AWS 跨 AZ 部署 FortiGate HA

版本	V1.0
时间	2021 年 9 月
作者	王祥
状态	
反馈	support_cn@fortinet.com

目录

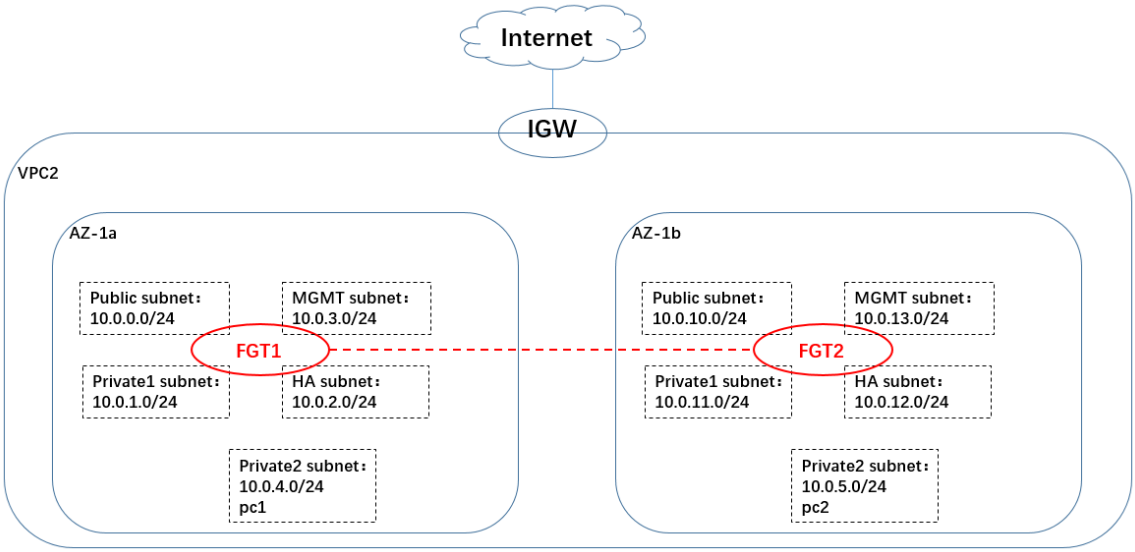
1. 介绍

本文档介绍如何在 AWS 跨 AZ 部署 FortiGate HA，以提供统一的威胁管理安全解决方案，保护您在 AWS 中的工作负载。

2. 网络拓扑

FGT1 和 FGT2 部署在不同的 AZ 中，FGT1 和 FGT2 的实例分别需要 4 块网卡。AWS 每种实例类型的最大接口数及每个网络接口的 IP 地址数的查询链接如下：

https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/UserGuide/using-eni.html



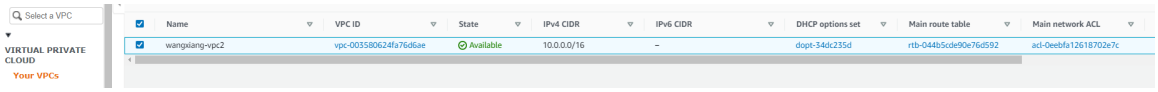
3. 地址规划

FGT1 地址规划（AZ-1a）	
Port	AWS primary address
Port1	10.0.0.11
Port2	10.0.1.11
Port3	10.0.2.11
Port4	10.0.3.11
FGT2 地址规划（AZ-1b）	
Port	AWS primary address
Port1	10.0.10.11
Port2	10.0.11.11
Port3	10.0.12.11
Port4	10.0.13.11
测试 PC	
PC 名称	测试地址
PC2	10.0.4.20
PC3	10.0.5.20

