阿里云部署 **FortiGate**

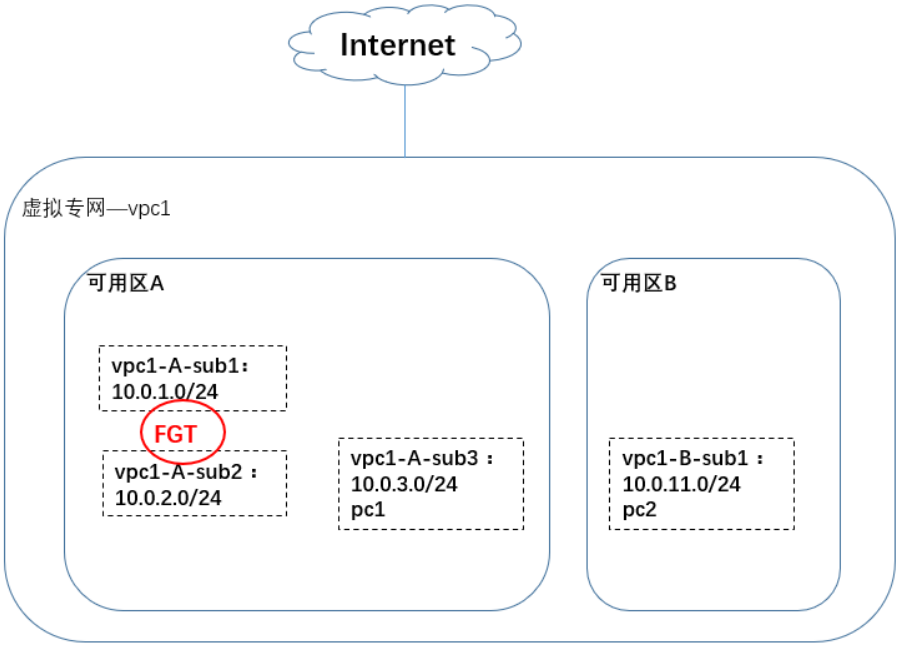
版本	V1.0
时间	2023 年 4 月
作者	王祥
状态	
反馈	support_cn@fortinet.com

