# 阿里云同 AZ 部署 FortiGate HA

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

# 目录

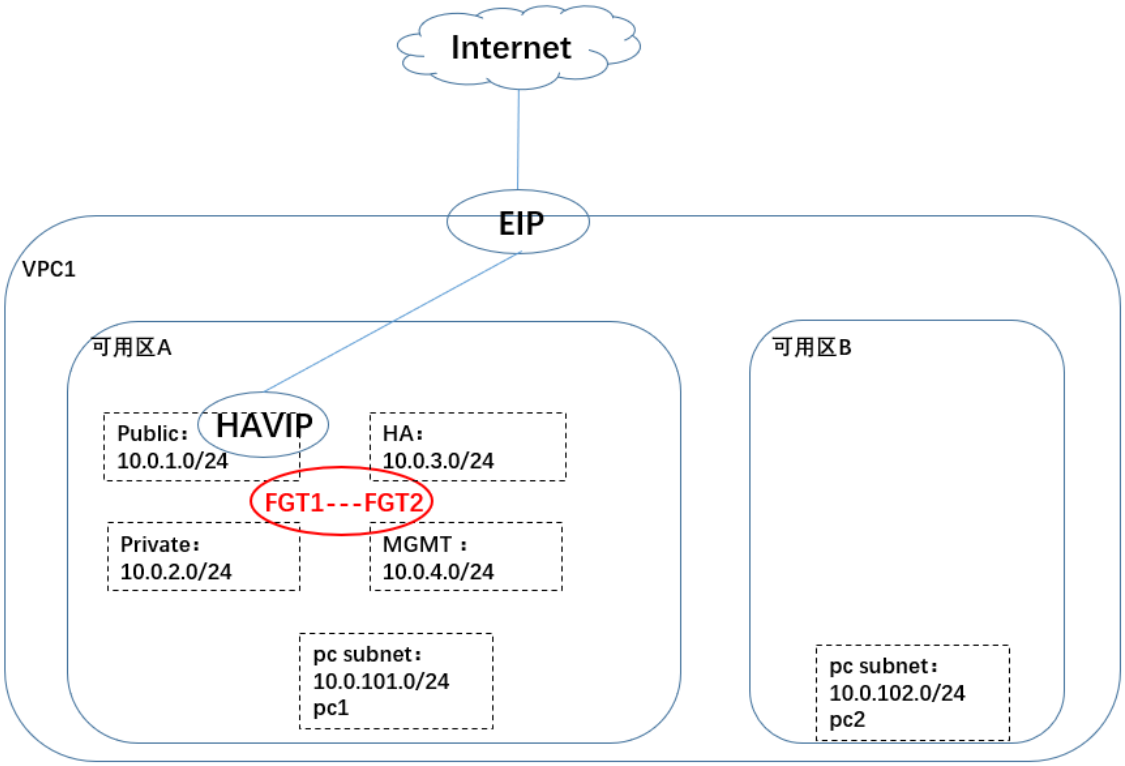
# 1. 介绍

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

# 2. 网络拓扑

FGT1 和 FGT2 部署在同一 AZ 中，FGT1 和 FGT2 的实例分别需要 4 块网卡。阿里云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://www.alibabacloud.com/help/zh/elastic-compute-service/latest/instance-family?spm=a2c63.p38356.0.0.27a13647EWsnuZ#concept-sx4-lxv-tdb



# 3. 地址规划

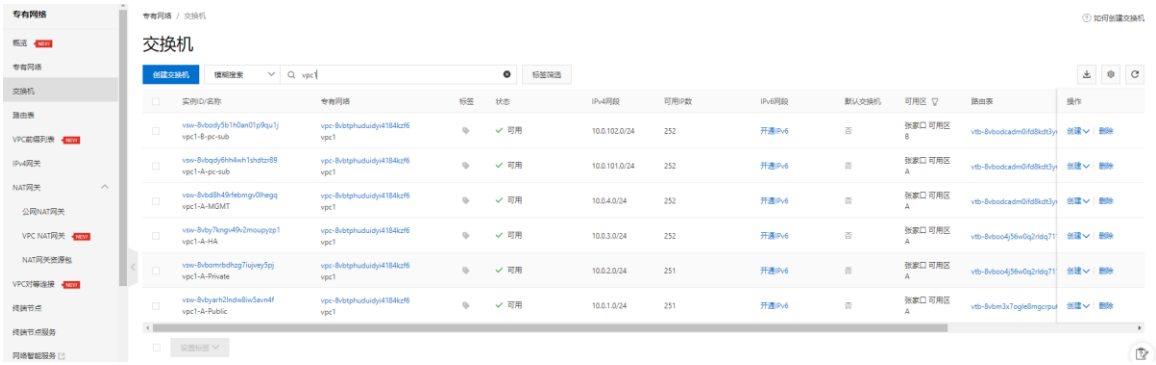
| **FGT1 地址规划（可用区 A）** | | |
|---|---|---|
| Port | 阿里云 primary address | HAVIP 地址 |
| Port1 | 10.0.1.11 | 10.0.1.101 |
| Port2 | 10.0.2.11 | NA |
| Port3 | 10.0.3.11 | NA |
| Port4 | 10.0.4.11 | NA |
| **FGT2 地址规划（可用区 A）** | | |
| Port | 阿里云 primary address | HAVIP 地址 |
| Port1 | 10.0.1.12 | 10.0.1.101 |
| Port2 | 10.0.2.12 | NA |
| Port3 | 10.0.3.12 | NA |
| Port4 | 10.0.4.12 | NA |
| **测试 PC** | | |
| PC 名称 | 测试地址 | AZ |
| PC1 | 10.0.101.10 | 可用区 A |
| PC2 | 10.0.102.10 | 可用区 B |

# 4. 配置步骤

## 4.1. 创建 VPC、子网

创建 VPC。

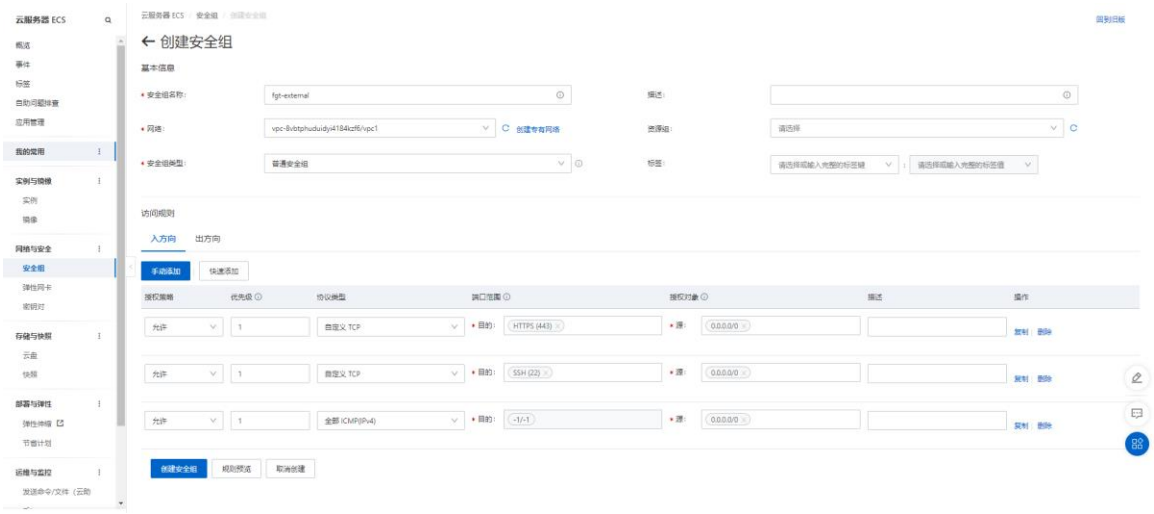

创建子网。



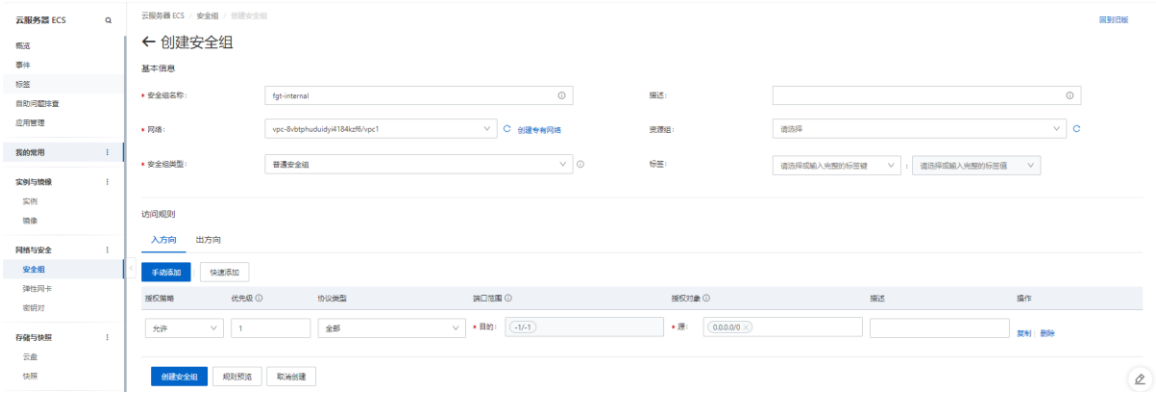
## 4.2. 创建安全组

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。FortiGate port3 是 HA 接口，互通的是 HA 交换的数据，安全组全放通，和 port2 共用同一个安全组；FortiGate port4 是 MGMT 接口，用于管理，放通 HTTPS，SSH 和 ICMP。

