



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	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	15
4.6. 创建高可用虚拟 IP	18
4.7. 弹性 IP	20
4.8. 配置 VPC 路由表	21
4.9. 访问 FortiGate	23
4.10. 格式化硬盘	24
4.11. 配置 FortiGate	24
4.12. FortiGate 配置源 NAT	28
4.13. FortiGate 配置目的 NAT	28
5. 业务测试	30
6. HA 切换测试	31

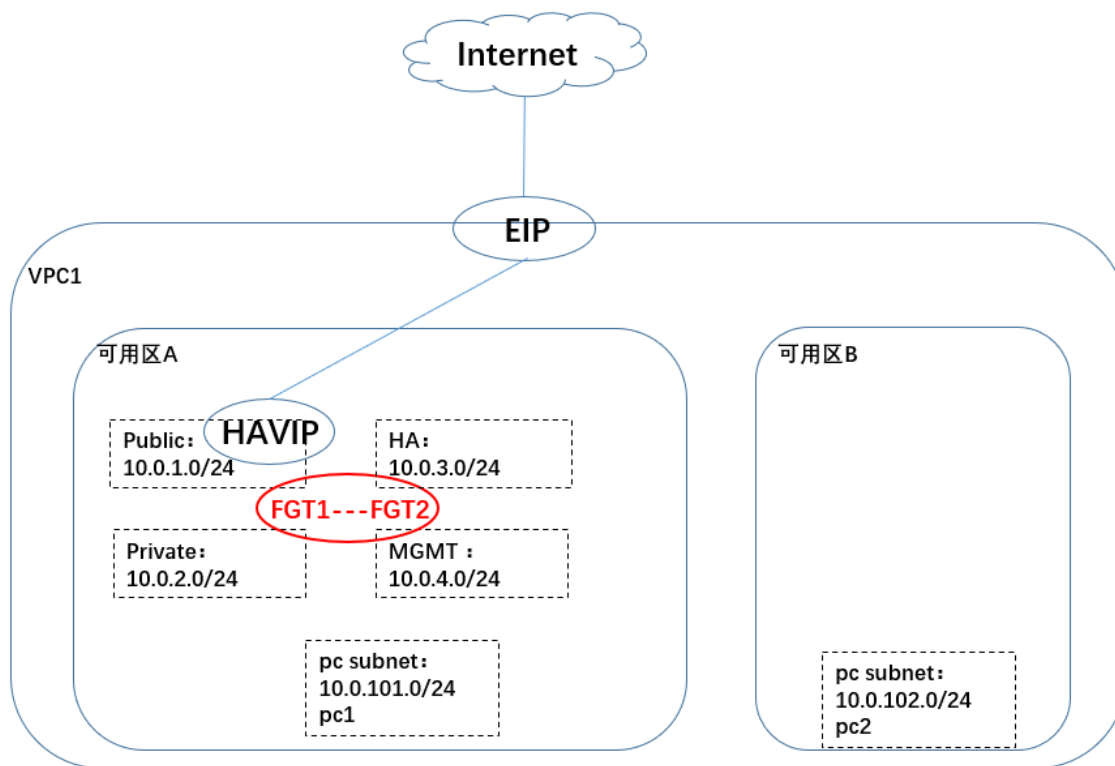
1. 介绍

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

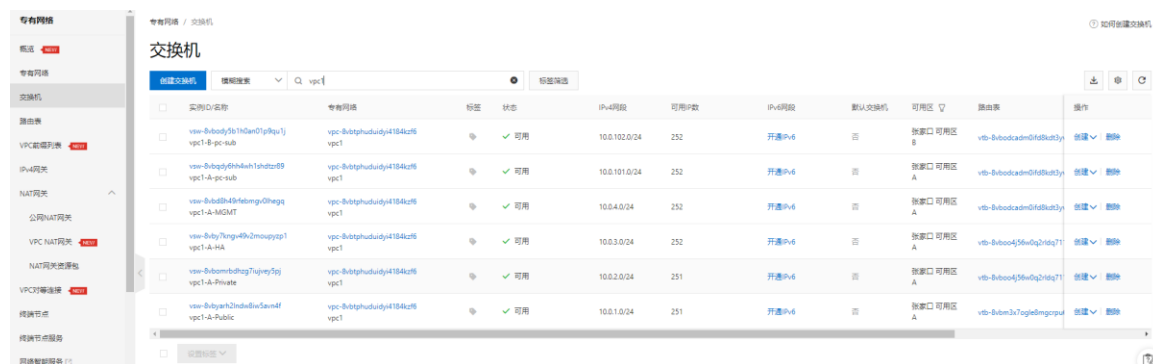
4. 配置步骤

4.1. 创建 VPC、子网

创建 VPC。



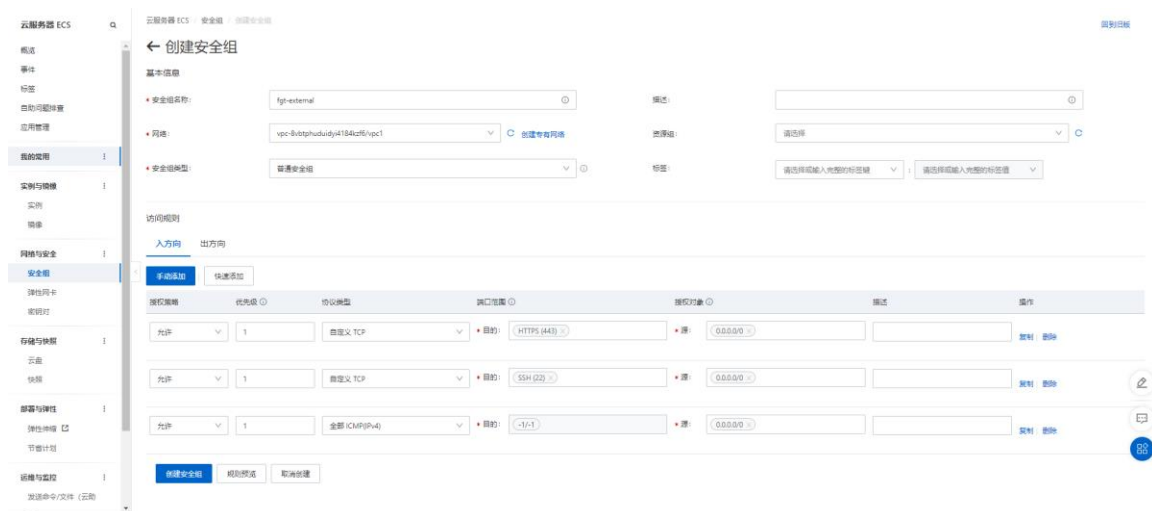
创建子网。