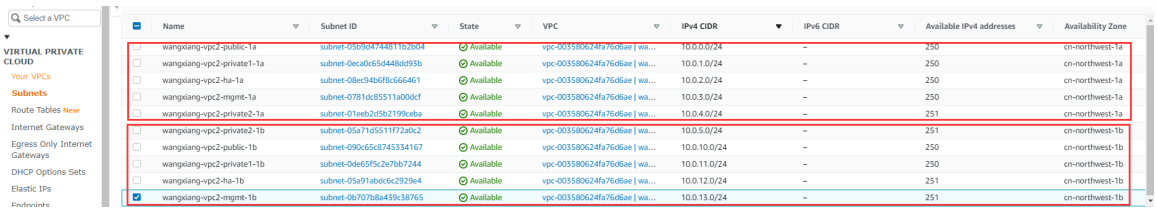
4. 配置步骤

4.1. 创建 VPC、子网和 IGW

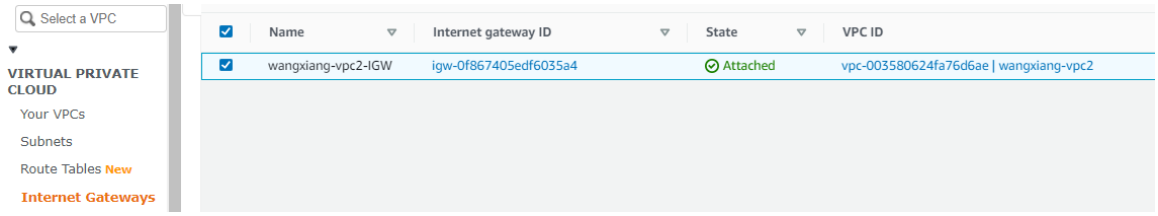
创建 VPC。



创建子网。

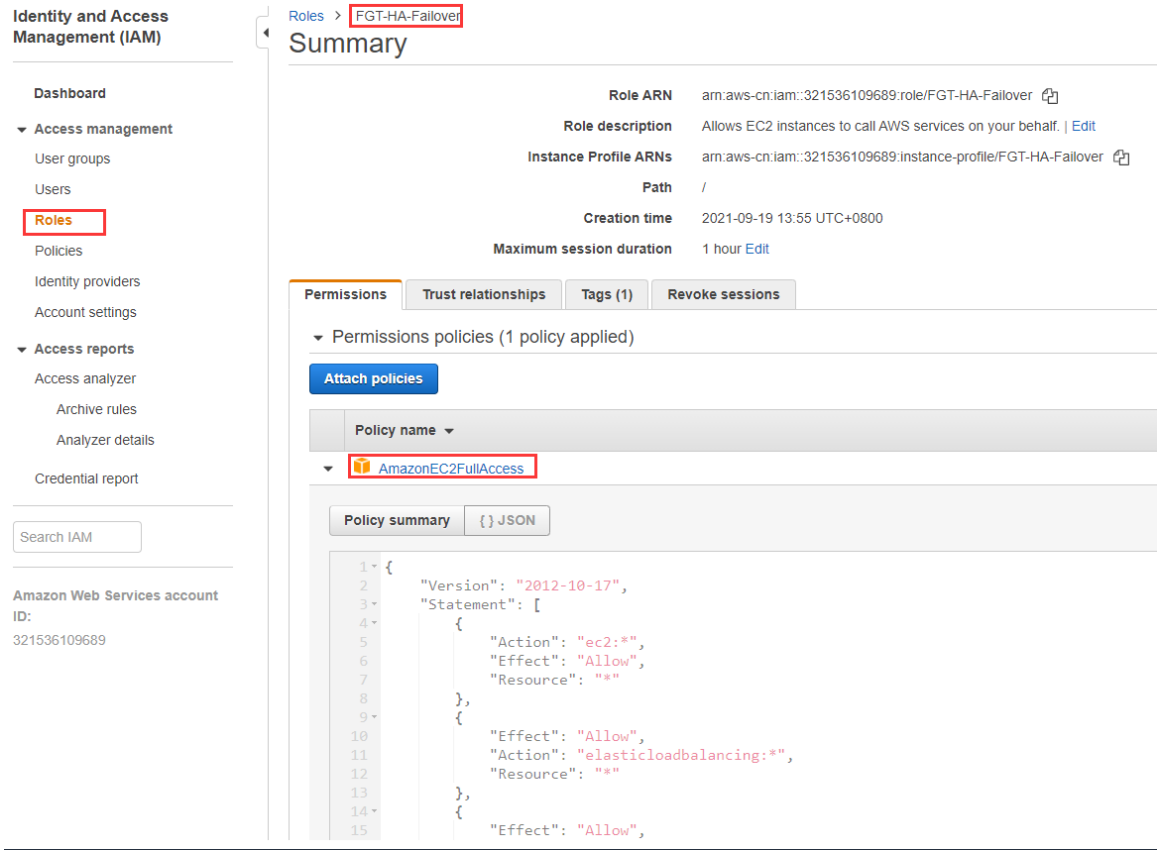


创建 IGW 并关联此 VPC。



4.2. 创建 IAM 角色

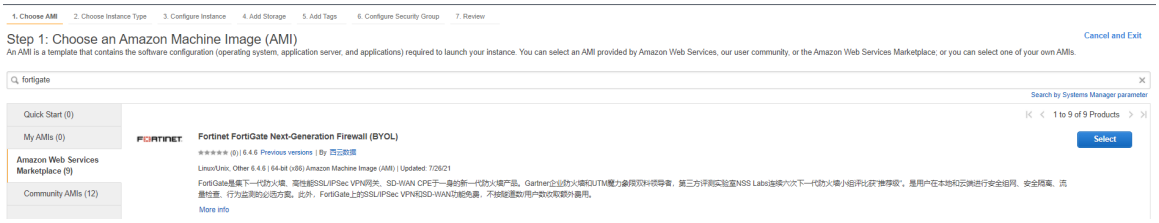
EC2 实例赋予角色后，才能根据权限使用 API 操作和资源。



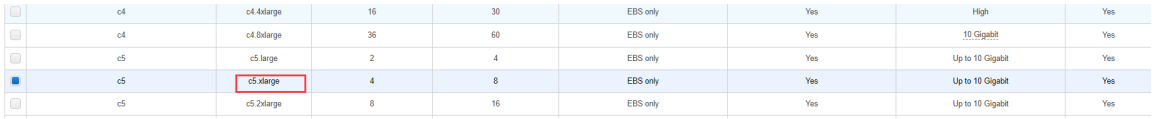
4.3. 创建 FortiGate 实例

部署实例时请提前准备好两台 FGT 的 license。

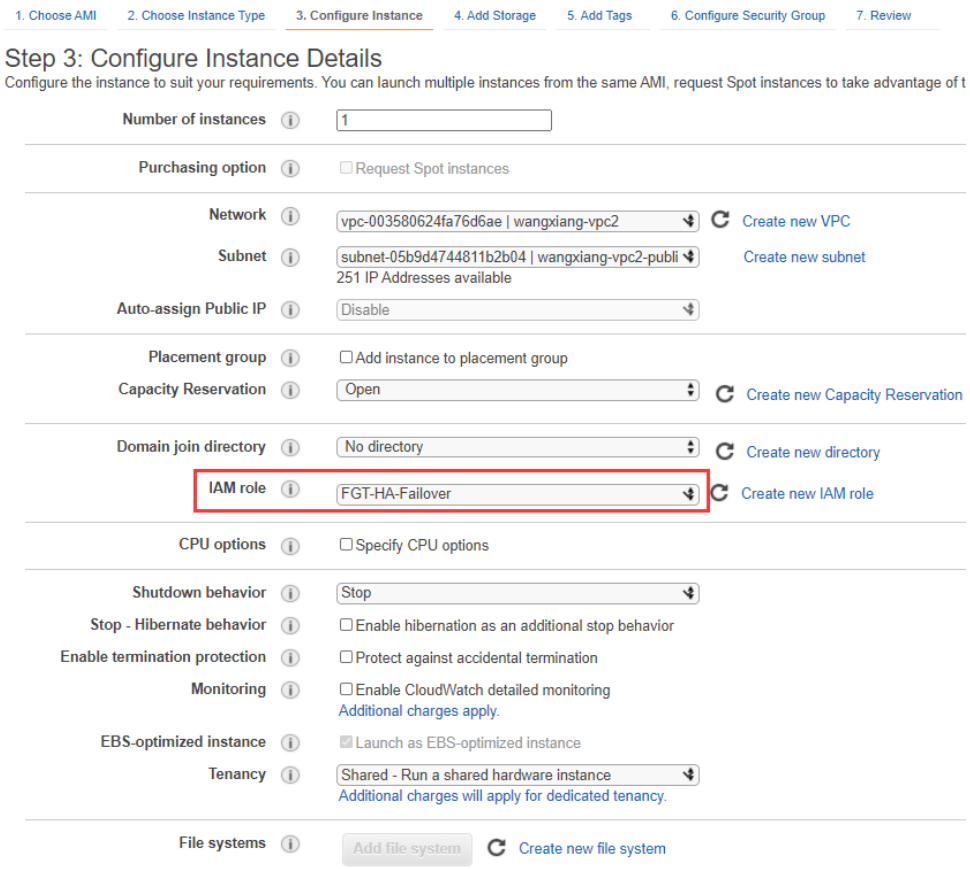
创建 FGT1，选择 FortiGate 镜像。



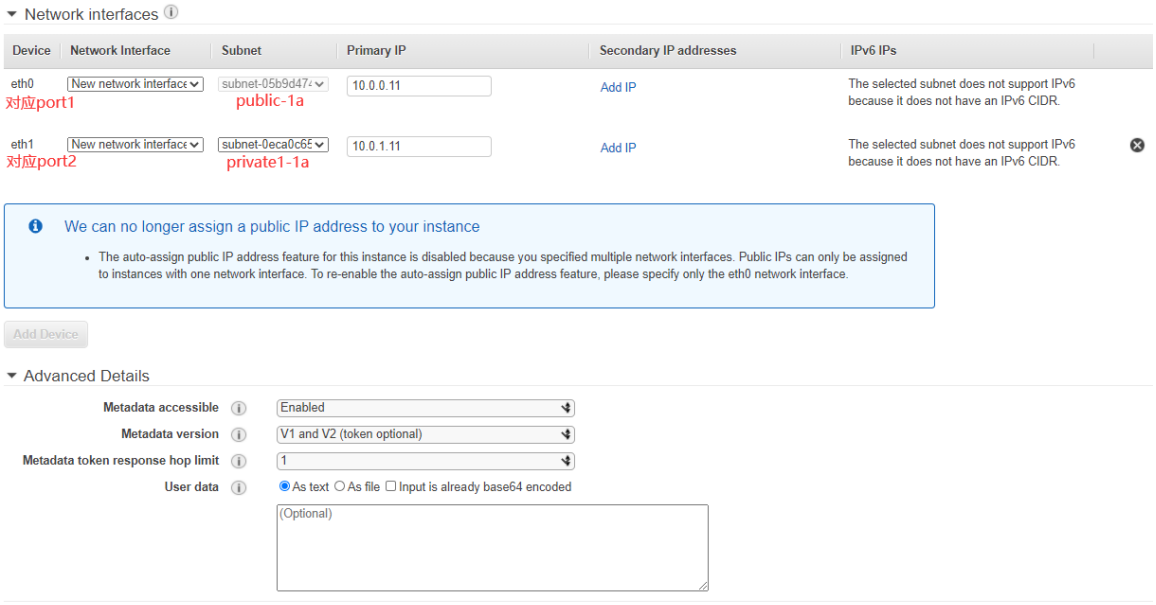
实例类型请选择**计算优化型**，这里使用 c5.xlarge。



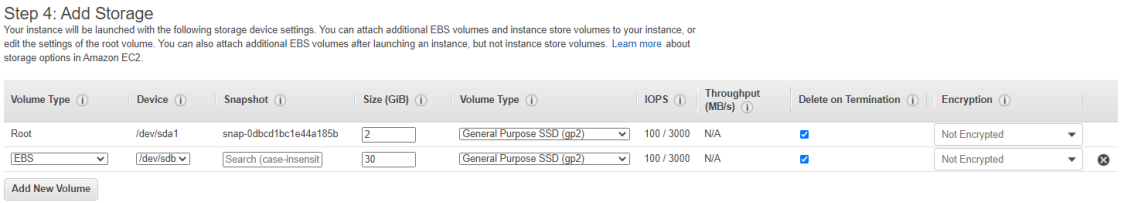
部署实例时关联 IAM 角色。



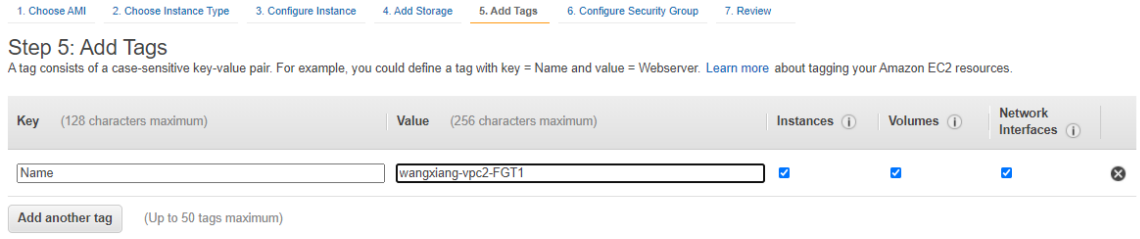
GUI 创建实例时，最多只能创建两块网卡，另外两块需要单独创建。



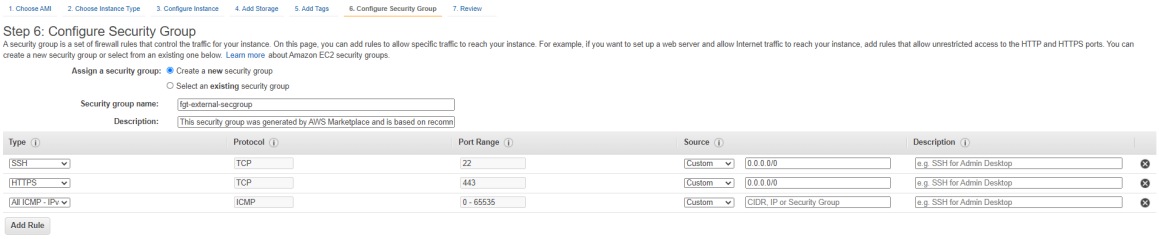
添加存储，第二块磁盘用于记录日志，如果 FGT 需要开启流量日志，建议发送到 FAZ 或者 syslog 服务器。



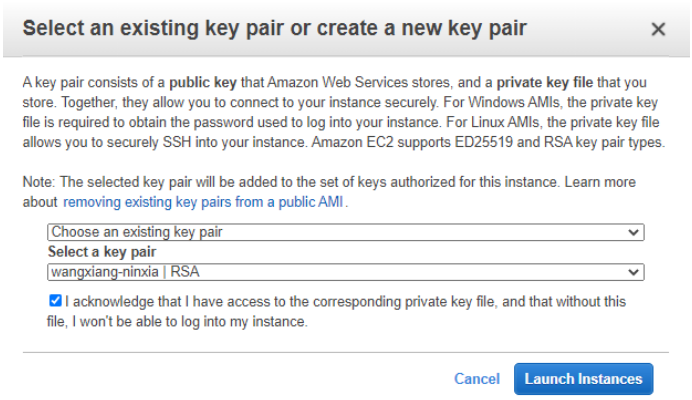
添加标签用于标识一个实例。



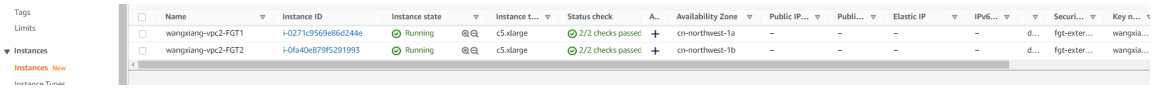
创建安全组 fgt-external-secgroup，对于管理 FortiGate 需要放行 22、443 端口，ICMP，其他端口根据业务需求放行。



创建 key，或者选择自己已经存在的 key，并启动实例。

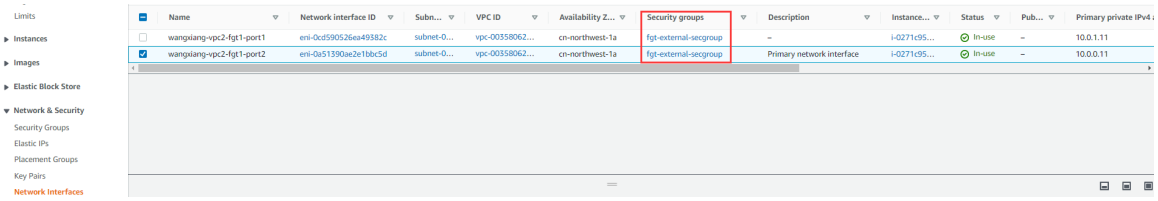


创建完成。FGT2 同理。



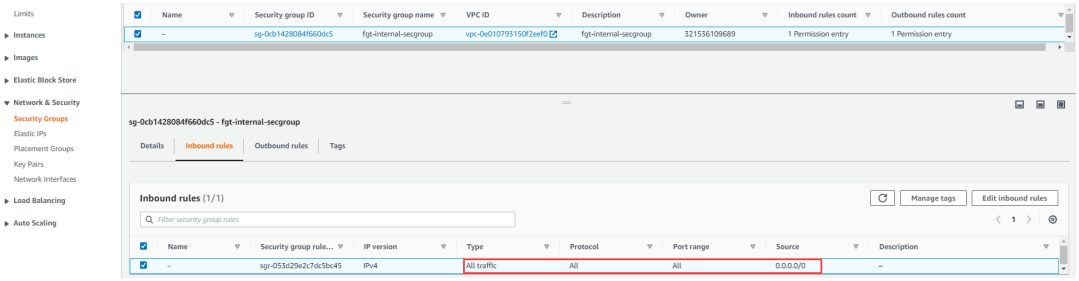
4. 4. 安全组

点击网络接口可以查看到 FGT 实例创建的接口，建议给每个接口命名以便查询。FortiGate 实例给其两个接口使用的安全组都是刚新建的 fgt-external-secgroup。

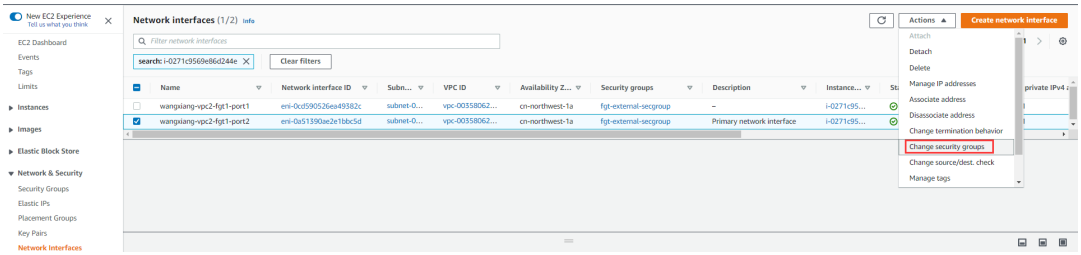


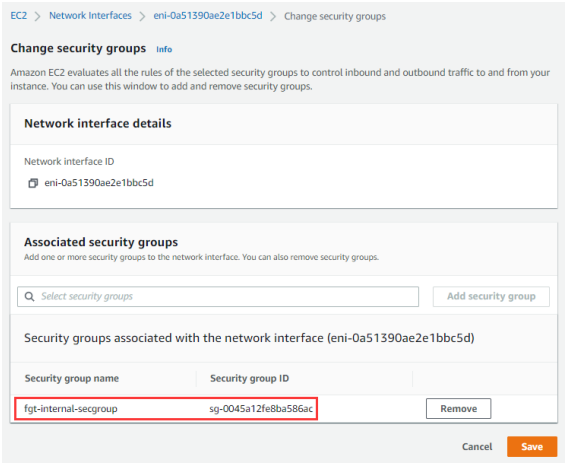
AWS 安全组是基于接口的，对于 FortiGate port2 而言，port2 对应的是由内向外的数据，因此 port2 的安全组要全放通。