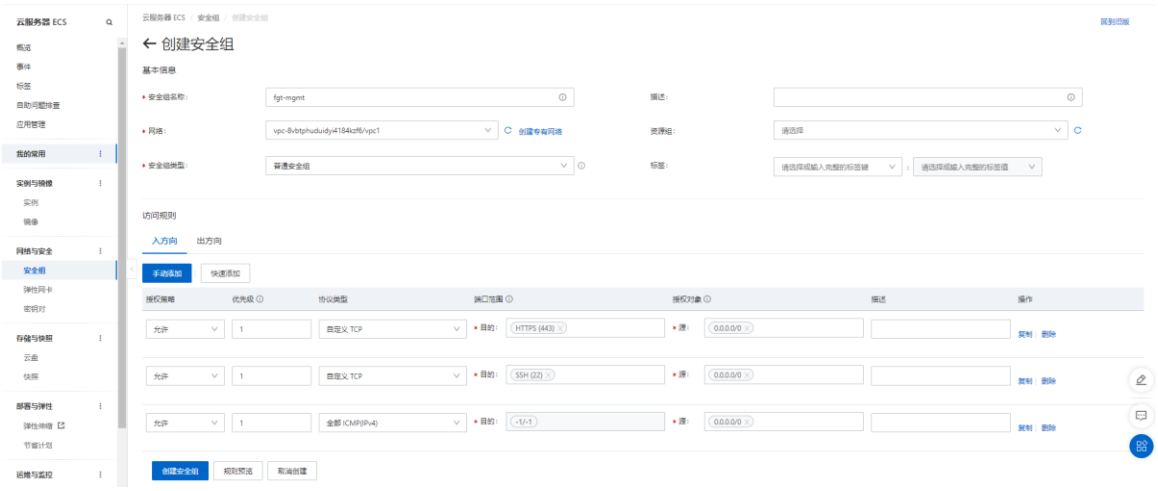
新建安全组 fgt-external，用于 port1。这里先放通管理所需的端口 HTTPS，SSH 和 ICMP。




再新建安全组 fgt-internal，用于 port2 和 port3，放通所有。



新建安全组 fgt-mgmt，用于 port4，放通管理所需的端口 HTTPS，SSH 和 ICMP。



## 4.3. 创建 IAM 角色

FortiGate 实例赋予角色后，才能根据权限使用 API 操作和资源。

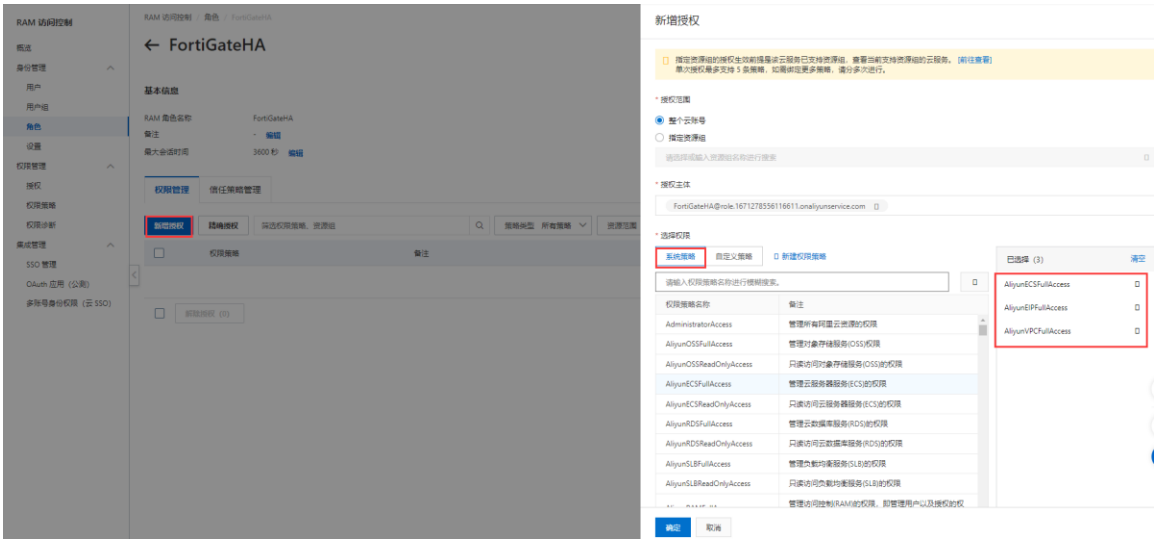
选择“访问控制”→“身份管理”→“角色”，点击“创建角色”。


选择“阿里云服务”，点击“下一步”。


输入“角色名称”，在“选择受信服务”中选择“云服务器”，并点击“完成”。

点击角色 FortiGateHA。


点击“新增授权”，新增“AliyunECSFullAccess”，“AliyunEIPFullAccess”“AliyunVPCFullAccess”三个权限，并点击“确定”。