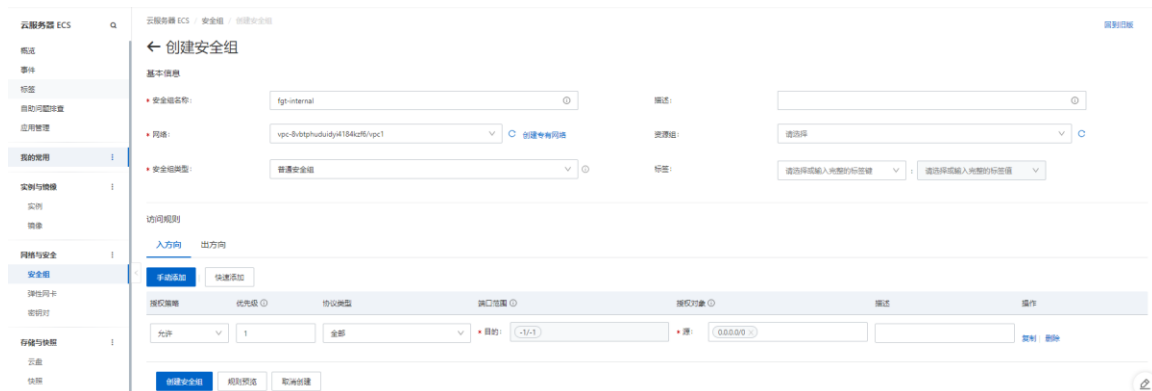
4.2. 创建安全组

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。

云服务器 ECS

概览

事件

标签

自助问题排查

应用管理

我的资源

实例与镜像

实例

镜像

网络与安全

安全组

弹性网卡

密钥对

存储与快照

云盘

快照

部署与弹性

弹性伸缩

计费计划

运维与监控

云原生 ECS

安全组

创建安全组

← 创建安全组

基本设置

安全组名称:

fgt-mgmt

网络:

vpc-8vdtgphududy4t84kz6/vpc1

创建专有网络

安全组类型:

普通安全组

描述:

类型:

请选择

标签:

请选择或输入标签的键名

请选择或输入标签的值

访问规则

入方向

出方向

手动添加

快速添加

授权策略	优先级	协议类型	端口范围	授权对象	描述	操作
允许	1	自定义 TCP	HTTPS (443)	源: 0.0.0.0/0		复制 删除
允许	1	自定义 TCP	SSH (22)	源: 0.0.0.0/0		复制 删除
允许	1	全部 (ICMPv4)	-1/-1	源: 0.0.0.0/0		复制 删除