新建安全组 fgt-internal-secgroup。

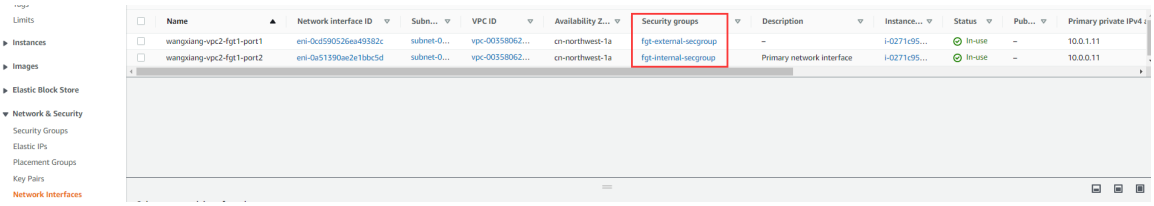


修改 port2 接口的安全组为 fgt-internal-secgroup。

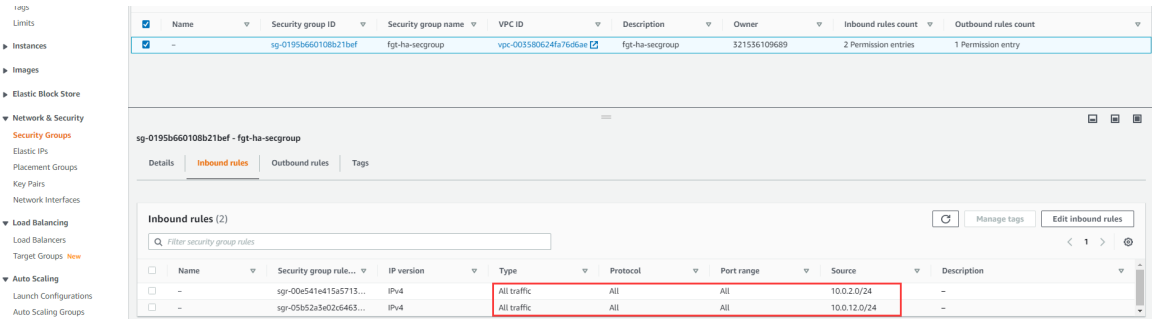




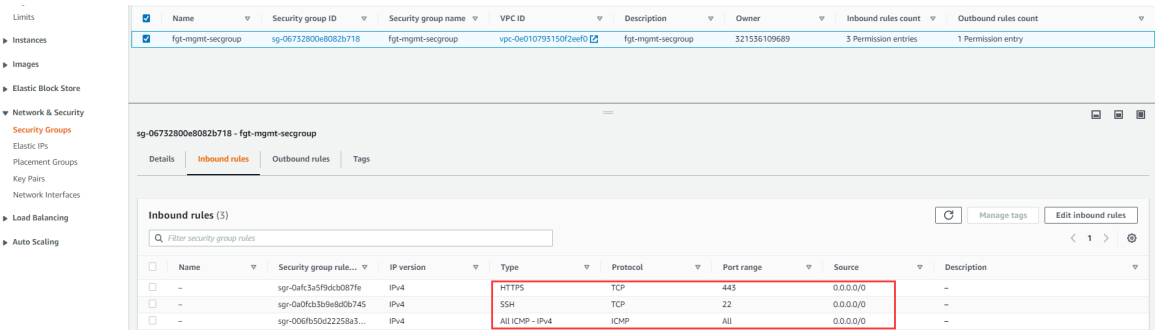
修改完成。



FortiGate 还需要新建两个端口，一个 HA 接口 port3，新建对应的安全组 fgt-ha-secgroup，放通 port3 接口网段（FGT1：10.0.2.0/24，FGT2：10.0.12.0/24）的所有流量。



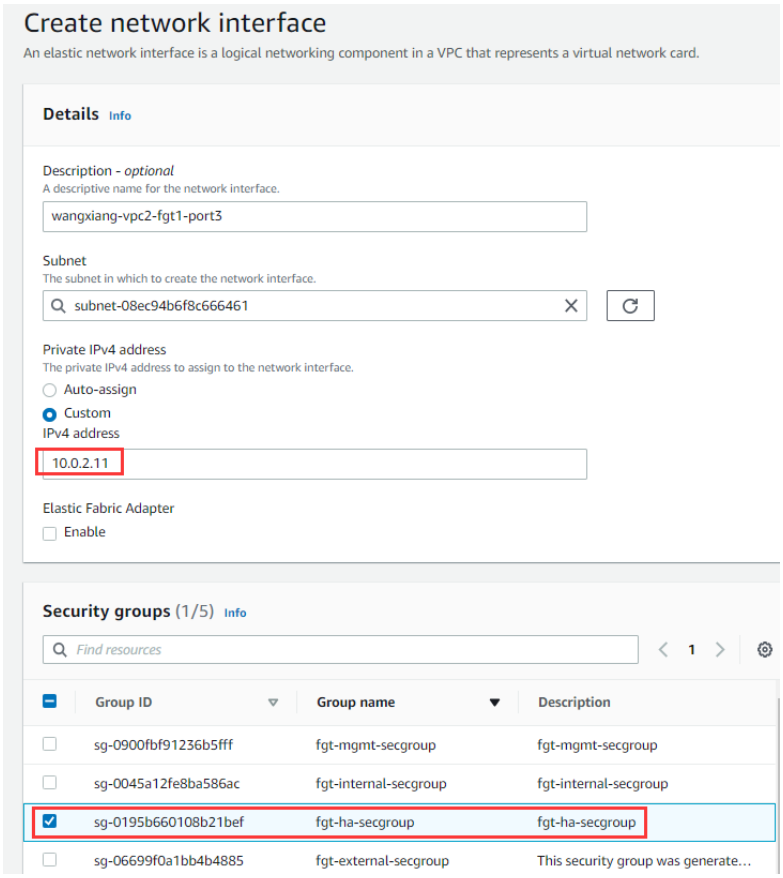
一个MGMT管理口port4，新建对应的安全组 fgt-mgmt-secgroup，放通SSH，HTTPS 和 ICMP。



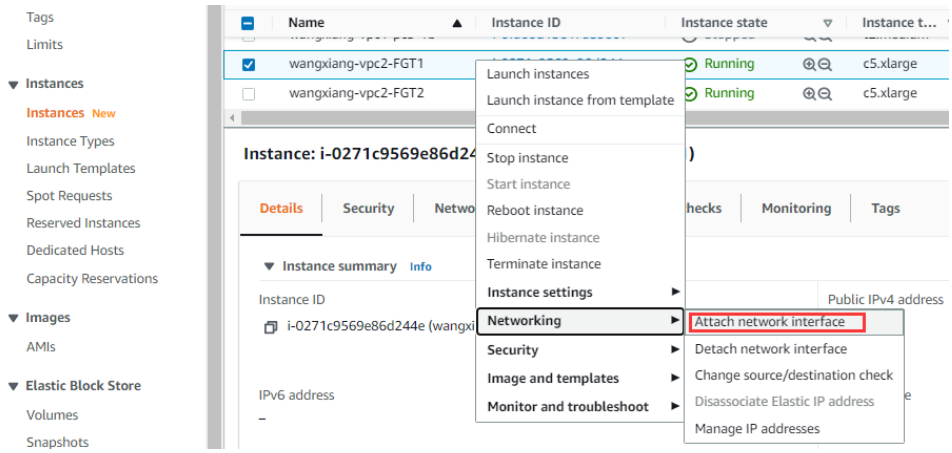
备注：FortiGate 本身就有防火墙策略对流量进行控制，如果嫌安全组控制太麻烦，可以将 FortiGate 的所有端口都应用**允许所有**的安全组。

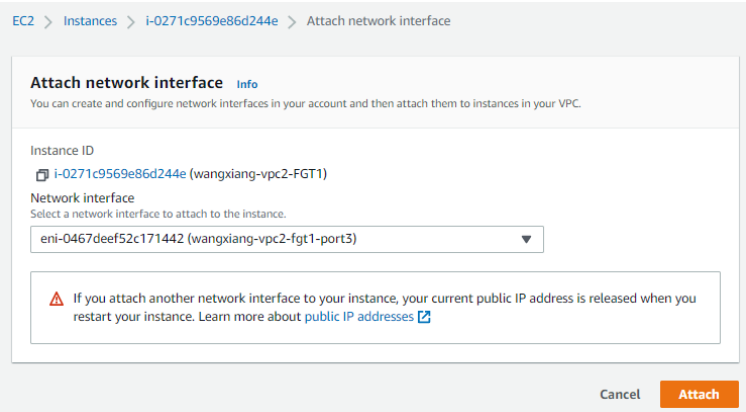
4.5. 创建网卡

选择 Services→ Network & Security→ Network interfaces，点击 Create Network interface，创建 FGT1 的 port3 接口，安全组选择 fgt-ha-secgroup，如果是 port4，则选择 fgt-mgmt-secgroup。

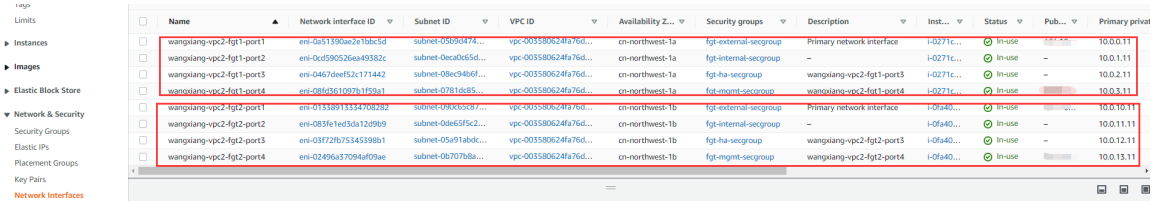


关联网卡到 FGT 实例。请先关联 port3，port3 关联成功后，再关联 port4。




EC2 > Instances > i-0271c9569e86d244e > Attach network interface
Attach network interface Info
You can create and configure network interfaces in your account and then attach them to instances in your VPC.
Instance ID
i-0271c9569e86d244e (wangxiang-vpc2-FGT1)
Network interface
Select a network interface to attach to the instance.
eni-0467deef52c171442 (wangxiang-vpc2-fgt1-port3)
If you attach another network interface to your instance, your current public IP address is released when you restart your instance. Learn more about public IP addresses
Cancel
Attach