目录

1. 介绍

本文档介绍如何在阿里云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，保护您在阿里云中的工作负载。

2. 网络拓扑



3. 地址规划

FGT 实例地址规划	
Port	地址
Port1	10.0.1.10
Port2	10.0.2.10
测试 PC	
pc1	10.0.3.228

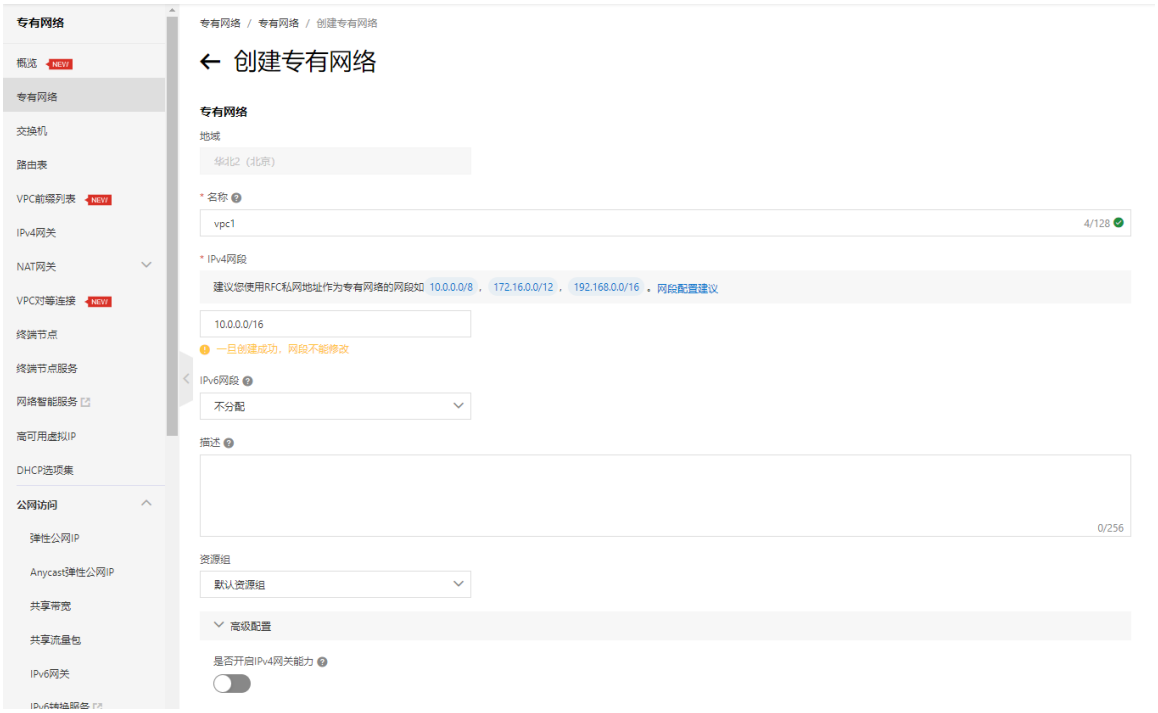
pc2	10.0.11.238

4. 配置步骤

4. 1. 创建专有网络和交换机

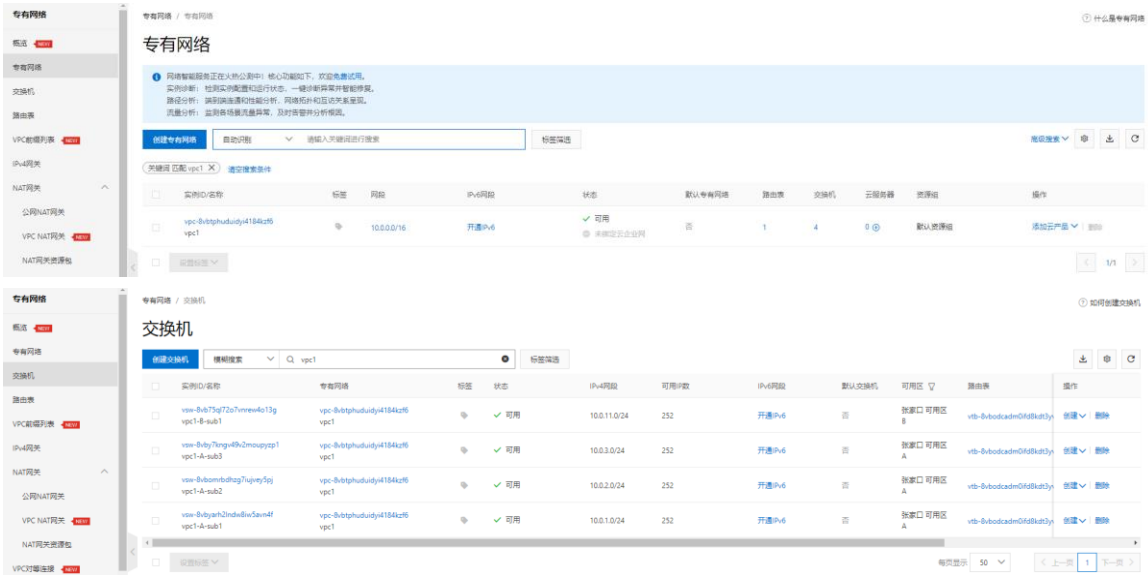
专有网络，即一个虚拟网络，交换机，即虚拟网络下的子网。

选择“专有网络”→“专有网络”，点击“创建专有网络”。



在当前页面下创建交换机，也可以“专有网络”→“交换机”下单独创建。

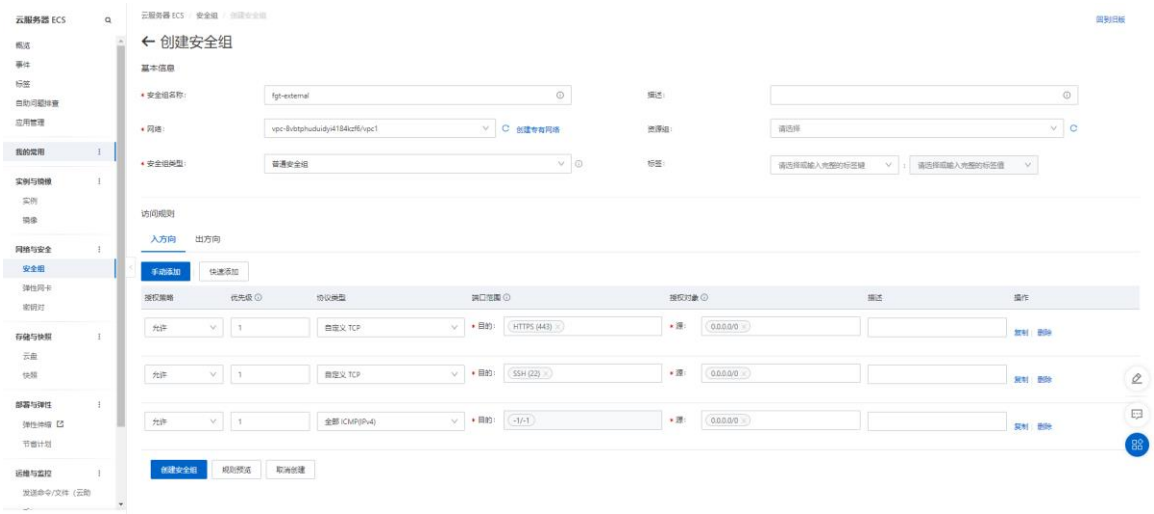
创建完成。



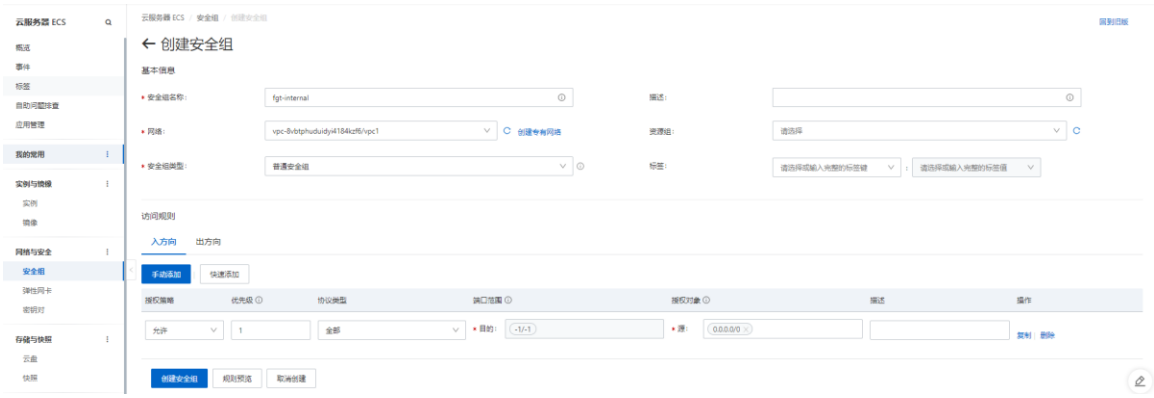
4. 2. 创建安全组

安全组是基于接口的，FortiGate port1 是外网接口，对应的是由外向内的数据，可以根据需求开放所需的端口；FortiGate port2 对应的是由内向外的数据，因此 port2 的安全组要全放通。

选择“云服务器 ECS”→“网络与安全”→“安全组”，新建安全组 fgt-external，用于 port1。这里先放通管理所需的端口 HTTPS，SSH 和 ICMP。