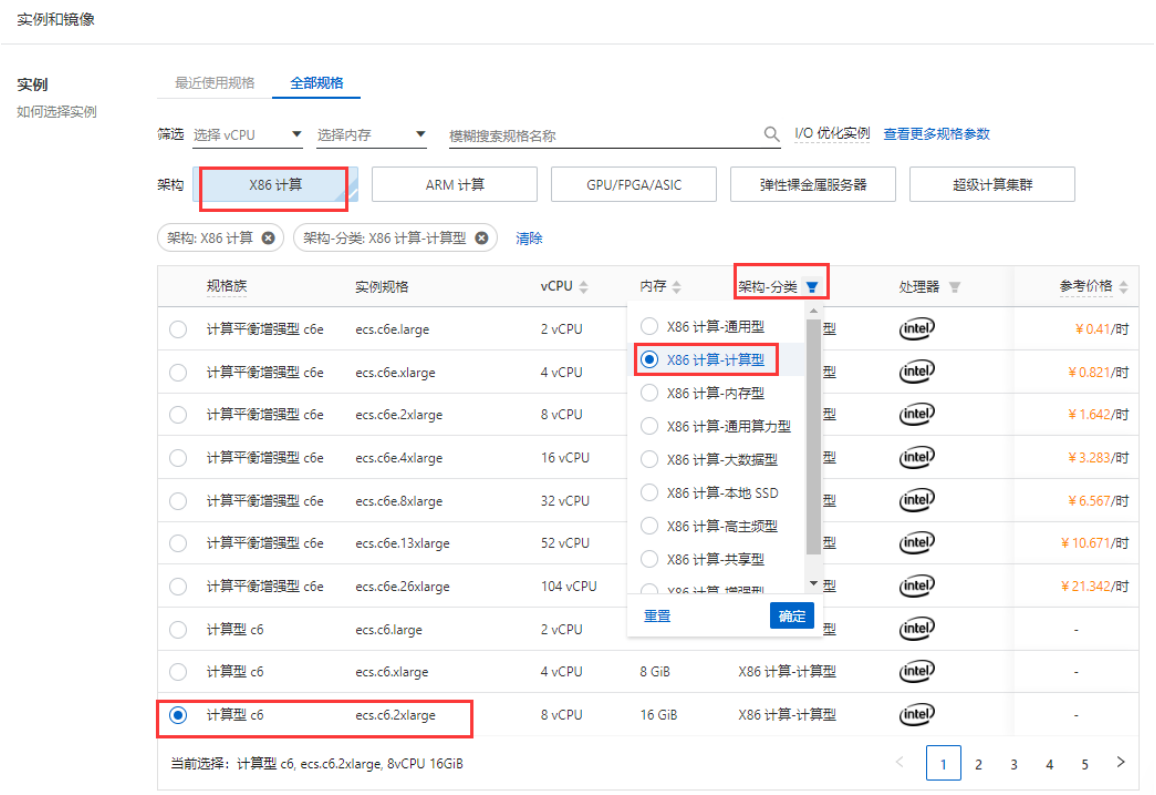


## 4.4. 创建 FortiGate 实例

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-Public，IP 地址指定为 10.0.1.11，


“架构”选择“X86 计算”，“架构-分类”选择“计算型”，这里使用计算型 ecs.c6.2xlarge（支持 4 块网卡）。

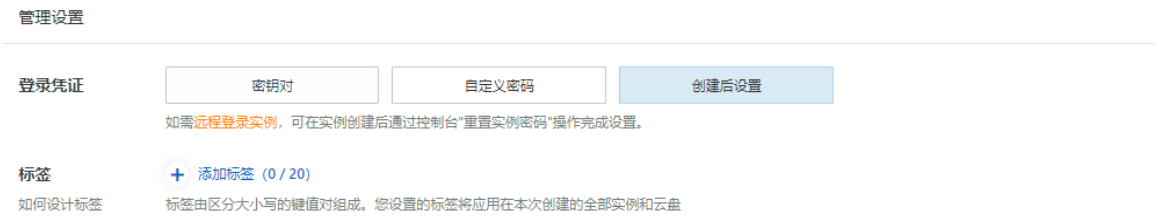


在“云市场镜像”选择 FortiGate 版本，这里使用的是 7.0.8。


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”，选择“实例 RAM 角色”为“FortiGateHA”。

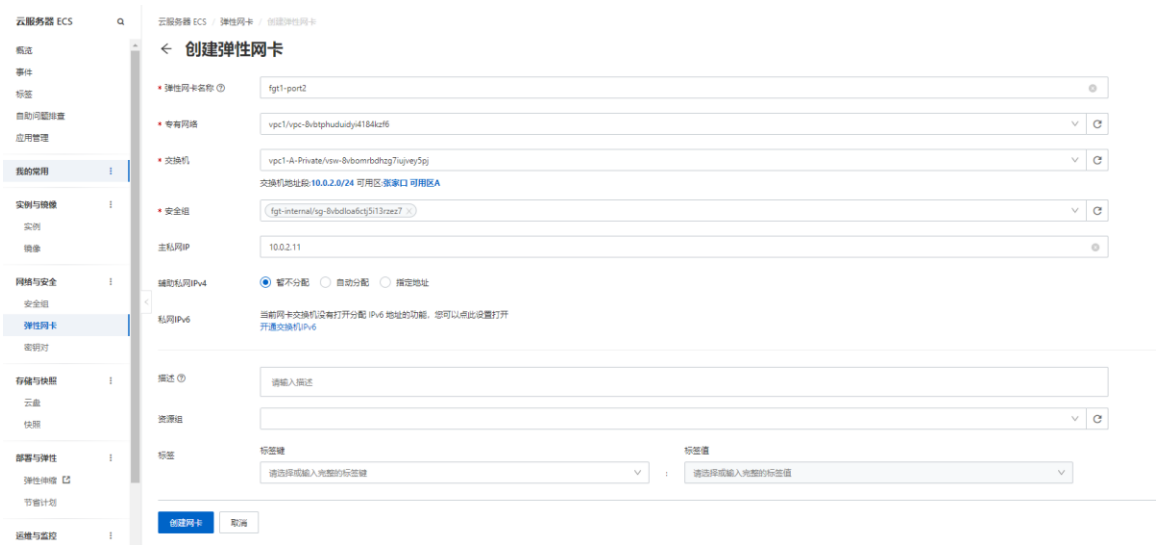

查看实例当前配置，确认无误后点击“确认下单”。


实例创建完成。同理创建另外一个 FortiGate 实例。

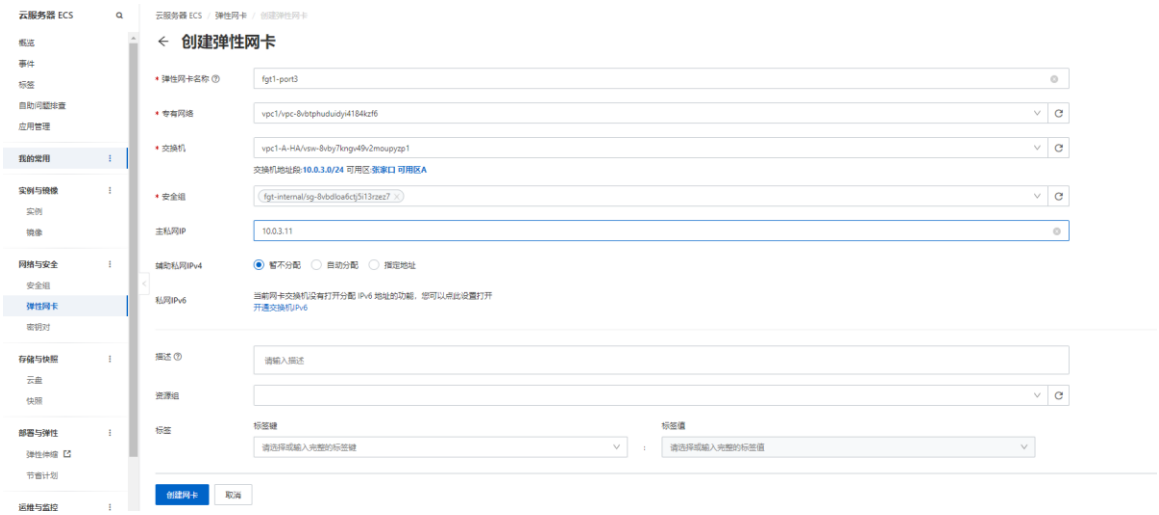
## 4. 5. 创建弹性网卡

FGT1 实例当前只有一个接口 port1，需要再创建 3 个弹性网卡。选择“云服务器 ECS”→“网络与安全”→“弹性网卡”，点击“创建弹性网卡”。

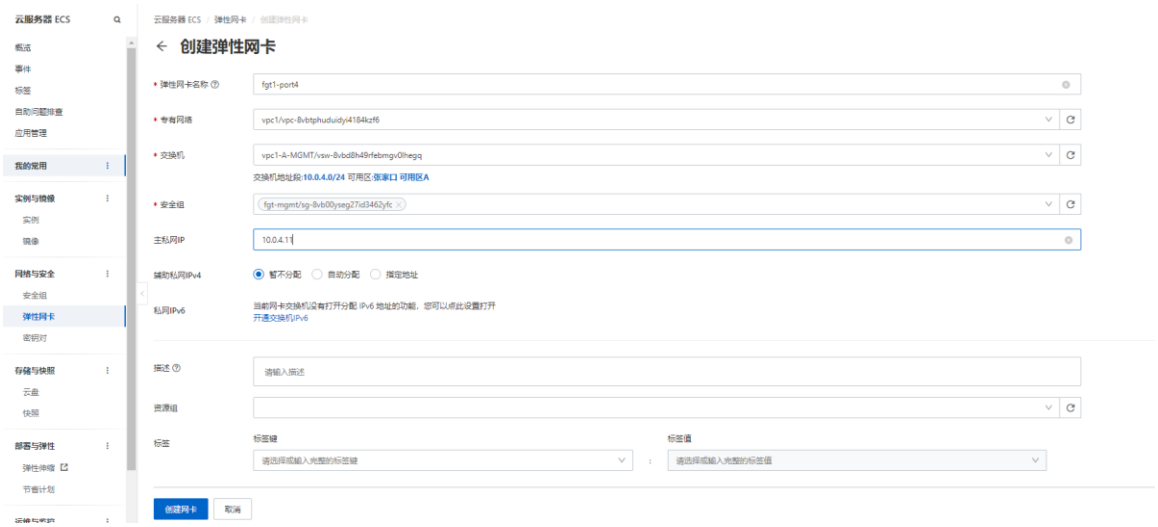
创建弹性网卡 fgt1-port2，配置“弹性网卡名称”，专有网络选择 vpc1，交换机选择 port2 的所在的子网 vpc1-A-Private，安全组选择“fgt-internal”，主私网 IP 指定为 10.0.2.11。



