

**阿里云跨 AZ 部署 FortiGate HA**

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	3
2. 网络拓扑	3
3. 地址规划	4
4. 配置步骤	5
4.1. 创建 VPC、子网	5
4.2. 创建安全组	6
4.3. 创建 IAM 角色	8
4.4. 创建 FortiGate 实例	10
4.5. 创建弹性网卡	14
4.6. 弹性 IP	17
4.7. 配置 VPC 路由表	18
4.8. 访问 FortiGate	20
4.9. 格式化硬盘	21
4.10. 配置 FortiGate	22
4.11. FortiGate 配置源 NAT	27
4.12. FortiGate 配置目的 NAT	27
5. 业务测试	29
6. HA 切换测试	30

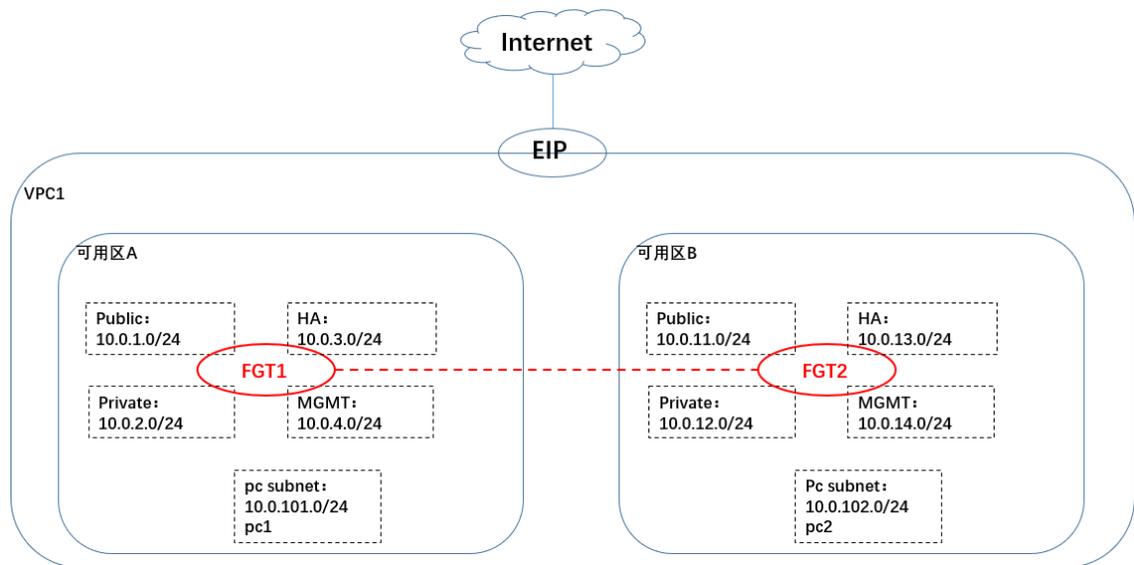
1. 介绍

本文档介绍如何在阿里云跨 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 (AZ-1a)	
Port	阿里云 primary address
Port1	10.0.1.11
Port2	10.0.2.11
Port3	10.0.3.11
Port4	10.0.4.11
FGT2 地址规划 (AZ-1b)	
Port	阿里云 primary address
Port1	10.0.11.11
Port2	10.0.12.11
Port3	10.0.13.11
Port4	10.0.14.11
测试 PC	
PC 名称	测试地址
PC2	10.0.101.10
PC3	10.0.102.20

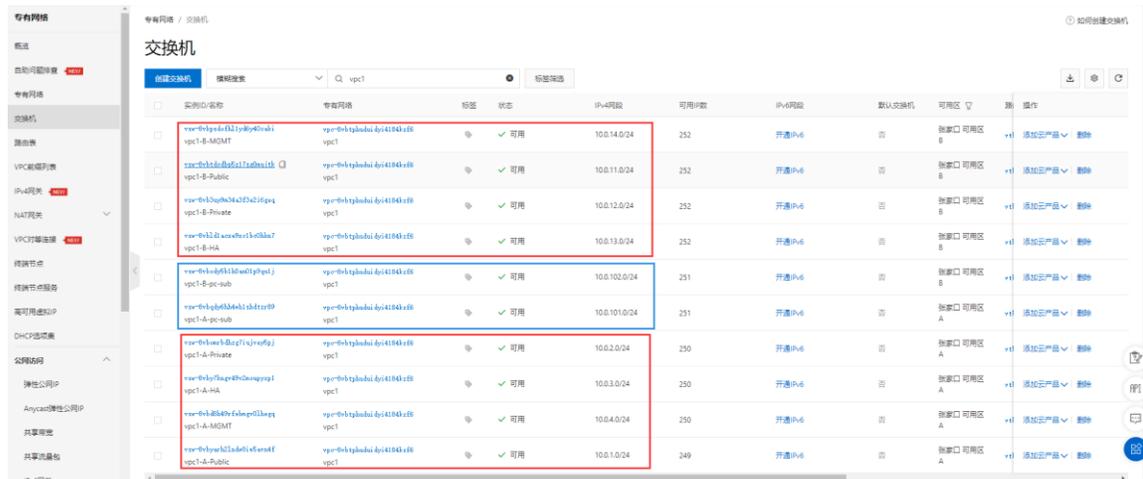
4. 配置步骤

4.1. 创建 VPC、子网

创建 VPC。



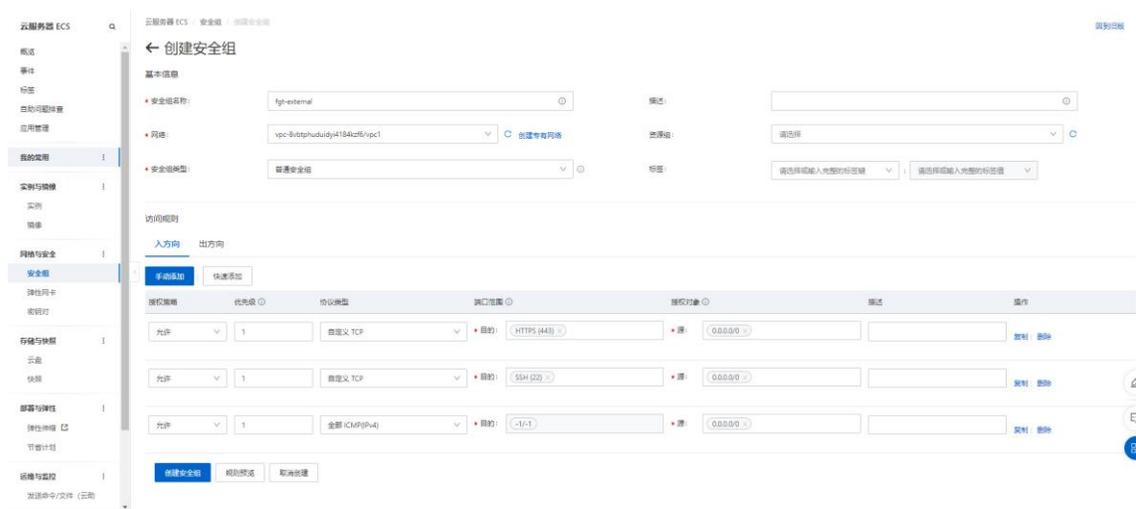
创建子网。



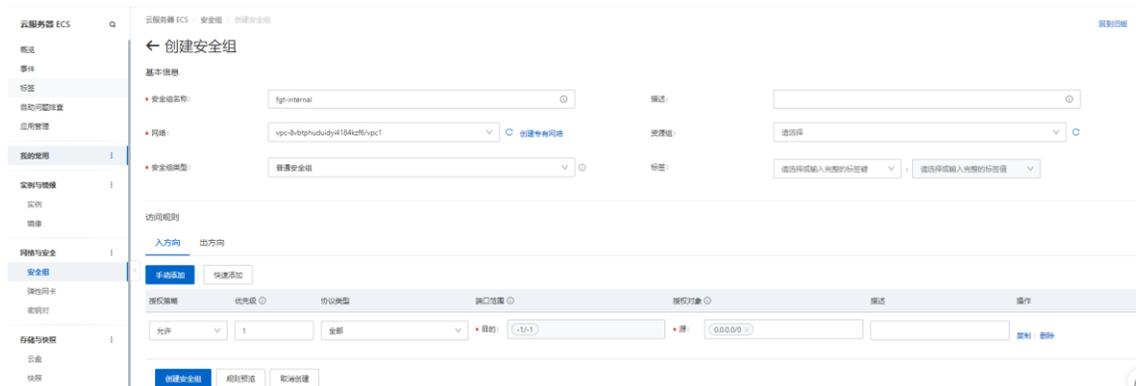
4.2. 创建安全组

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。

云服务平台 ECS 安全组 创建安全组

← 创建安全组

基本信息

- 安全组名称: fgt-mgmt
- 网络: vpc-8-btpghududy4t184kz6/vpc1
- 安全组类型: 普通安全组

访问规则

入方向 出方向

手动添加 快速添加

操作策略	优先级	协议类型	端口范围	源地址	操作
允许	1	自定义 TCP	HTTPS (443)	0.0.0.0	复制 删除
允许	1	自定义 TCP	SSH (22)	0.0.0.0	复制 删除
允许	1	全部 ICMP(v4)	-1/-1	0.0.0.0	复制 删除

