AWS 部署 FortiGate

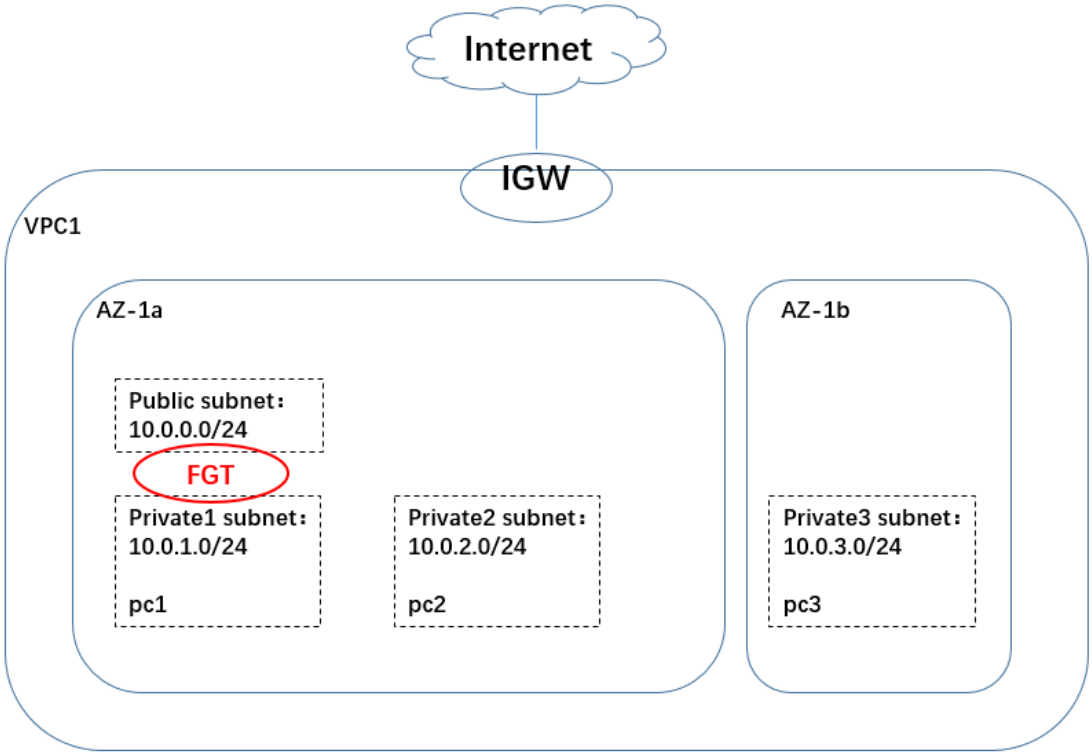
版本	V1.0
时间	2021 年 9 月
作者	王祥
状态	
反馈	support_cn@fortinet.com

目录

1. 介绍

本文档介绍如何在 AWS 上安装和配置单实例 FortiGate-VM，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

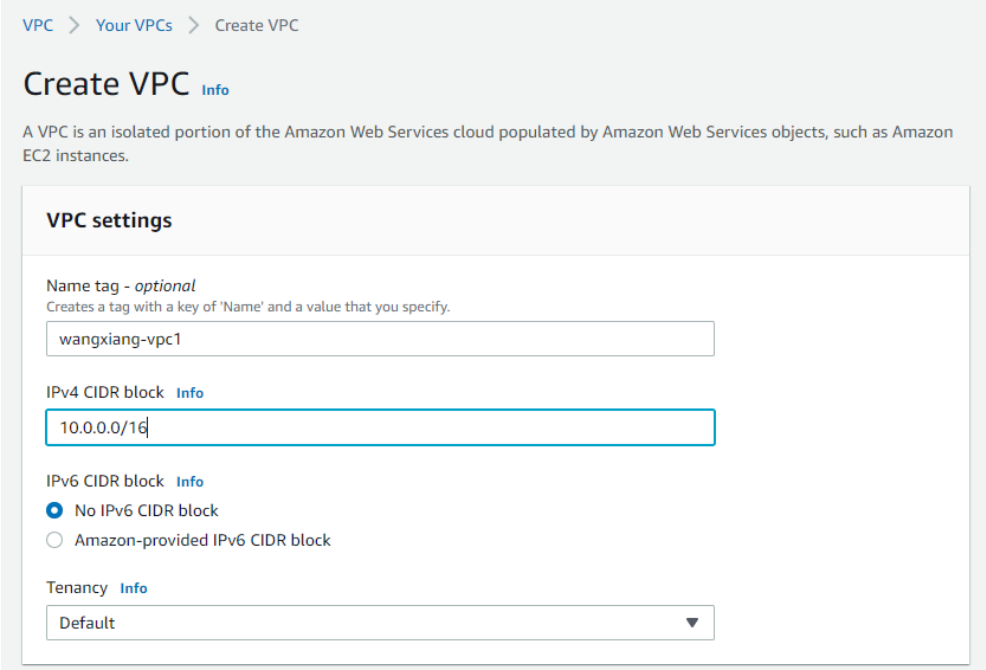


3. 配置步骤

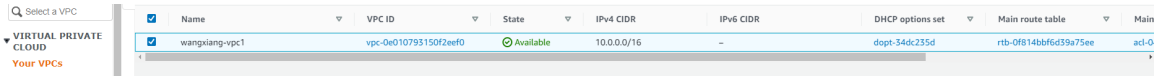
3.1. 创建 VPC 和子网

VPC，即一个虚拟子网。

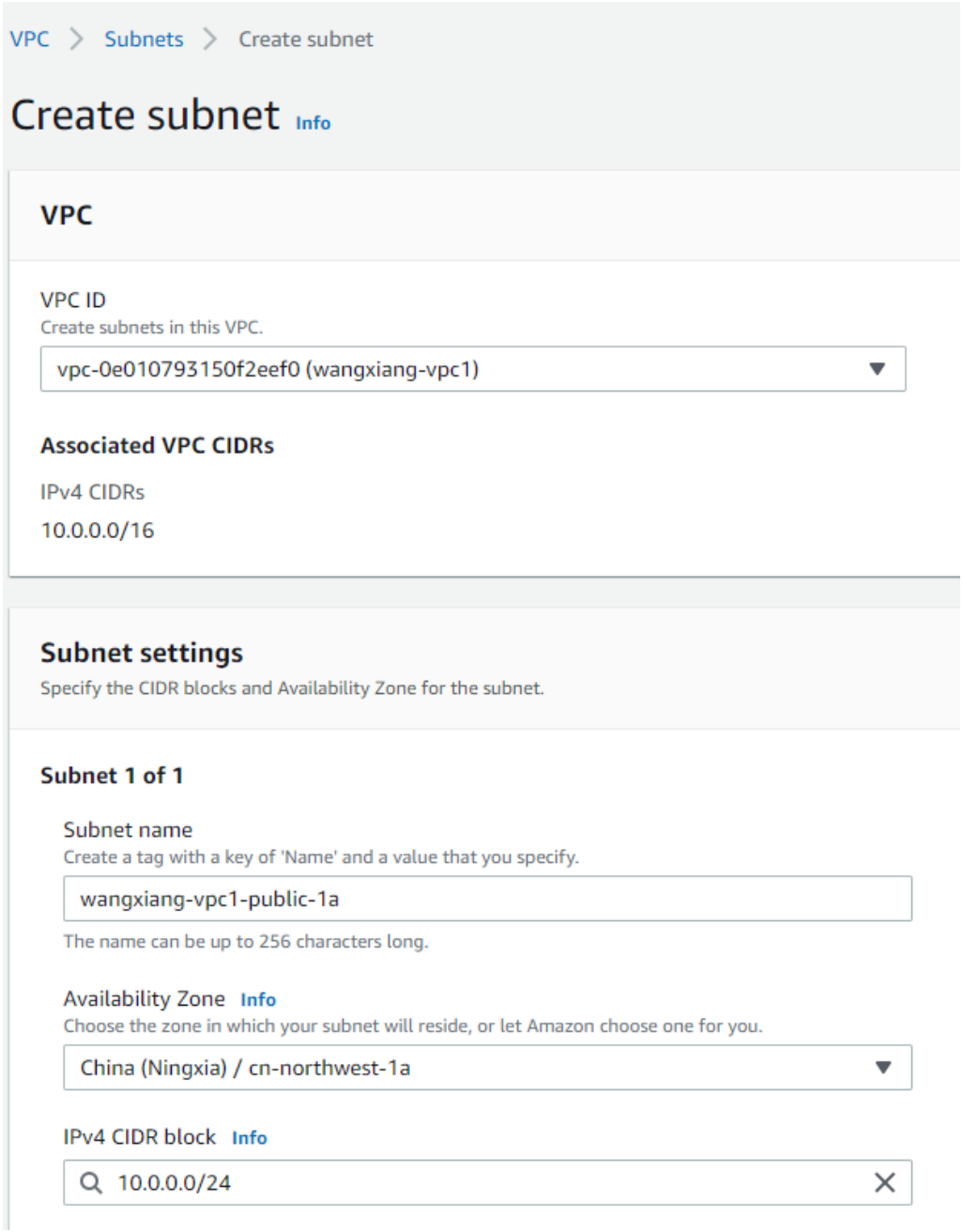
选择 Services→ VIRTUAL PRIVATE CLOUD→Your VPCs，点击 Create VPC。