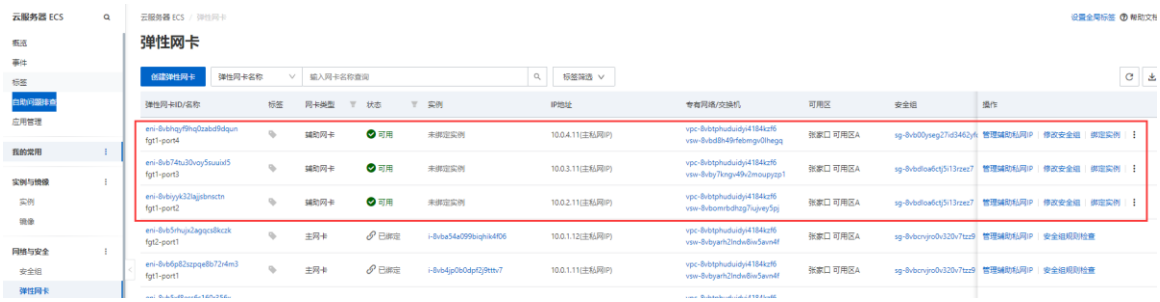

创建弹性网卡 fgt1-port3，配置“弹性网卡名称”，专有网络选择 vpc1，交换机选择 port3 的所在的子网 vpc1-A-HA，安全组选择“fgt-internal”，主私网 IP 指定为 10.0.3.11。



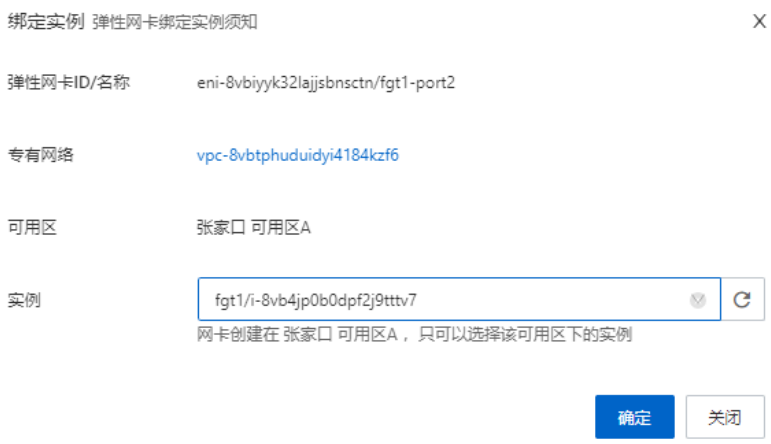
创建弹性网卡 fgt1-port4，配置“弹性网卡名称”，专有网络选择 vpc1，交换机选择 port4 的所在的子网 vpc1-A-MGMT，安全组选择“fgt-mgmt”，主私网 IP 指定为 10.0.4.11。