创建安全组 取消完成 取消创建

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”。



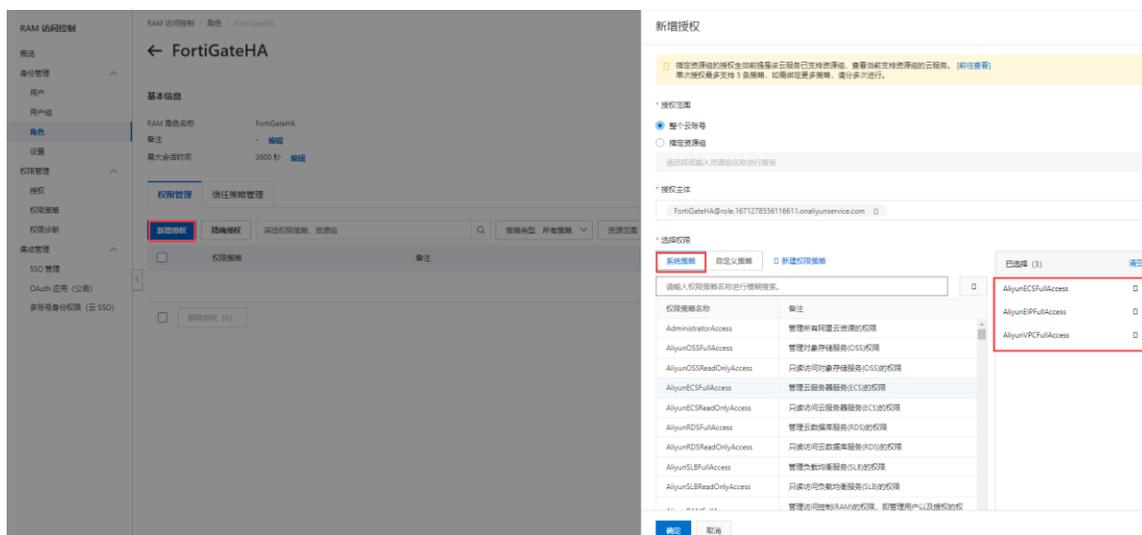
输入“角色名称”，在“选择受信服务”中选择“云服务器”，并点击“完成”。



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）。

实例和镜像

实例

如何选择实例

最近使用规格 **全部规格**

筛选 选择 vCPU 选择内存 模糊搜索规格名称 I/O 优化实例 [查看更多规格参数](#)

架构 **X86 计算** ARM 计算 GPU/FPGA/ASIC 弹性裸金属服务器 超级计算集群

架构: X86 计算 架构-分类: X86 计算-计算型 清除

规格族	实例规格	vCPU	内存	架构-分类	处理器	参考价格
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.large	2 vCPU	<input type="radio"/> X86 计算-通用型	intel	¥ 0.41/时
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.xlarge	4 vCPU	<input checked="" type="radio"/> X86 计算-计算型	intel	¥ 0.821/时
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.2xlarge	8 vCPU	<input type="radio"/> X86 计算-内存型	intel	¥ 1.642/时
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.4xlarge	16 vCPU	<input type="radio"/> X86 计算-通用算力型	intel	¥ 3.283/时
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.8xlarge	32 vCPU	<input type="radio"/> X86 计算-大数据型	intel	¥ 6.567/时
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.13xlarge	52 vCPU	<input type="radio"/> X86 计算-本地 SSD	intel	¥ 10.671/时
<input type="radio"/>	计算平衡增强型 c6e	ecs.c6e.26xlarge	104 vCPU	<input type="radio"/> X86 计算-高主频型	intel	¥ 21.342/时
<input type="radio"/>	计算型 c6	ecs.c6.large	2 vCPU	<input type="radio"/> X86 计算-增强型	intel	-
<input type="radio"/>	计算型 c6	ecs.c6.xlarge	4 vCPU	<input type="radio"/> X86 计算-计算型	intel	-
<input checked="" type="radio"/>	计算型 c6	ecs.c6.2xlarge	8 vCPU	<input type="radio"/> X86 计算-计算型	intel	-

当前选择: 计算型 c6, ecs.c6.2xlarge, 8vCPU 16GiB

1 2 3 4 5 >

在“云市场镜像”选择 FortiGate 版本，这里使用的是 7.0.8。

镜像 ? 最近使用镜像 公共镜像 自定义镜像 共享镜像 **云市场镜像** 荐 社区镜像

当前选择的镜像 飞塔_Fortinet_FortiGate防火墙(BYOL正式版) ?

[重新选择镜像](#)

镜像市场[华北3 (张家口)]

fortigate [搜索](#)

精选镜像

操作系统 292
运行环境 807
管理与监控 82
建站系统 94
应用开发 40
数据库 112
服务器软件 60
企业应用 13
云安全市场 78

全部操作系统 全部架构 按分值筛选

Fortinet FortiManager 集中管理平台	基础系统: linux 架构: 64位 最新更新: 2022-07-28	v6.2.2	★★★★★ 32人已使用	¥0 /时	使用
飞塔_Fortinet_FortiGate防火墙(BYOL正式版)	基础系统: linux 架构: 64位 最新更新: 2022-10-31 FortiGate: 以更低的复杂性提供业内首屈一指的威胁防护和性能。...	V7.0.8	★★★★★ 216人已使用	¥0 /时	使用
Fortinet FortiGate (BYOL) 下一代防火墙	基础系统: linux 架构: 64位 最新更新: 2022-07-28 本产品许可方式为BYOL, 需自行导入License。 Fortinet FortiGate...	v6.2.2	★★★★★ 34人已使用	¥0 /时	使用
飞塔_Fortinet_FortiGate防火墙(免费试用版)	基础系统: linux 架构: 64位 最新更新: 2022-07-28 免费测试需使用1CPU的ECS实例。 FortiGate下一代防火墙产品采...	V6.2.4	★★★★★ 75人已使用	¥0 /时	使用
Fortinet FortiGate (BYOL) 下一代防火墙	基础系统: linux 架构: 64位 最新更新: 2022-07-28 本产品许可方式为BYOL, 需自行导入License。 Fortinet FortiGate...	v6.2.2	★★★★★ 39人已使用	¥0 /时	使用

共有7条 < 1 2 >

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。

存储

系统盘

类型	容量	数量	IOPS	性能	操作
ESSD云盘	40 GiB	1	3800	PL1 (单盘IOPS性能上限5万)	<input type="checkbox"/> 加密

云盘性能 不同云盘性能不同, 各云盘性能指标>

数据盘

+ 添加数据盘 (1/16)

类型	容量	数量	IOPS	性能	操作
ESSD云盘	40 GiB	1	3800	PL1 (单盘IOPS性能上限5万)	<input checked="" type="checkbox"/> 系统默认分配设备名 <input checked="" type="checkbox"/> 随实例释放 <input type="checkbox"/> 加密 用快照创建磁盘

快照服务 荐

系统盘快照策略 请选择系统盘自动快照策略 [创建自动快照策略](#)

数据盘快照策略 请选择数据盘自动快照策略 [创建自动快照策略](#)

快照服务特性 快照服务能定时对云盘进行备份, 可应对病毒感染、数据误删等风险。快照价格 (按量付费, 每小时扣费) >

使用须知 此次应用的快照策略仅针对此次创建的云盘进行保护, 后续新创建的云盘需要单独应用快照策略

共享盘 NAS (可选)

