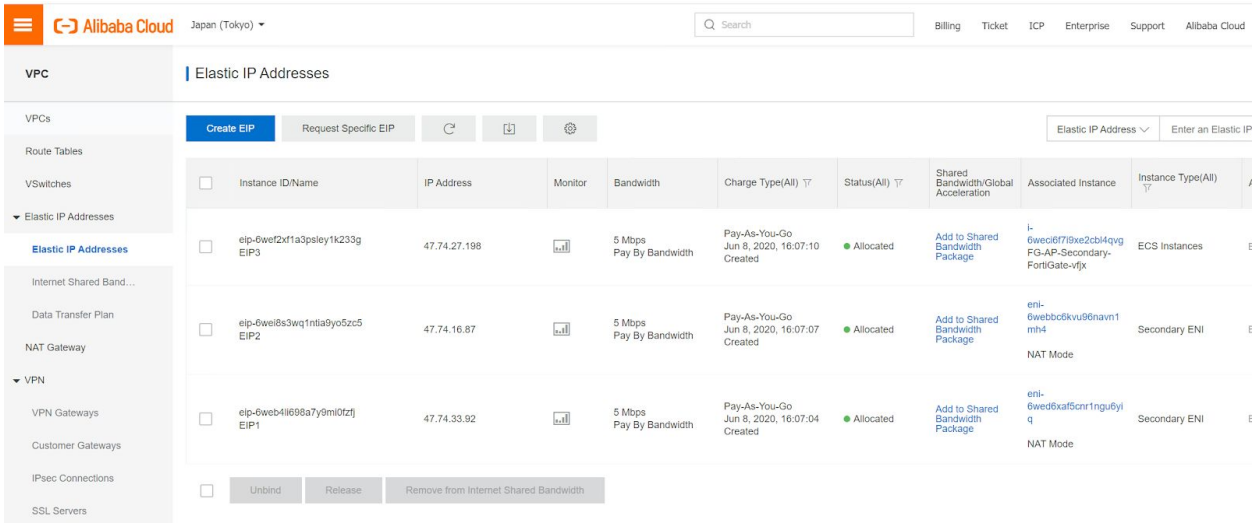
FGT-1 now becomes slave , FGT-2 becomes master.