关联完成。


Limits
Instances
Images
Elastic Block Store
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Name
Network interface ID
Subnet ID
VPC ID
Availability Z...
Security groups
Description
Inst...
Status
Pub...
Primary privat
wangxiang-vpc2-fgt1-port1 eni-0a51390ae2e1bbc5d cn-northwest-1a fgt-external-secgroup Primary network interface In-use 10.0.0.11
wangxiang-vpc2-fgt1-port2 eni-0cd590526ea49382c cn-northwest-1a fgt-internal-secgroup In-use 10.0.1.11
wangxiang-vpc2-fgt1-port3 eni-0467deef52c171442 cn-northwest-1a fgt-ha-secgroup wangxiang-vpc2-fgt1-port3 In-use 10.0.2.11
wangxiang-vpc2-fgt1-port4 eni-08fd3610097b1f59a1 cn-northwest-1a fgt-mgmt-secgroup wangxiang-vpc2-fgt1-port4 In-use 10.0.3.11
wangxiang-vpc2-fgt2-port1 cn-northwest-1b fgt-external-secgroup Primary network interface In-use 10.0.10.11
wangxiang-vpc2-fgt2-port2 eni-083fe1ed3da12d9b9 cn-northwest-1b fgt-internal-secgroup In-use 10.0.11.11
wangxiang-vpc2-fgt2-port3 eni-03f72fb75345398b1 cn-northwest-1b fgt-ha-secgroup wangxiang-vpc2-fgt2-port3 In-use 10.0.12.11
wangxiang-vpc2-fgt2-port4 eni-02496a37094af09ae cn-northwest-1b fgt-mgmt-secgroup wangxiang-vpc2-fgt2-port4 In-use 10.0.13.11

4.6. 弹性 IP

创建 4 个弹性 IP，最终使用 3 个，另外 1 个是临时的，HA 形成后可以释放。

最终使用的 3 个弹性 IP：

一个弹性 IP 关联 FGT1 实例 NIC4 10.0.3.11，即 FGT1 HA 的独立管理口 port4。

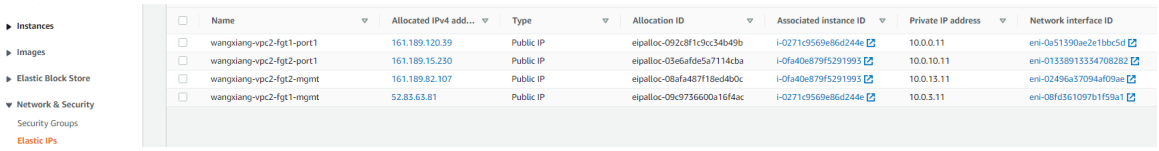
一个弹性 IP 关联 FGT2 实例 NIC4 10.0.13.11，即 FGT2 HA 的独立管理口 port4。

下面临时配置的弹性 IP 保留一个，关联 FGT HA 的 Master 实例（当前 FGT1）NIC1 的地址 10.0.0.11。

临时配置 FGT2 的弹性 IP:

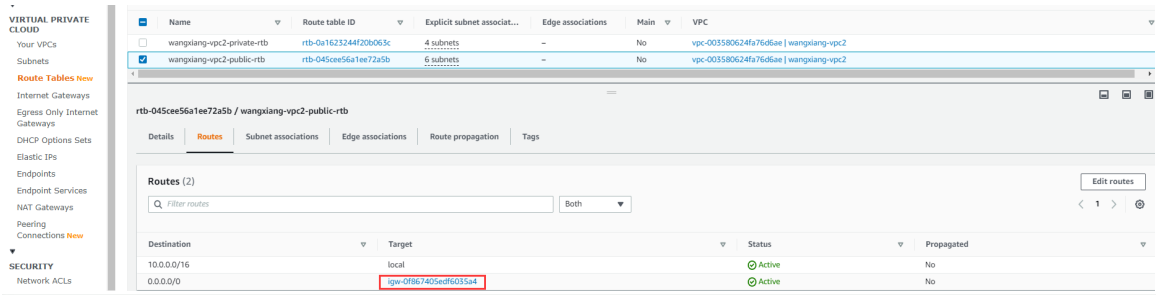
一个弹性 IP 关联 FGT1 实例 NIC1 10.0.0.11，即 FGT1 port1 接口。

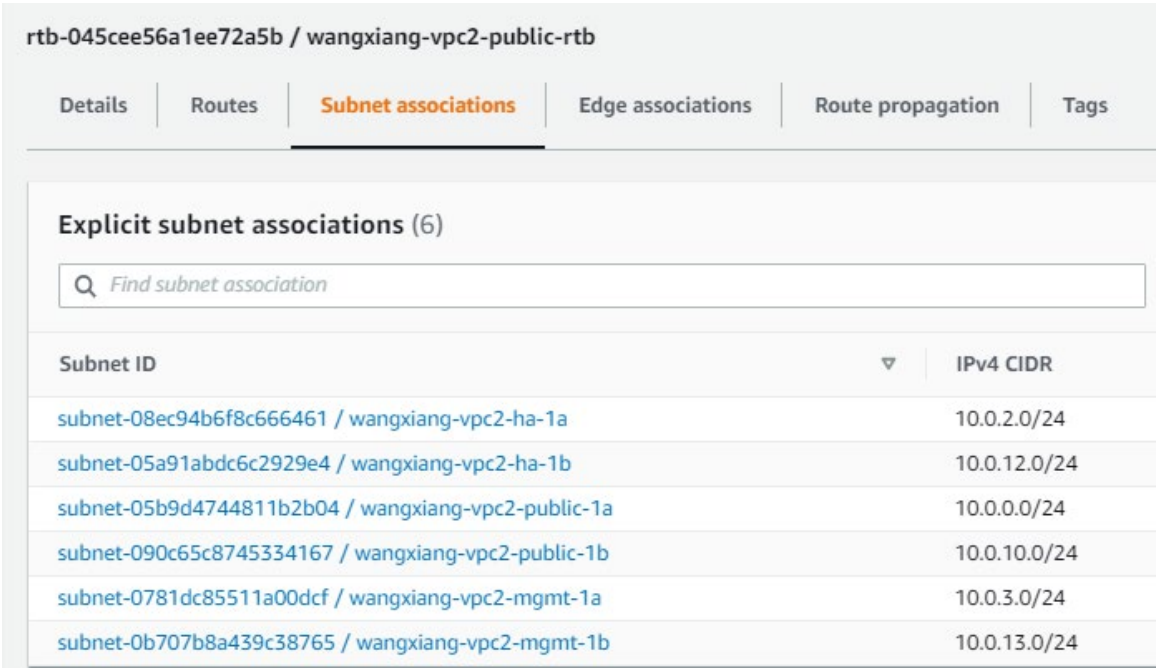
一个弹性 IP 关联 FGT2 实例 NIC1 10.0.10.11，即 FGT2 port1 接口。



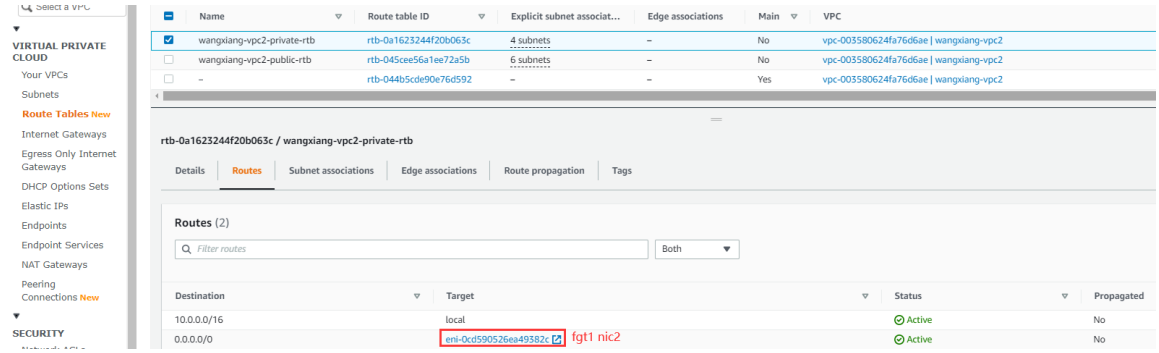
4.7. 配置 VPC 路由表

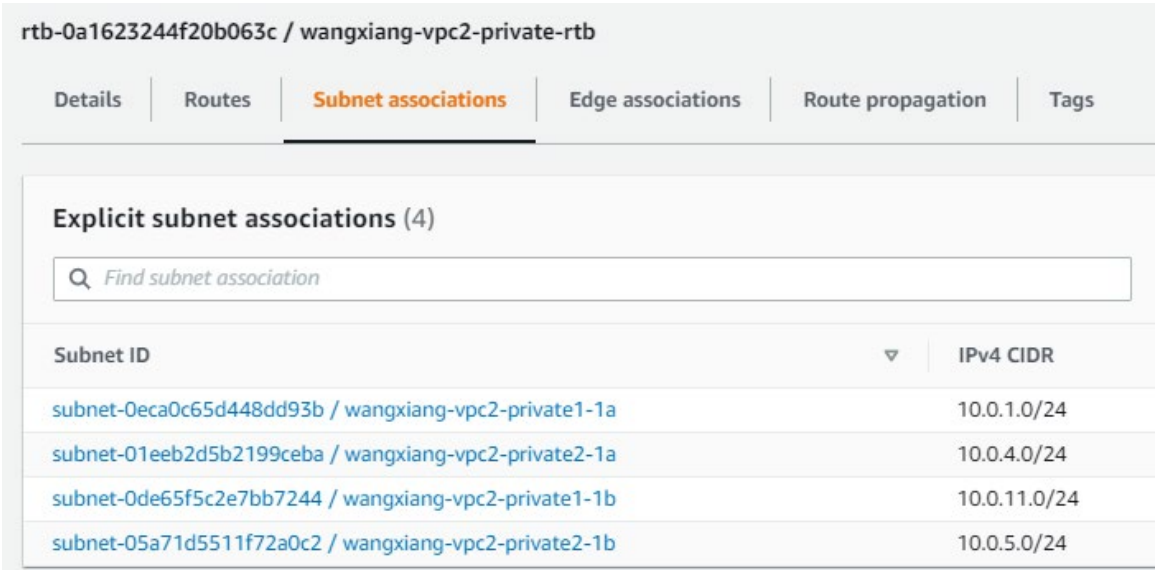
Public 路由表默认路由指向 IGW，关联 public（10.0.0.0/24，10.0.10.0/24），ha（10.0.2.0/24，10.0.12.0/24），mgmt（10.0.3.0/24，10.0.13.0/24）6 个子网。





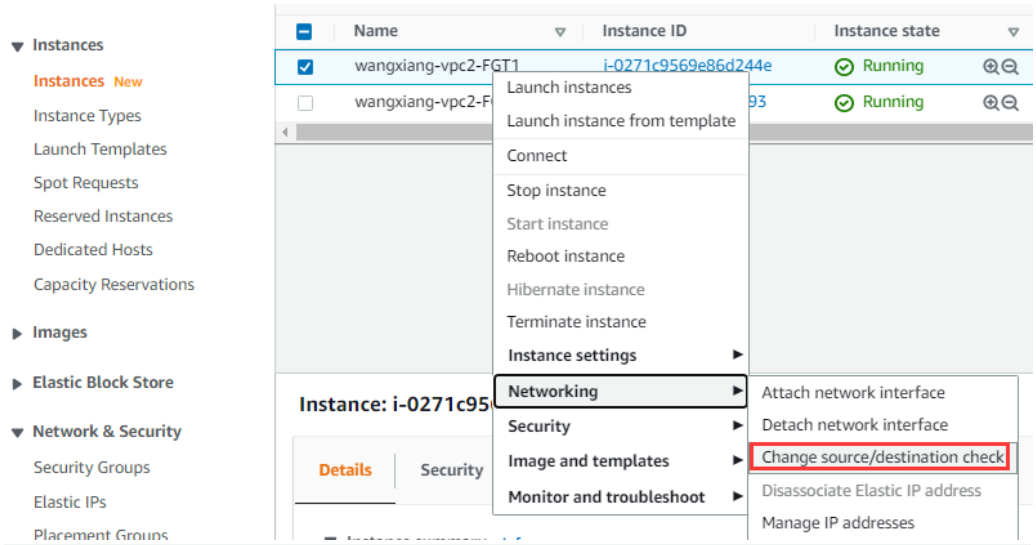
Private 路由表默认路由指向 FGT HA Master（当前 FGT1）实例的 NIC2 的接口 ID，关联 private 子网（10.0.1.0/24，10.0.11.0/24，10.0.4.0/24，10.0.5.0/24）