创建完成。

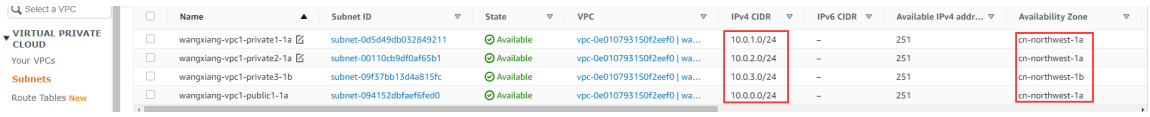


选择 Services→ VIRTUAL PRIVATE CLOUD→ Subnets，点击 Create Subnet。



同理，创建其他三个 private 子网。

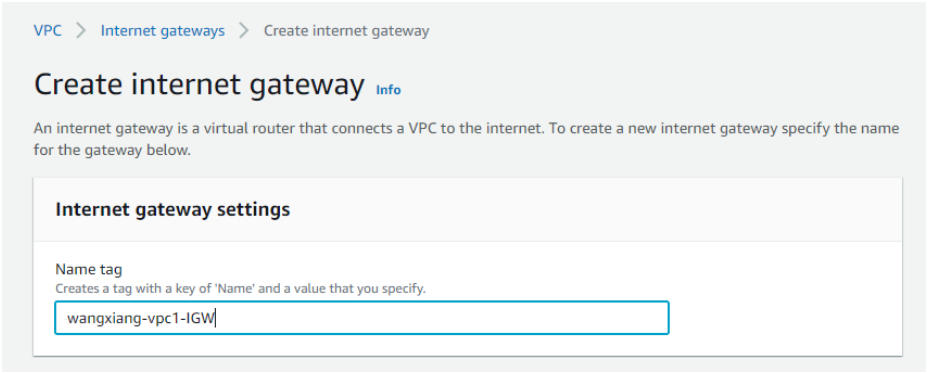
创建完成。



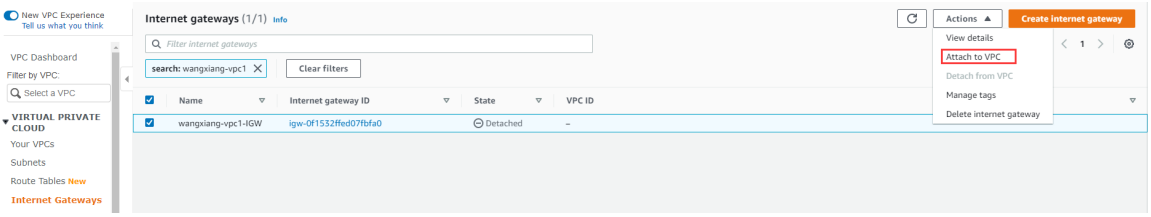
3.2. 创建 IGW

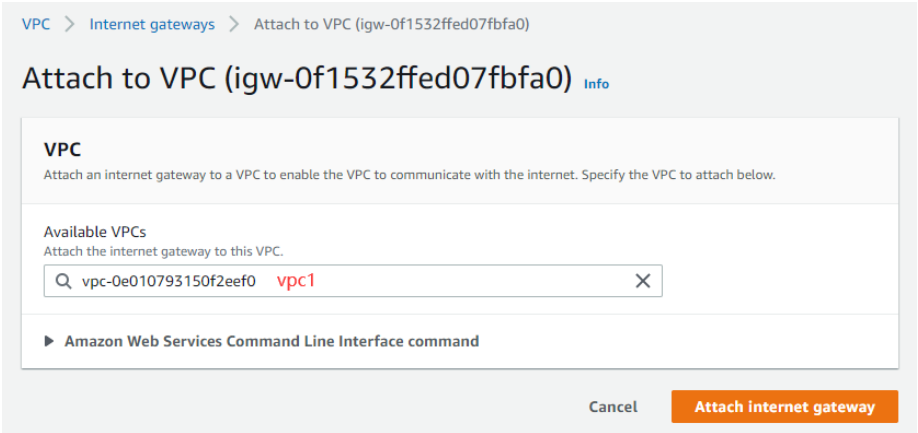
VPC 中的子网通过 IGW 才能访问 Internet。

选择 Services→ VIRTUAL PRIVATE CLOUD→ Internet gateways，点击 Create Internet gateways。

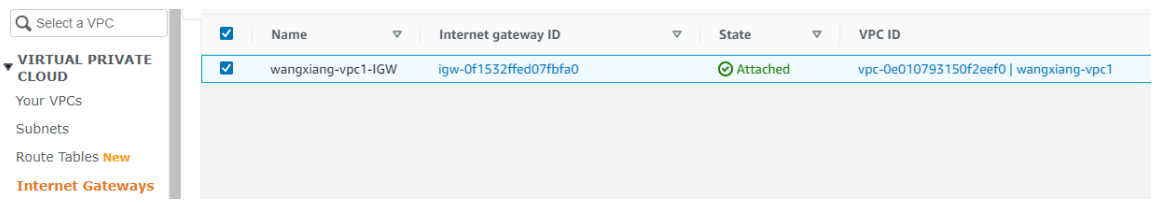


关联刚创建的 VPC1。





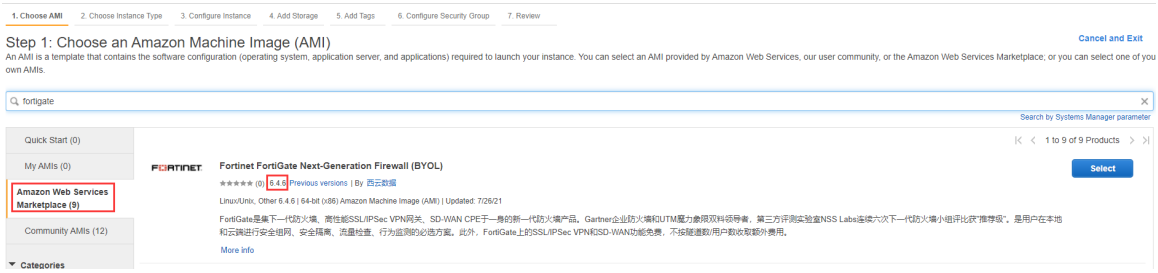
创建完成。



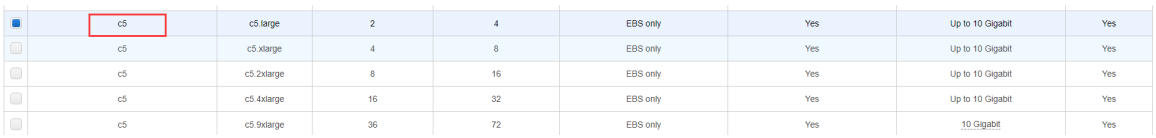
3.3. 部署 FortiGate

选择 Services→EC2→Instances，点击 Create Instance。

这里选择 FortiGate v6.4.6 的版本。

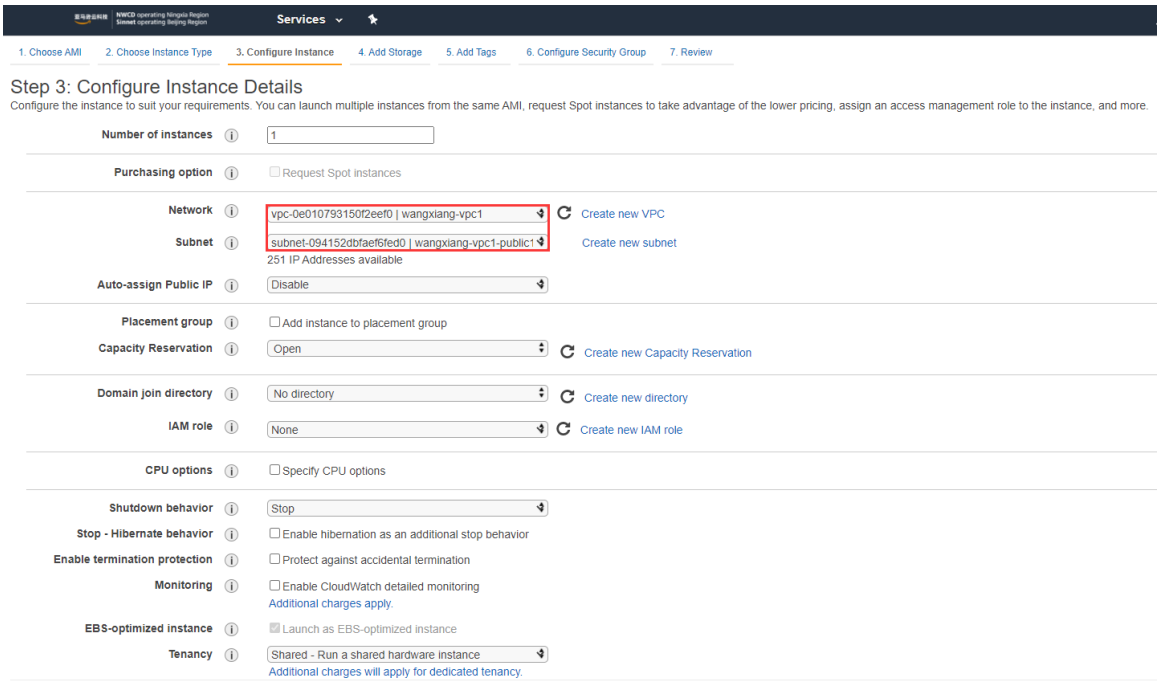


实例类型请选择**计算优化型**，这里使用 c5.xlarge。

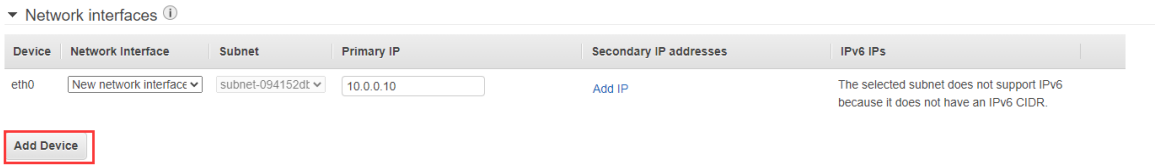


☑	c5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.4xlarge	16	32	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.9xlarge	36	72	EBS only	Yes	10 Gigabit	Yes