创建安全组

取消添加

取消设置

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”。



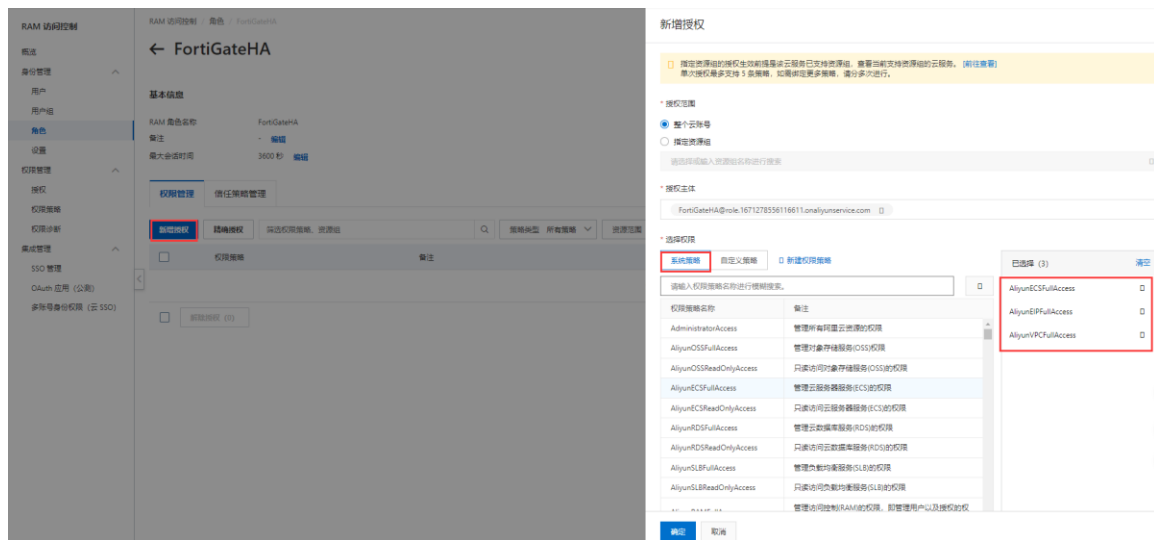
输入“角色名称”，在“选择受信服务”中选择“云服务器”，并点击“完成”。



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）。

规格族	实例规格	vCPU	内存	架构-分类	处理器	参考价格
计算平衡增强型 c6e	ecs.c6e.large	2 vCPU		X86 计算-通用型	intel	¥ 0.41/时
计算平衡增强型 c6e	ecs.c6e.xlarge	4 vCPU		X86 计算-通用型	intel	¥ 0.821/时
计算平衡增强型 c6e	ecs.c6e.2xlarge	8 vCPU		X86 计算-通用型	intel	¥ 1.642/时
计算平衡增强型 c6e	ecs.c6e.4xlarge	16 vCPU		X86 计算-通用型	intel	¥ 3.283/时
计算平衡增强型 c6e	ecs.c6e.8xlarge	32 vCPU		X86 计算-通用型	intel	¥ 6.567/时
计算平衡增强型 c6e	ecs.c6e.13xlarge	52 vCPU		X86 计算-通用型	intel	¥ 10.671/时
计算平衡增强型 c6e	ecs.c6e.26xlarge	104 vCPU		X86 计算-通用型	intel	¥ 21.342/时
计算型 c6	ecs.c6.large	2 vCPU		X86 计算-计算型	intel	-
计算型 c6	ecs.c6.xlarge	4 vCPU	8 GiB	X86 计算-计算型	intel	-
计算型 c6	ecs.c6.2xlarge	8 vCPU	16 GiB	X86 计算-计算型	intel	-

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

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

镜像分类

- 全部
- 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
Fortinet FortiManager通过易于使用的、集中式的管理控制台, 让您...		
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	V7.0.8	★★★★★ 216人已使用
FortiGate: 以更低的复杂性提供业内首屈一指的威胁防护和性能。...		
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	v6.2.2	★★★★★ 34人已使用
本产品许可方式为BYOL, 需自行导入License。Fortinet FortiGate...		
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	V6.2.4	★★★★★ 75人已使用
免费测试需使用1CPU的ECS实例。FortiGate下一代防火墙产品采...		
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	v6.2.2	★★★★★ 39人已使用
本产品许可方式为BYOL, 需自行导入License。Fortinet FortiGate...		

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

如何选择云盘

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)

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)

系统默认分配设备名 ☒ 随实例释放

加密 ☐ 加密

用快照创建磁盘

快照服务

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 (选填)

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

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

密钥对 自定义密码 **创建后设置**

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	fgt1	4 / 128
	如何自定义有序实例名称	
描述	输入描述 0 / 256	
主机名	操作系统内部的计算机名，选填项 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	FortiGateHA 创建实例RAM角色	
元数据访问模式	普通模式 (兼容加固模式)	
自定义数据	☐ 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	请选择资源组 创建资源组	
部署集	请选择部署集 管理部署集	
专有宿主机	创建专有宿主机	
私有池类型	请选择私有池类型 资源预定	

查看实例当前配置，确认无误后点击“确认下单”。

确认下单

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。

云服务器 ECS / 弹性网卡 / 创建弹性网卡

创建弹性网卡

- 弹性网卡名称: fgt1-port2
- 专有网络: vpc1/vpc-8btpghududy4184kz6
- 交换机: vpc1-A-Private/vsw-8bomdbd8g7upwey5q
交换机地址段: 10.0.2.0/24 可用区: 东家口 可用区A
- 安全组: fgt-internal/sg-8bdloa6c513cnez7
- 主私网IP: 10.0.2.11
- 辅助私网IPv4: ☒ 暂不分配 ☐ 自动分配 ☐ 指定地址
- 私网IPv6: 当前网卡交换机没有打开分配 IPv6 地址的功能，您可以通过设置打开 开通交换机IPv6
- 描述: 请输入描述
- 资源组: 选择资源组
- 标签: 标签键: 选择或输入完整的标签键; 标签值: 选择或输入完整的标签值