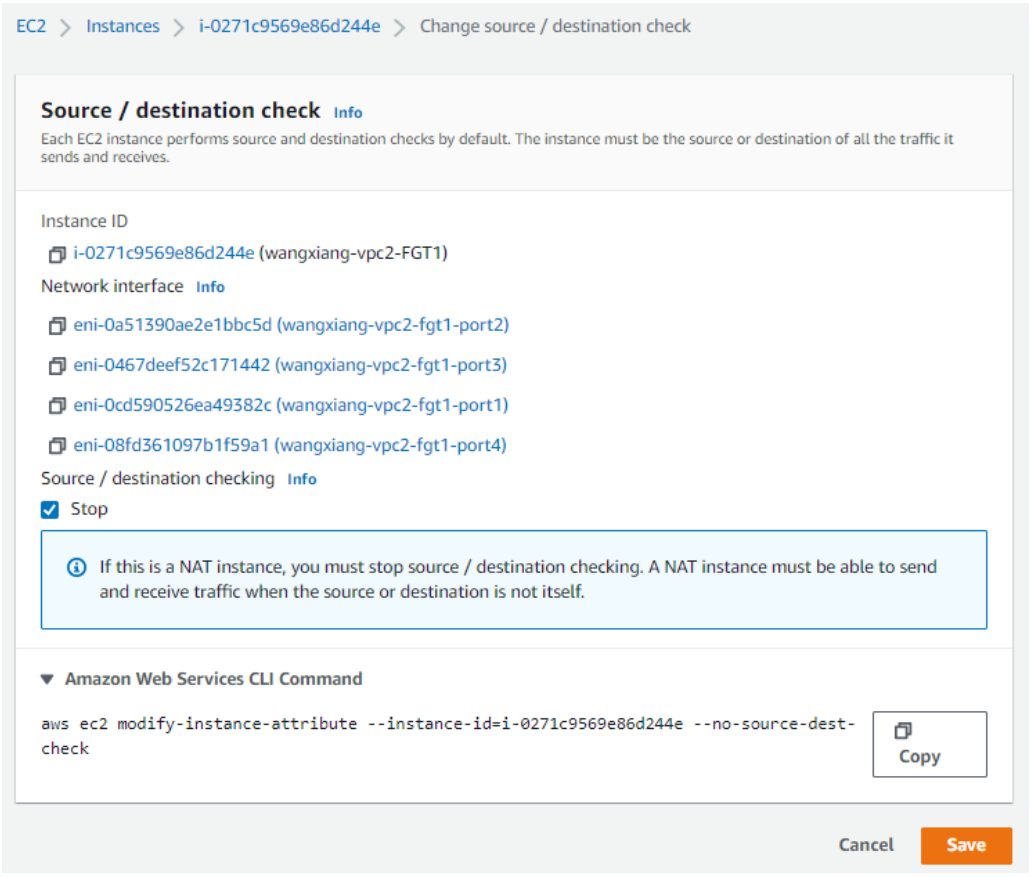




4. 8. 禁用源/目标检查

每个 EC2 实例都会默认执行源/目标检查。这意味着实例必须为其发送或接收的数据流的源头或目标。 但是，NAT 实例必须能够在源或目标并非其本身时发送和接收数据流。因此，FGT 实例必须禁用源/目标检查。

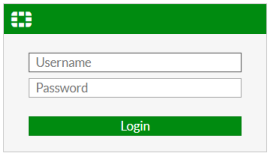




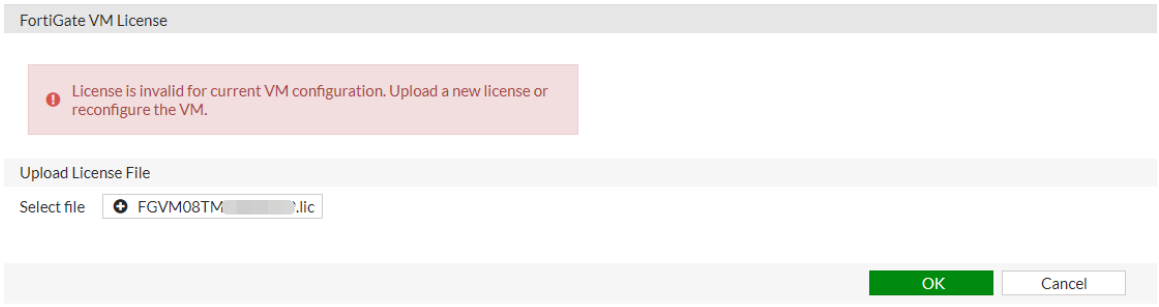
4.9. 访问 FortiGate

Https 访问 FortiGate：

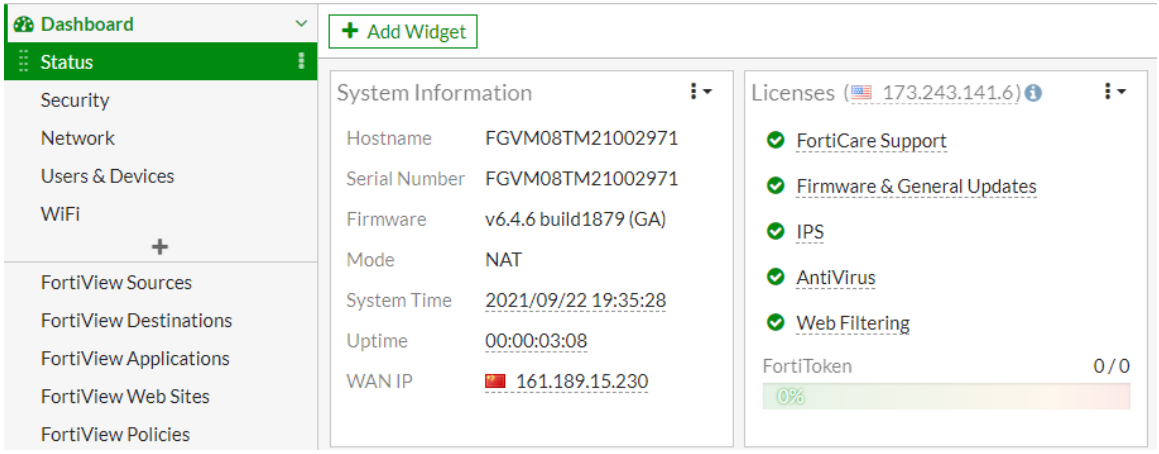
使用 https://161.189.15.230/ （弹性 IP）访问 FortiGate，账号是 admin，密码默认是实例 ID。首次登录后，请按照提示修改密码。



登录后，请先上传购买好的 license，导入 license 会重启 FortiGate。

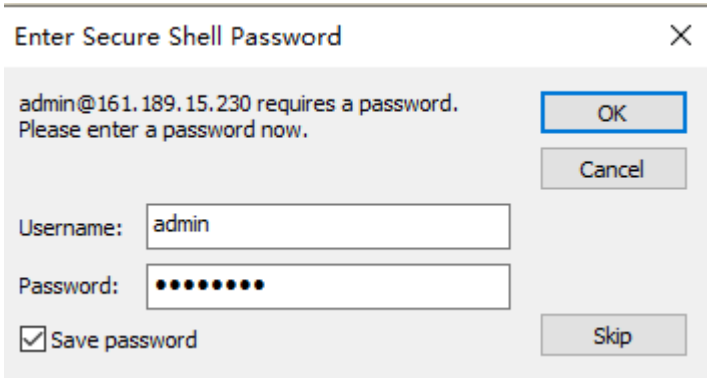


FortiGate 登录成功。

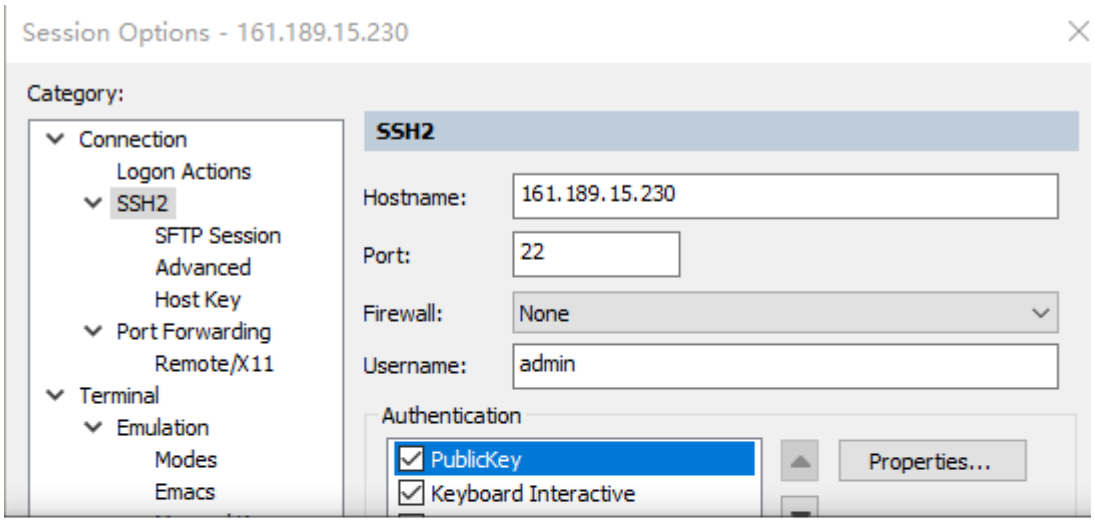


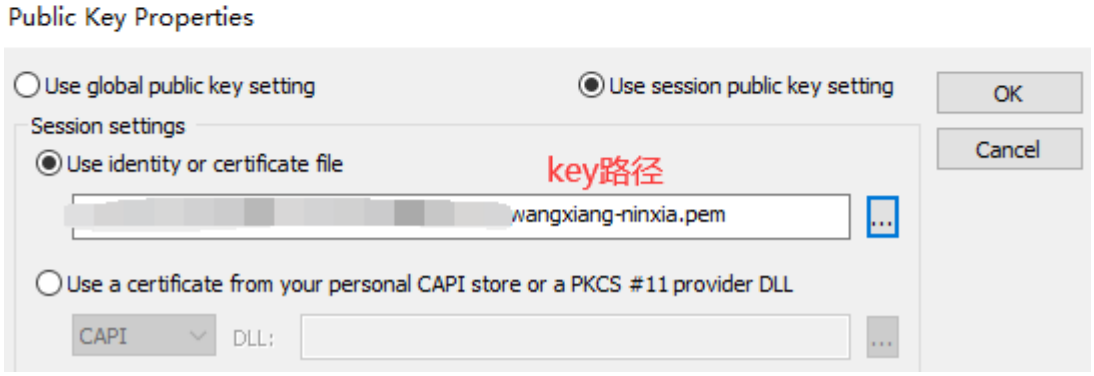
SSH 访问 FortiGate 有两种方式，下图是 CRT 软件的访问截图：

一种是通过账号密码的方式：



一种是通过 key 的方式：





4.10. 配置 FortiGate

FGT1 基本配置，先配置路由，再修改地址，否则 FGT1 将无法访问。

```
config router static
    edit 1
        set gateway 10.0.0.1
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.1.1
        set device "port2"
    next
end
config system interface
    edit "port1"
        set mode static
        set ip 10.0.0.11 255.255.255.0
        set allowaccess ping https ssh
    next
    edit "port2"
        set mode static
        set ip 10.0.1.11 255.255.255.0
        set allowaccess ping
    next
    edit "port3"
        set mode static
        set ip 10.0.2.11 255.255.255.0
        set allowaccess ping
    next
    edit "port4"
        set mode static
        set ip 10.0.3.11 255.255.255.0
        set allowaccess ping https ssh
    next
end
config system global
    set admintimeout 50
    set hostname "FGT1"
    set timezone 55
```

```
end
#因为不同 AZ 的地址段是不一样的，因此下面的配置不需要同步
config system vdom-exception
    edit 1
        set object system.interface
    next
    edit 2
        set object router.static
    next
    edit 3
        set object firewall.vip
    next
end
```