实例配置，选择 VPC1 和子网 public1-1a。



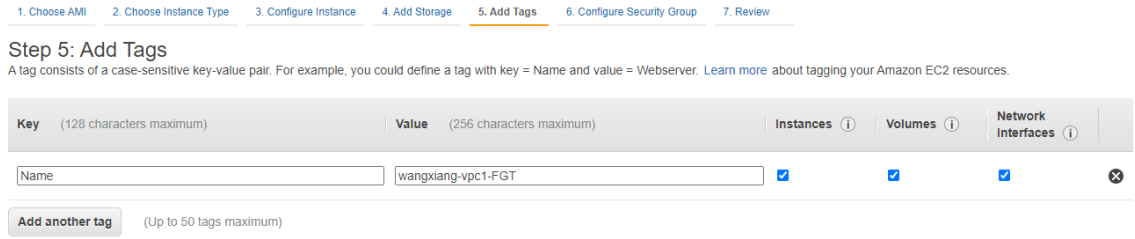
默认实例只有一块网卡 eth0，对应 FortiGate port1 接口，eth0 会自动分配地址，也可以手动指定，这里指定 10.0.0.10。



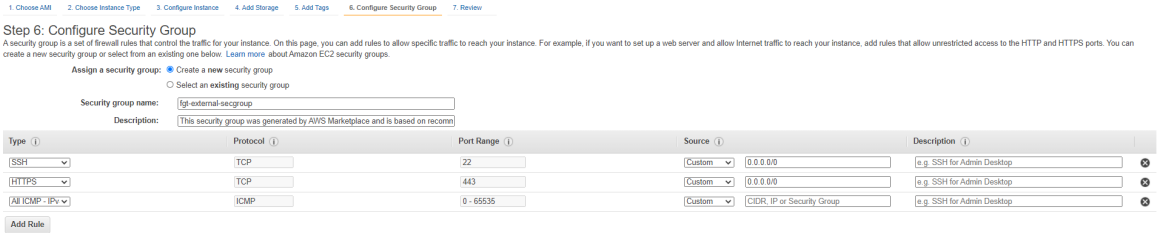
也可以通过 Add Device 再添加一块网卡 eth1，对应 FortiGate port2 接口。

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

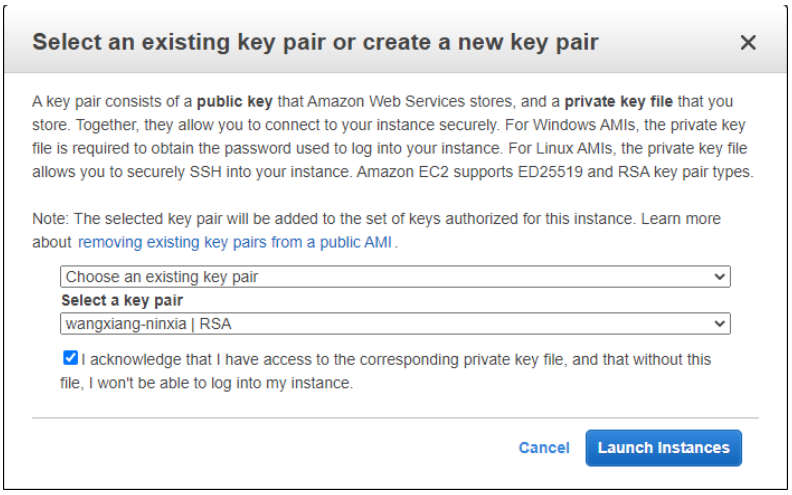
添加标签用于标识一个实例。



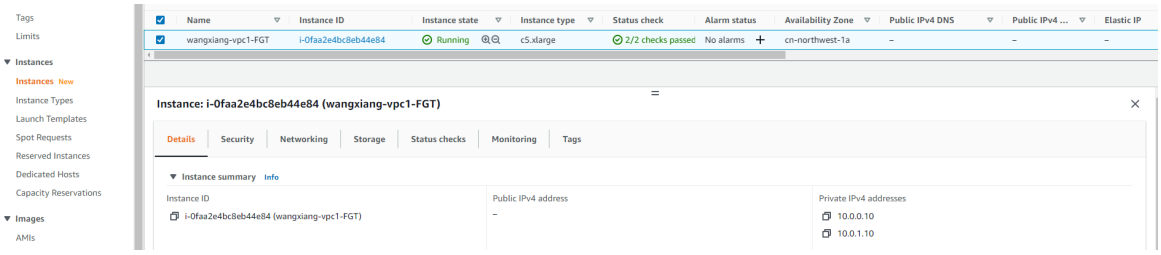
创建安全组 fgt-external-secgroup，对于管理 FortiGate 需要放行 22、443 端口及 ICMP，其他端口根据业务需求放行。



创建 key，或者选择自己已经存在的 key，并启动实例。

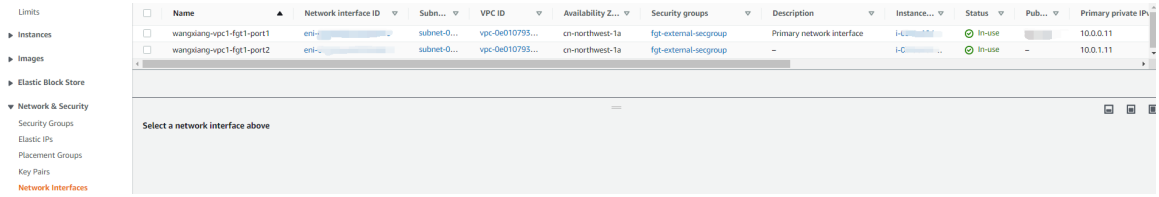


创建完成，实例 ID 是 i-0faa2e4bc8eb44e84。



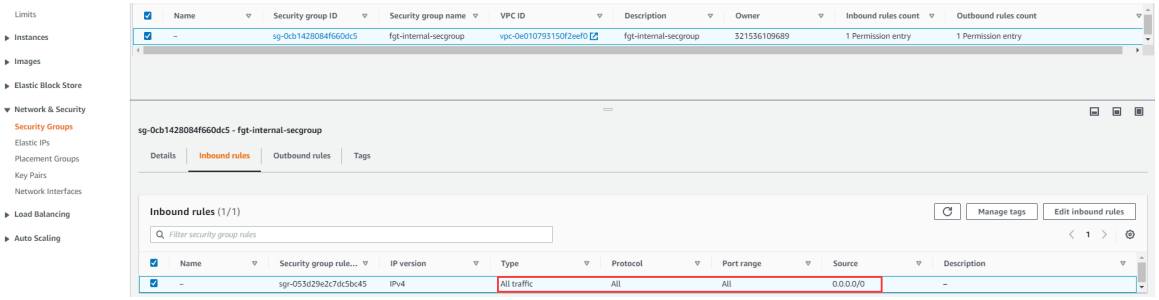
3. 4. 安全组

点击网络接口可以，可以查看到实例创建的两个接口。输入 Name 的名称，便于管理。FortiGate 实例的两个接口的安全组都是刚新建的 fgt-external-secgroup。

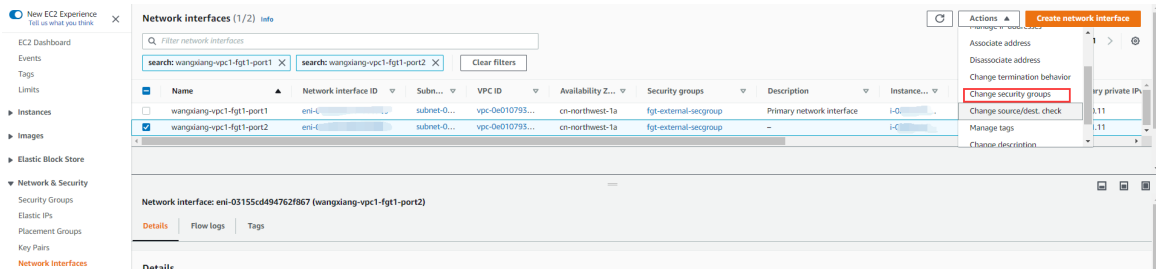


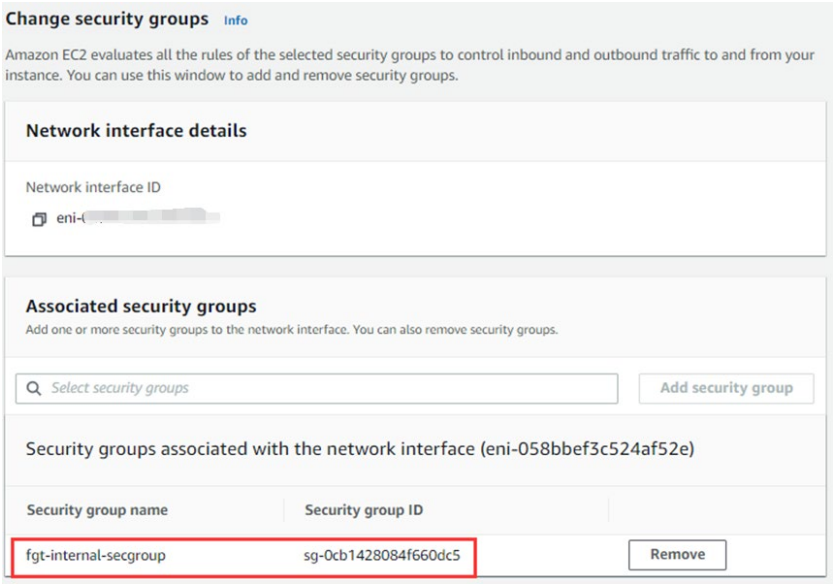
AWS 安全组是基于接口的，对于 FortiGate port2 而言，port2 对应的是由内向外的数据，因此 port2 的安全组要全放通。