创建网卡 取消

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。

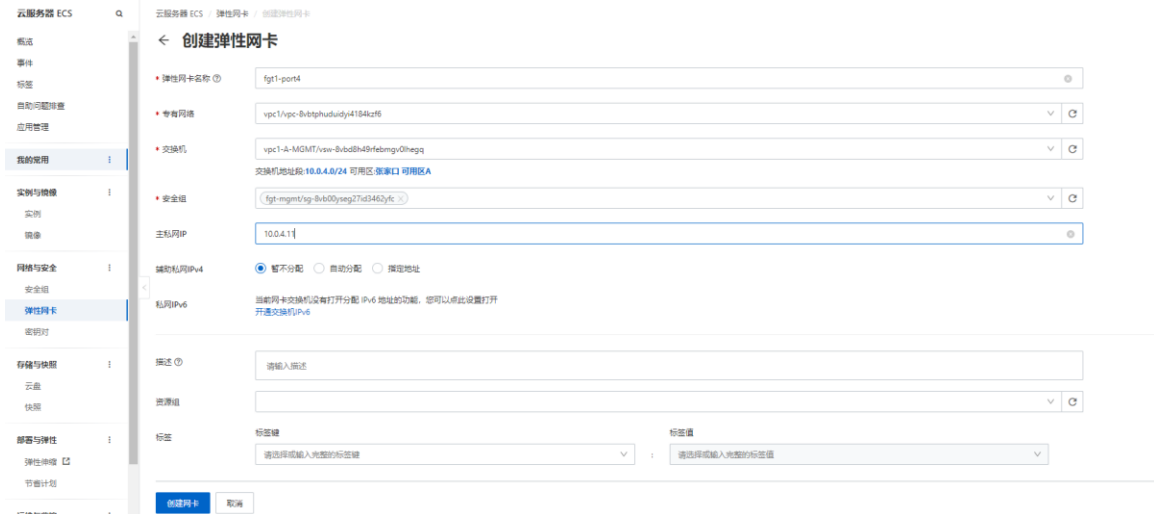
云服务器 ECS / 弹性网卡 / 创建弹性网卡

创建弹性网卡

- 弹性网卡名称: fgt1-port3
- 专有网络: vpc1/vpc-8btpghududy4184kz6
- 交换机: vpc1-A-HA/vsw-8bby7hng49v2moupyt1
交换机地址段: 10.0.3.0/24 可用区: 东家口 可用区A
- 安全组: fgt-internal/sg-8bdloa6c513cnez7
- 主私网IP: 10.0.3.11
- 辅助私网IPv4: ☒ 暂不分配 ☐ 自动分配 ☐ 指定地址
- 私网IPv6: 当前网卡交换机没有打开分配 IPv6 地址的功能，您可以通过设置打开 开通交换机IPv6
- 描述: 请输入描述
- 资源组: 选择资源组
- 标签: 标签键: 选择或输入完整的标签键; 标签值: 选择或输入完整的标签值

创建网卡 取消

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。

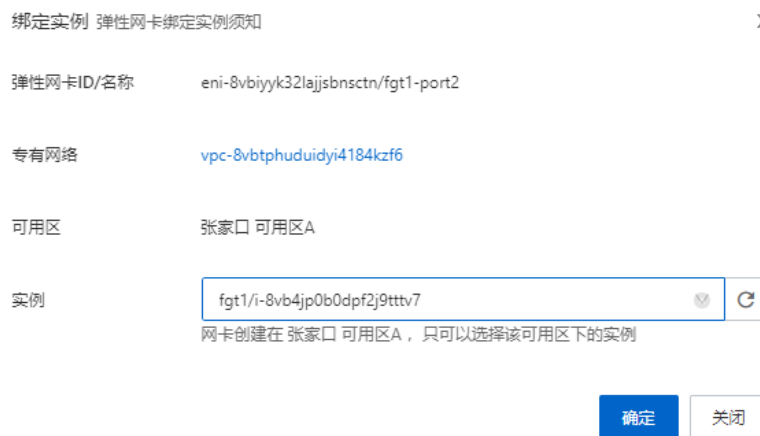


FGT1 实例 3 块网卡创建完成。



弹性网卡ID(名称)	标签	网卡类型	状态	实例	IP地址	专有网络/交换机	可用区	安全组	操作
eni-bv8h4y0h9q2ab8f84qen fgt1-port4		辅助网卡	可用	未绑定实例	10.0.4.11(主私网IP)	vpc-bvtpshudyd4184kzf6 vsw-bvdb848f6bmgq0hegq	张家口 可用区A	sg-bvdb0yseg27d3462y6	管理辅助私网IP 修改安全组 绑定实例
eni-bv874u30v955uau5 fgt1-port3		辅助网卡	可用	未绑定实例	10.0.3.11(主私网IP)	vpc-bvtpshudyd4184kzf6 vsw-bv874xg49u2mouyyp1	张家口 可用区A	sg-bvdb0a6c5131zce7	管理辅助私网IP 修改安全组 绑定实例
eni-bv8y8k32lajjsbnsctn fgt1-port2		辅助网卡	可用	未绑定实例	10.0.2.11(主私网IP)	vpc-bvtpshudyd4184kzf6 vsw-bvdb0mbd8zg7u9ey5g	张家口 可用区A	sg-bvdb0a6c5131zce7	管理辅助私网IP 修改安全组 绑定实例
eni-bv85h4u3agp0l8c2k fgt2-port1		主网卡	已绑定	i-bv8a4a2099bqih40R	10.0.1.12(主私网IP)	vpc-bvtpshudyd4184kzf6 vsw-bv8yah2indw8w5awm8	张家口 可用区A	sg-bvbcy9o0v320v7tzc5	管理辅助私网IP 安全组规则检查
eni-bv86f82agp0l8c2k fgt1-port1		主网卡	已绑定	i-bv84p0b0dp2j9tttv7	10.0.1.11(主私网IP)	vpc-bvtpshudyd4184kzf6 vsw-bv8yah2indw8w5awm8	张家口 可用区A	sg-bvbcy9o0v320v7tzc5	管理辅助私网IP 安全组规则检查