FGT2 基本配置，先配置路由，再修改地址，否则 FGT2 将无法访问。

```
config router static
    edit 1
        set gateway 10.0.10.1
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.11.1
        set device "port2"
    next
end
config system interface
    edit "port1"
        set mode static
        set ip 10.0.10.11 255.255.255.0
        set allowaccess ping https ssh
    next
    edit "port2"
        set mode static
        set ip 10.0.11.11 255.255.255.0
        set allowaccess ping
    next
    edit "port3"
        set mode static
        set ip 10.0.12.11 255.255.255.0
        set allowaccess ping
    next
```

```
        edit "port4"
            set mode static
            set ip 10.0.13.11 255.255.255.0
            set allowaccess ping https ssh
        next
end
config system global
        set admintimeout 50
        set hostname "FGT2"
        set timezone 55
end
#因为不同 AZ 的地址段是不一样的，因此下面的配置不需要同步
config system vdom-exception
        edit 1
            set object system.interface
        next
        edit 2
            set object router.static
        next
        edit 3
            set object firewall.vip
        next
end
```

FGT1 HA 配置：

```
config system ha
        set group-name "FGTHA"
        set mode a-p
        set password fortinet
        set hbdev "port3" 50
        set session-pickup enable
        set session-pickup-connectionless enable
        set ha-mgmt-status enable
        config ha-mgmt-interfaces
            edit 1
                set interface "port4"
                set gateway 10.0.3.1
            next
        end
        set override disable
        set priority 200
        set unicast-hb enable
```

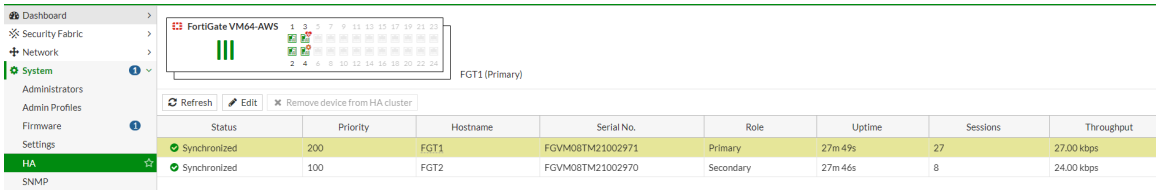
```
        set unicast-hb-peerip 10.0.12.11
    end
```

FGT2 HA 配置：

```
    config system ha
        set group-name "FGTHA"
        set mode a-p
        set password fortinet
        set hbdev "port3" 50
        set session-pickup enable
        set session-pickup-connectionless enable
        set ha-mgmt-status enable
        config ha-mgmt-interfaces
            edit 1
                set interface "port4"
                set gateway 10.0.13.1
            next
        end
        set override disable
        set priority 100
        set unicast-hb enable
        set unicast-hb-peerip 10.0.2.11
    end
```

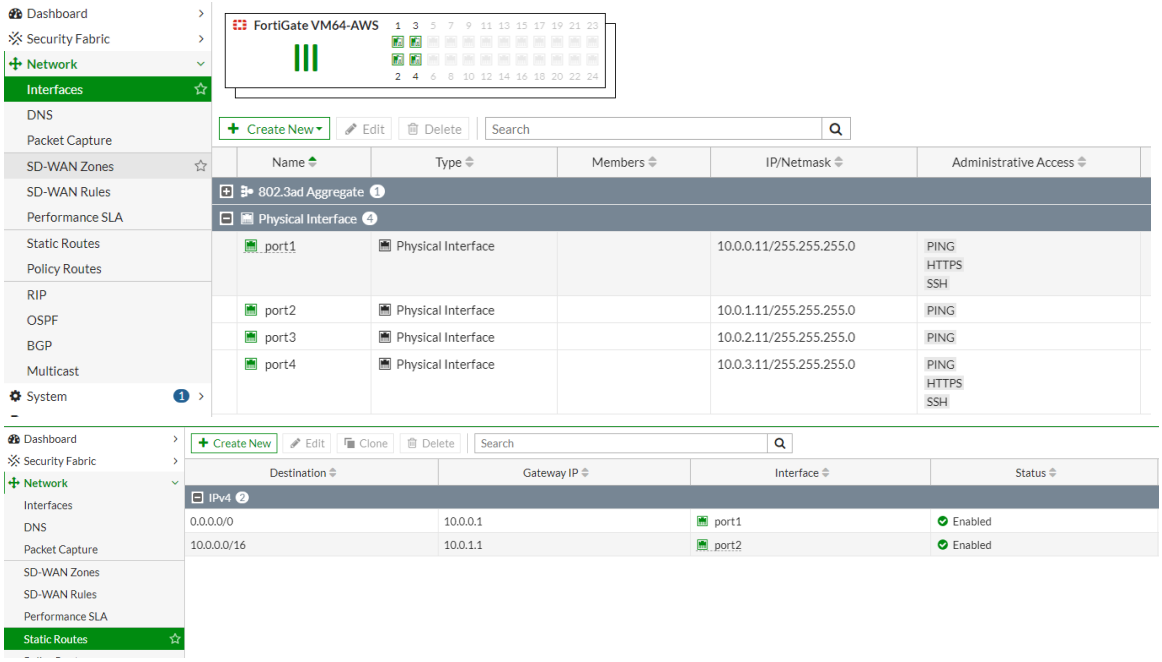
配置完成后，即可使用 FGT 实例 NIC4 关联的弹性 IP 进行访问。

注意：如果删除 HA 的配置，port3 和 port4 的接口地址也会移除。

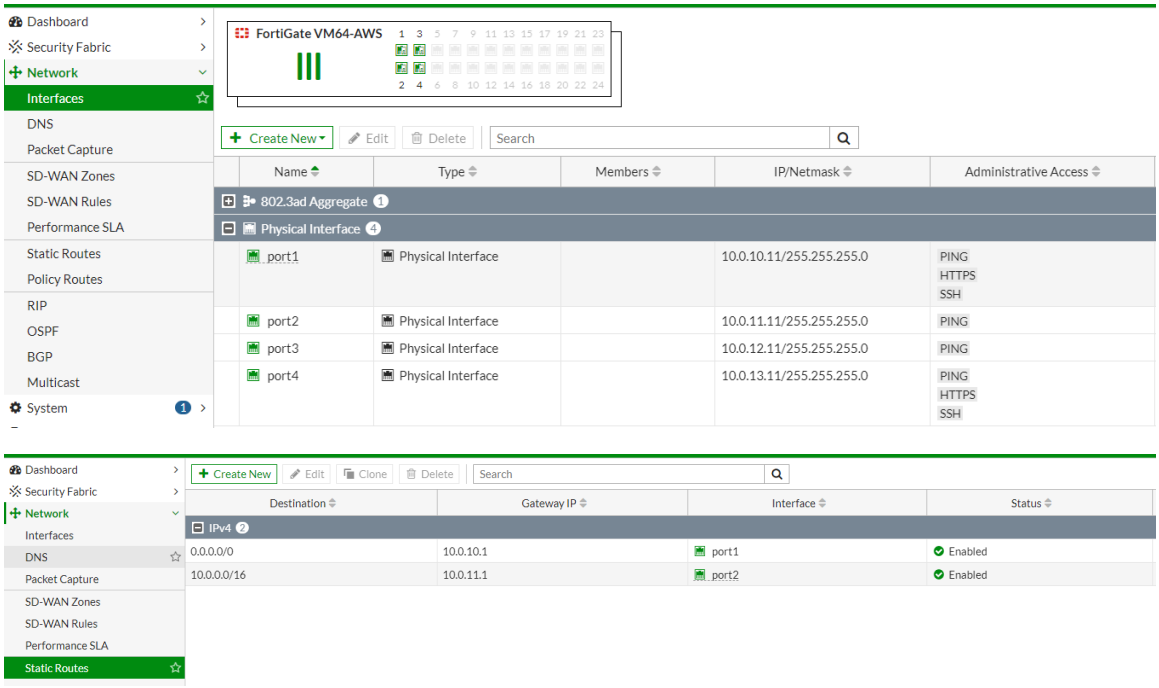


形成 HA 后，即可删除临时配置一个弹性 IP。

FGT1 接口及路由：



FGT2 接口及路由：

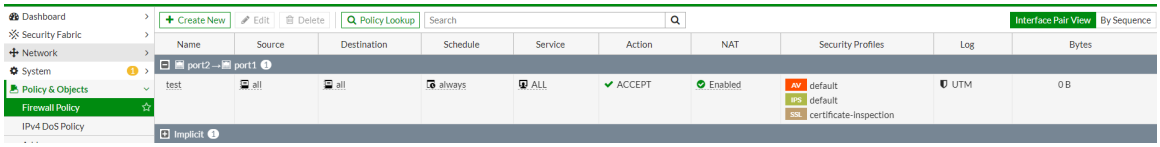


4.11. FortiGate 配置源 NAT

使用接口地址做源 NAT：

FGT1 配置防火墙策略，会自动同步给 FGT2：

注意：因为 FGT1 和 FGT2 的接口 ip 地址或者 pool 地址池是不一样的，因此 snat 的会话同步没有意义，HA 切换时，原有的 snat 连接会断开。