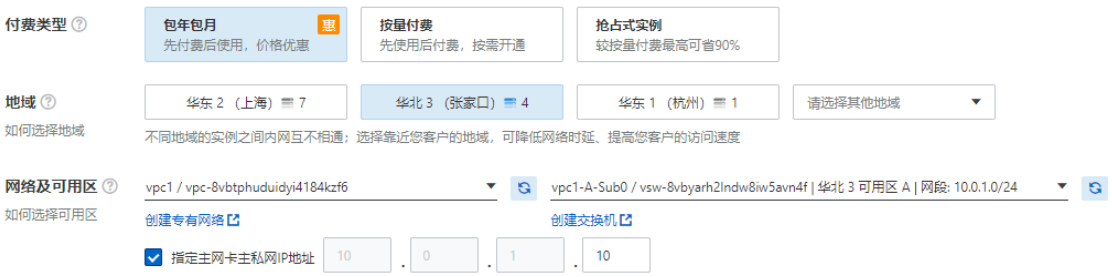
再新建安全组 fgt-internal，用于 port2，放通所有。



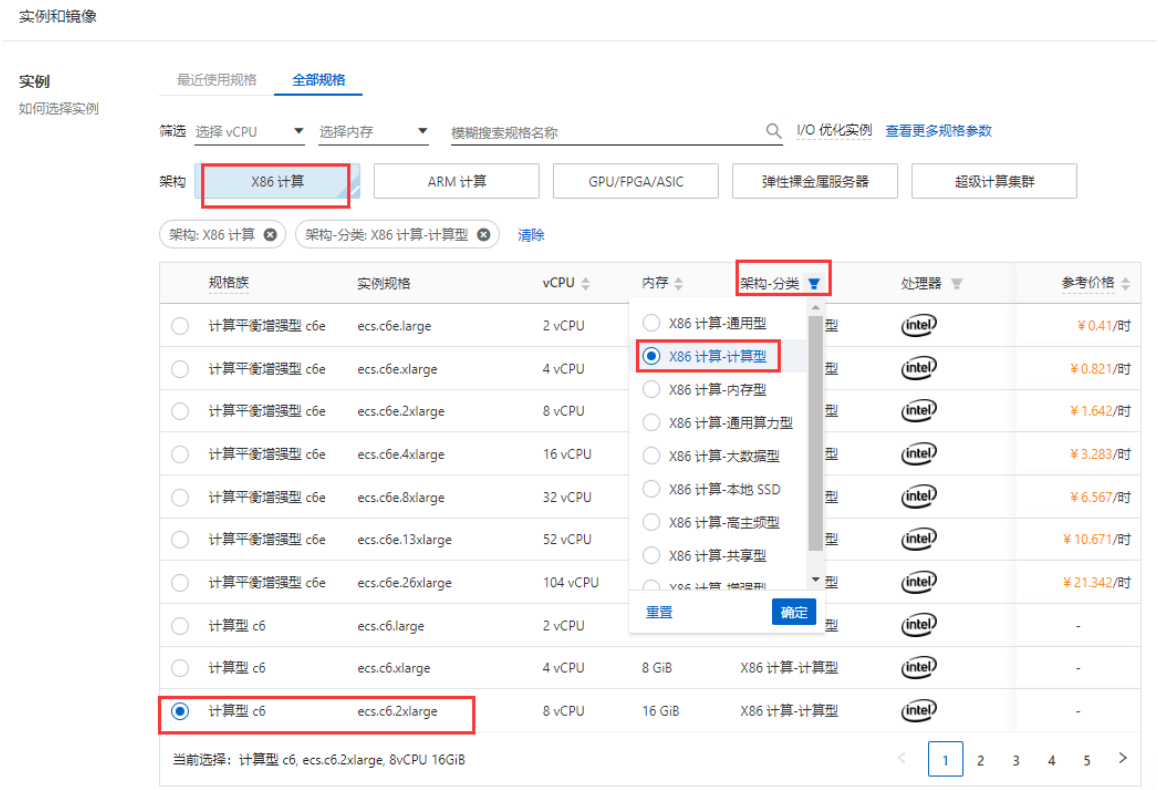
4.3. 部署 FortiGate

选择“云服务器 ECS”→“实例与镜像”→“实例”，点击“创建实例”。

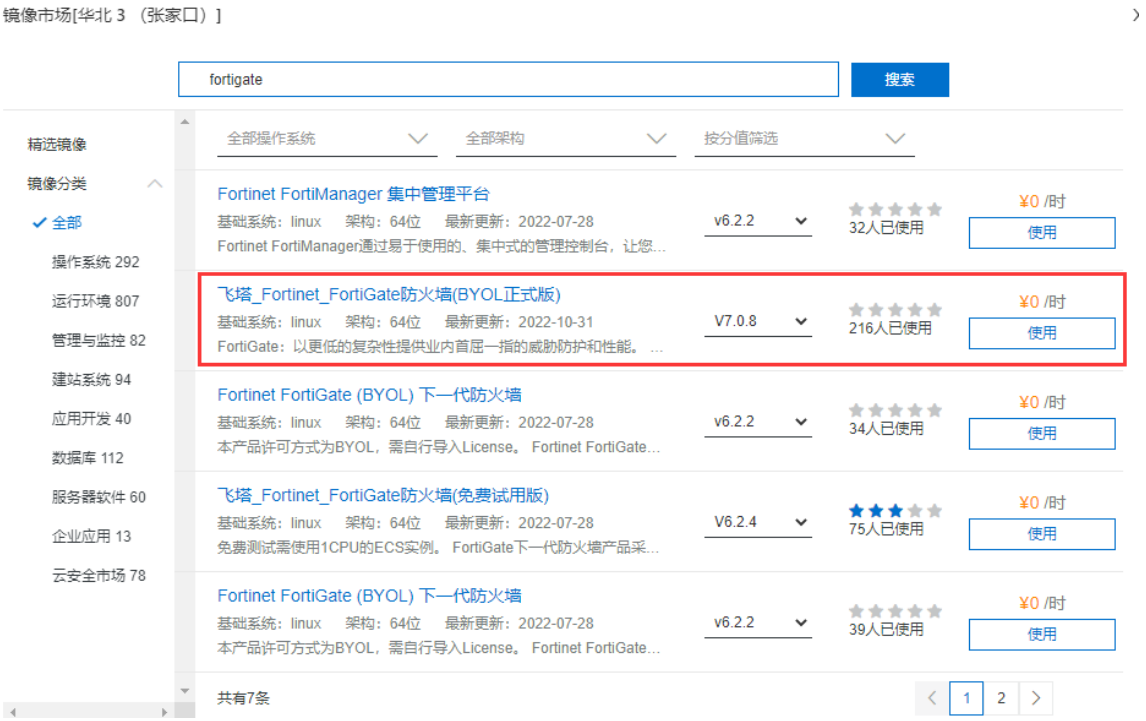
选择“付费模式”和“地域及可用区”，指定实例所在的 VPC，这里是 vpc1，FortiGate port1 所在的子网是 vpc1-A-sub0，IP 地址指定为 10.0.1.10，