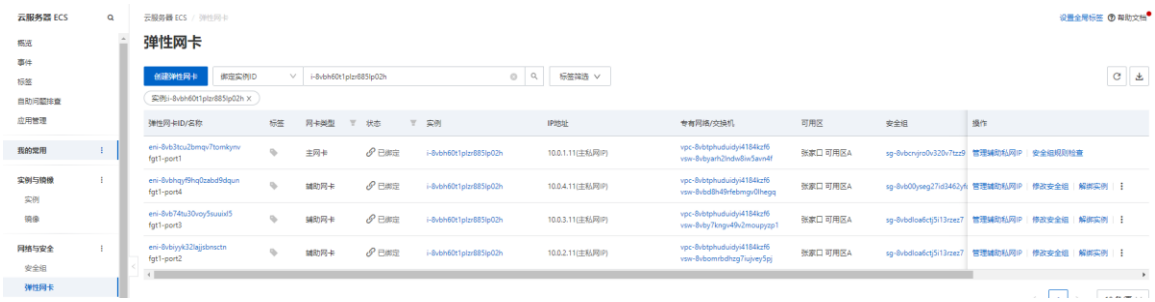

FGT1 实例 3 块网卡创建完成。



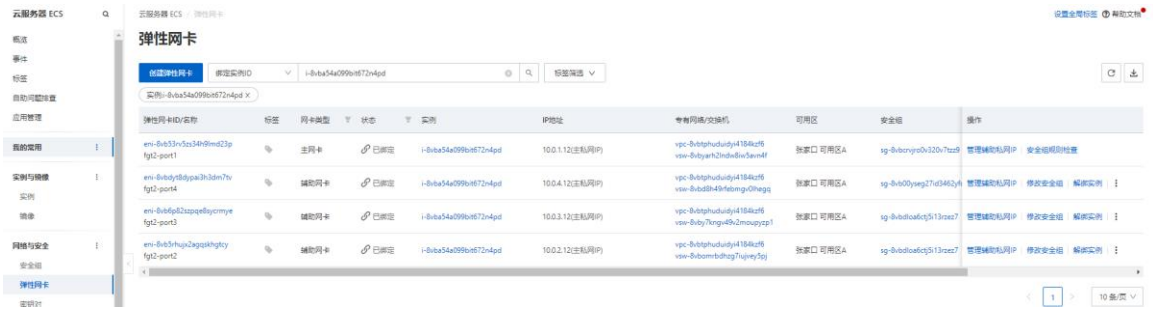

将 3 块网卡分别绑定到 FGT1 实例，port2 绑定成功后，再绑定 port3，最后绑定 port4。



绑定成功。

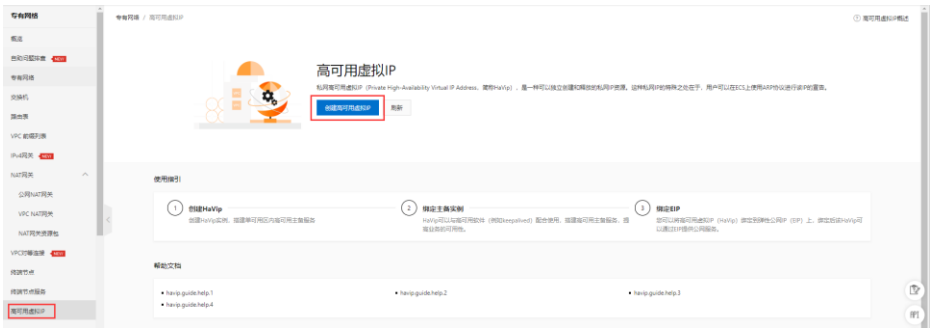



同理创建实例 FGT2 的另外 3 块网卡，并绑定到 FGT2。



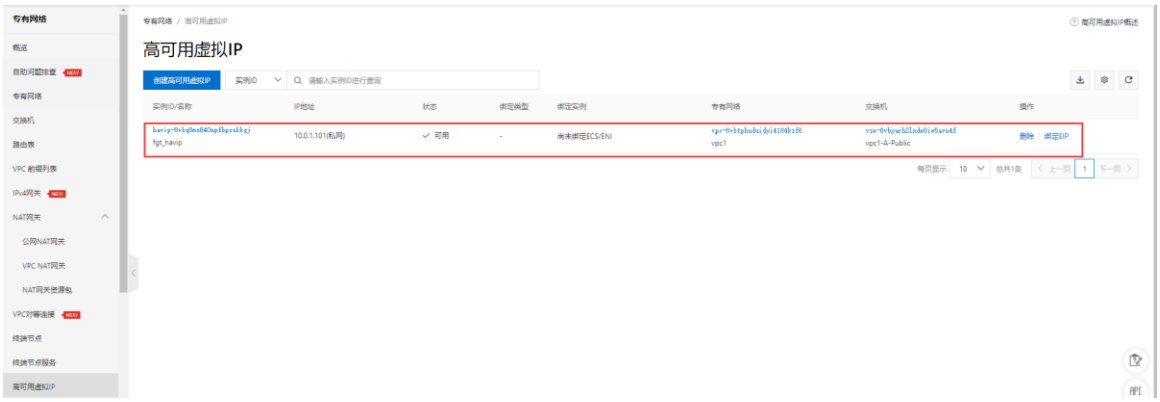
## 4.6. 创建高可用虚拟 IP

选择“专有网络 VPC”→“高可用虚拟 IP”，点击“创建高可用虚拟 IP”。

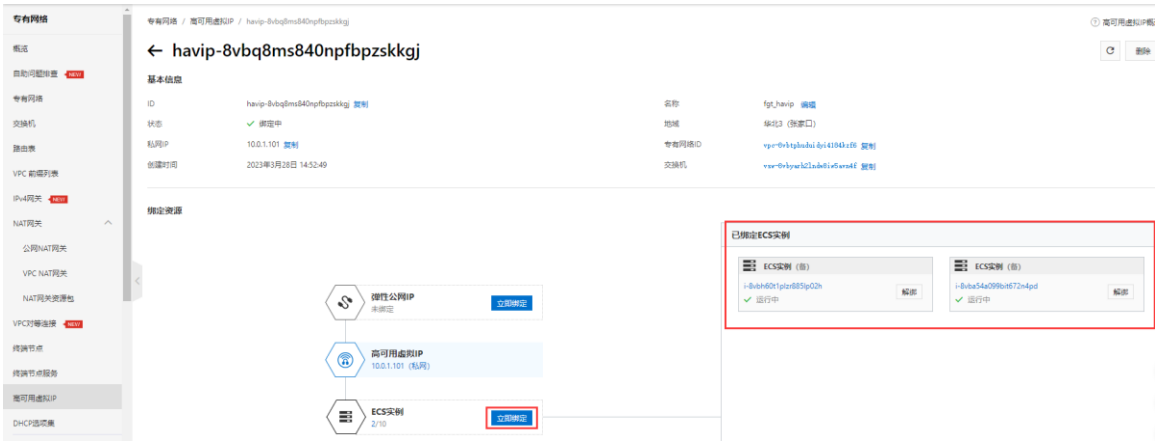



设置“名称”，专有网络即 FortiGate 实例所在的 VPC，交换机选择 FortiGate port1 所在的子网，并点击“确定”。

创建成功。




点击高可用虚拟 IP，绑定 ECS 实例。



## 4.7. 弹性 IP

创建 5 个弹性 IP，最终使用 3 个，另外两个是临时的，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 port4 10.0.4.11。