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。



绑定实例 弹性网卡绑定实例须知

弹性网卡ID/名称 eni-bv8y8k32lajjsbnsctn/fgt1-port2

专有网络 vpc-bvtpshudyd4184kzf6

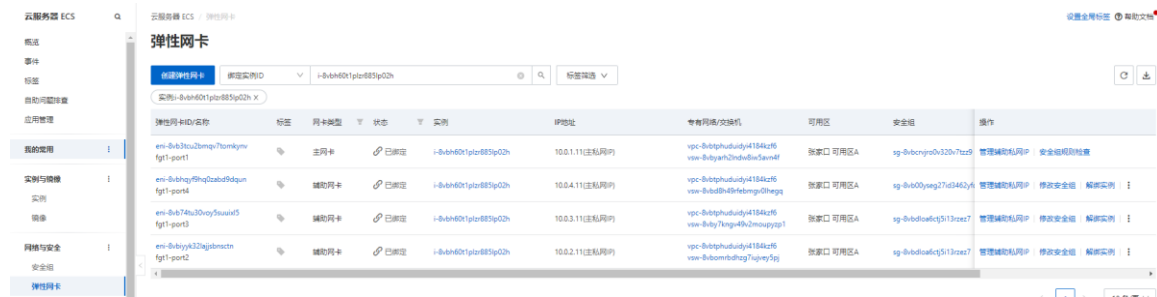
可用区 张家口 可用区A

实例 fgt1/i-bv84jp0b0dp2j9tttv7

网卡创建在 张家口 可用区A，只可以选择该可用区下的实例

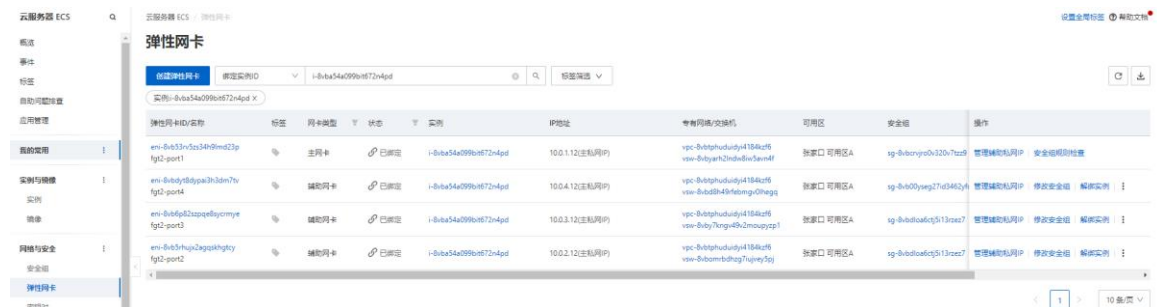
确定 关闭

绑定成功。



弹性网卡ID名称	标签	网卡类型	状态	实例	IP地址	专有网络/交换机	可用区	安全组	操作
eni-b4b3ru2m9p7omkywv fgt1-por1		主网卡	已绑定	i-b4b60t1p0r885p02h	10.0.1.11(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b3arh2nd4b0a5aevd8	张家口_可用区A	sg-b4b3cnyso3220v7az9	管理辅助私网IP 安全组规则检查
eni-b4b3huy9hg2oab8d9un fgt1-por4		辅助网卡	已绑定	i-b4b60t1p0r885p02h	10.0.4.11(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b3arh2nd4b0a5aevd8	张家口_可用区A	sg-b4b30yng27u3462y6	管理辅助私网IP 修改安全组 解除实例
eni-b4b74u30oxy5suw45 fgt1-por3		辅助网卡	已绑定	i-b4b60t1p0r885p02h	10.0.3.11(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b37ng49b2mouyyp1	张家口_可用区A	sg-b4b3oia6c513zaz7	管理辅助私网IP 修改安全组 解除实例
eni-b4b3yk32agjbrnctn fgt1-por2		辅助网卡	已绑定	i-b4b60t1p0r885p02h	10.0.2.11(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b3arh2nd4b0a5aevd8	张家口_可用区A	sg-b4b3oia6c513zaz7	管理辅助私网IP 修改安全组 解除实例

同理创建实例 FGT2 的另外 3 块网卡，并绑定到 FGT2。



弹性网卡ID名称	标签	网卡类型	状态	实例	IP地址	专有网络/交换机	可用区	安全组	操作
eni-b4b33v3m349m423p fgt2-por1		主网卡	已绑定	i-b4b34a099bu672n4pd	10.0.1.12(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b3arh2nd4b0a5aevd8	张家口_可用区A	sg-b4b3cnyso3220v7az9	管理辅助私网IP 安全组规则检查
eni-b4b3d89paw3h3dm7v fgt2-por4		辅助网卡	已绑定	i-b4b34a099bu672n4pd	10.0.4.12(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b3arh2nd4b0a5aevd8	张家口_可用区A	sg-b4b30yng27u3462y6	管理辅助私网IP 修改安全组 解除实例
eni-b4b3d82zqqe8fyymye fgt2-por3		辅助网卡	已绑定	i-b4b34a099bu672n4pd	10.0.3.12(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b37ng49b2mouyyp1	张家口_可用区A	sg-b4b3oia6c513zaz7	管理辅助私网IP 修改安全组 解除实例
eni-b4b37huj23gpxhgtcy fgt2-por2		辅助网卡	已绑定	i-b4b34a099bu672n4pd	10.0.2.12(主私网IP)	vpc-b4b3phududy4184zr6 vsw-b4b3arh2nd4b0a5aevd8	张家口_可用区A	sg-b4b3oia6c513zaz7	管理辅助私网IP 修改安全组 解除实例