“架构”选择“X86 计算”，“架构-分类”选择“计算型”，这里使用计算型 ecs.c6.xlarge。



在“云市场镜像”选择 FortiGate 版本，这里使用的是 7.0.8。

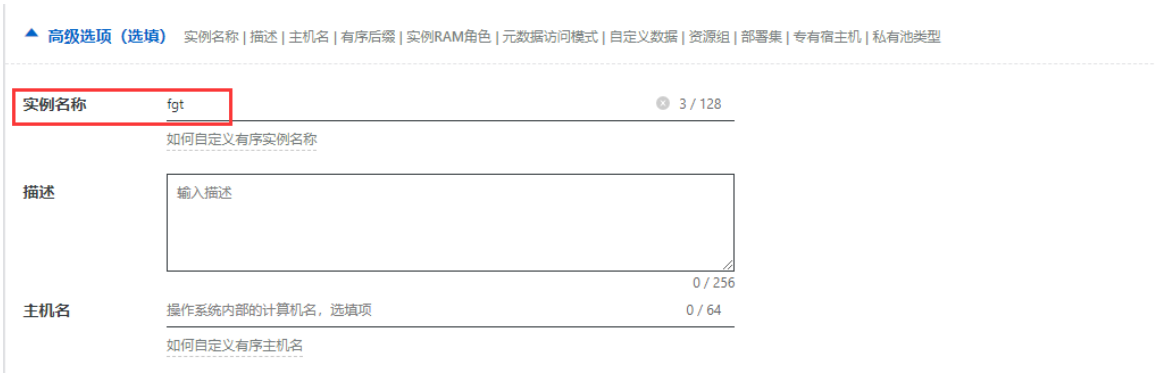


添加存储，数据盘用于记录事件日志，如果 FortiGate 需要开启流量日志，建议发送到 FAZ 或者 syslog 服务器。

安全组选择“fgt-external”，然后点击“下一步”，后续再为 FGT1 实例绑弹性公网 IP。

登录凭证选择“创建后设置”，FortiGate 默认的管理用户是 admin，密码是实例的 ID；设置实例名称。

设置“实例名称”。

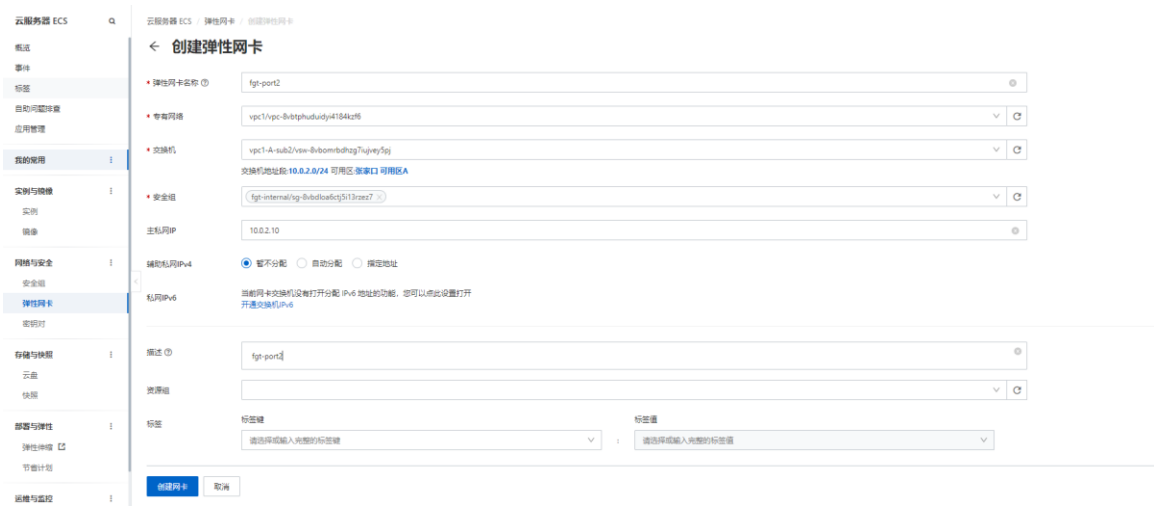


实例创建完成，实例 id 是 i-8vbczxu0ao830f6jk7pe。

4. 4. 创建弹性网卡

FortiGate 实例当前只有一个接口 port1，再增加一个弹性网卡，作为 FortiGate port2 接口。选择“云服务器 ECS”→“网络与安全”→“弹性网卡”，点击“创建弹性网卡”。

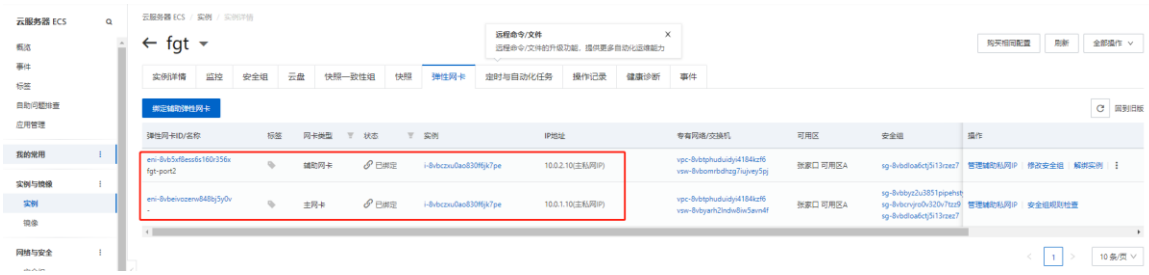
配置弹性网卡名称，专有网络选择 vpc1，交换机选择 port2 的所在的子网 vpc1-A-sub2，安全组选择“fgt-internal”，主私网 IP 指定为 10.0.2.10。