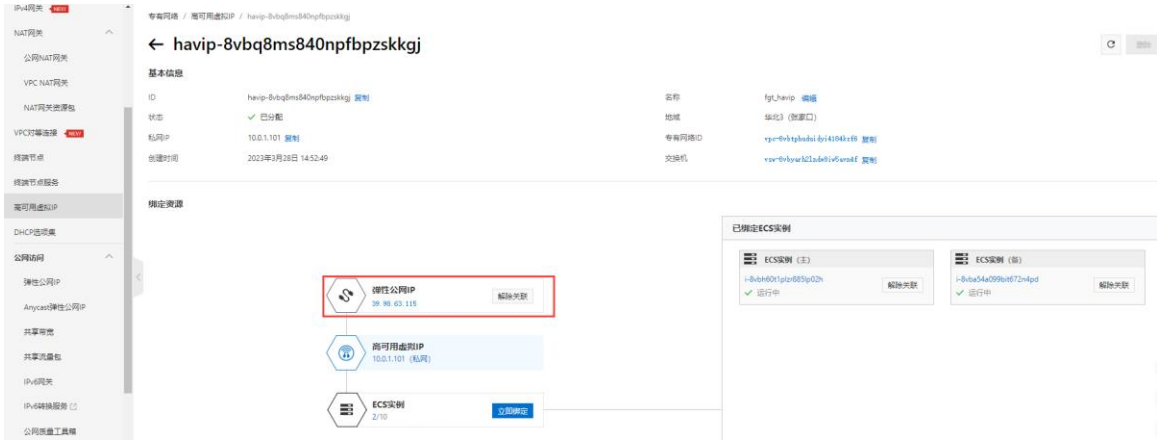
一个弹性 IP 关联 FGT2  实例 port4 10.0.4.12。

一个弹性 IP 关联高可用虚拟 IP。

**临时配置的 2 个弹性 IP:**

一个弹性 IP 关联 FGT1 实例 port1 10.0.0.11。

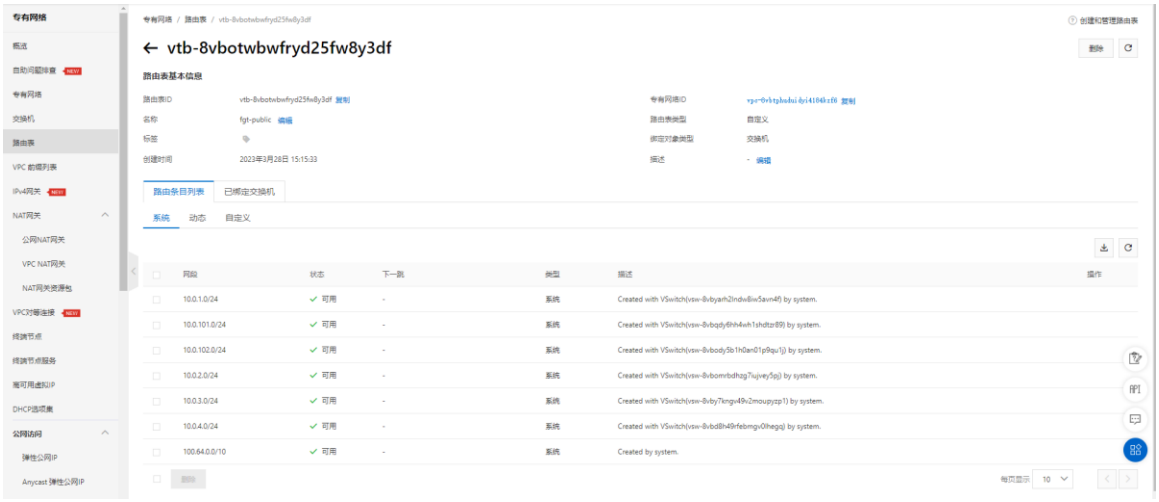
一个弹性 IP 关联 FGT2 实例 port1 10.0.0.12。

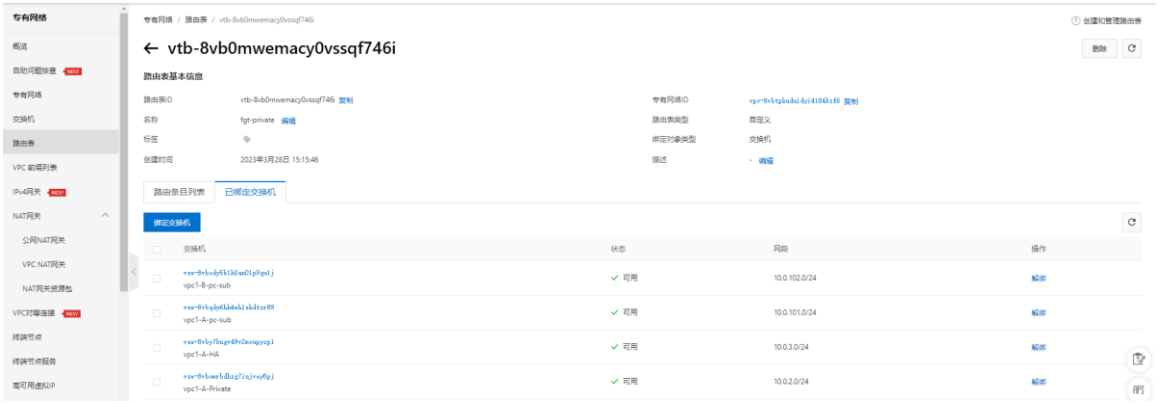
## 4.8. 配置 VPC 路由表

新建 fgt-public 路由表，关联 public（10.0.1.0/24），mgmt（10.0.4.0/24）2 个子网。

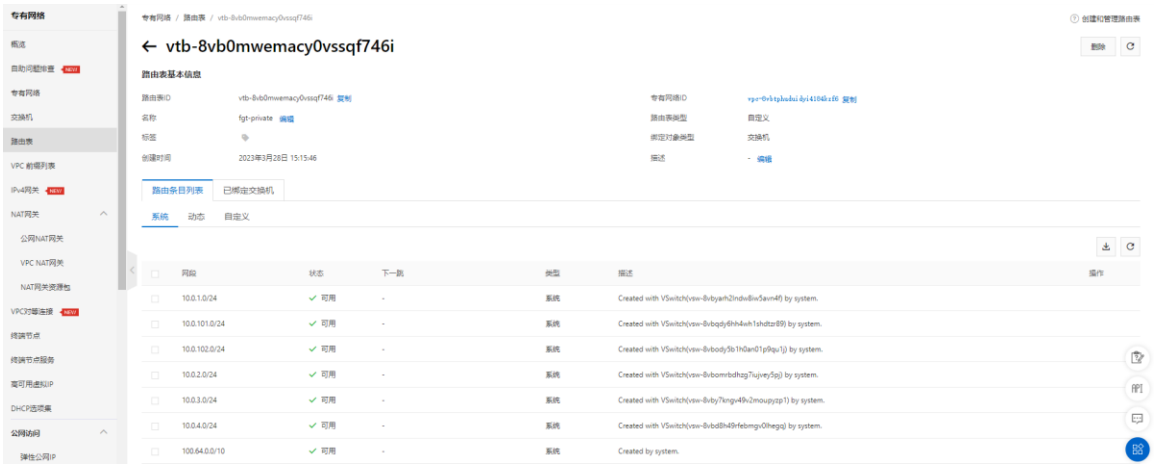

fgt-public 路由表系统自带路由。



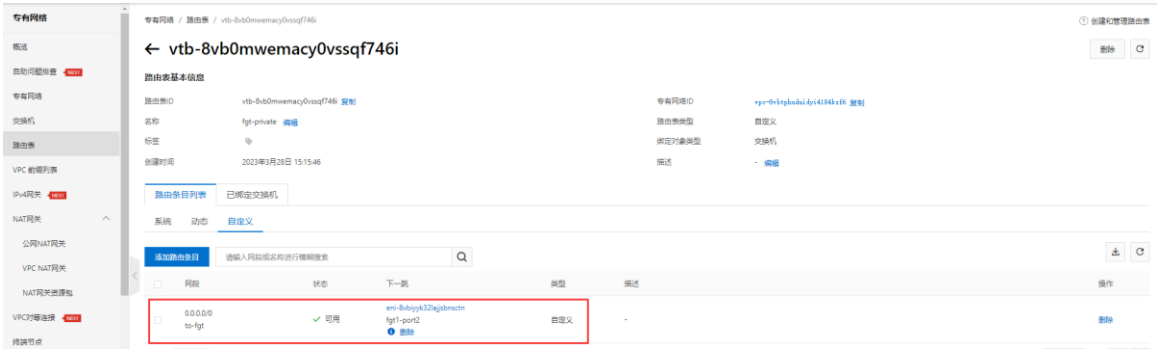
新建 fgt-private 路由表，关联 private 子网，ha 子网，pc 子网（10.0.2.0/24，10.0.3.0、24，10.0.101.0/24，10.0.102.0/24）4 个。




Private 路由表系统自带路由。



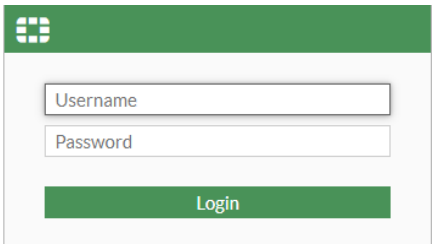

fgt-private 默认路由指向 FGT HA Master（当前 FGT1）实例的 port2 的接口 ID。



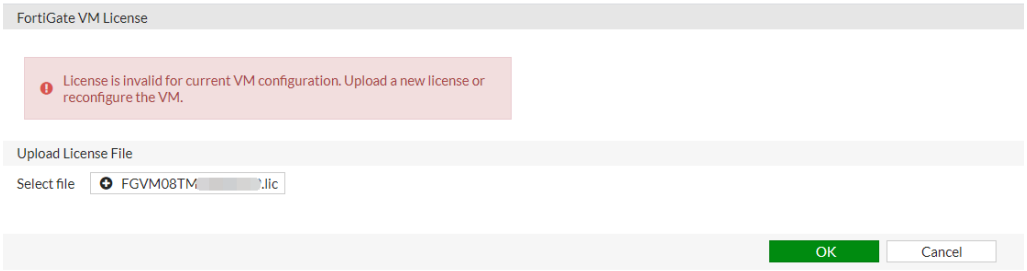
## 4.9. 访问 FortiGate

HTTPS 访问 FGT1，同理访问 FGT2：

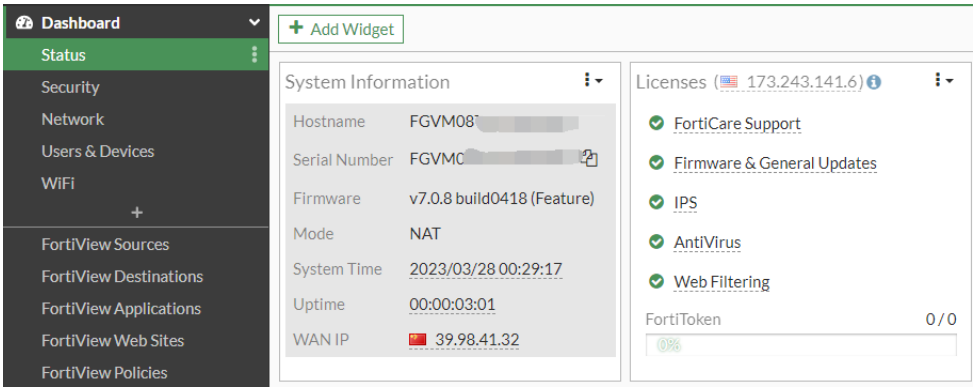
使用 https://39.98.41.32/（弹性 IP）访问 FortiGate，账号是 admin，密码默认是实例 ID。首次登录后，请按照提示修改密码。




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。

## 4.10. 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
```

## 4.11. 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 10.0.1.253      #网关为所在子网的倒数第 2 个 IP
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.2.253      #网关为所在子网的倒数第 2 个 IP
        set device "port2"
    next
end
config system interface
    edit "port1"
        set mode static
        set ip 10.0.1.11 255.255.255.0
        set allowaccess ping https ssh
        set secondary-IP enable
        config secondaryip
            edit 1
                set ip 10.0.1.101 255.255.255.0     #havip 的地址作为 FortiGate 的第二地址
                set allowaccess ping
            next
        end
    next
```

```
        edit "port2"
            set mode static
            set ip 10.0.2.11 255.255.255.0
            set allowaccess ping
        next
        edit "port3"
            set mode static
            set ip 10.0.3.11 255.255.255.0
            set allowaccess ping
        next
        edit "port4"
            set mode static
            set ip 10.0.4.11 255.255.255.0
            set allowaccess ping https ssh
        next
end
config system global
        set admintimeout 50
        set hostname "FGT1"
        set timezone 55
end
```

FGT2 基本配置，先配置路由，再修改地址，否则 fgt 2 将无法访问。

```
config router static
        edit 1
            set gateway 10.0.1.253      #网关为所在子网的倒数第 2 个 IP
            set device "port1"
        next
        edit 2
            set dst 10.0.0.0 255.255.0.0
            set gateway 10.0.2.253      #网关为所在子网的倒数第 2 个 IP
            set device "port2"
        next
end
config system interface
        edit "port1"
            set mode static
            set ip 10.0.1.12 255.255.255.0
            set allowaccess ping https ssh
            set secondary-IP enable
            config secondaryip
                edit 1
```

```
                set ip 10.0.1.101 255.255.255.0     #havip 的地址作为 FortiGate 的第二地址
                set allowaccess ping
            next
        end
    next
    edit "port2"
        set mode static
        set ip 10.0.2.12 255.255.255.0
        set allowaccess ping
    next
    edit "port3"
        set mode static
        set ip 10.0.3.12 255.255.255.0
        set allowaccess ping
    next
    edit "port4"
        set mode static
        set ip 10.0.4.12 255.255.255.0
        set allowaccess ping https ssh
    next
end
config system global
    set admintimeout 50
    set hostname "FGT2"
    set timezone 55
end
```

在配置 HA 之前，先测试 FGT1 和 FGT2 port3 之前互 ping 是否能通。

```
fgt1 # execute ping-options source 10.0.3.11

fgt1 # execute ping 10.0.3.12
PING 10.0.3.12 (10.0.3.12): 56 data bytes
64 bytes from 10.0.3.12: icmp_seq=0 ttl=255 time=1.1 ms
64 bytes from 10.0.3.12: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 10.0.3.12: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.0.3.12: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.0.3.12: icmp_seq=4 ttl=255 time=0.2 ms

--- 10.0.3.12 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.4/1.1 ms
```