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”。

创建高可用虚拟IP



地域

华北3 (张家口)

实例名称

fgt_havip

9/128

* 专有网络

vpc-8vbtphuidyi4184kzf6 | vpc1



* 交换机

vsw-8vbyarh2lndw8iw5avn4f | vpc1-A-Public



交换机网段

10.0.1.0/24

* 是否自动分配私网IP地址

☐ 是 ☒ 否

10

0

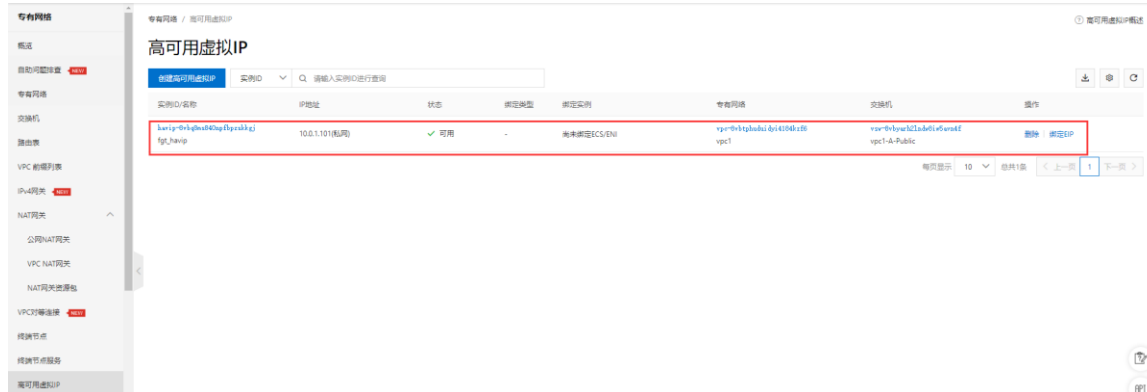
1

101

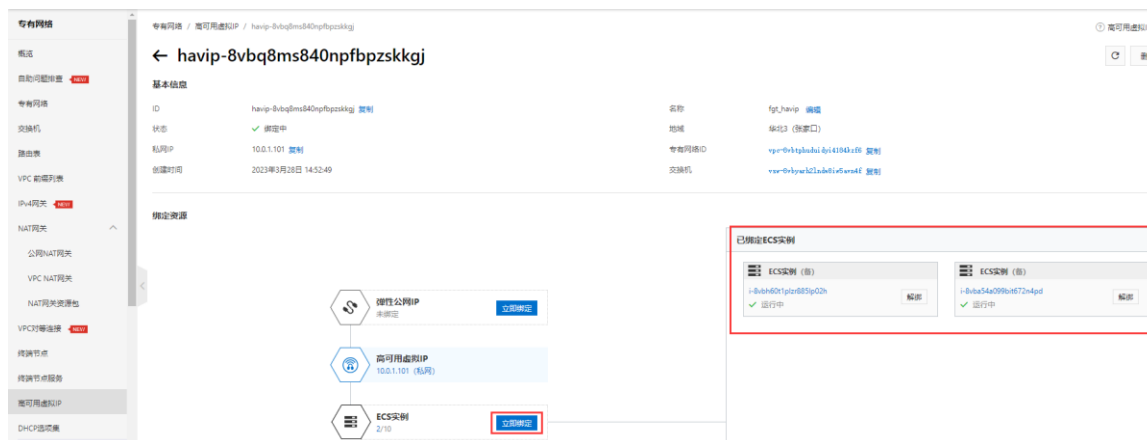
确定

取消

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。

The screenshot displays the Alibaba Cloud console interface for managing Elastic IP addresses. The left sidebar shows the navigation menu with '弹性公网IP' (Elastic Public IP) selected under '公网服务' (Public Network Services).

The main content area is titled '弹性公网IP' (Elastic Public IP) and shows a list of five created Elastic IP addresses. The first three are highlighted with a red box, indicating they are the ones used for the final configuration:

实例ID/名称	安全组	IP地址	IP地址端口	状态	实例刷新	带宽	带宽计费模式	带宽峰值	IP状态	绑定实例ID	操作
elp-b4b4a27819f9e9 最近添加 fgt1-port1		39.86.41.32	-	已分配	发起刷新	200 Mbps 按流量计费 变配	未加入带宽包服务 加入	已分配	已分配	ECS实例 i-b4b4a01paz85p02h 标准模式	解绑
elp-b4b4a4e9e9e9e9 最近添加 fgt2-port1		39.86.93.9	-	已分配	发起刷新	200 Mbps 按流量计费 变配	未加入带宽包服务 加入	已分配	已分配	ECS实例 i-b4b4a4a09e9e9e9 标准模式	解绑
elp-b4b4a27819f9e9 最近添加 fgt1-port4		47.82.233.204	-	已分配	发起刷新	200 Mbps 按流量计费 变配	未加入带宽包服务 加入	已分配	已分配	辅助弹性网卡 eni-b4b4a4e9e9e9e9 10.0.4.11 标准模式	解绑
elp-b4b4a27819f9e9 最近添加 fgt2-port4		39.86.160.152	-	已分配	发起刷新	200 Mbps 按流量计费 变配	未加入带宽包服务 加入	已分配	已分配	辅助弹性网卡 eni-b4b4a4e9e9e9e9 10.0.4.12 标准模式	解绑
elp-b4b4a4e9e9e9e9 最近添加 fgt-havip		39.86.63.115	-	已分配	发起刷新	200 Mbps 按流量计费 变配	未加入带宽包服务 加入	已分配	已分配	高可用虚拟IP hvip-b4b4a4e9e9e9e9	解绑