创建完成。

将网卡绑定到 fgt 实例中。

绑定成功后，可以看到 fgt 实例存在两块网卡。



4.5. 弹性 IP

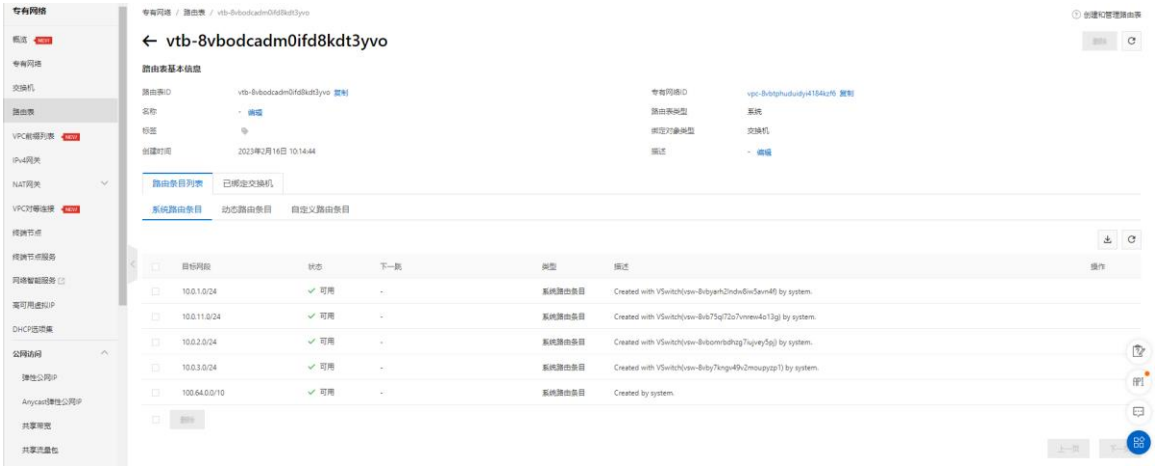
选择“专有网络”→ “公网访问”→ “弹性公网 IP”，创建弹性公网 IP。

绑定弹性 IP 到 fgt 实例。

绑定成功。

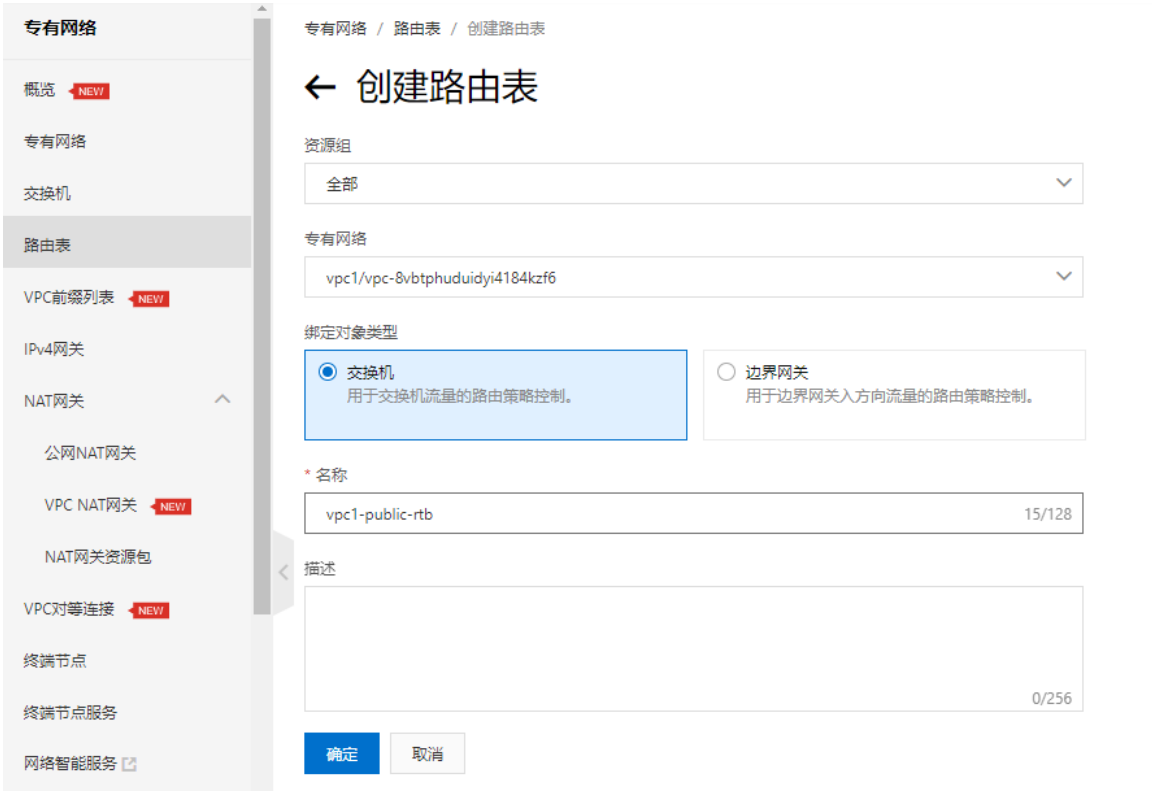
4. 6. 阿里云路由表

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。



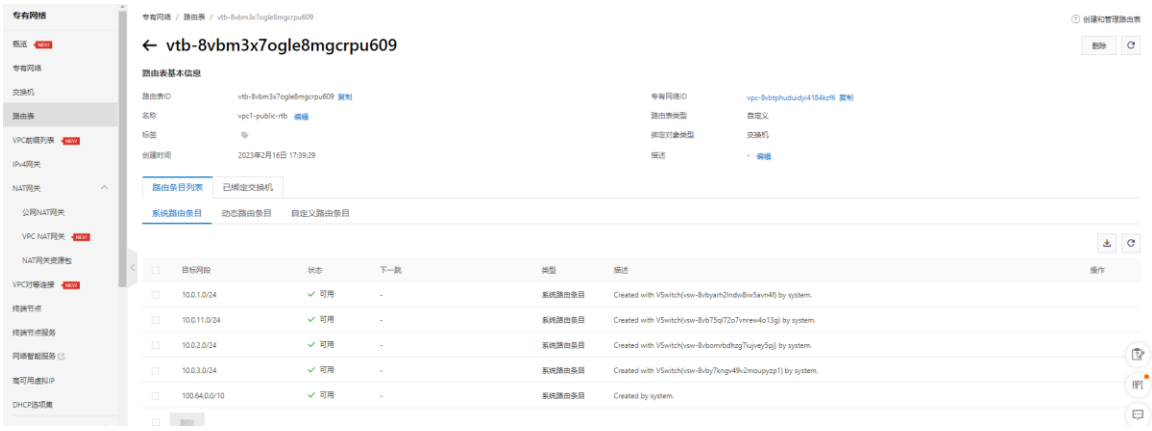
选择“专有网络”→“路由表”，点击“创建路由表”。

创建名称 vpc1-public-rtb 的路由表，关联专有网络 vpc1，用于 fgt 实例外部子网路由。

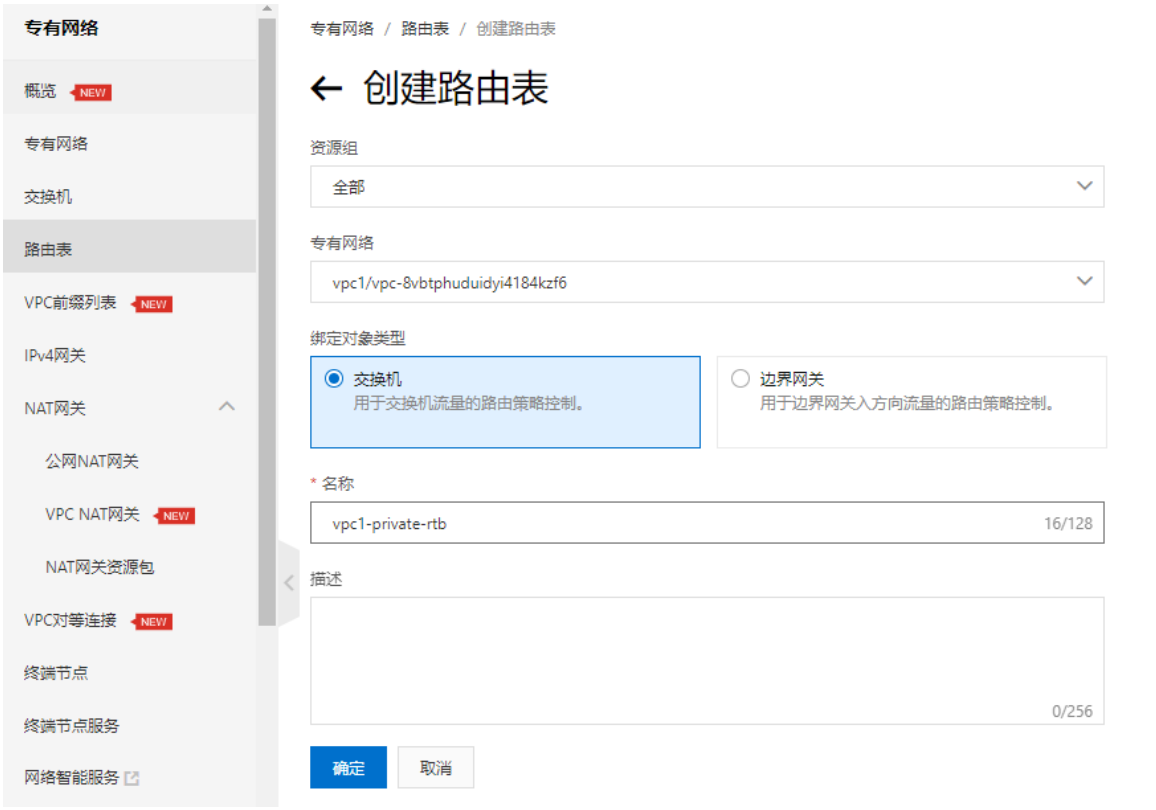


关联 fgt 实例 port1 接口的交换机。

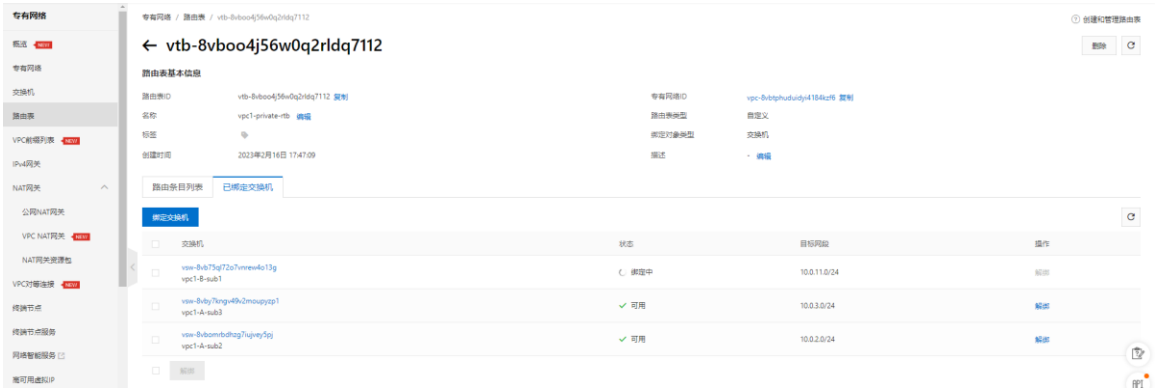
系统自动生成的路由条目如下，阿里云上 Internet 不用单独指定默认路由。



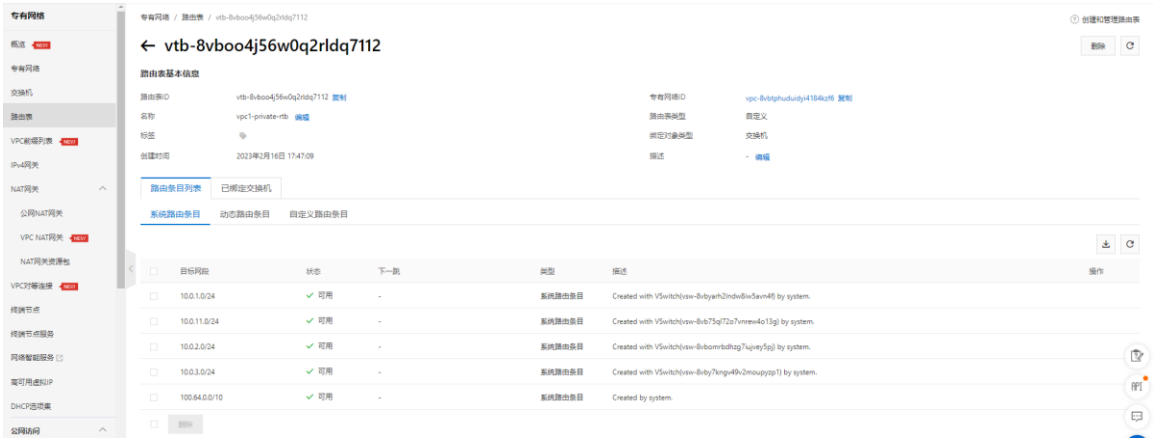
创建名称 vpc1-public-rtb 的路由表，关联专有网络 vpc1，用于 fgt 实例内部子网路由。



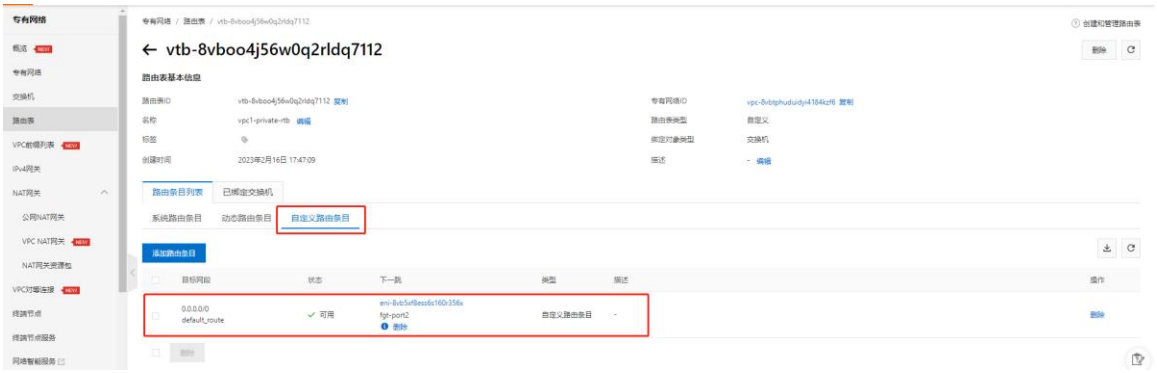
关联 fgt 实例 port2 接口的交换机，以及内网 PC 所在的交换机。