FGT1 HA 配置：

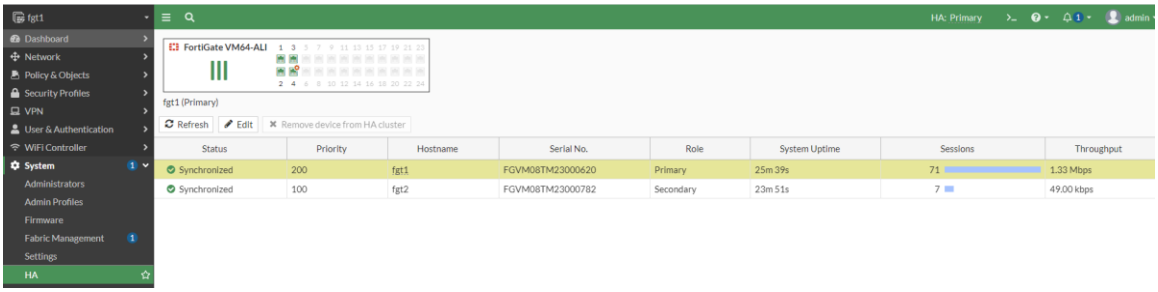
```
config system ha
    set group-name "FGTHA"
    set mode a-p
```

```
        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 10.0.4.253
            next
        end
        set override disable
        set priority 200
        set unicast-hb enable
        set unicast-hb-peerip 10.0.3.12
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 10.0.4.253
            next
        end
        set override disable
        set priority 100
        set unicast-hb enable
        set unicast-hb-peerip 10.0.3.11
end
```

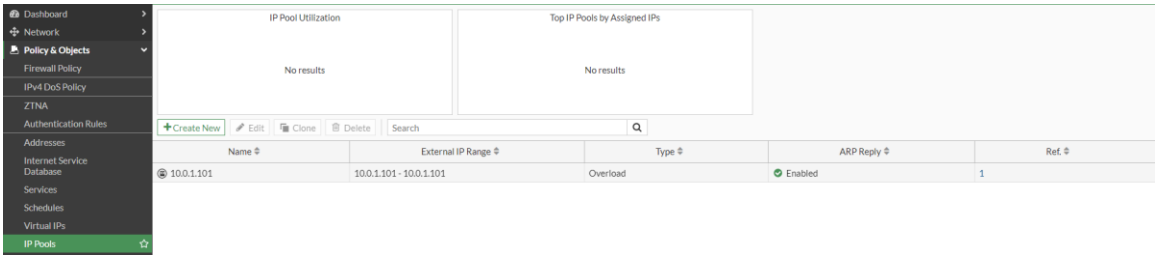
配置完成后，查看 HA 状态。如果 HA 状态没有同步，请稍等一会再查看。



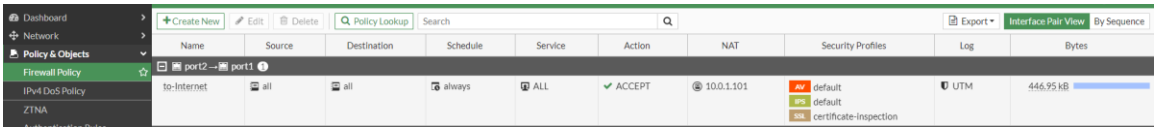

现在可以使用 FortiGate 实例 port4 关联的弹性 IP 进行访问，此时可以删除临时的 2 个弹性 IP。

## 4.12. FortiGate 配置源 NAT

FGT1 配置地址池，地址池的地址是 havip 的地址 10.0.1.101，会自动同步给 FGT2。



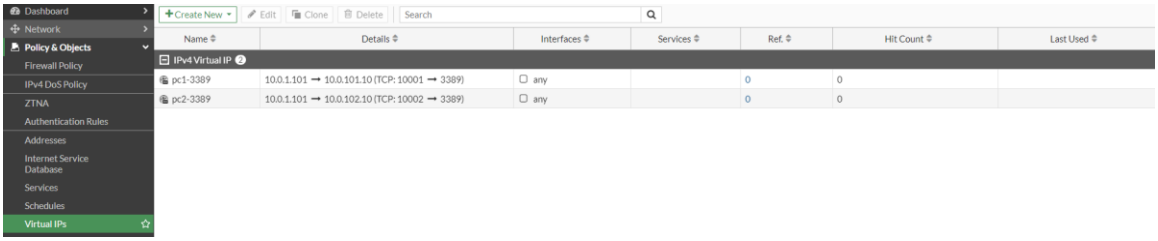

配置防火墙策略，会自动同步给 FGT2。

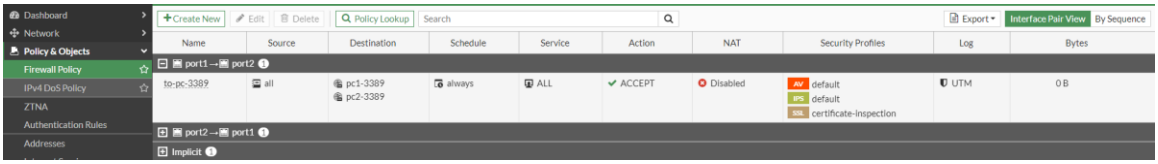



## 4.13. FortiGate 配置目的 NAT

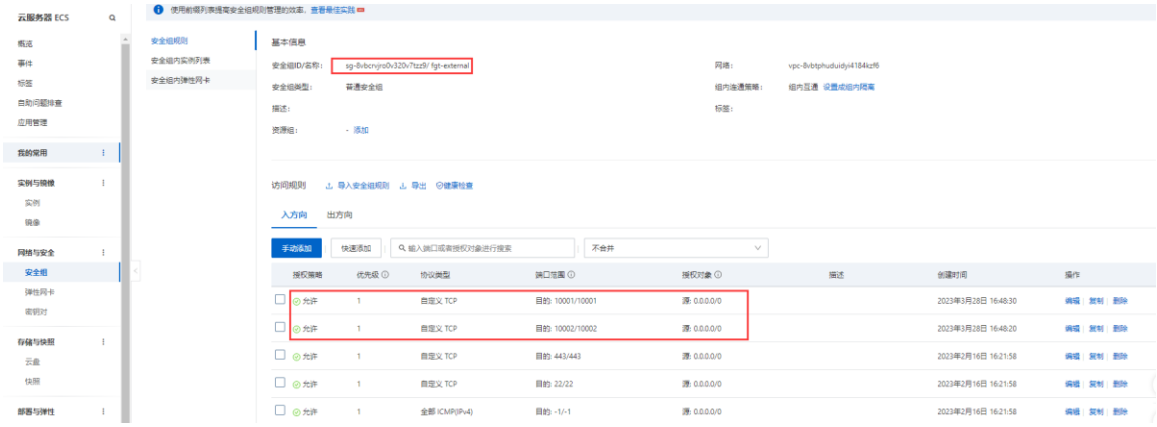
创建两个 PC 实例。

使用 havip 的地址作为目的 NAT 的外部地址，将两个 PC 的 3389 端口映射出去，对外的端口分别是 10001 和 10002。FGT1 配置 VIP 和策略，会同步给 FGT2。