新建安全组 fgt-internal-secgroup。

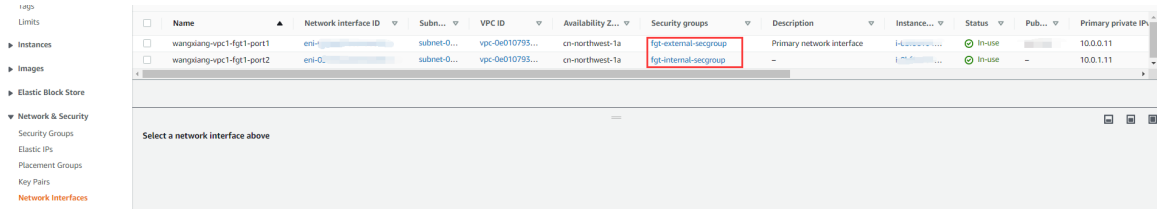


修改 port2 接口的安全组。





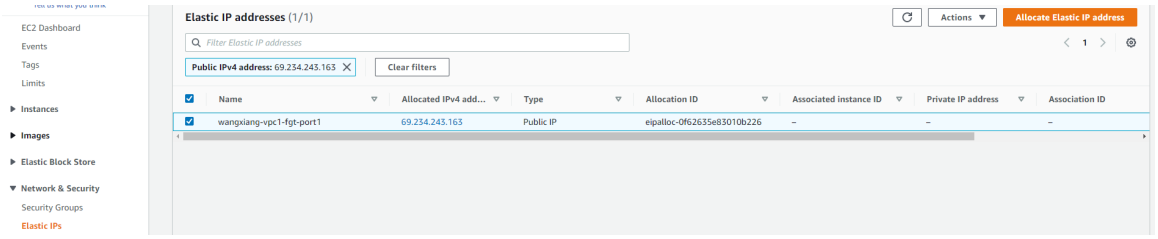
修改完成。



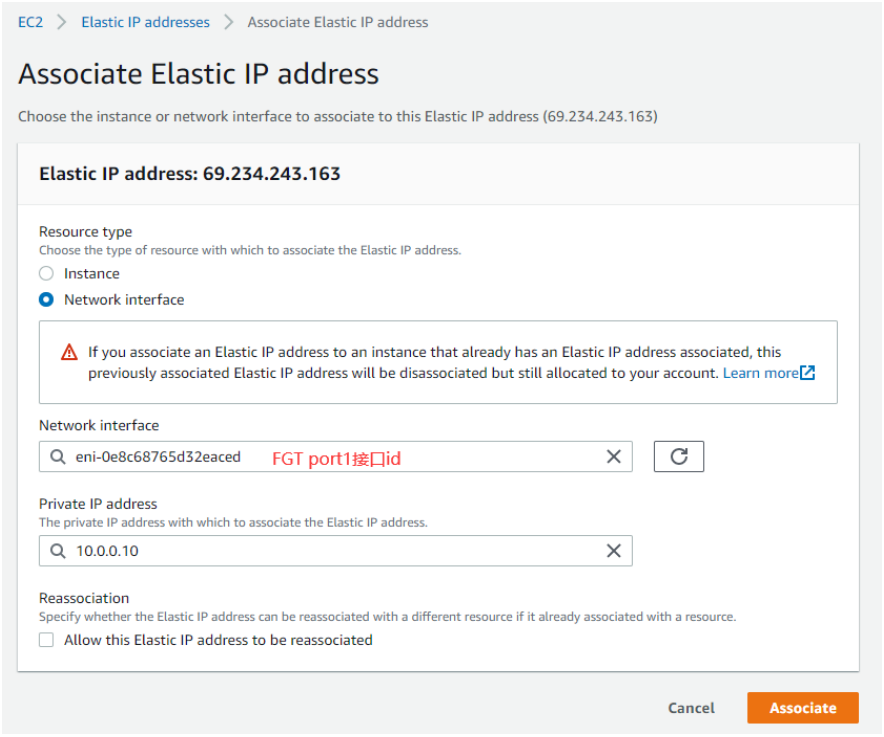
备注：FortiGate 本身就有防火墙策略对流量进行控制，如果嫌安全组控制太麻烦，可以将 FortiGate 的所有端口都应用**允许所有**的安全组。

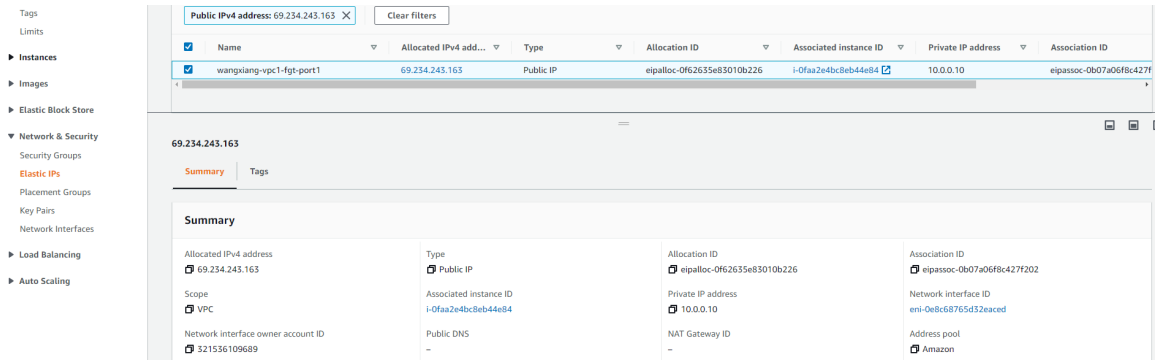
3.5. 弹性 IP

选择 Services→ Network & Security→ Elastic IPs，点击 Allocate Elastic IP address。



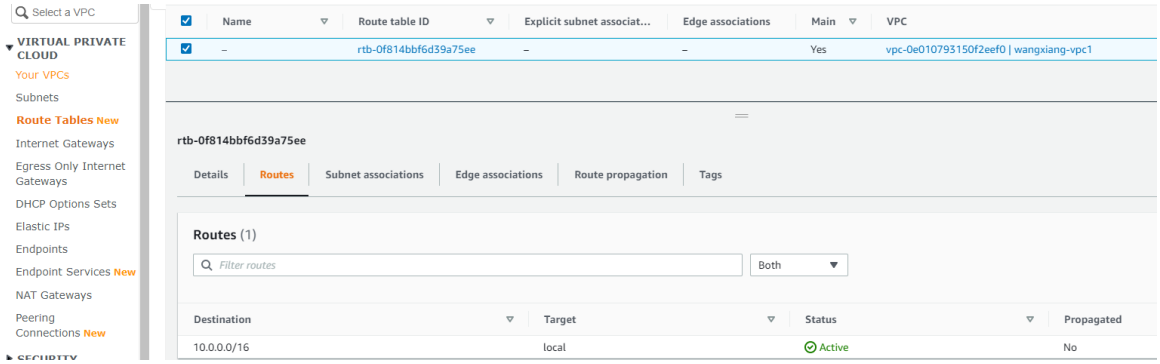
关联弹性 IP 到 FortiGate port1 接口，即 FortiGate 连接 Internet 的公网地址就是该 IP，选中该弹性 IP，点击 Action→Associate Elastic IP address。