系统自动生成的条目如下：



再增加一条默认路由，网关指向 fgt 实例 port2 接口 id，用于内网 PC 通过 fgt 实例上网。



4.7. 访问 FortiGate

政府要求所有的通过互联网访问的 HTTP 和 HTTPS 服务都要进行 ICP 的备案才可以访问 HTTP 80 和 HTTPS 443 端口。

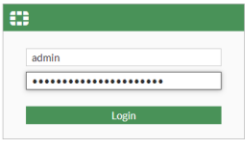
在没有备案之前可以通过修改 FortiGate 的 HTTPS 的登录端口来解决，通过 SSH 登录 FortiGate 修改 HTTPS 端口号。这样就可以通过 GUI 访问 FortiGate。

```
config system global
    set admin-sport 8443
end
```

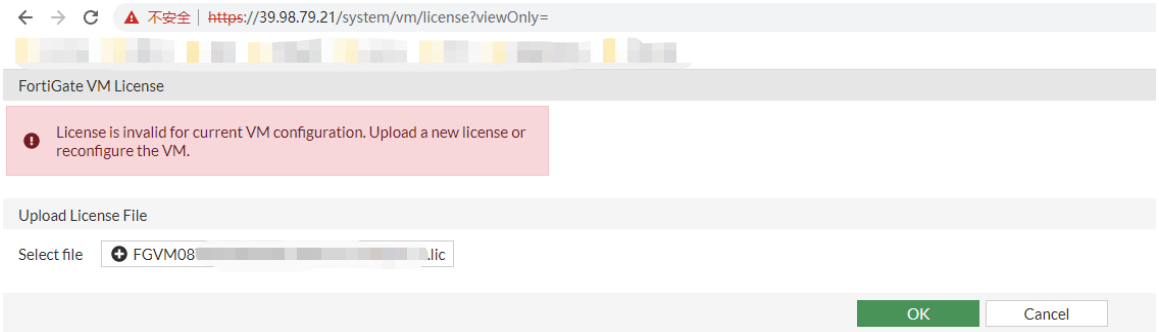
这里使用的阿里云账号已经备案，可以使用 443 端口。

HTTPS 访问 FortiGate：

使用 https:// 39.98.79.21（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。

注意：在第一次部署时，建议升级到当前系列版本的最新版本，如部署的是 6.4.x 的版本，那么建议升级到 6.4 的最新版本；如部署的 7.0.x 的版本，那么建议升级到 7.0 的最新版本。 升级完成后执行“execute factoryreset keepvmlicense”将配置恢复出厂且保存 license，然后再执行后续的配置。