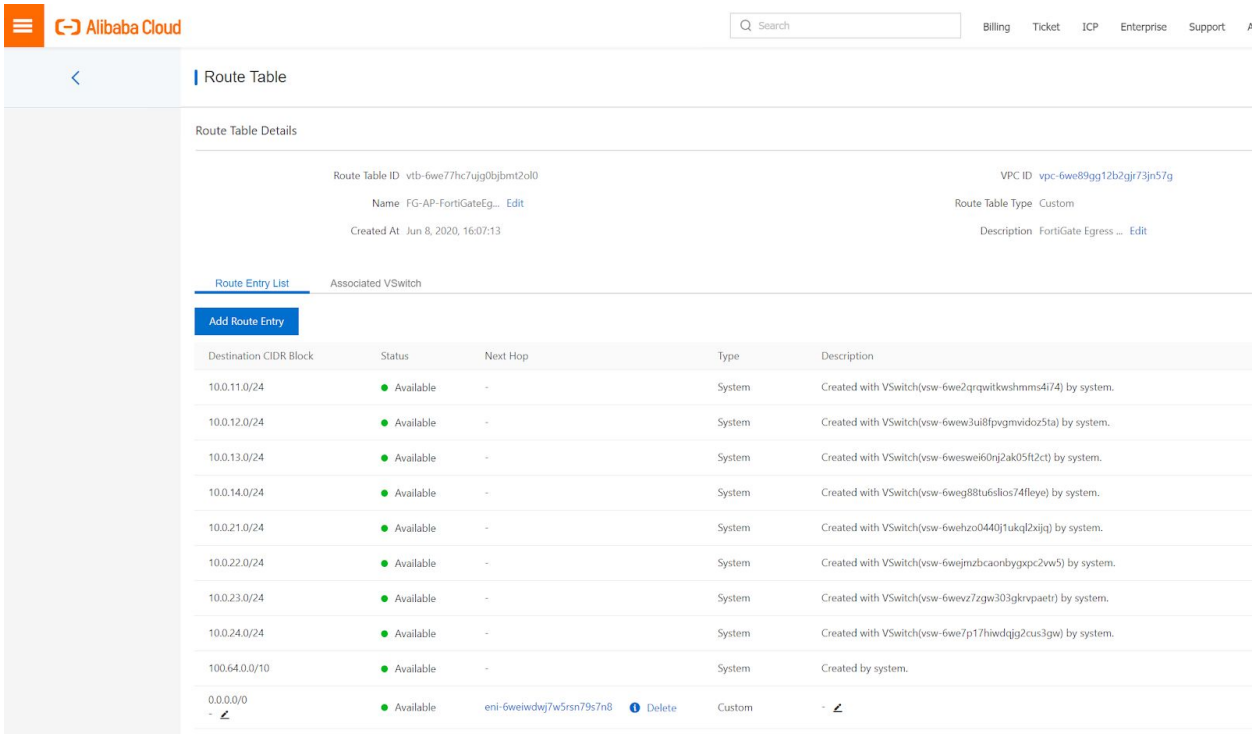
EIP3 moving

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



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



Terraform code for automating the deployment

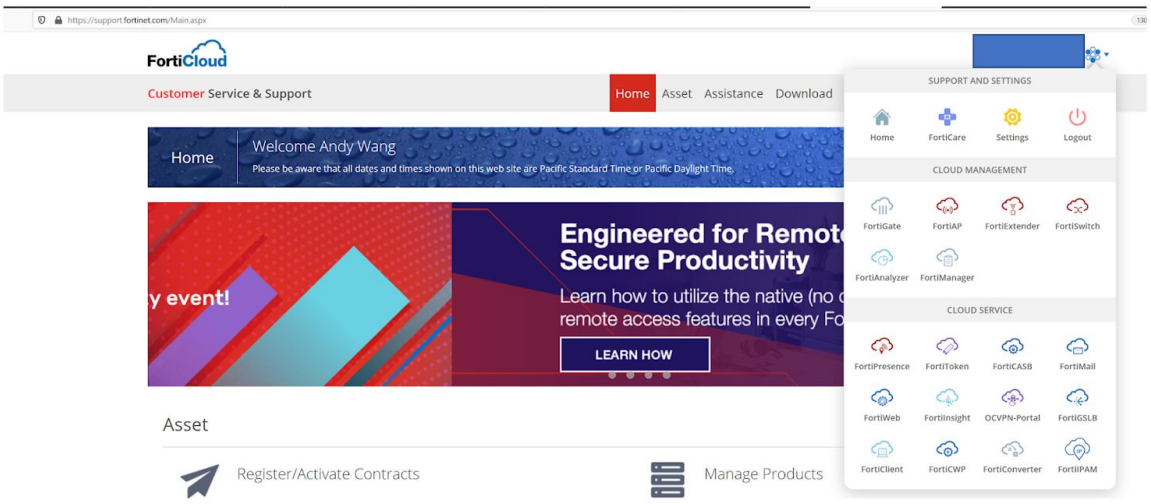
if you want to use terraform instead GUI to deploy the resource. clone the code below