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。

带宽和安全组

公网 IP 分配公网 IPv4 地址
 不为实例分配公网 IP 地址，如需访问公网，请配置并 [绑定弹性公网 IP 地址](#)，或者购买实例后升级实例的带宽，系统会自动为实例分配公网 IP

安全组 ^② [已有安全组](#) [新建安全组](#)

如何配置安全组 [重新选择安全组](#)

1) fgt-external / sg-8vbcvjro0v320v7tzz9 (已有 1 个实例+辅助网卡，还可以加入 1999 个实例+辅助网卡)

使用须知 请确保所选安全组开放包含 22 (Linux) 或者 3389 (Windows) 端口，否则无法远程登录ECS，[前往设置](#)

▼ 弹性网卡 | IPv6 (选填)

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。

管理设置

登录凭证

如需[远程登录实例](#)，可在实例创建后通过控制台“重置实例密码”操作完成设置。

标签 [+ 添加标签 \(0 / 20\)](#)

如何设计标签 标签由区分大小写的键值对组成。您设置的标签将应用在本次创建的全部实例和云盘

设置“实例名称”，选择“实例 RAM 角色”为“FortiGateHA”。

▲ 高级选项 (选填) 实例名称 | 描述 | 主机名 | 有序后缀 | 实例释放保护 | 实例RAM角色 | 元数据访问模式 | 自定义数据 | 资源组 | 部署集 | 专有宿主机 | 私有池类型

实例名称 4 / 128
 如何自定义有序实例名称

描述 0 / 256

主机名 0 / 64
 如何自定义有序主机名

有序后缀 为实例名称和主机名添加有序后缀

实例释放保护 防止通过控制台或API误删除释放

实例RAM角色 ^① [创建实例RAM角色](#)

元数据访问模式

自定义数据 ^① 输入已采用 Base64 编码
 Linux 操作系统支持 shell 脚本；Windows 操作系统支持 bat 和 powershell 两种格式，在 Base64 编码前，第一行为 [bat] 或者 [powershell]，最大支持16KB

资源组 ^② [创建资源组](#)

部署集 [管理部署集](#)

专有宿主机 [创建专有宿主机](#)

私有池类型 [资源预定](#)

查看实例当前配置，确认无误后点击“确认下单”。

购买实例数量

使用时限 设置自动释放服务时间

配置概要

付费类型	按量付费
地域	华北3 (张家口)
可用区	华北3 可用区 A
网络类型	专有网络
专有网络	vpc1 / vpc-8vbtphuidiyi4184kzf6
交换机	vpc1-A-Public / vsw-8vbyarh2lndw8iw5avn4f
私网IP地址	10.0.1.11
实例规格	计算型 c6 / ecs.c6.2xlarge (8vCPU 16GiB)
镜像	飞塔_Fortinet_FortiGate防火墙(BYOL 正式版) V7.0.8
系统盘	ESSD云盘 40GiB 不随实例释放 PL1 (单盘IOPS性能上限5万)
数据盘	1 块...
公网带宽	您没有为实例分配公网IP地址
安全组	fgt-external / sg-8vbcrvjro0v320v7tzz9

配置费用：¥ 1.258/时

镜像费用：¥ 0.000/时

[查看明细](#)

《云服务器 ECS 服务条款》 | 《镜像商品使用条款》

确认下单

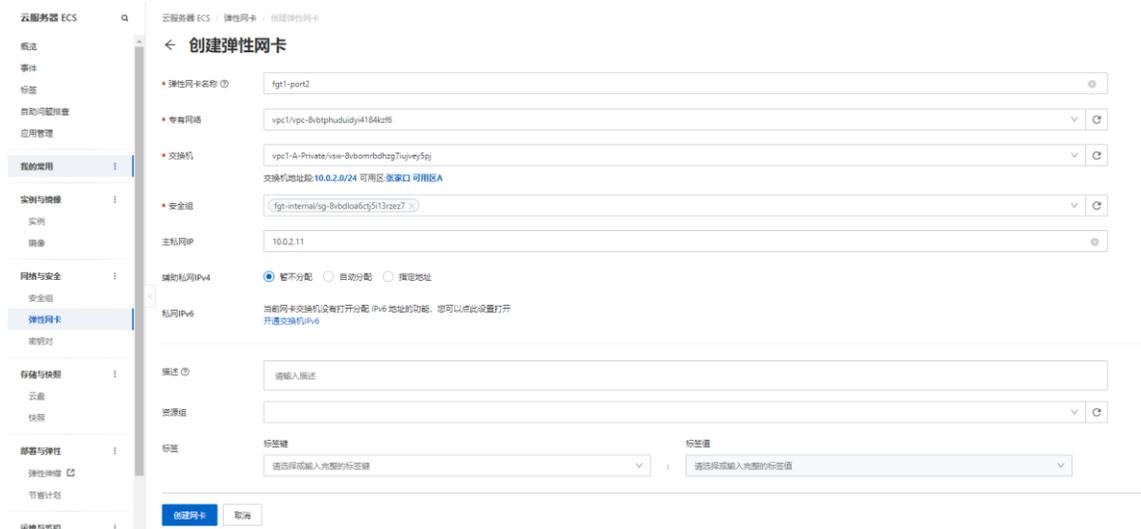
实例创建完成。同理创建可用区 B 的 FortiGate 实例。

实例 ID / 名称	状态	标签	操作面板	监控	可用区	配置	IP 地址	计费方式	网络类型	操作
i-bd817s3uqem-4d0cng-fgt2	运行中				华北3 (张家口) B	8vCPU 16 GB 0 Mbps ecs.e6.2xlarge	10.0.1.11 (私网)	按量付费 2023年3月29日 09:30:00创建	专有网络	远程连接 资源变配 停止 启动
i-bd9ca273oog74ehqhw-fgt1	运行中				华北3 (张家口) A	8vCPU 16 GB 0 Mbps ecs.e6.2xlarge	10.0.1.11 (私网)	按量付费 2023年3月29日 09:29:00创建	专有网络	远程连接 资源变配 停止 启动