4.8. 格式化硬盘

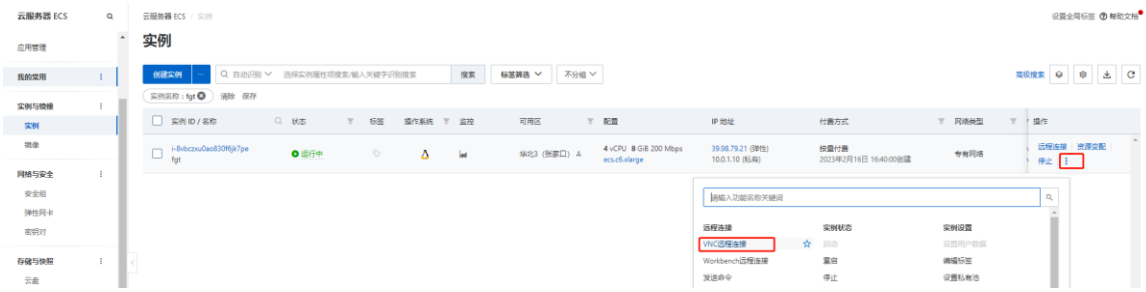
执行 execute formatlogdisk 格式化记录日志的硬盘。

CLI控制台(1)

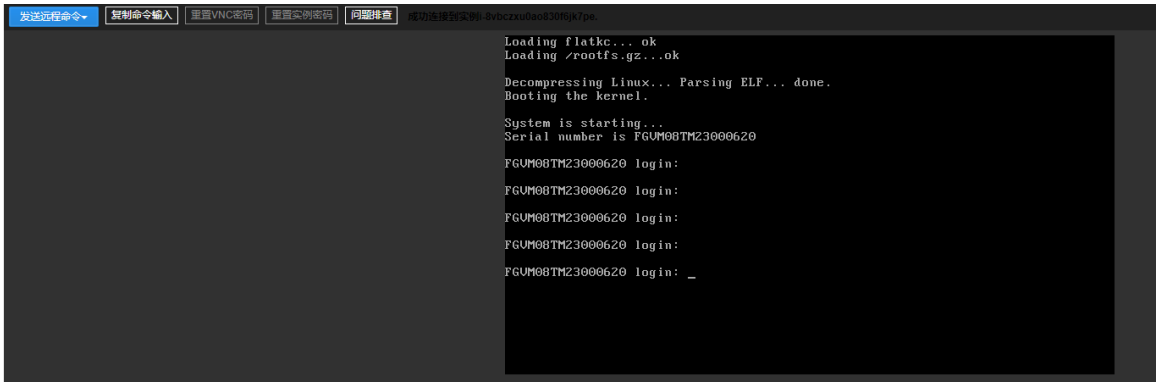
```
FGVM08[redacted] # execute formatlogdisk
Log disk is /dev/vdb1.
Formatting this storage will erase all data on it, including
  logs, quarantine files;
and require the unit to reboot.
Do you want to continue? (y/n)y
```

4.9. Console 查看 FortiGate 实例

在实例右侧，点击⋮，选择“VNC 远程连接”

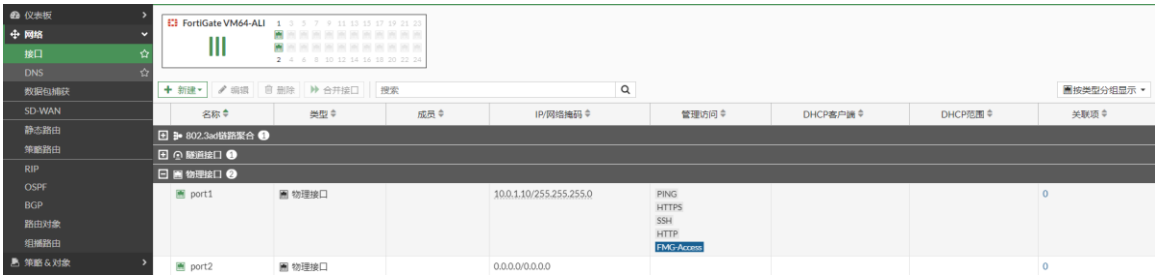


在 VNC 界面敲回车，可以查看到 fgt 实例的 console。



4.10. FortiGate 配置源 NAT

FortiGate 默认会 DHCP 获取阿里云分配的地址及路由表如下：

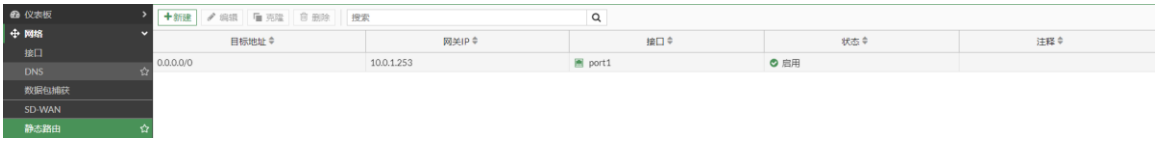



```
FGVM08          # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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 10.0.1.253, port1, [1/0]
C       10.0.1.0/24 is directly connected, port1
```

Port2 接口是附加的弹性接口，接口 ip 默认是静态配置。这里将 port1 的接口 IP 也从 DHCP 改为静态配置，并添加默认的路由。

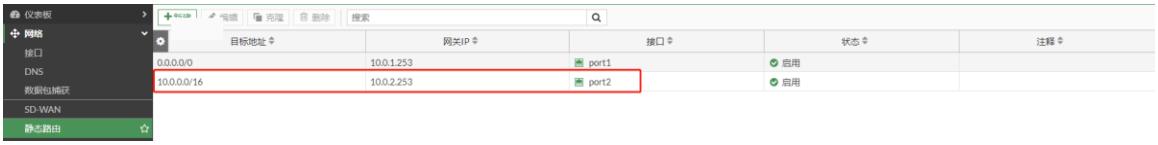
先配置默认路由，网关为 port1 所在子网的倒数第 2 个 IP，避免 port1 接口改为静态配置 IP 后无法管理。