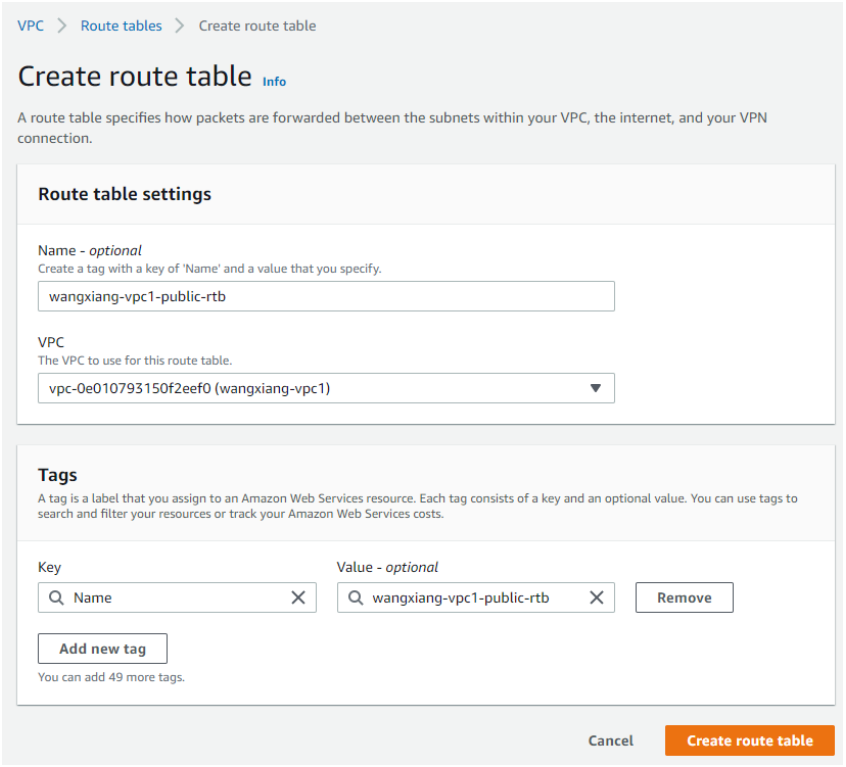
3.6. AWS 路由表

创建 VPC 后，默认会为该 VPC 创建一张主路由表，默认关联了该 VPC 的所有子网。

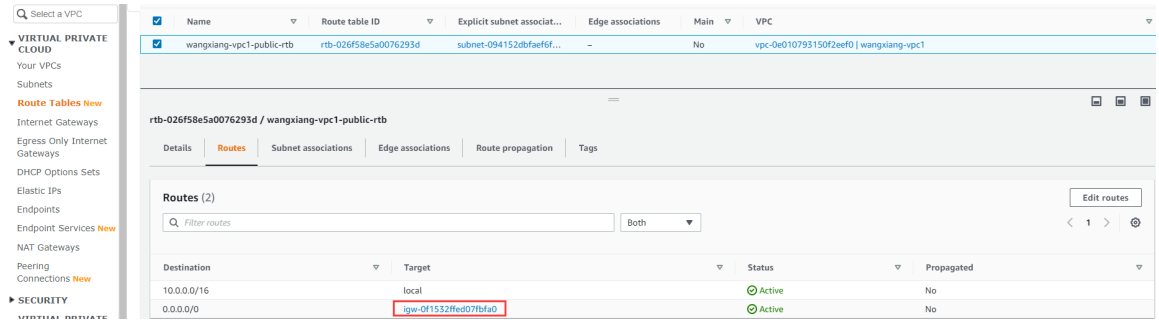


这里创建 public 路由表和 private 路由表用于 AWS 网络的路由。

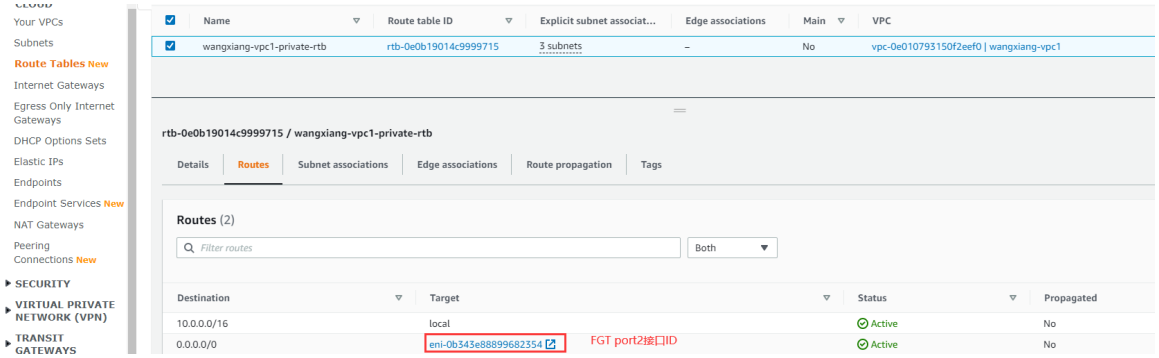
选择 Services→ VIRTUAL PRIVATE CLOUD→ Route tables，点击 Create Route table。