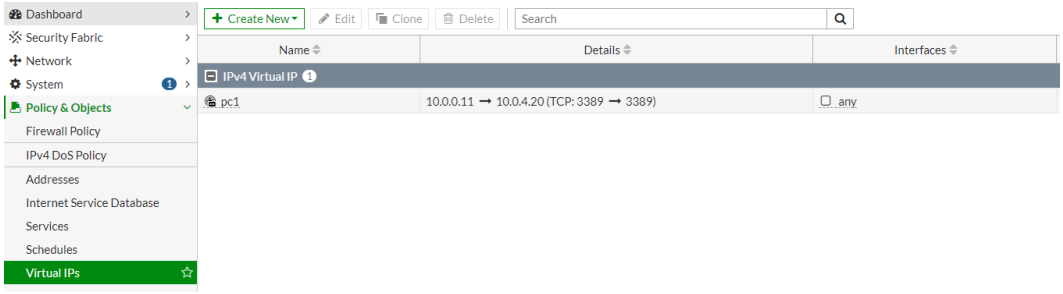
4.12. FortiGate 配置目的 NAT

可以使用 port1 接口的地址做目的 NAT，也可以分配一个单独的 IP 来做目的 NAT。

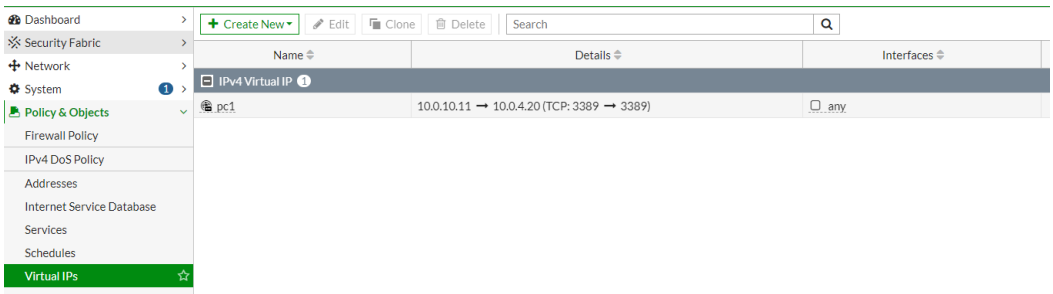
注意：因为 FGT1 和 FGT2 的 vip 地址是不一样的，因此目的 nat 的会话同步没有意义，HA 切换时，原有的目的 nat 连接会断开。

用 port1 接口的地址做目的 NAT：

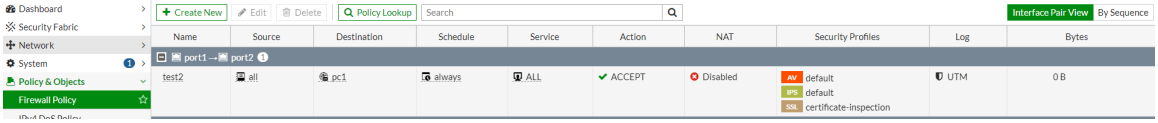
FGT1 配置 VIP，名称 pc1：



FGT2 配置 VIP，名称 pc1，要和 FGT1 的 VIP 名称一样，这样防火墙策略才能够同步：

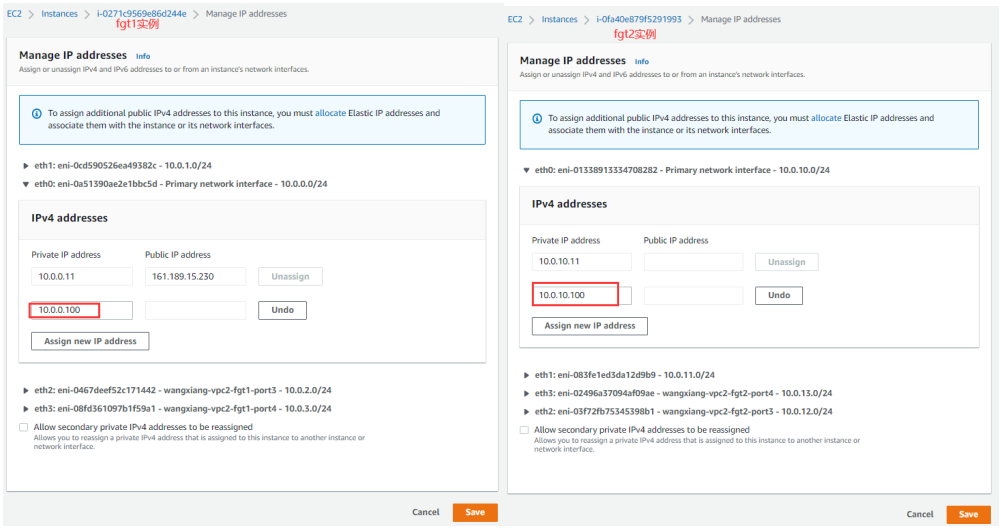


FGT1 配置防火墙策略调用此 VIP，会同步给 FGT2：

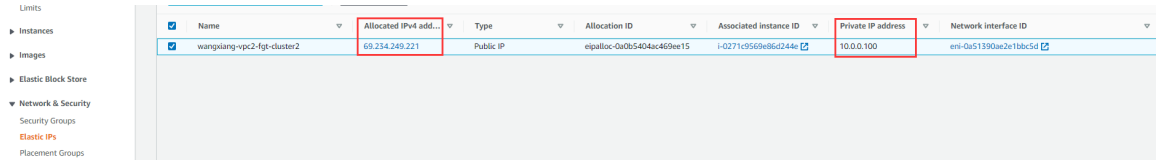


分配单独的 IP 来做目的 NAT：

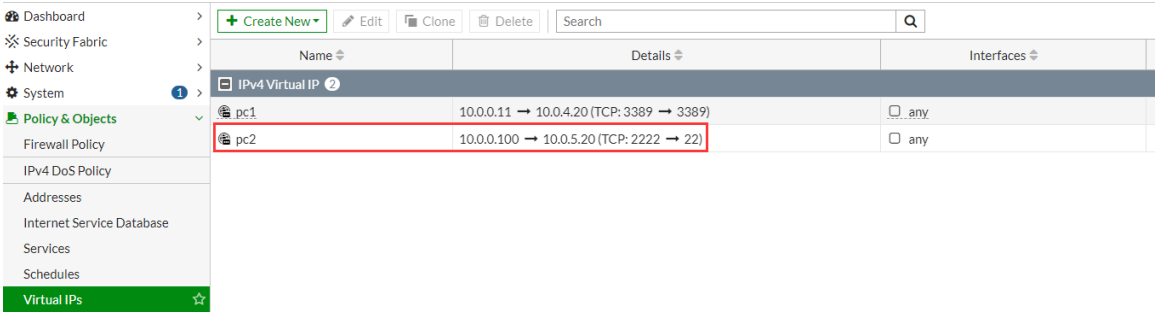
因为 FGT1 和 FGT2 的地址段不一样，因此 FGT1 和 FGT2 给 NIC1 都需要单独分配一个地址。



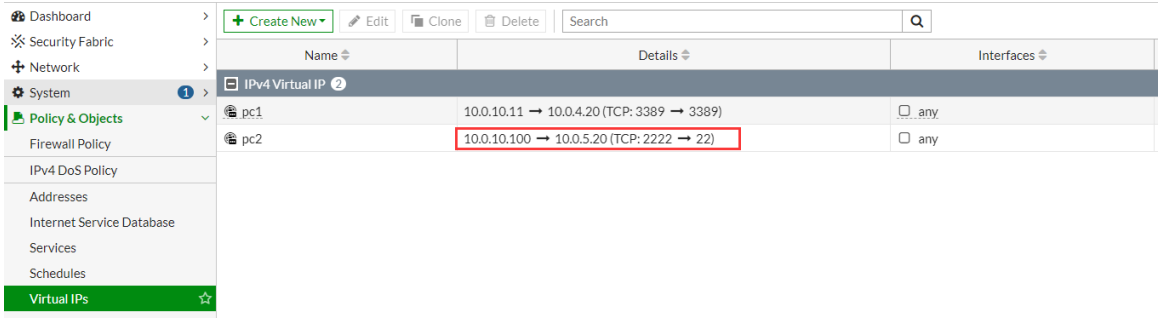
分配弹性 IP 关联 FGT1 实例的 NIC1 10.0.0.100。FGT2 不用关联。



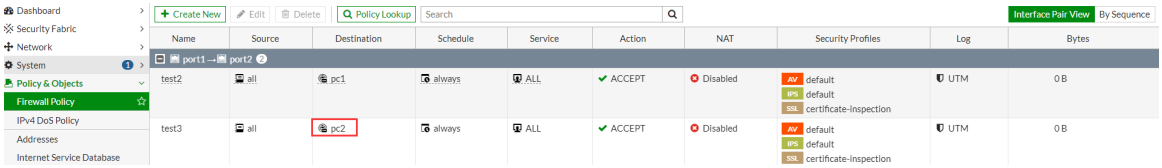
FGT1 配置 VIP，名称 pc2:



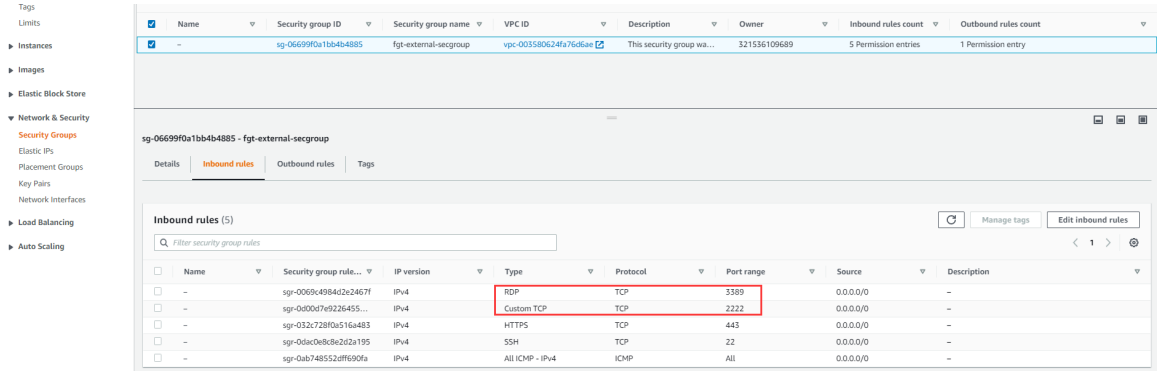
FGT2 配置 VIP，名称 pc2，要和 FGT1 的 VIP 名称一样，这样防火墙策略才能够同步：



FGT1 配置防火墙策略调用此 VIP，会同步给 FGT2：

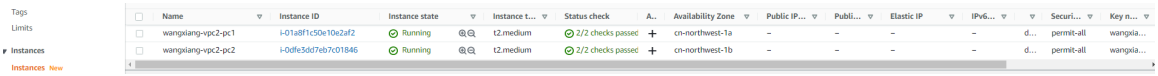


FGT 实例 NIC1，即 port1 安全组 fgt-external-secgroup 放通 3389，2222 这 2 个对外的端口。



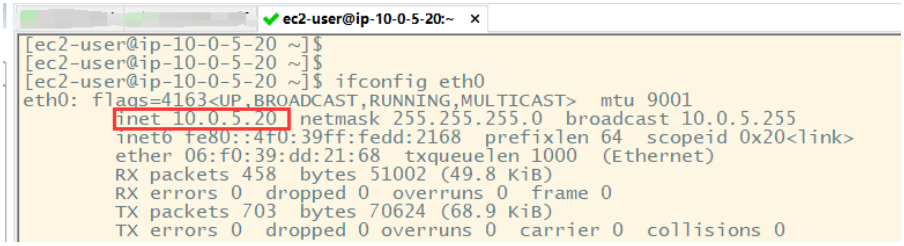
5. 业务测试

测试的 PC 如下：

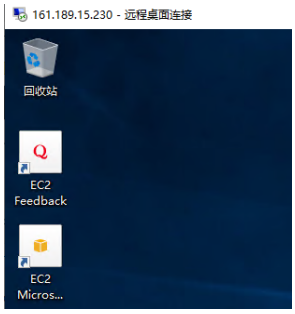


目的 NAT 测试：

ssh 69.234.249.221 2222 访问正常。



远程桌面访问正常。



源 NAT 测试：

PC2 10.0.5.20 ping 114.114.114.114 正常

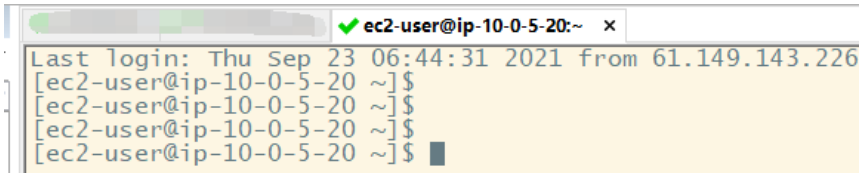
```
[ec2-user@ip-10-0-5-20 ~]$ ping 114.114.114.114
PING 114.114.114.114 (114.114.114.114) 56(84) bytes of data.
64 bytes from 114.114.114.114: icmp_seq=1 ttl=83 time=40.5 ms
64 bytes from 114.114.114.114: icmp_seq=2 ttl=66 time=40.5 ms
64 bytes from 114.114.114.114: icmp_seq=3 ttl=57 time=40.4 ms
64 bytes from 114.114.114.114: icmp_seq=4 ttl=71 time=40.4 ms
^C
--- 114.114.114.114 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 40.398/40.453/40.518/0.148 ms
```