修改 port1 ip 的配置为手动。

同样设置 port2 接口的 IP。

配置内网网段的路由从 port2 接口发出，网关是 port2 接口所在子网的倒数第 2 个 IP。

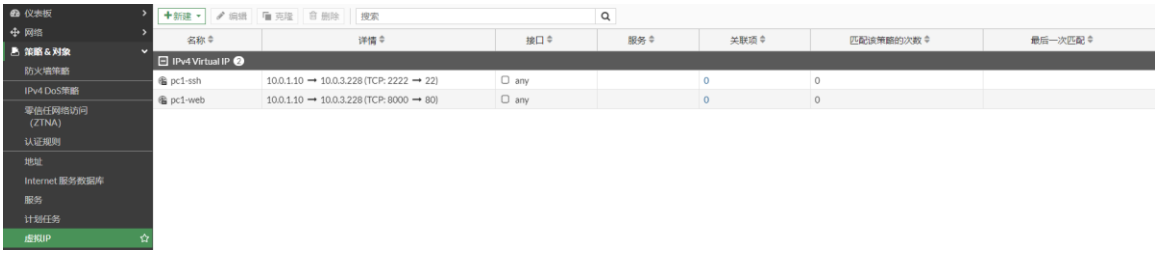


配置防火墙策略。

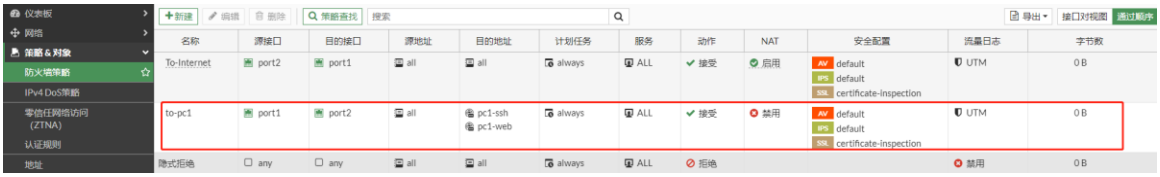
4.11. FortiGate 配置目的 NAT

使用 port1 接口的地址做目的 NAT：

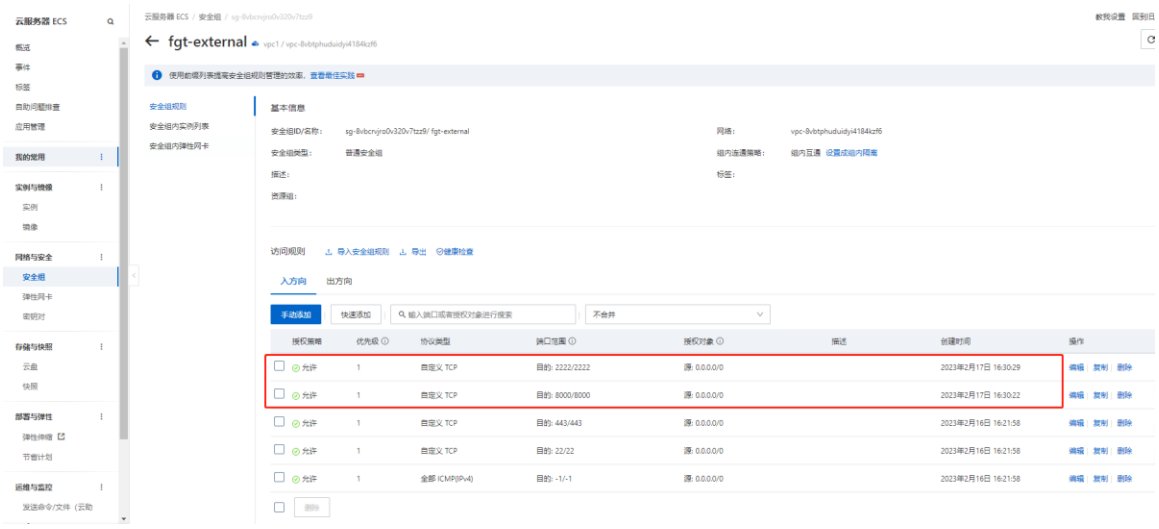
配置虚拟 IP，外部地址是 fgt 实例 port1 的接口地址 10.0.1.10，内部地址是内网 PC 的地址。



配置防火墙策略。



fgt 实例安全组放通 8000 和 2222 端口。



5. 业务测试

测试的 PC 如下

目的 NAT 测试：

ssh 39.98.79.21 2222 访问正常。

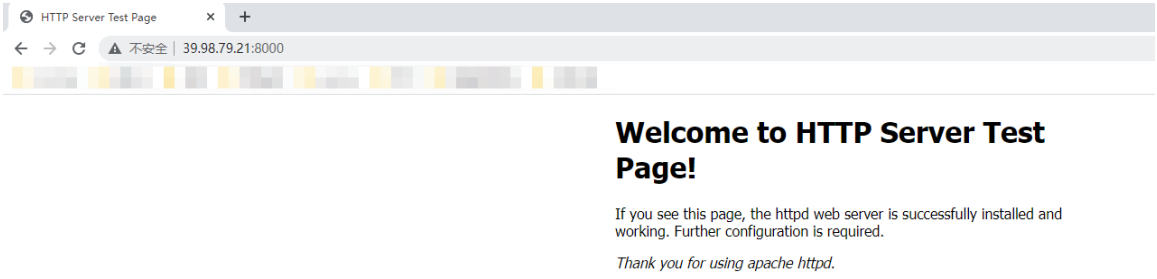
```
root@pc1:~

Welcome to Alibaba Cloud Elastic Compute Service !

Updates Information Summary: available
    6 Security notice(s)
        2 Important Security notice(s)
        4 Moderate Security notice(s)
Run "dnf upgrade-minimal --security" to apply all updates.More details please refer to:
https://help.aliyun.com/document_detail/416274.html
Last login: Fri Feb 17 16:37:10 2023 from 61.149.143.226
[root@pc1 ~]#
[root@pc1 ~]#
[root@pc1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.228  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::216:3eff:fe02:a26b  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:02:a2:6b  txqueuelen 1000  (Ethernet)
        RX packets 4621  bytes 3401928 (3.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3273  bytes 842234 (822.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@pc1 ~]#
```

http:// 39.98.79.21:8000 访问正常。



源 NAT 测试：

pc1 ping www.baidu.com 正常

root@pc1:~ × ecs-user@pc2:~

```
[root@pc1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.228  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::216:3eff:fe02:a26b  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:02:a2:6b  txqueuelen 1000  (Ethernet)
        RX packets 24732  bytes 32390934 (30.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5973  bytes 1368788 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@pc1 ~]# ping www.baidu.com -c 4
PING www.a.shifen.com (110.242.68.3) 56(84) bytes of data.
64 bytes from 110.242.68.3 (110.242.68.3): icmp_seq=1 ttl=49 time=17.2 ms
64 bytes from 110.242.68.3 (110.242.68.3): icmp_seq=2 ttl=49 time=17.0 ms
64 bytes from 110.242.68.3 (110.242.68.3): icmp_seq=3 ttl=49 time=17.1 ms
64 bytes from 110.242.68.3 (110.242.68.3): icmp_seq=4 ttl=49 time=17.1 ms

--- www.a.shifen.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 17.043/17.073/17.151/0.166 ms
[root@pc1 ~]#
```

pc2 ping www.baidu.com 正常

root@pc1:~ ecs-user@pc2:~ ×

```
Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Fri Feb 17 16:50:01 2023 from 61.149.143.226
[ecs-user@pc2 ~]$
[ecs-user@pc2 ~]$ sudo ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.11.238  netmask 255.255.255.0  broadcast 10.0.11.255
        inet6 fe80::216:3eff:fe18:cceb  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:18:cc:eb  txqueuelen 1000  (Ethernet)
        RX packets 85520  bytes 123653576 (117.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9375  bytes 2987307 (2.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[ecs-user@pc2 ~]$ ping www.baidu.com -c 4
PING www.a.shifen.com (110.242.68.4) 56(84) bytes of data.
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=1 ttl=49 time=18.5 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=2 ttl=49 time=18.3 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=3 ttl=49 time=18.2 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=4 ttl=49 time=18.2 ms

--- www.a.shifen.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 18.248/18.322/18.509/0.198 ms
[ecs-user@pc2 ~]$
```