Below the list, the details for the Elastic IP 'hvip-b4b4a4e9e9e9e9' are shown. The '绑定资源' (Bind Resource) section includes a diagram showing the Elastic IP associated with the '高可用虚拟IP' (High Availability Virtual IP) and the 'ECS实例' (ECS Instance).

The '已绑定ECS实例' (Already Bound ECS Instance) section shows two ECS instances:

- ECS实例 (主) i-b4b4a01paz85p02h: 运行中 (Running)
- ECS实例 (备) i-b4b4a4a09e9e9e9: 运行中 (Running)

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。

The screenshot shows the 'VPC 路由表' (VPC Route Table) configuration page in the Fortinet Cloud Management Console. The route table is named 'fgt-public' and is associated with the VPC 'vtb-8vbotbwbfryd25fw8y3df'. The route table is currently in a '待配置' (Pending Configuration) state. The configuration details show the route table ID, name, tags, creation time, and associated VPC. The route table is linked to the 'vtb-8vbotbwbfryd25fw8y3df' VPC. The route table is currently in a '待配置' (Pending Configuration) state. The configuration details show the route table ID, name, tags, creation time, and associated VPC. The route table is linked to the 'vtb-8vbotbwbfryd25fw8y3df' VPC.

路由表ID	名称	标签	创建时间	专有网络ID	路由表类型	路由对象类型	描述
vtb-8vbotbwbfryd25fw8y3df	fgt-public		2023年3月28日 15:15:33	vpc-8vbotbwbfryd25fw8y3df	自定义	交换机	

fgt-public 路由表系统自带路由。

The screenshot shows the 'VPC 路由表' (VPC Route Table) configuration page in the Fortinet Cloud Management Console. The route table is named 'fgt-public' and is associated with the VPC 'vtb-8vbotbwbfryd25fw8y3df'. The route table is currently in a '待配置' (Pending Configuration) state. The configuration details show the route table ID, name, tags, creation time, and associated VPC. The route table is linked to the 'vtb-8vbotbwbfryd25fw8y3df' VPC. The route table is currently in a '待配置' (Pending Configuration) state. The configuration details show the route table ID, name, tags, creation time, and associated VPC. The route table is linked to the 'vtb-8vbotbwbfryd25fw8y3df' VPC.

路由表ID	名称	标签	创建时间	专有网络ID	路由表类型	路由对象类型	描述
vtb-8vbotbwbfryd25fw8y3df	fgt-public		2023年3月28日 15:15:33	vpc-8vbotbwbfryd25fw8y3df	自定义	交换机	

路由表ID	名称	标签	创建时间	专有网络ID	路由表类型	路由对象类型	描述
vtb-8vbotbwbfryd25fw8y3df	fgt-public		2023年3月28日 15:15:33	vpc-8vbotbwbfryd25fw8y3df	自定义	交换机	

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。

vtb-8vb0mwemacy0vssqf746i

路由表基本信息

路由表ID: vtb-8vb0mwemacy0vssqf746i

名称: fgt-private

标签: 路由表

创建时间: 2023年3月28日 15:15:46

路由表ID: vtb-8vb0mwemacy0vssqf746i

路由表类型: 自定义

路由表对象类型: 交换机

描述: -

路由表列表

路由表ID	名称	状态	网络	操作
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.102.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.101.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.3.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.2.0/24	删除

Private 路由表系统自带路由。

vtb-8vb0mwemacy0vssqf746i

路由表基本信息

路由表ID: vtb-8vb0mwemacy0vssqf746i

名称: fgt-private

标签: 路由表

创建时间: 2023年3月28日 15:15:46

路由表ID: vtb-8vb0mwemacy0vssqf746i

路由表类型: 自定义

路由表对象类型: 交换机

描述: -

路由表列表

路由表ID	名称	状态	网络	操作
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.1.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.101.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.102.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.3.0/24	删除

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

vtb-8vb0mwemacy0vssqf746i

路由表基本信息

路由表ID: vtb-8vb0mwemacy0vssqf746i

名称: fgt-private

标签: 路由表

创建时间: 2023年3月28日 15:15:46

路由表ID: vtb-8vb0mwemacy0vssqf746i

路由表类型: 自定义

路由表对象类型: 交换机

描述: -

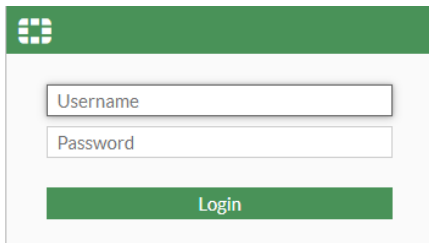
路由表列表

路由表ID	名称	状态	网络	操作
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.1.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.101.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.102.0/24	删除
vtb-8vb0mwemacy0vssqf746i	vtb-8vb0mwemacy0vssqf746i	可用	10.0.3.0/24	删除