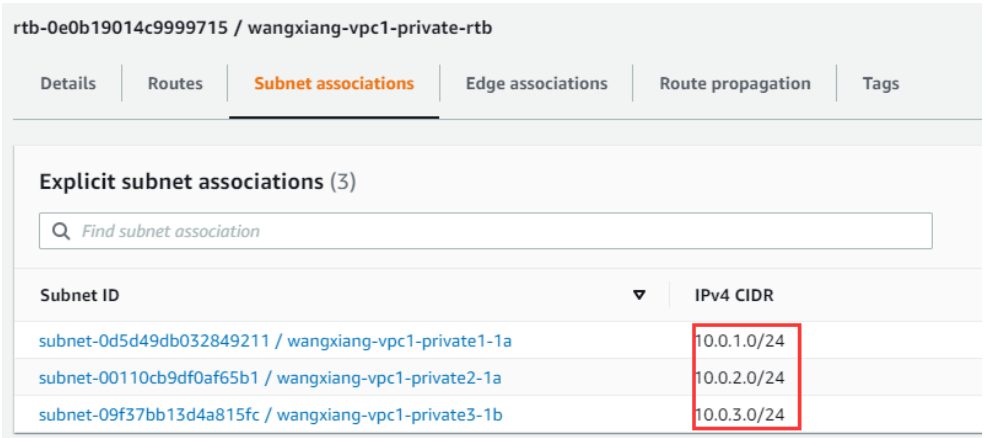


创建 public 路由表关联 public 子网，默认路由指向 IGW：



创建 private 路由表关联 private 子网，默认路由指向 FortiGate port2 接口：

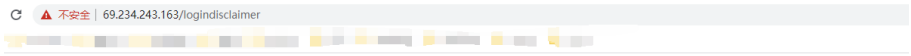


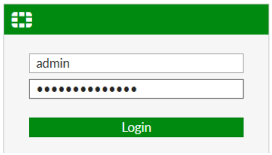


3.7. 访问 FortiGate

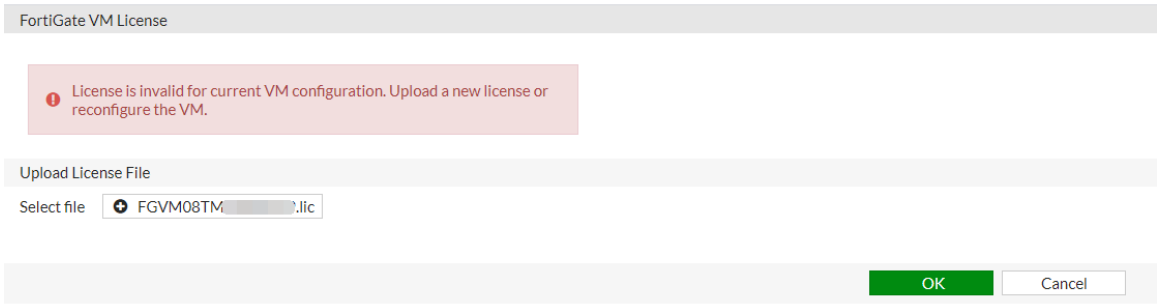
Https 访问 FortiGate：

使用 https://69.234.243.163（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。

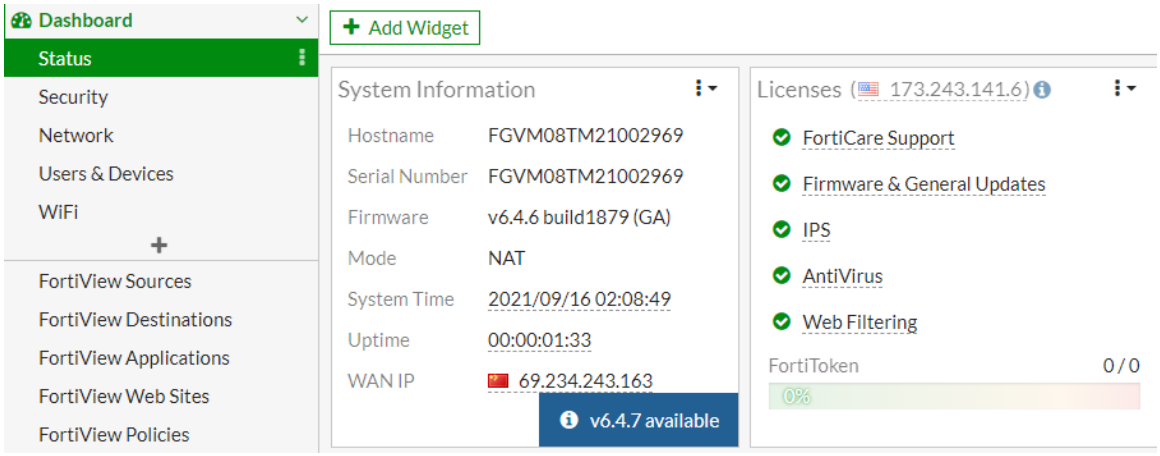




登录后，请先上传购买好的 license，导入 license 会重启 FortiGate。

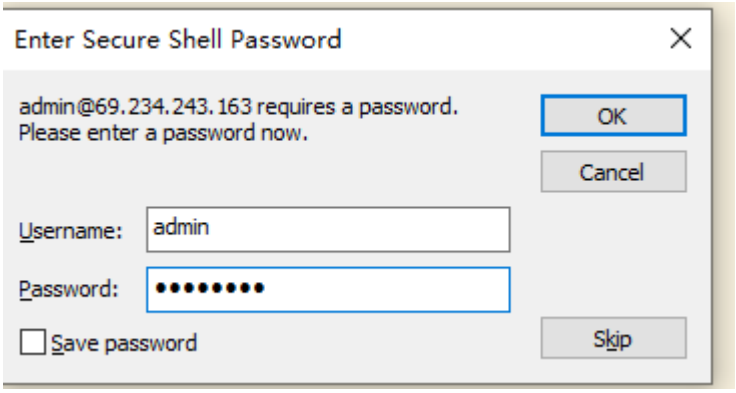


FortiGate 登录成功。

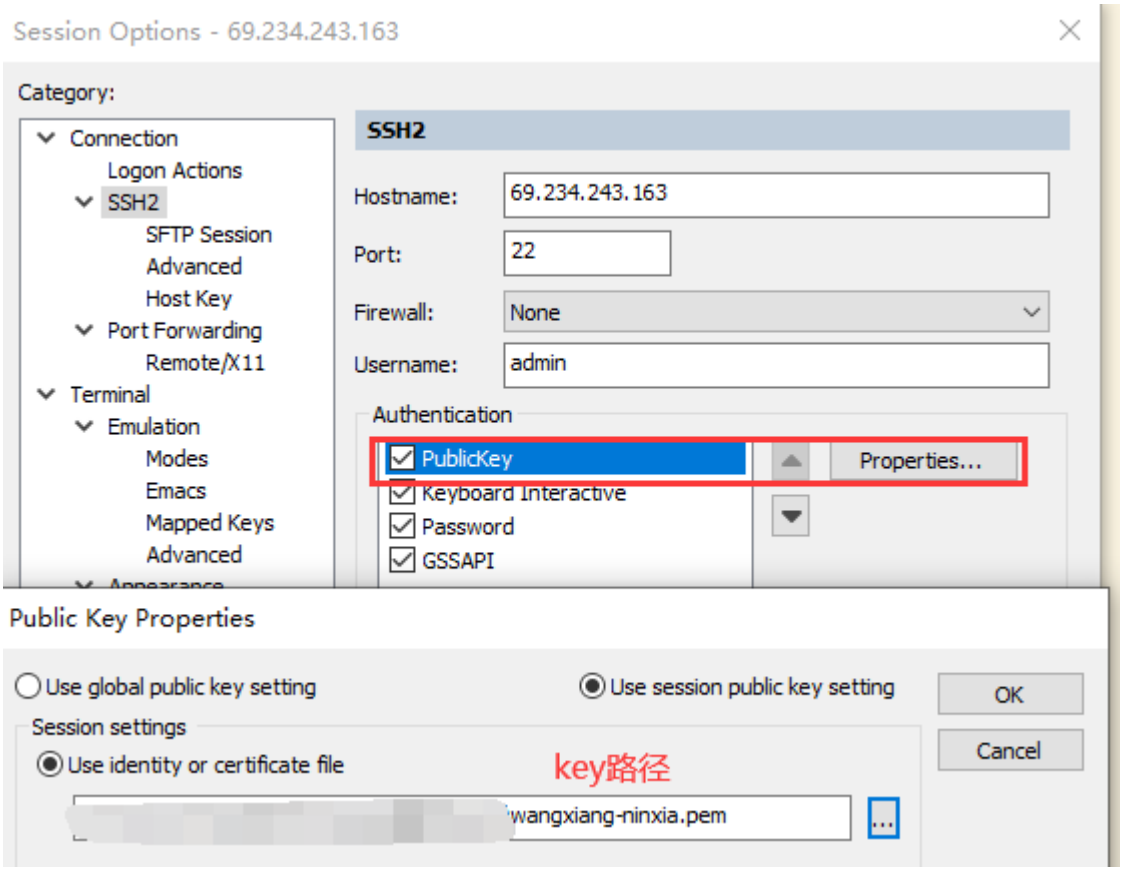


SSH 访问 FortiGate 有两种方式，一下是 CRT 软件的访问截图：

一种是通过账号密码的方式：

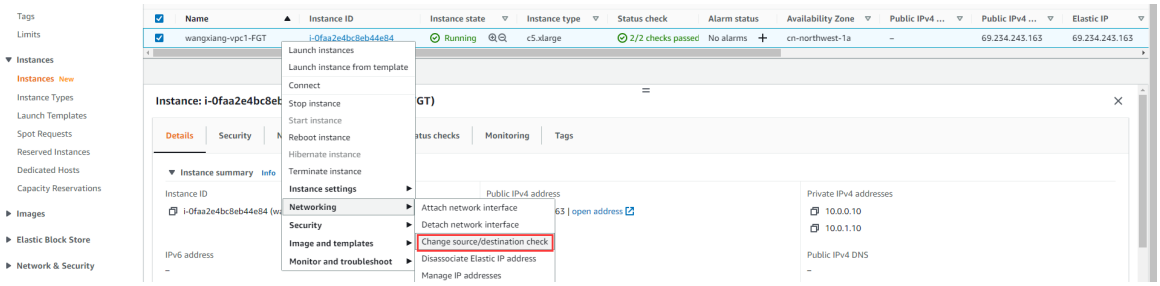


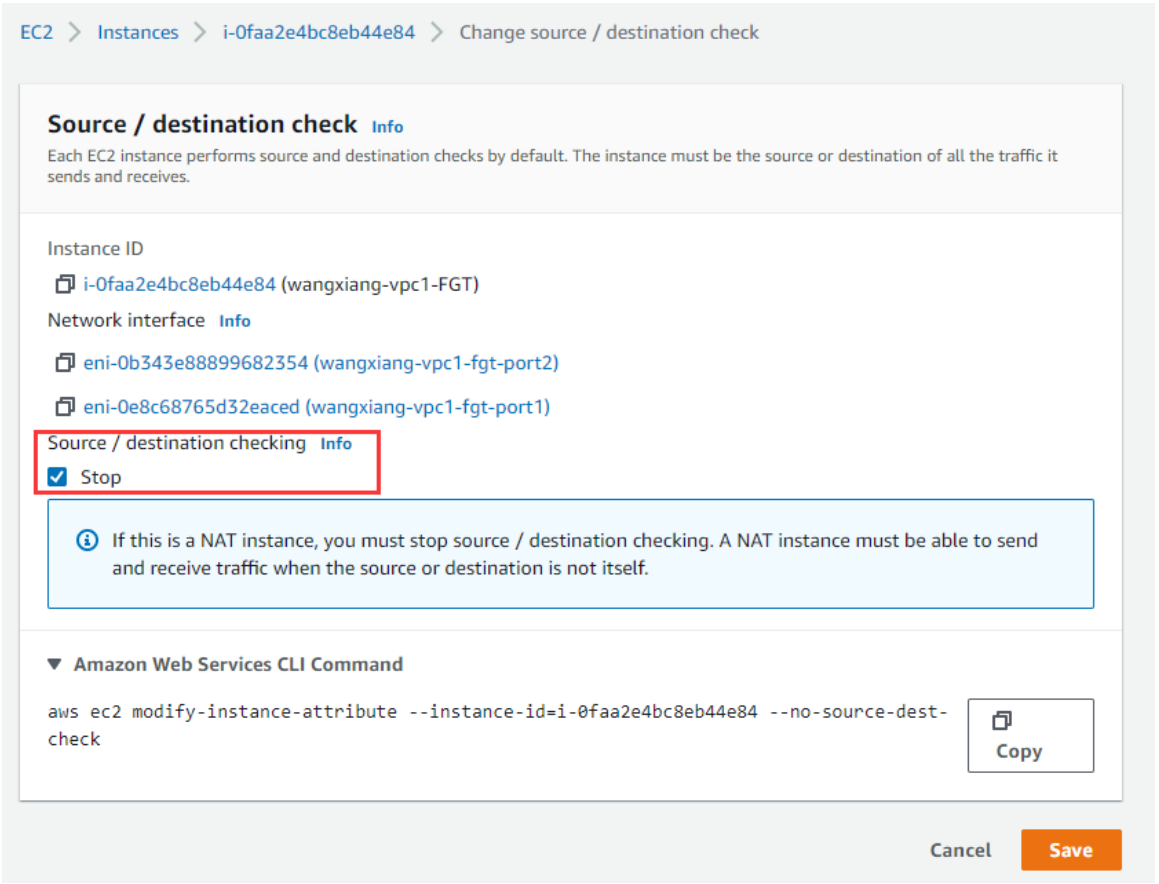
一种是通过 key 的方式：



3.8. 禁用源/目标检查

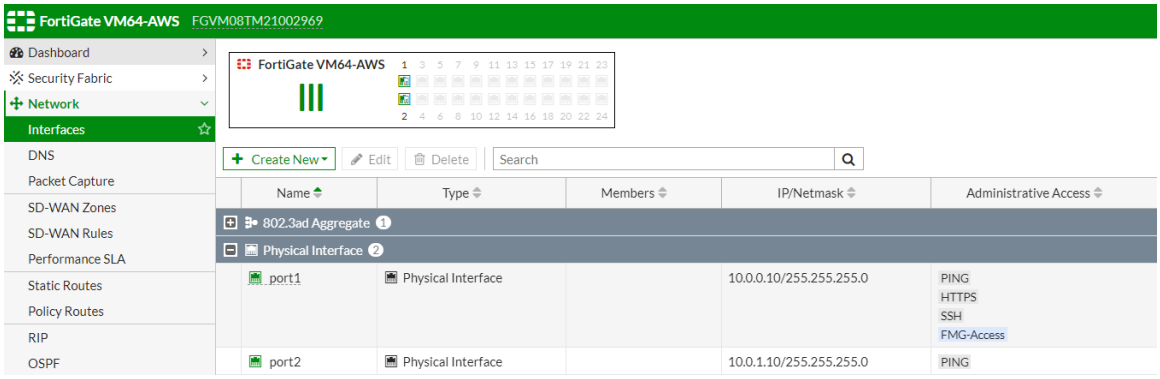
每个 EC2 实例都会默认执行源/目标检查。这意味着实例必须为其发送或接收的数据流的源头或目标。 但是，NAT 实例必须能够在源或目标并非其本身时发送和接收数据流。因此，FortiGate 实例必须禁用源/目标检查。