https://github.com/yagosys/fortigate_aliyun/tree/master/AP-CrossZone

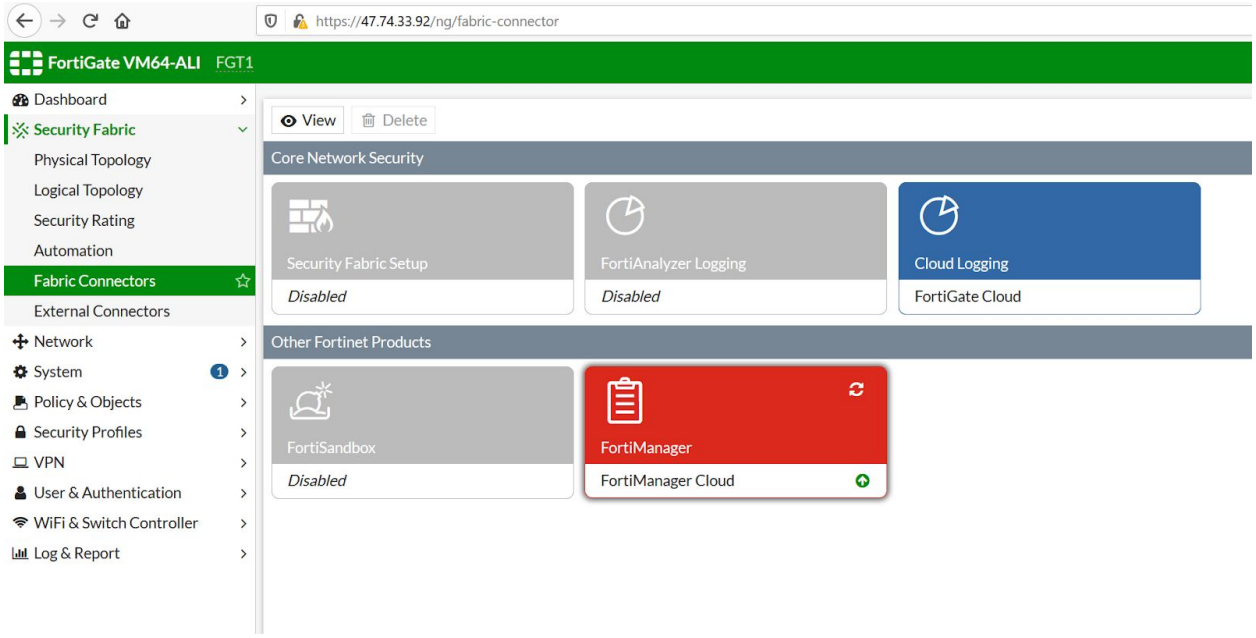
optional

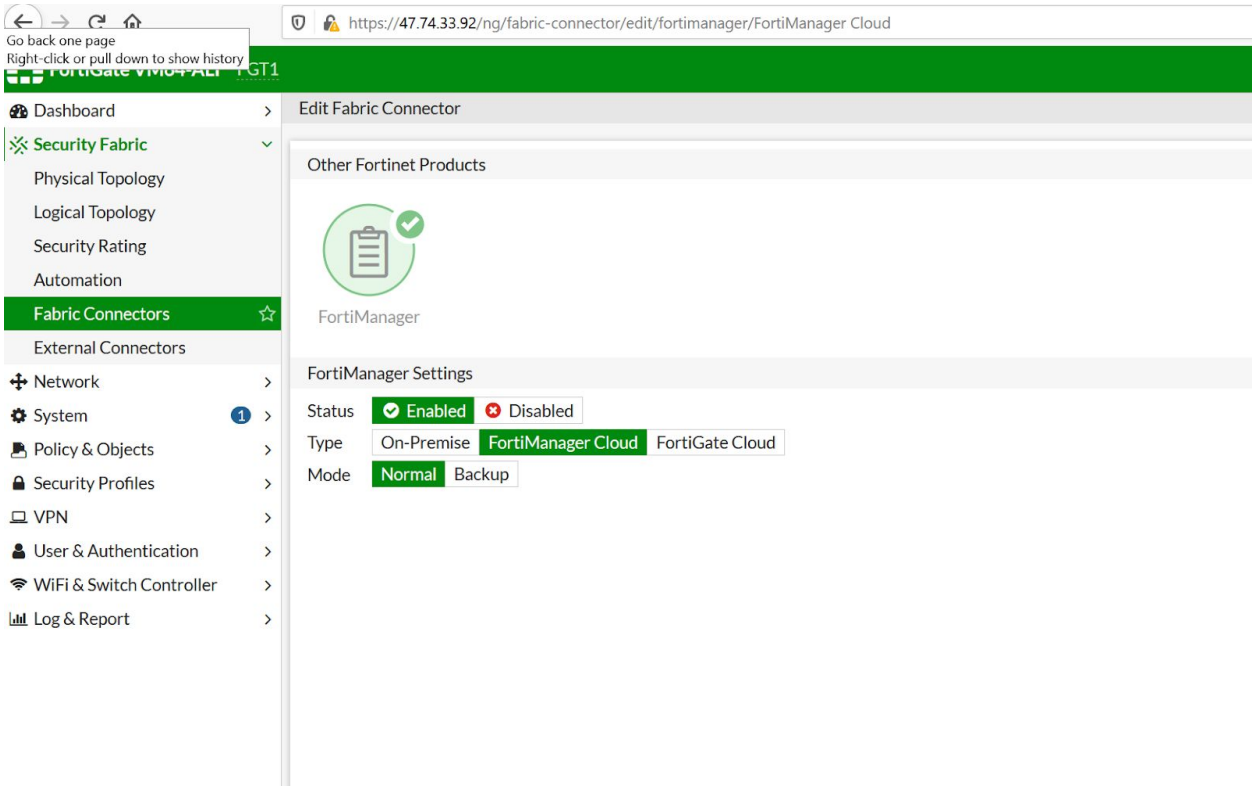
Connect Fortigate to FortiManager Cloud