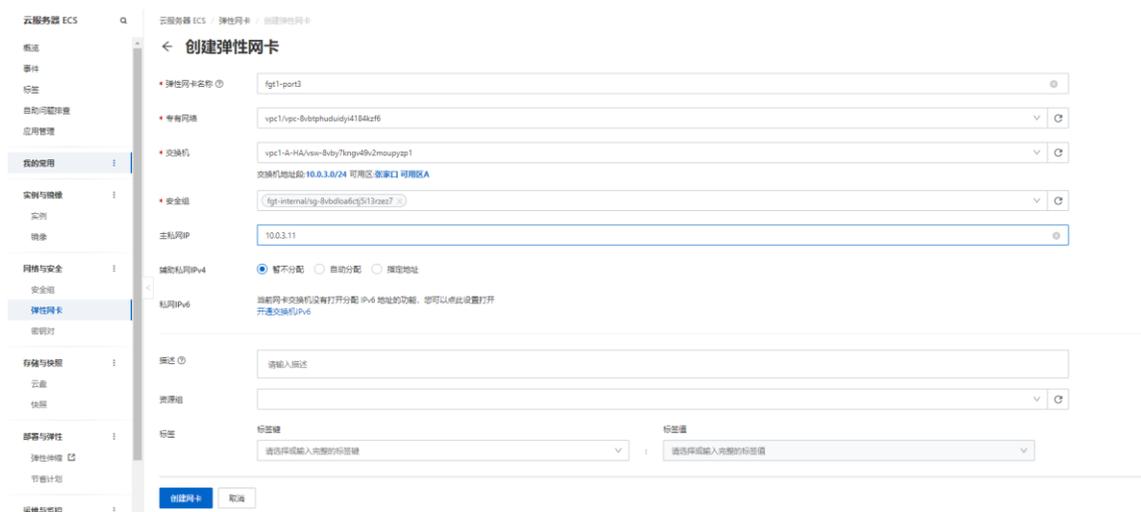
4.5. 创建弹性网卡

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”。

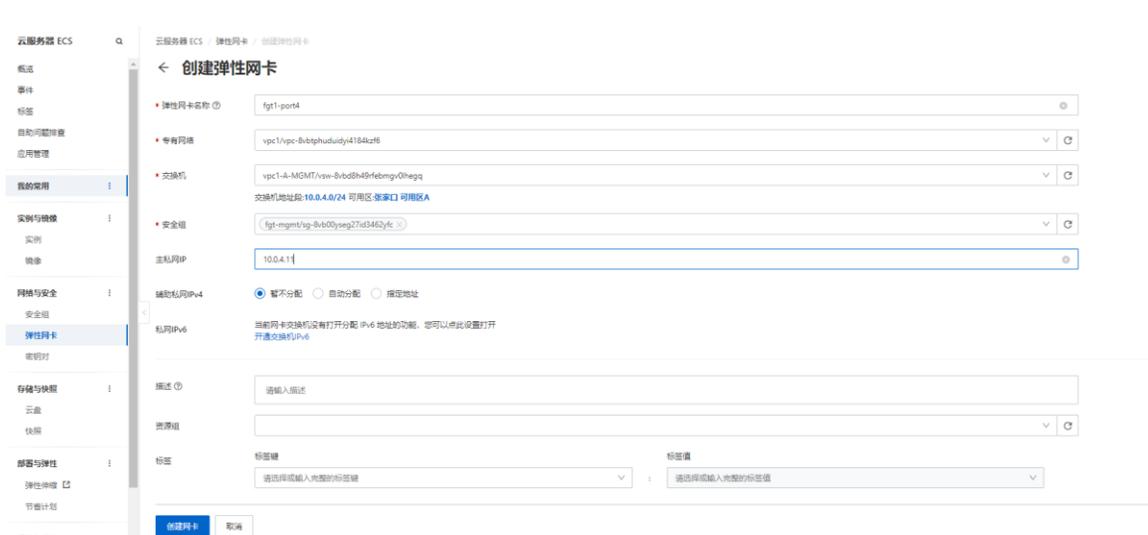
创建弹性网卡 fgt1-port2，配置“弹性网卡名称”，专有网络选择 vpc1，交换机选择 port2 的所在的子网 vpc1-A-Private，安全组选择“fgt-internal”，主私网 IP 指定为 10.0.2.11。



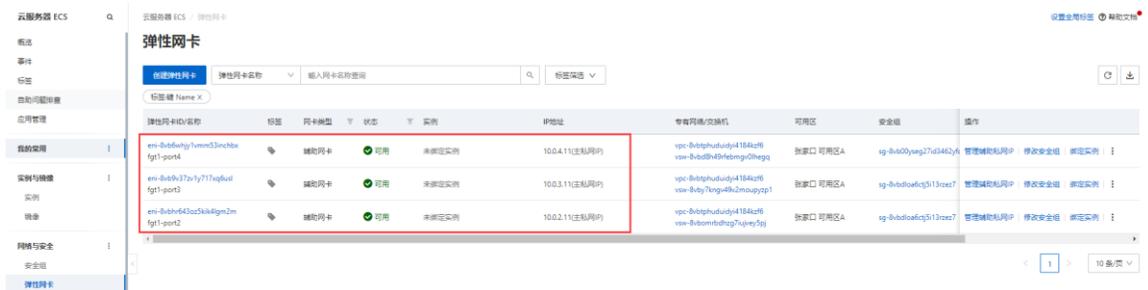
创建弹性网卡 fgt1-port3，配置“弹性网卡名称”，专有网络选择 vpc1，交换机选择 port3 的所在的子网 vpc1-A-HA，安全组选择“fgt-internal”，主私网 IP 指定为 10.0.3.11。



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。



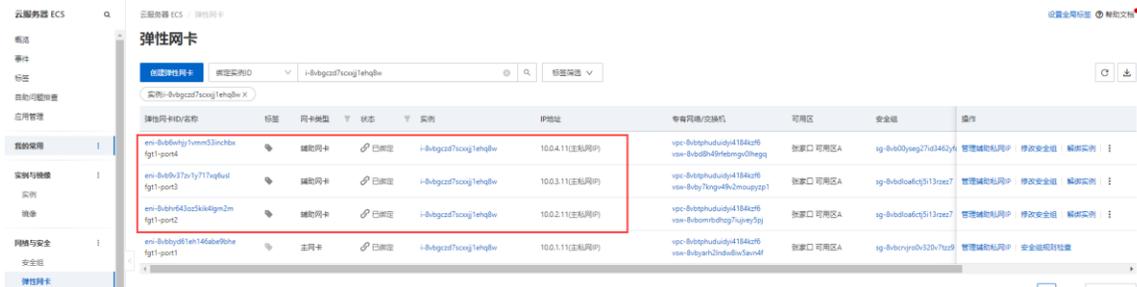
FGT1 实例 3 块网卡创建完成。



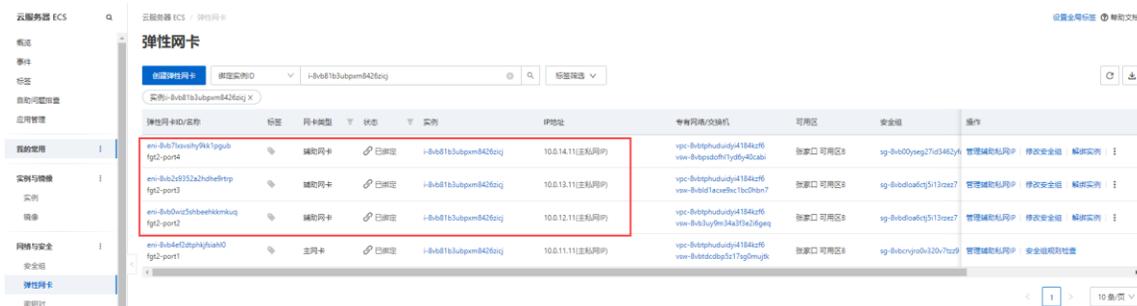
将 3 块网卡分别绑定到 FGT1 实例，port2 绑定成功后，再绑定 port3，最后绑定 port4。



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. 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 fgt1-port4 10.0.4.11。

一个弹性 IP 关联 FGT2 实例 fgt2-port4 10.0.14.11。

关联 FGT HA 的 Master 实例（当前 FGT1） fgt1-port1 的地址 10.0.0.11。

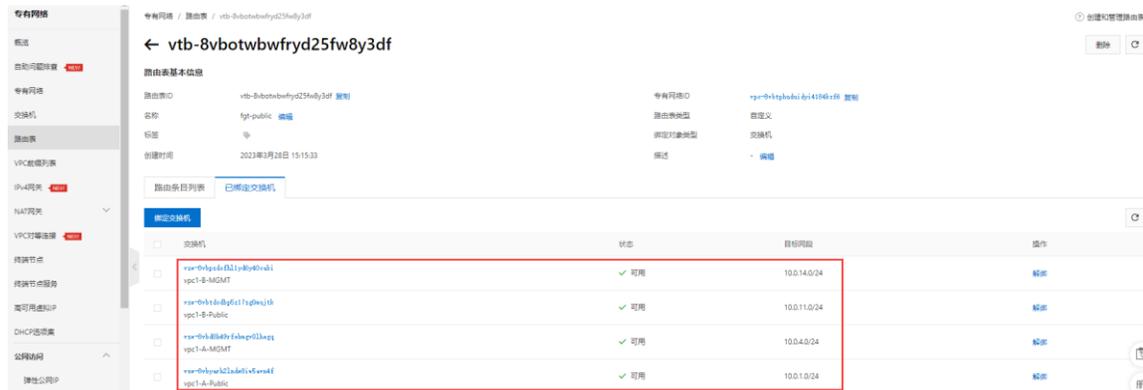
临时配置 FGT2 的弹性 IP:

一个弹性 IP 关联 FGT2 实例 fgt2-port1 10.0.11.11。

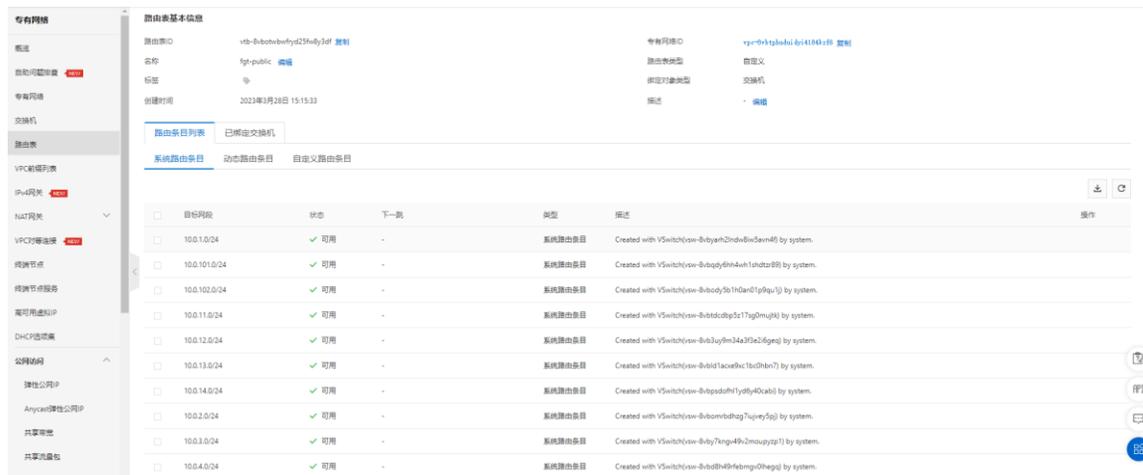
实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称	实例ID名称
ep-8k80qg30p5e3cd8c11	弹性公网IP	39.98.234.42	-	发起申请	200 Mbps	按使用流量计费	未加入实例的保留	已分配	ECS实例	i-8k80qg30p5e3cd8c11	弹性公网IP	释放
ep-8k80qg30p5e3cd8c11	弹性公网IP	39.98.234.232	-	发起申请	200 Mbps	按使用流量计费	未加入实例的保留	已分配	ECS实例	i-8k80qg30p5e3cd8c11	弹性公网IP	释放
ep-8k80qg30p5e3cd8c11	弹性公网IP	39.98.234.140	-	发起申请	200 Mbps	按使用流量计费	未加入实例的保留	已分配	ECS实例	i-8k80qg30p5e3cd8c11	弹性公网IP	释放
ep-8k80qg30p5e3cd8c11	弹性公网IP	39.98.234.76	-	发起申请	200 Mbps	按使用流量计费	未加入实例的保留	已分配	ECS实例	i-8k80qg30p5e3cd8c11	弹性公网IP	释放

4.7. 配置 VPC 路由表

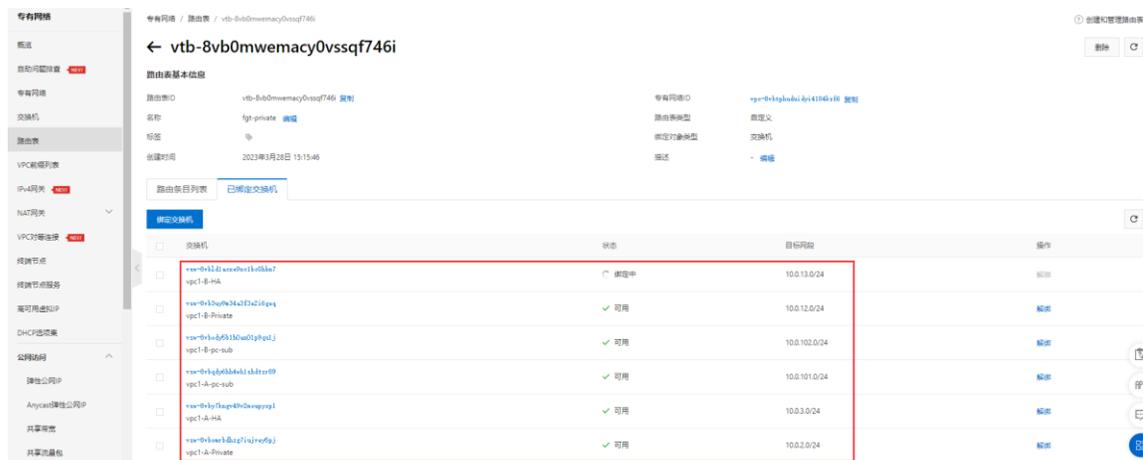
新建 fgt-public 路由表，关联 public 和 mgmt 子网（10.0.1.0/24，10.0.11.0/24，10.0.4.0/24，10.0.14.0/24）4 个子网。



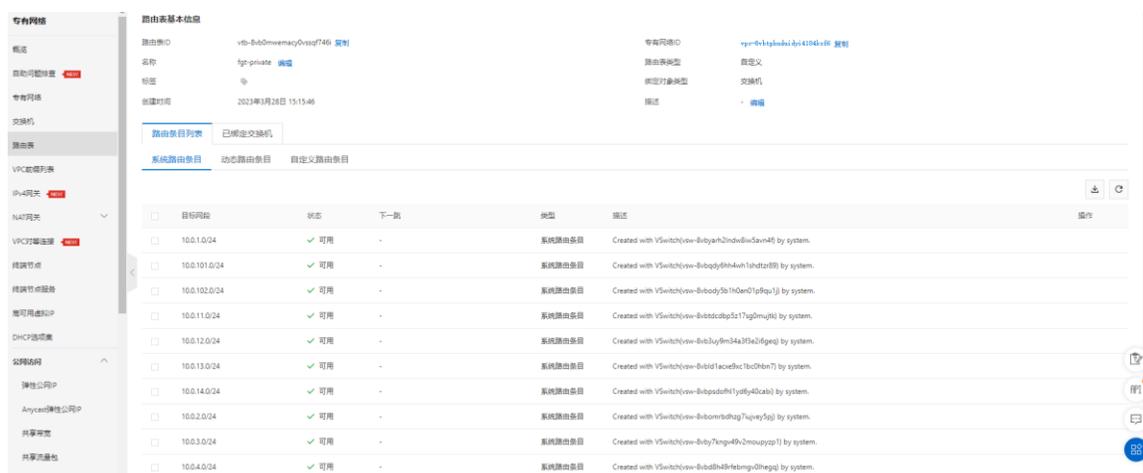
fgt-public 路由表系统自带路由。



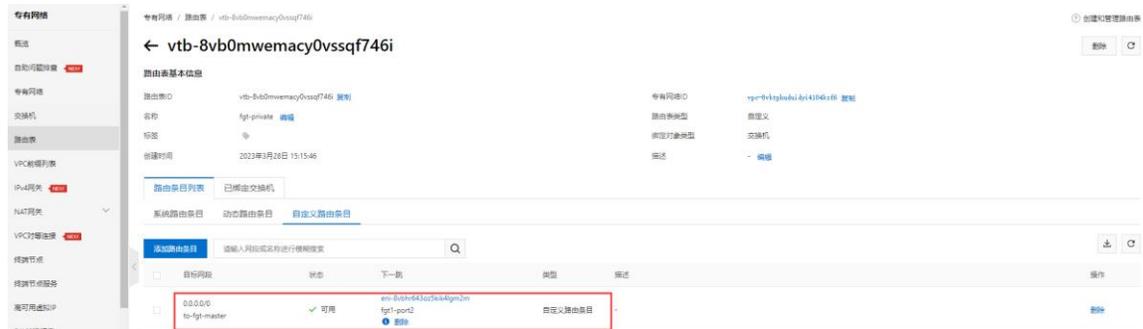
新建 fgt-private 路由表，关联 private 子网，ha 子网，pc 子网（10.0.2.0/24，10.0.3.0、24，10.0.12.0/24，10.0.13.0/24，10.0.101.0/24，10.0.102.0/24）6 个子网。



Private 路由表系统自带路由。



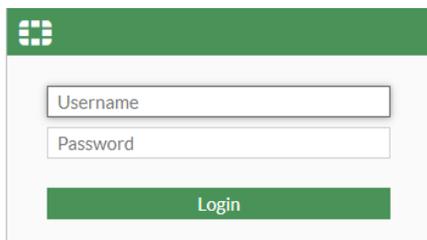
fgt-private 默认路由指向 FGT HA Master（当前 FGT1）实例的 port2 的接口 ID。