3.9. FortiGate 配置源 NAT

FortiGate 默认会 DHCP 获取 AWS 分配的地址及路由表如下：

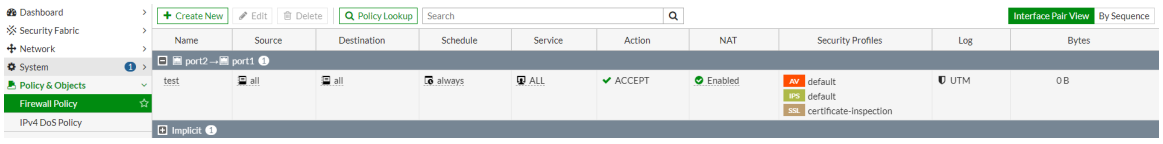



```
FGVM08TM21002969 # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 10.0.0.1, port1
C       10.0.0.0/24 is directly connected, port1
C       10.0.1.0/24 is directly connected, port2
```

配置 10.0.0.0/16 的内部路由指向 10.0.1.1。AWS 虚拟路由的器的地址为每个子网的第一个地址，port2 接口的子网是 10.0.1.0/24，因此虚拟路由器的地址是 10.0.1.1。

配置防火墙策略。

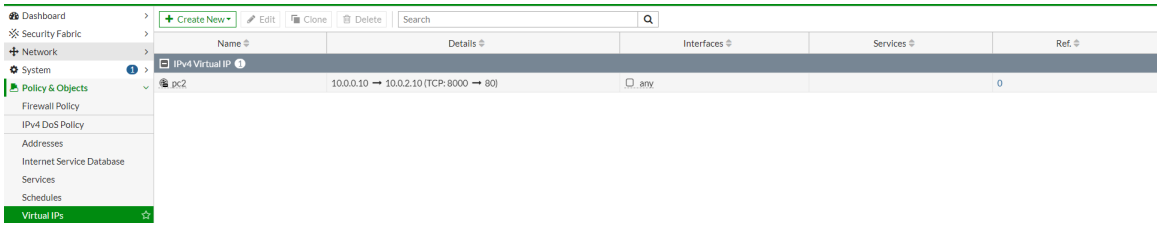


3.10. FortiGate 配置目的 NAT

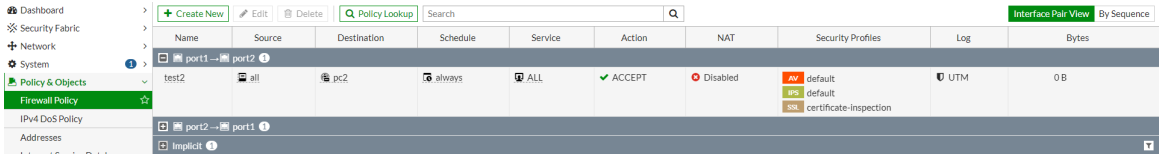
可以使用 port1 接口的地址做目的 NAT，也可以分配一个单独的 IP 来做目的 NAT。

用 port1 接口的地址做目的 NAT：

配置 VIP，external 地址是 10.0.0.10，internal 地址是 10.0.2.10：

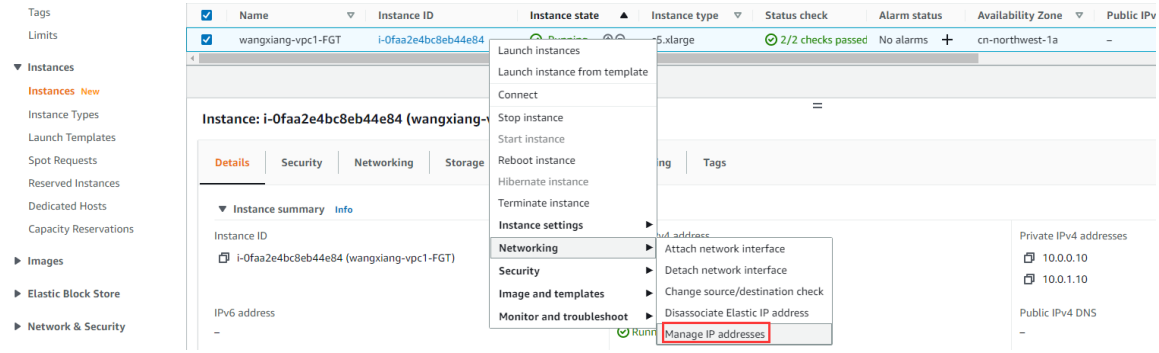


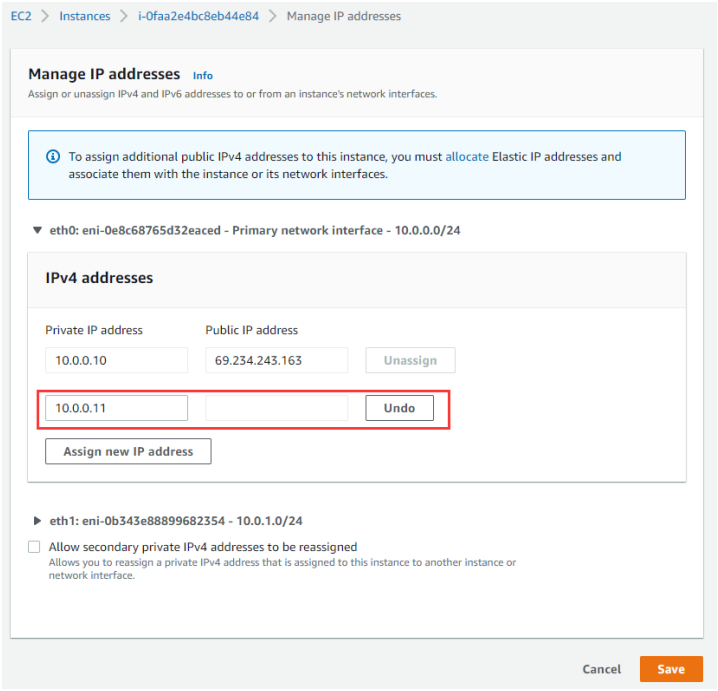
配置防火墙策略调用 VIP：



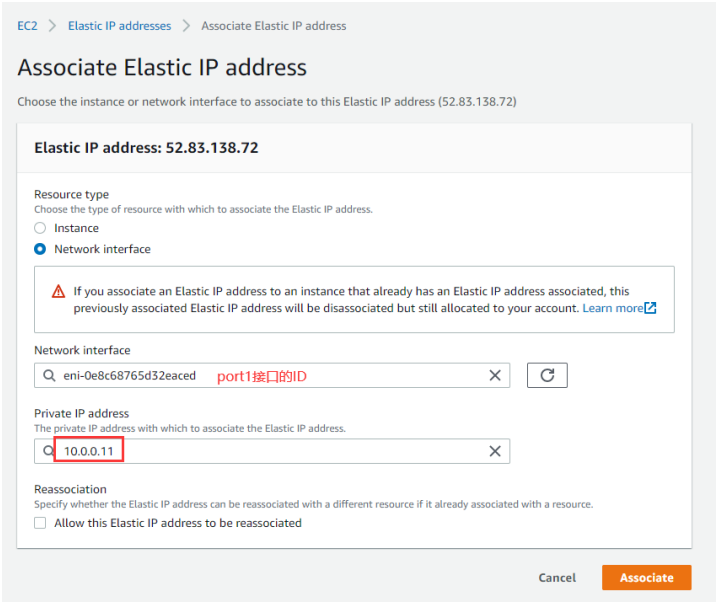
分配单独的 IP 来做目的 NAT：

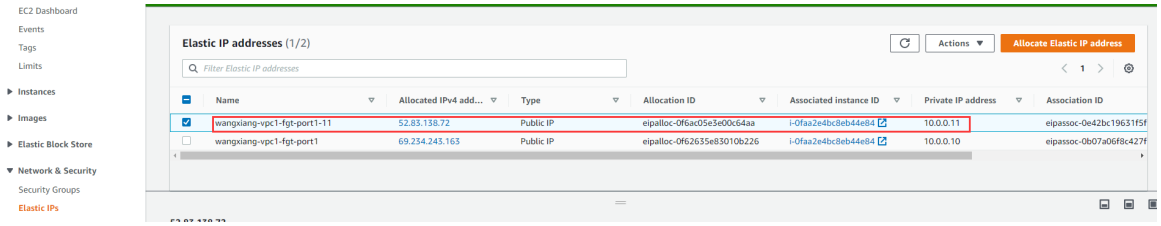
如下图，右击实例，选择 Networking→Manage IP addresses