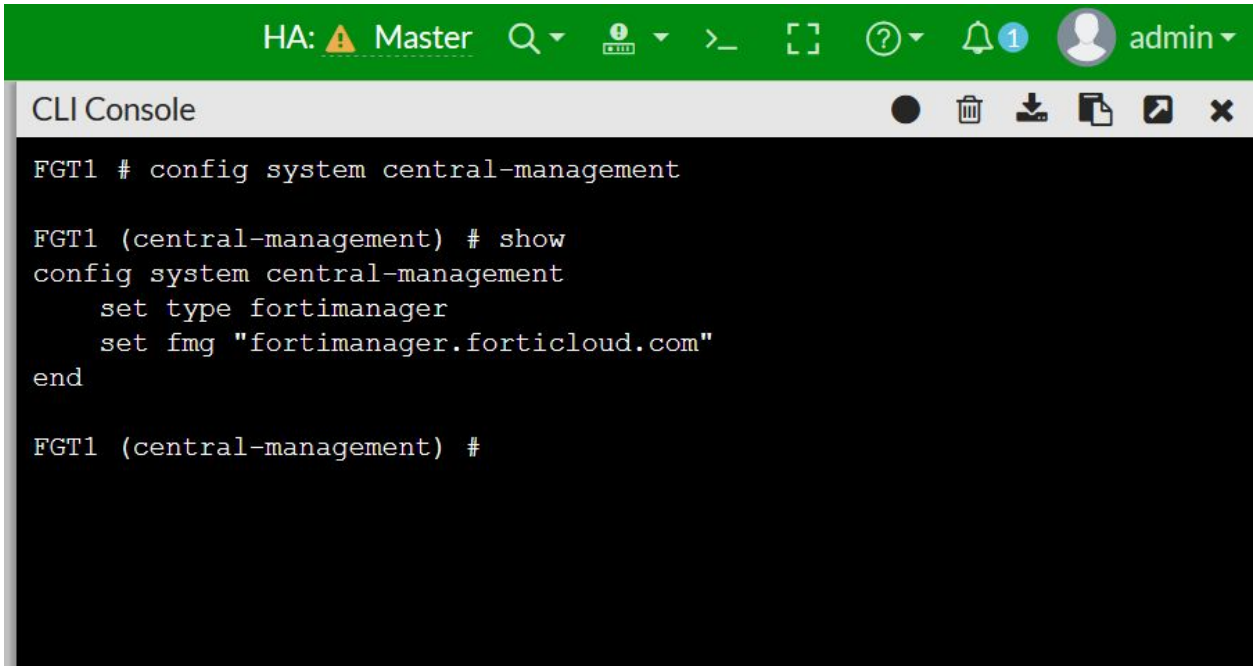
obtain FortiManager Cloud license.



Setup FortiGate







config fortimanager

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