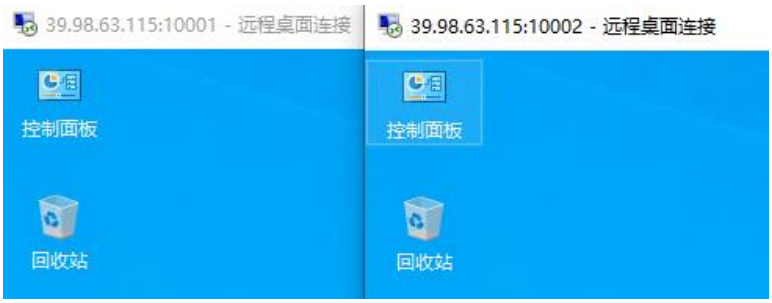




FortiGate 实例 port1 安全组 fgt-external 放通 10001，10002 这两个对外的端口。

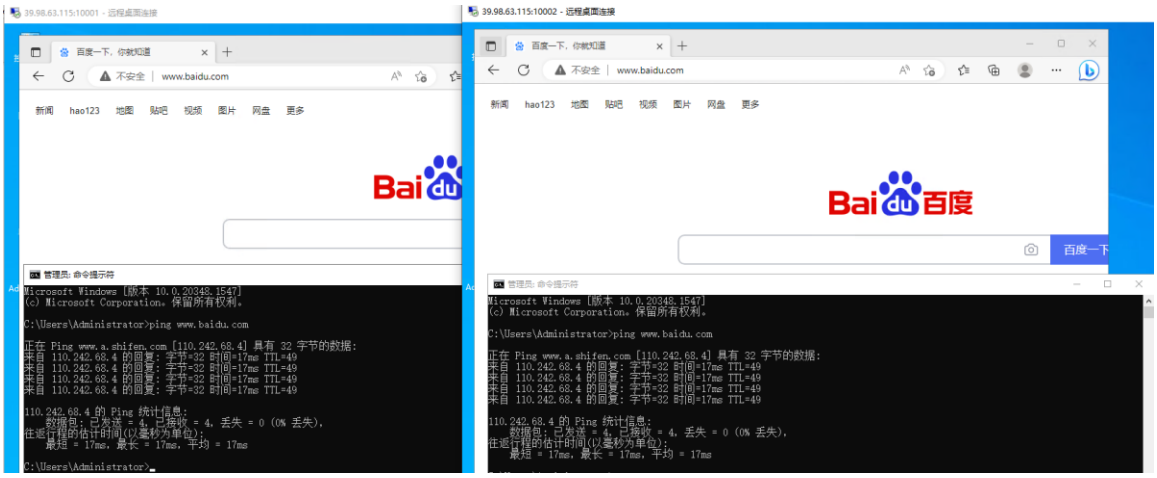


# 5. 业务测试

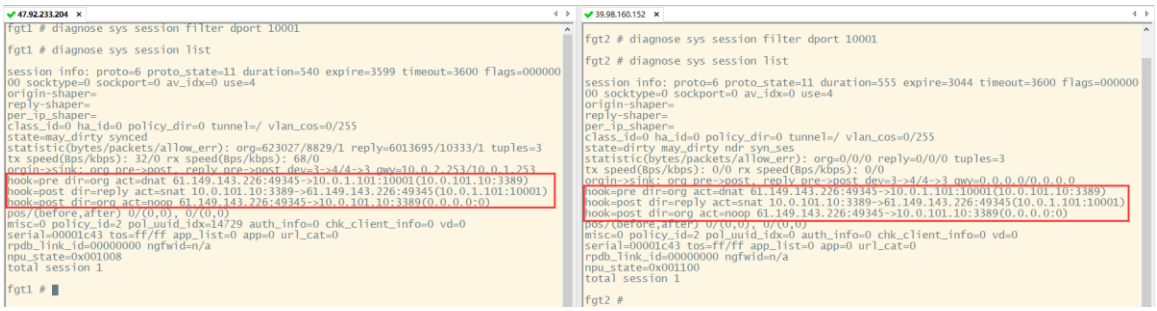
远程桌面访问两台 PC 正常。




两台 PC 访问外网正常。



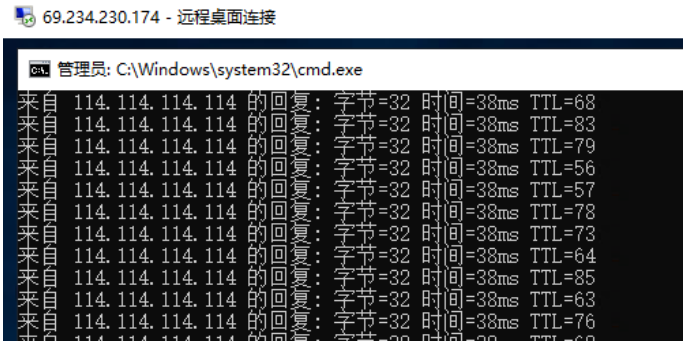
会话同步正常。



# 6. HA 切换测试

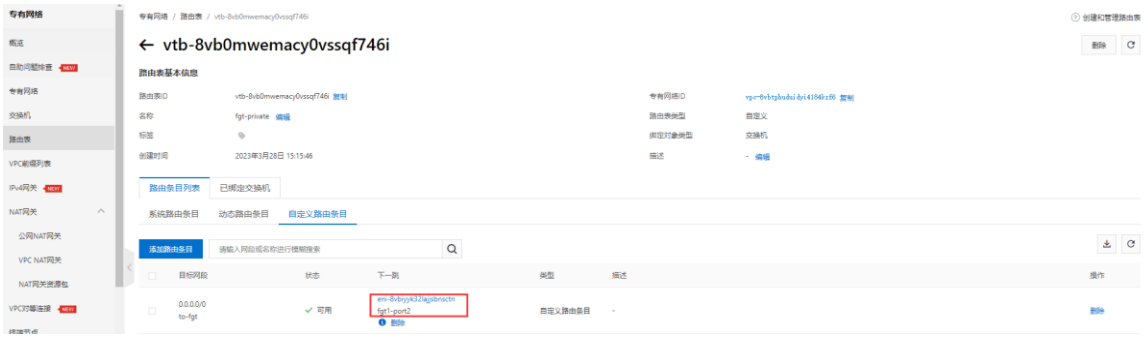
**HA 切换测试目的：**FGT 支持同 AZ 的 HA，查看 HA 切换时，RDP 连接是否会断开，内网 ping 会丢几个包。

从外网 RDP 连接到 pc1 和 pc2，从 pc1 ping 114.114.114.114。



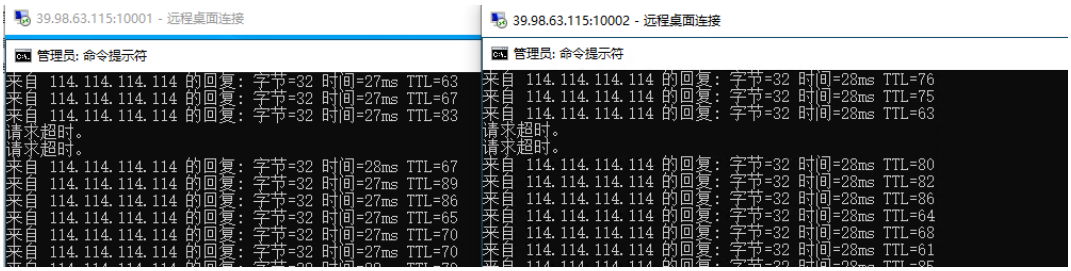

**HA 切换前，FGT1 是主，FGT2 是备：**

fgt-private 路由表默认路由指向 FGT1 port2 网卡。




**重启 FGT2，HA 切换后，FGT2 是主，FGT1 是备：**

RDP 连接闪断，重连后恢复，ping 丢两个包。FortiGate HA 切换除了自身的切换以外，还需要 FortiGate 调用 aliyun API 切换阿里云的路由表。



从 FGT2 debug 可以看出，除了 FGT 本身的 HA 切换以外，还需要更新阿里云 private 路由表的默认路由指向 FGT2 port2。

```
fgt2 # diagnose debug application alicloud-ha -1
Debug messages will be on for 28 minutes.

fgt2 # diagnose debug  enable

fgt2 # HA event
HA state: active
acs is checking eip/route status
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.12
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
send_vip_arp: vd root primary 1 intf port2 ip 10.0.2.12
send_vip_arp: vd root primary 1 intf fortilink ip 10.255.1.1
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
send_vip_arp: vd root primary 1 intf port1 ip 10.0.1.101
acs meta info [ram role]: FortiGateHA
acs is parsing page 1 of total 4(1 page) EIPs
acs local instance: fgt2(i-8vba54a099bit672n4pd)
    eni: 0, 10.0.1.12(eni-8vb53rv5zs34h9lmd23p, port1)
    eni: 1, 10.0.2.12(eni-8vb5rhujx2agqskhgtcy, port2)
    eni: 2, 10.0.3.12(eni-8vb6p82szpqe8sycrmye, port3)
    eni: 3, 10.0.4.12(eni-8vbdyt8dypai3h3dm7tv, port4) <--- 39.98.160.152(eip)
acs peer instance: fgt1(i-8vbh60t1plzr885lp02h)
    eni: 0, 10.0.1.11(eni-8vb3tcu2bmqv7tomkynv, port1)
    eni: 1, 10.0.2.11(eni-8vbiyyk32lajjsbnsctn, port2)
    eni: 2, 10.0.3.11(eni-8vb74tu30voy5suuixl5, port3)
    eni: 3, 10.0.4.11(eni-8vbhqyf9hq0zabd9dqun, port4) <--- 47.92.233.204(eip)
acs route table: vtb-8vb0mwemacy0vssqf746i
    rule: cidr: 0.0.0.0/0, nexthop: 10.0.2.11(eni-8vbiyyk32lajjsbnsctn)
acs is updating route table: vtb-8vb0mwemacy0vssqf746i
acs is deleting route table entry: 0.0.0.0/0 via 10.0.2.11
acs route table entry: Deleting
acs route table entry: Deleting
acs route table entry: Deleted
acs deleted route table entry: 0.0.0.0/0 via 10.0.2.11 successfully
acs is creating route table entry: 0.0.0.0/0 via 10.0.2.12
HA event
acs route table entry: Pending
HA state: active
acs failover process is running
acs route table entry: Pending
acs route table entry: Available
acs created route table entry: 0.0.0.0/0 via 10.0.2.12 successfully
```

fgt-private 路由表默认路由指向 FGT2 NIC2。