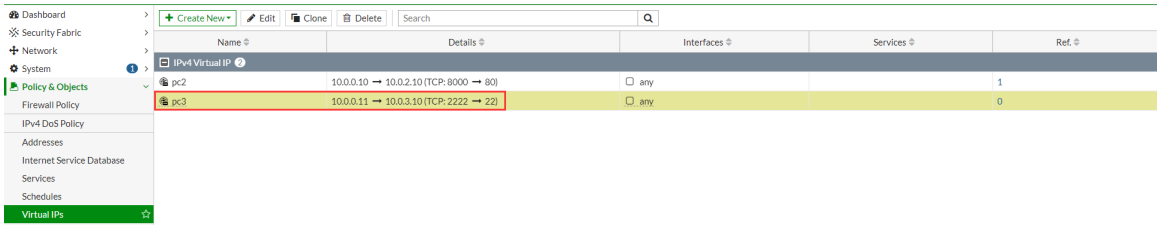


10.0.0.11 是没有关联弹性 IP 的，因此给此 IP 关联弹性 IP 才可以连接 Internet。分配弹性 IP 并关联 10.0.0.11。

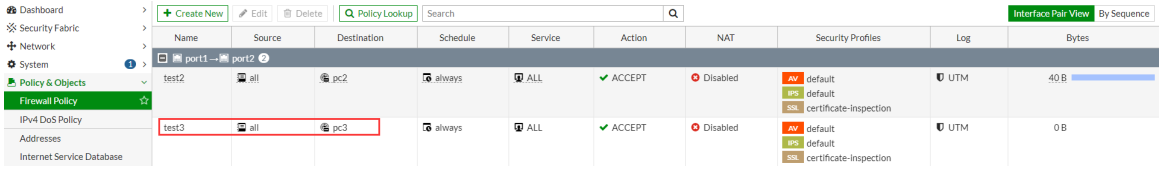




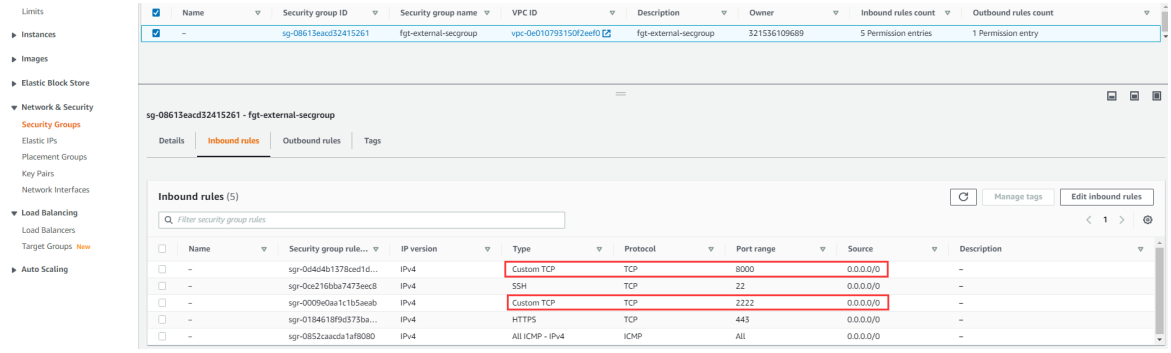
配置 VIP，external 地址是 10.0.0.11，internal 地址是 10.0.3.10：



配置防火墙策略：

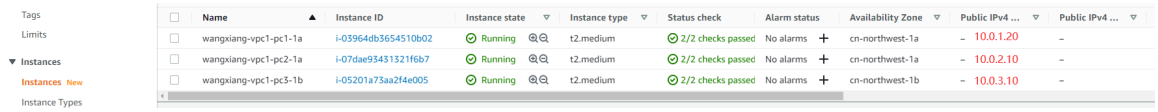


FGT 实例 NIC1，即 port1 安全组 fgt-external-secgroup 放通 8000 和 2222 这两个对外的端口。



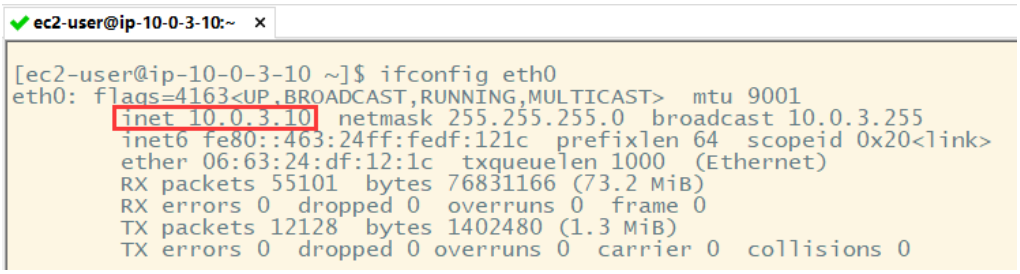
4. 业务测试

测试的 PC 如下



目的 NAT 测试：

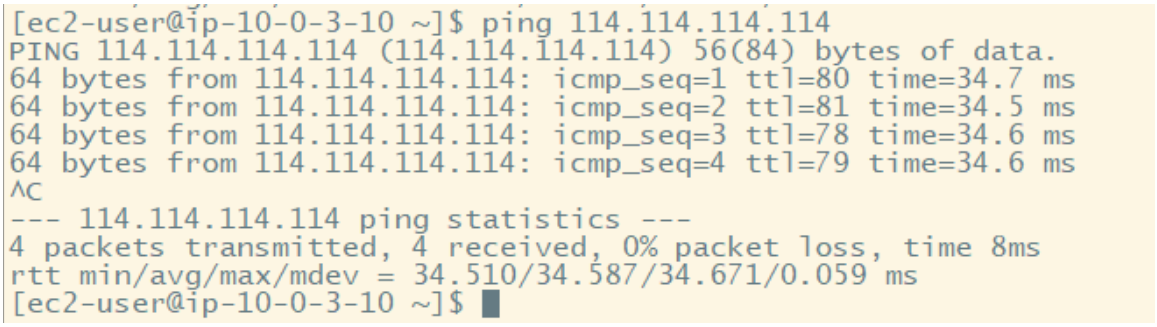
ssh 52.83.138.72 2222 访问正常。



http://69.234.243.163:8000 访问正常。

源 NAT 测试：

ping 114.114.114.114 正常



使用 10.0.3.10 作为跳板登录到 10.0.20.10，访问 baidu 正常。

sudo ssh -i "wangxiang-ninxia.pem" ec2-user@10.0.2.10

```
[ec2-user@ip-10-0-3-10 ~]$ sudo  ssh -i "wangxiang-ninxia.pem" ec2-user@10.0.2.10
Last login: Thu Sep 16 12:00:06 2021 from 10.0.3.10
[ec2-user@ip-10-0-2-10 ~]$ curl www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8
me=referrer><link rel=stylesheet type=text/css href=http://s1.bdstatic.com/r/www/cache/bdo
Occ> <div id=wrapper> <div id=head> <div class=head_wrapper> <div class=s_form> <div class
bd_logo1.png width=270 height=129> </div> <form id=form name=f action=//www.baidu.com/s c
me=ie value=utf-8> <input type=hidden name=f value=8> <input type=hidden name=rsv_bp value
alue=baidu><span class="bg s_ipt_wr"><input id=kw name=wd class=s_ipt value maxlength=255
ubmit id=su value=百度一下 class="bg s_btn"></span> </form> </div> </div> <div id=u1> <a h
://www.hao123.com name=tj_trhao123 class=mnav>hao123</a> <a href=http://map.baidu.com name
class=mnav>视频</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnav>贴吧</a> <no
;u=http%3A%2F%2Fwww.baidu.com%2f%3fbdorz_come%3d1 name=tj_login class=lb>登录</a> </noscr
?login&tpl=mn&u='+ encodeURIComponent(window.location.href+ (window.location.search === ""
</script> <a href=//www.baidu.com/more/ name=tj_briicon class=bri style="display: block;">
> <a href=http://home.baidu.com>关于百度</a> <a href=http://ir.baidu.com>About Baidu</a> <
/>使用百度前必读</a>  <a href=http://jianyi.baidu.com/ class=cp-feedback>意见反馈</a
iv> </div> </div> </body> </html>
```

同理 10.0.1.20 访问外网也正常。

```
[ec2-user@ip-10-0-3-10 ~]$ sudo  ssh -i "wangxiang-ninxia.pem" ec2-user@10.0.1.20
Last login: Thu Sep 16 12:26:10 2021 from 10.0.3.10
[ec2-user@ip-10-0-1-20 ~]$ curl www.hao123.com
<!DOCTYPE html><html><head><noscript><meta http-equiv="refresh" content="0; URL='/?__no
"_blank"><meta charset="utf-8"/><meta http-equiv=X-UA-Compatible content="IE=edge,chrom
dns-prefetch" href="//s1.hao123img.com" /><link rel="dns-prefetch" href="//s0.hao123img
refetch" href="//img1.hao123.com" /><meta name="keywords" content="上网导航,网址大全,网
活动"/><meta name="description"content="hao123是汇集全网优质网址及资源的中文上网导航。
上网，从hao123开始。"/><script>window.HAO=window.HAO||{};window.HAO.https = false;windo
></style><script>(function (win) {var HAO = win.HAO = win.HAO || {};HAO.domainMap = {"h
com","https:\/\/dgss1.bdstatic.com\/5eN1dDebRNRTm2_p8IuM_a":"http:\/\/s1.hao123img.com"
3img.com","https:\/\/dgss1.bdstatic.com\/5bVXsi_n_tVS5dKfpU_Y_D3":"http:\/\/sc1.hao123i
```