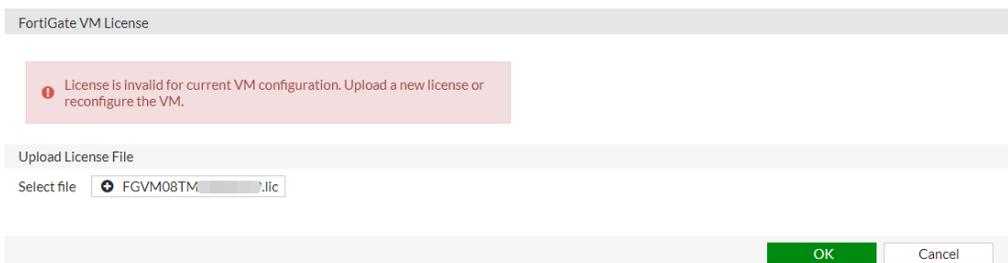
4.8. 访问 FortiGate

HTTPS 访问 FGT1，同理访问 FGT2：

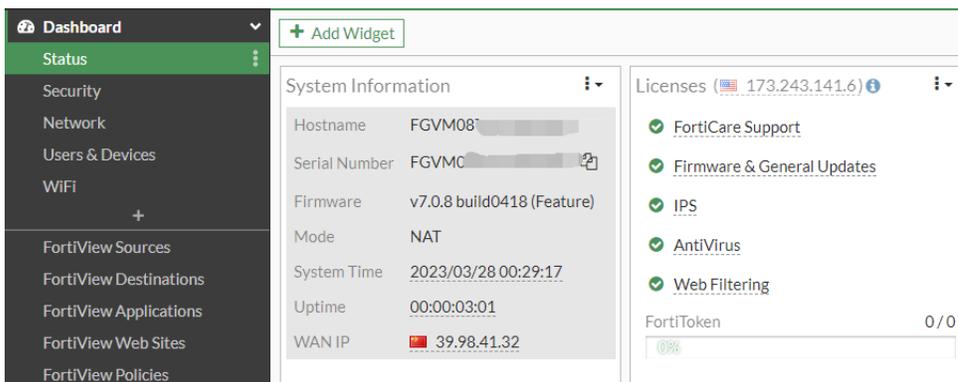
使用 <https://39.98.234.62/>（弹性 IP）访问 FortiGate，账号是 admin，密码默认是实例 ID。首次登录后，请按照提示修改密码。



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。

4.9. 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 # 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. 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 10.0.1.253  #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
  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
#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
  edit 4
    set object firewall.ippool
  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 10.0.11.253 #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 10.0.12.253 #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 10.0.11.11 255.255.255.0
    set allowaccess ping https ssh
  next
  edit "port2"
    set mode static
    set ip 10.0.12.11 255.255.255.0
    set allowaccess ping
  next
  edit "port3"
    set mode static
```

```
        set ip 10.0.13.11 255.255.255.0
        set allowaccess ping
    next
    edit "port4"
        set mode static
        set ip 10.0.14.11 255.255.255.0
        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
    edit 4
        set object firewall.ippool
    next
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 10.0.3.11
PING 10.0.3.11 (10.0.3.11): 56 data bytes
64 bytes from 10.0.3.11: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.0.3.11: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.0.3.11: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.0.3.11: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.0.3.11: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.0.3.11 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

注意: FortiGate 跨可用区 HA 中, 由于可用区 A 和可用区 B 的地址是不一样的, 因为两台 FortiGate 是无法共享相同的 NAT 地址池或者目的 NAT 的虚拟 IP, 所以 NAT 环境下会话同步没有意义, 不需要在 HA 配置中开启会话同步。

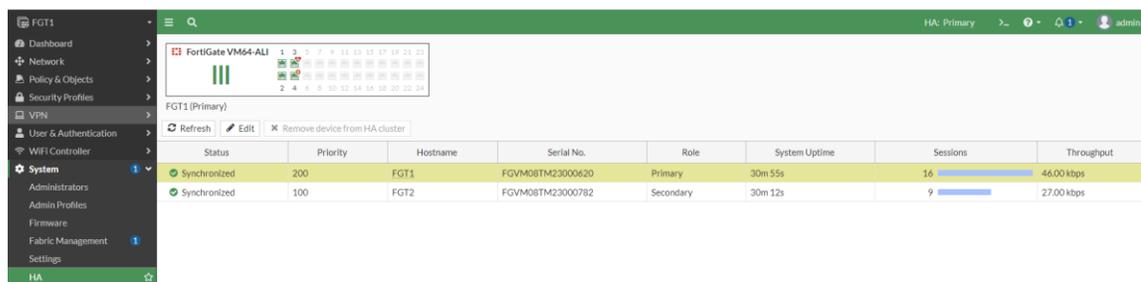
FGT1 HA 配置:

```
config system ha
  set group-name "FGTHA"
  set mode a-p
  set password fortinet
  set hbdev "port3" 50
  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 10.0.13.11
end
```

FGT2 HA 配置:

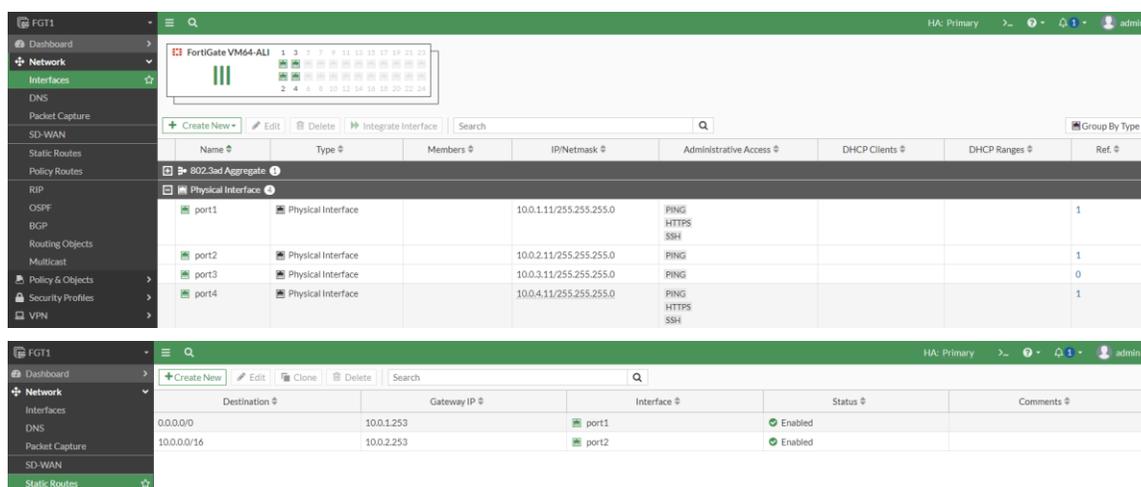
```
config system ha
  set group-name "FGTHA"
  set mode a-p
  set password fortinet
  set hbdev "port3" 50
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
      set gateway 10.0.14.253
    next
  end
  set override disable
  set priority 100
  set unicast-hb 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。

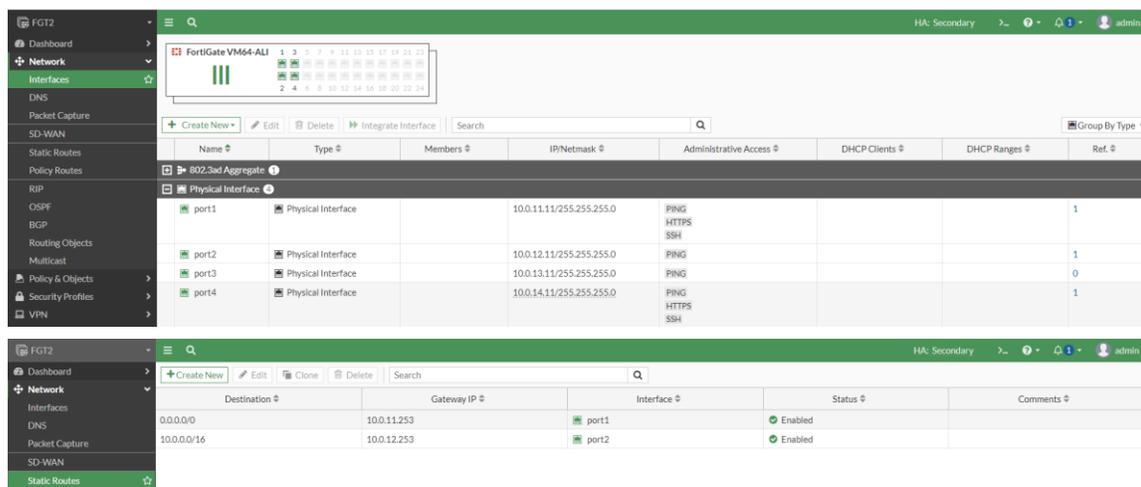


现在可以使用 FortiGate 实例 port4 关联的弹性 IP 进行访问，此时可以删除临时的弹性 IP。

FGT1 接口 IP 及路由：



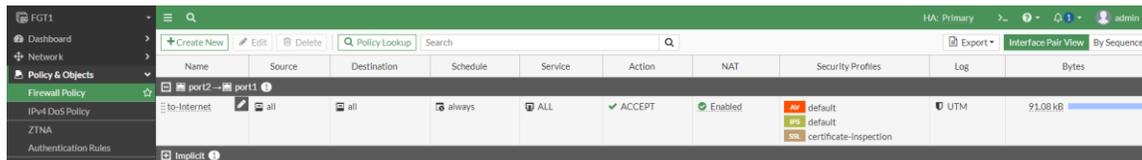
FGT2 接口 IP 及路由：



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:



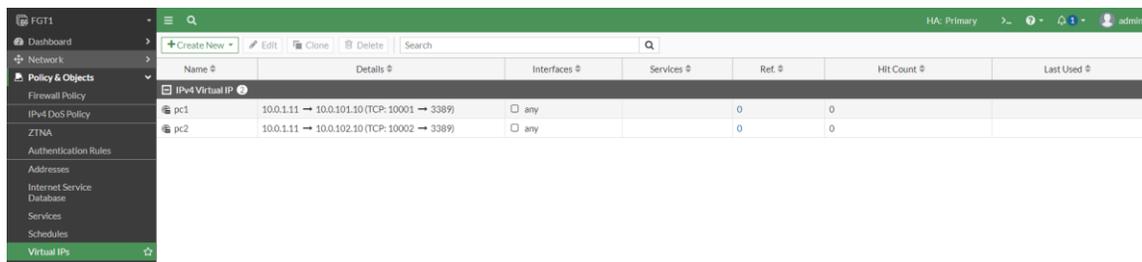
4.12. FortiGate 配置目的 NAT

创建两个 PC 实例。

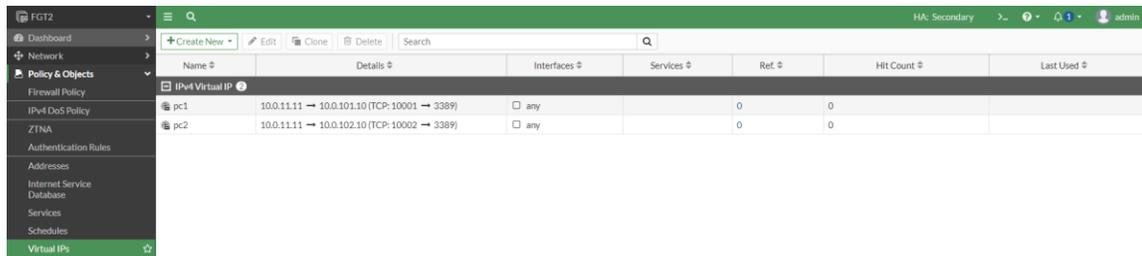


使用 port1 接口的地址做目的 NAT:

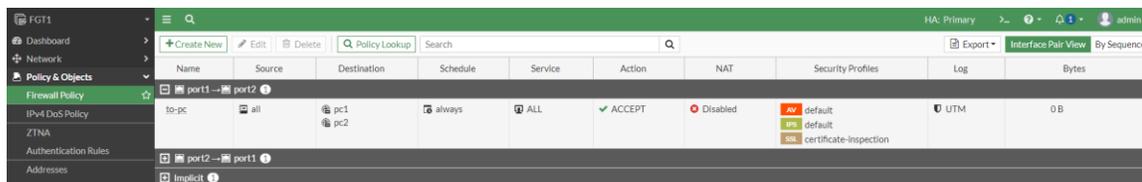
FGT1 配置 VIP, 名称 pc1 和 pc2, 将两个 PC 的 3389 端口映射出去, 对外的端口分别是 FGT1 port1 接口 ip 的 10001 和 10002:



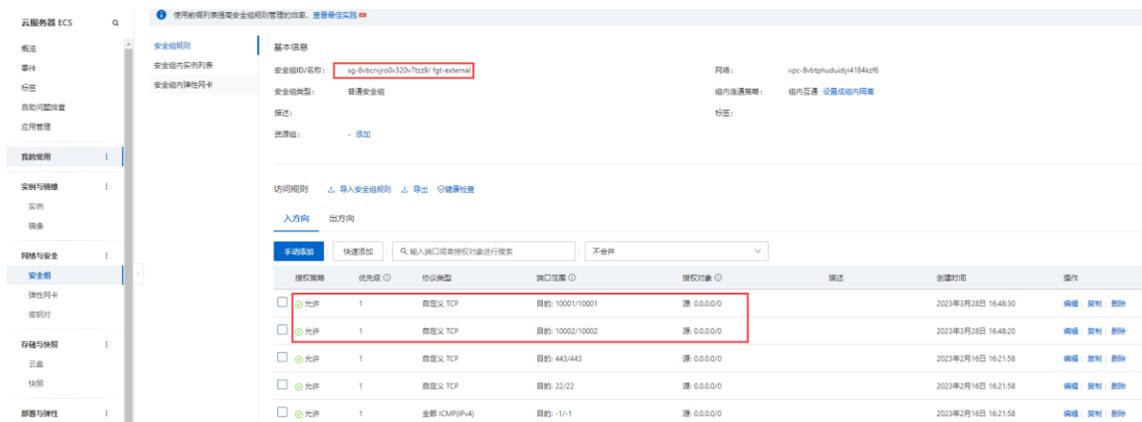
FGT2 配置 VIP，名称是 pc1 和 pc2，要和 FGT1 的 VIP 名称一样，这样防火墙策略才能够同步。将两个 PC 的 3389 端口映射出去，对外的端口分别是 FGT2 port1 接口 ip 的 10001 和 10002



FGT1 配置防火墙策略调用此 VIP，会同步给 FGT2:

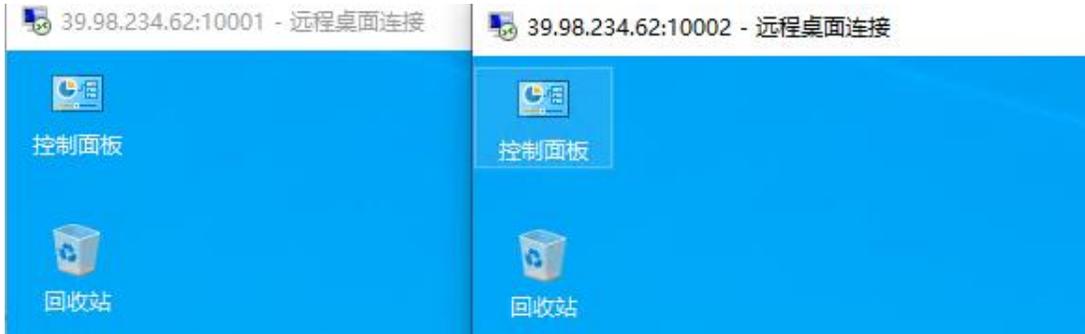


FortiGate 实例 port1 安全组 fgt-external 放通 10001, 10002 这两个对外的端口。

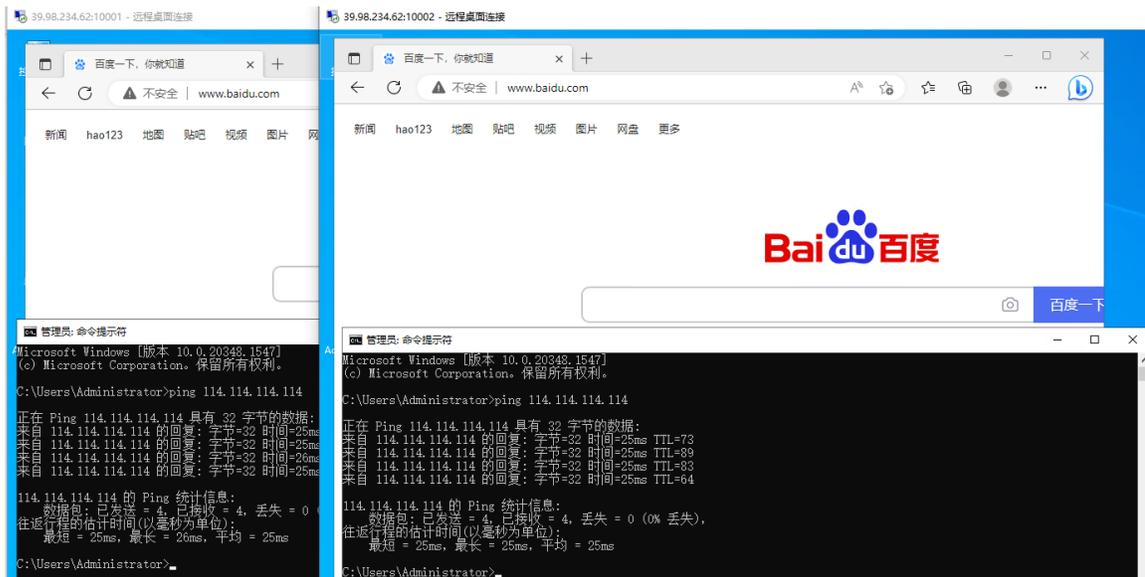


5. 业务测试

远程桌面访问两台 PC 正常。



两台 PC 访问外网正常。



6. HA 切换测试

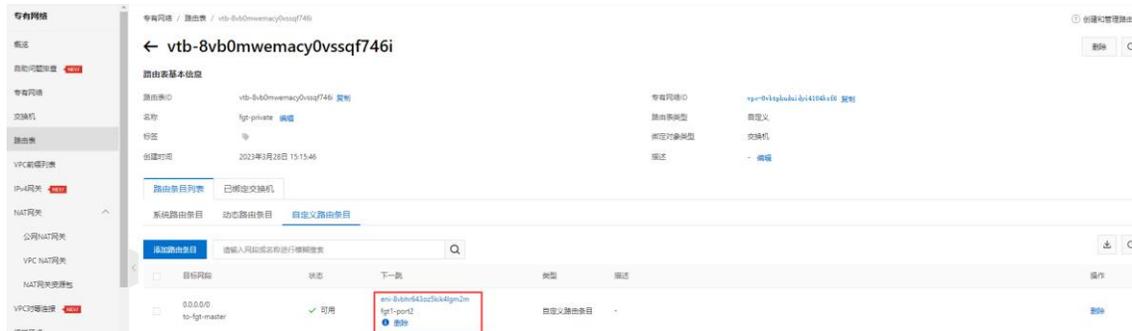
HA 测试目的：FGT 支持跨 AZ 的 HA，但不同 AZ 的地址段不一样，无法共享相同的地址池和目的 NAT 虚拟 IP，因此 SNAT 和 DNAT 的会话同步无意义，HA 切换后 SNAT 和 DNAT 的连接会断开，需要重新连接。查看 HA 切换时，pc ping 114.114.114.114 丢几个包。

HA 切换前，FGT 是主，FGT2 是备：

FortiGate HA 集群的弹性 IP 关联到 FGT1 实例。

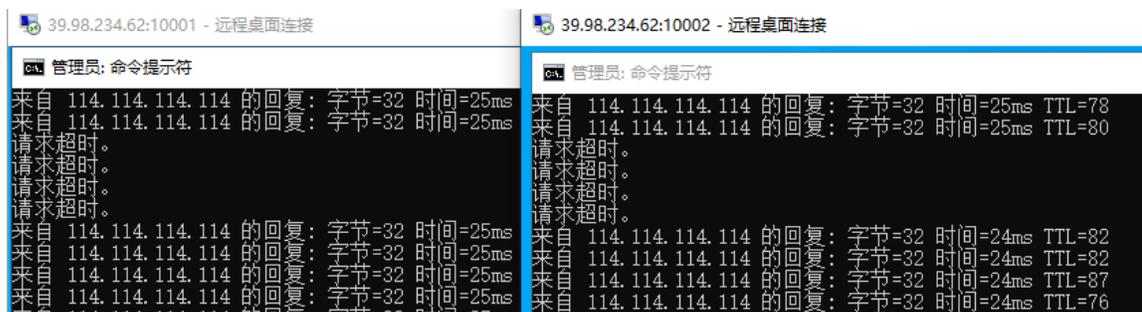


Private 路由表默认路由指向 FGT1 fgt-port2 网卡。



重启 FGT2，HA 切换后，FGT2 是主，FGT1 是备：

Ping 丢 4 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，更新阿里云 private 路由表的默认路由指向 FGT2 fgt2-port2 接口。