PC1 10.0.4.20 访问 baidu 正常。

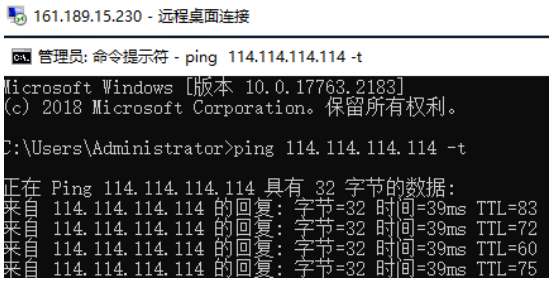
6. HA 切换测试

HA 测试目的：FGT 支持跨 AZ 的 HA，但不同 AZ 的地址段不一样，因此 SNAT 和 DNAT 的会话同步无意义，HA 切换后 SNAT 和 DNAT 的连接会断开，需要重新连接。

从外网 ssh 到 pc2。

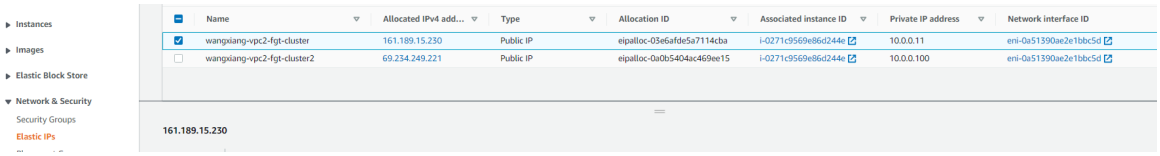


从外网 RDP 连接到 pc1，从 pc1 ping 114。

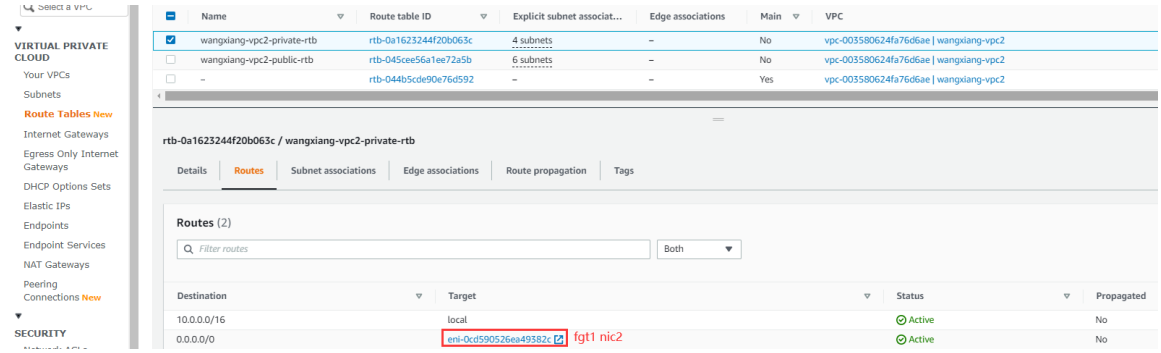


HA 切换前，FGT 是主，FGT2 是备：

业务口的弹性 IP 关联到 FGT1 NIC1 网卡，即 port1。

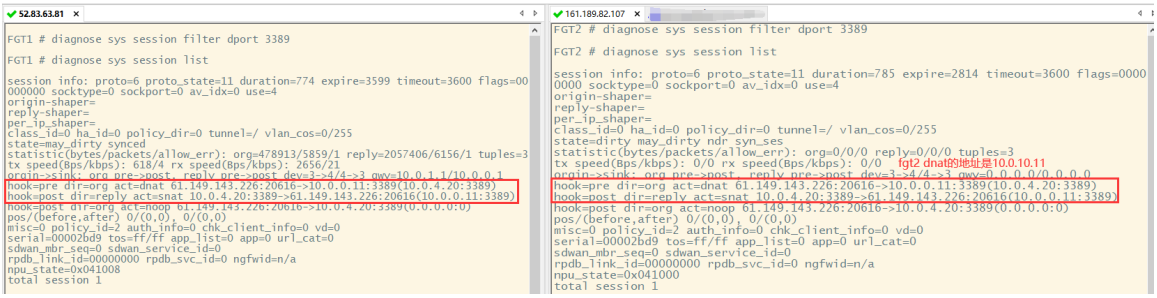


Private 路由表默认路由指向 FGT1 NIC2 网卡，即 port2

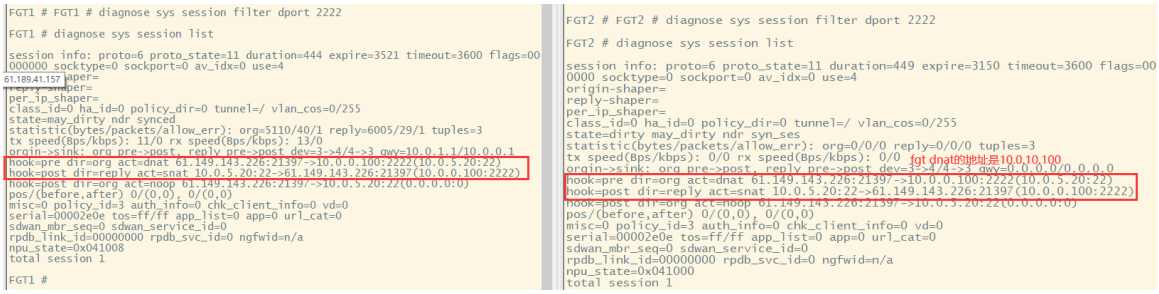


FGT1 的 SNAT 和 DNAT 会话同步到 FGT2，但是 FGT2 是利用不了的：

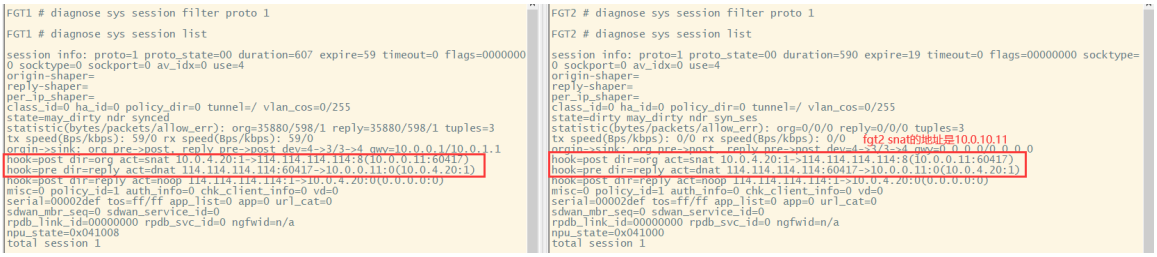
RDP 会话：



SSH 会话：



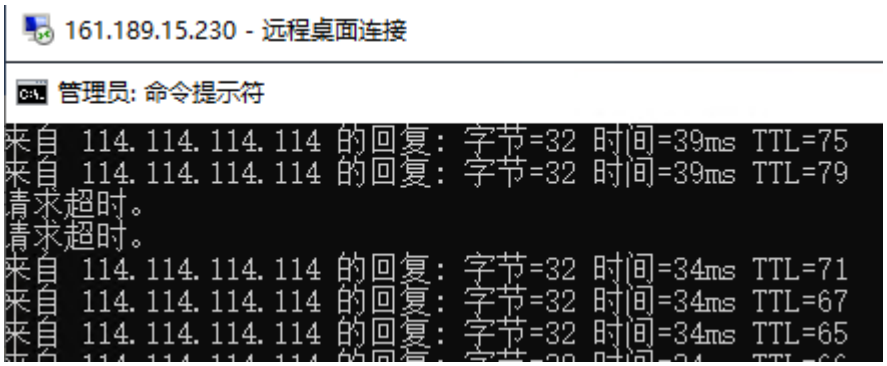
Ping 会话：



重启 FGT2，HA 切换后，FGT2 是主，FGT1 是备：

原有 RDP 和 SSH 连接断开，重新连接后正常。

Ping 丢 2 个包。



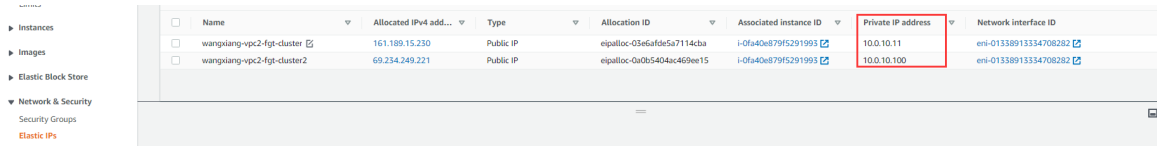
从 FGT2 debug 可以看出，除了 FGT 本身的 HA 切换以外，还需要移动弹性 ip 到 FGT2 实例，更新 AWS private 路由表的默认路由指向 FGT2 NIC2。

```
FGT2 # diagnose debug  application awsd  -1
Debug messages will be on for 30 minutes.

FGT2 # diagnose debug enable

FGT2 # HA event
HA state: primary
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port2 ip 10.0.11.11
send_vip_arp: vd root primary 1 intf fortilink ip 169.254.1.1
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.100
awsd get instance id i-0fa40e879f5291993
awsd get iam role FGT-HA-Failover
awsd get region cn-northwest-1
awsd get vpc id vpc-003580624fa76d6ae
awsd doing ha failover for vdom root
awsd associate elastic ip for port1
awsd associate elastic ip allocation eipalloc-03e6afde5a7114cba to 10.0.10.11 of eni eni-01338913334708282
awsd associate elastic ip successfully
awsd associate elastic ip allocation eipalloc-0a0b5404ac469ee15 to 10.0.10.100 of eni eni-01338913334708282
awsd associate elastic ip successfully
awsd associate elastic ip for port2
awsd update route table rtb-0a1623244f20b063c, replace route of dst 0.0.0.0/0 to eni-083fe1ed3da12d9b9
awsd update route successfully
HA event
HA state: primary
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port2 ip 10.0.11.11
send_vip_arp: vd root primary 1 intf fortilink ip 169.254.1.1
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.100
awsd get instance id i-0fa40e879f5291993
awsd get iam role FGT-HA-Failover
awsd get region cn-northwest-1
awsd get vpc id vpc-003580624fa76d6ae
awsd doing ha failover for vdom root
awsd associate elastic ip for port1
awsd associate elastic ip for port2
```

弹性 IP 重新在 FGT2 实例绑定。



Private 路由表默认路由指向 FGT2 NIC2。