```
FGT2 # diagnose debug application alicloud-ha -l
```

```
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 10.0.11.11
send_vip_arp: vd root primary 1 intf port2 ip 10.0.12.11
send_vip_arp: vd root primary 1 intf fortalink ip 10.255.1.1
send_vip_arp: vd root primary 1 intf port1 ip 10.0.11.11
send_vip_arp: vd root primary 1 intf port1 ip 10.0.11.11
acs meta info [ram role]: FortiGateHA
acs is parsing page 1 of total 4(1 page) EIPs
acs local instance: fgt2(i-8vb81b3ubpxm8426zicj)
eni: 0, 10.0.11.11(eni-8vb4ef2dtpkhjfsiah10, port1)
eni: 1, 10.0.12.11(eni-8vb0wiz5shbeehkkmkuq, port2)
eni: 2, 10.0.13.11(eni-8vb2s9352a2hdhe9rtrp, port3)
eni: 3, 10.0.14.11(eni-8vb71xsvsihy9kk1pgub, port4) <--- 39.98.238.78(eip)
acs peer instance: fgt1(i-8vbgczd7scxxjjlehq8w)
eni: 0, 10.0.1.11(eni-8vbbyd61eh146abe9bhe, port1) <--- 39.98.234.62(eip)
eni: 1, 10.0.2.11(eni-8vbhr643oz5kik41gm2m, port2)
eni: 2, 10.0.3.11(eni-8vb9v37zv1y71xq6usl, port3)
eni: 3, 10.0.4.11(eni-8vb6whjy1vmm53inchbx, port4) <--- 39.98.235.140(eip)
acs is moving eip(39.98.234.62) from eni0(10.0.1.11) to eni0(10.0.11.11)
acs eip(39.98.234.62) status: Unassociating
acs eip(39.98.234.62) status: Unassociating
acs eip(39.98.234.62) status: Available
acs unassociated eip(39.98.234.62) from peer instance fgt1 successfully
acs eip(39.98.234.62) status: Associating
HA event
acs eip(39.98.234.62) status: Associating
HA state: active
acs failover process is running
acs eip(39.98.234.62) status: InUse
acs associated eip(39.98.234.62) to instance fgt2 successfully
acs local instance: fgt2(i-8vb81b3ubpxm8426zicj)
eni: 0, 10.0.11.11(eni-8vb4ef2dtpkhjfsiah10, port1) <--- 39.98.234.62(eip)
eni: 1, 10.0.12.11(eni-8vb0wiz5shbeehkkmkuq, port2)
eni: 2, 10.0.13.11(eni-8vb2s9352a2hdhe9rtrp, port3)
eni: 3, 10.0.14.11(eni-8vb71xsvsihy9kk1pgub, port4) <--- 39.98.238.78(eip)
acs peer instance: fgt1(i-8vbgczd7scxxjjlehq8w)
eni: 0, 10.0.1.11(eni-8vbbyd61eh146abe9bhe, port1)
eni: 1, 10.0.2.11(eni-8vbhr643oz5kik41gm2m, port2)
eni: 2, 10.0.3.11(eni-8vb9v37zv1y71xq6usl, port3)
eni: 3, 10.0.4.11(eni-8vb6whjy1vmm53inchbx, port4) <--- 39.98.235.140(eip)
acs route table: vtb-8vb0mwemacy0vssqf746i
rule: cidr: 0.0.0.0/0, nexthop: 10.0.2.11(eni-8vbhr643oz5kik41gm2m)
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 10.0.12.11
acs route table entry: Pending
acs route table entry: Available
acs created route table entry: 0.0.0.0/0 via 10.0.12.11 successfully
acs route table: vtb-8vb0mwemacy0vssqf746i
rule: cidr: 0.0.0.0/0, nexthop: 10.0.12.11(eni-8vb0wiz5shbeehkkmkuq)
```

弹性 IP 重新绑定到 FGT2 实例。



Private 路由表默认路由指向 FGT2 fgt2-port2 接口。