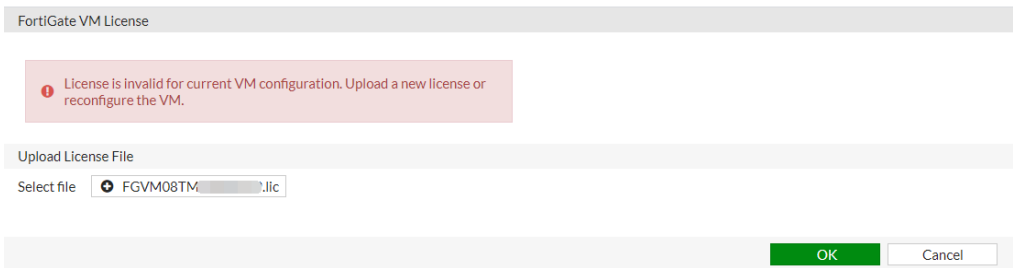
4.9. 访问 FortiGate

HTTPS 访问 FGT1，同理访问 FGT2：

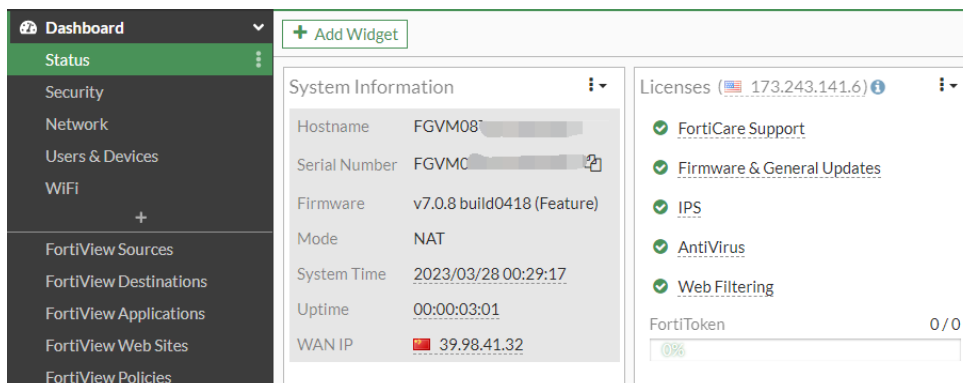
使用 `https://39.98.41.32/`（弹性 IP）访问 FortiGate，账号是 admin，密码默认是实例 ID。首次登录后，请按照提示修改密码。

The image shows the FortiGate login interface. It has a green header with the Fortinet logo. Below the header, there are two input fields: "Username" and "Password". At the bottom, there is a green "Login" button.

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

The image shows the "FortiGate VM License" dialog box. It has a red warning message: "License is invalid for current VM configuration. Upload a new license or reconfigure the VM." Below the message, there is a section titled "Upload License File" with a "Select file" button and a file name "FGVM08TM...ilic". At the bottom, there are "OK" and "Cancel" buttons.

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 # 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    #hvip 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:

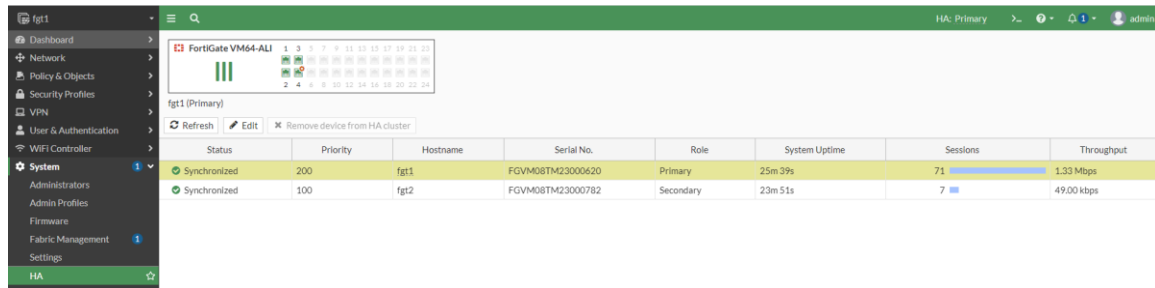
```
config system ha
    set group-name "FGTHA"
    set mode a-p
```

```
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
```

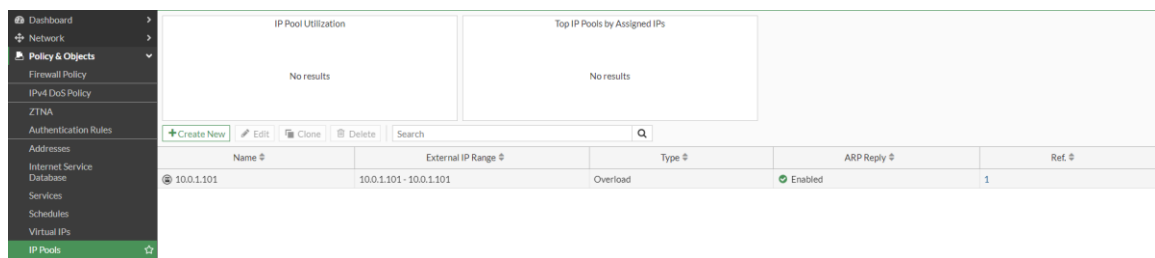
配置完成后，查看 HA 状态。如果 HA 状态没有同步，请稍等一会再查看。



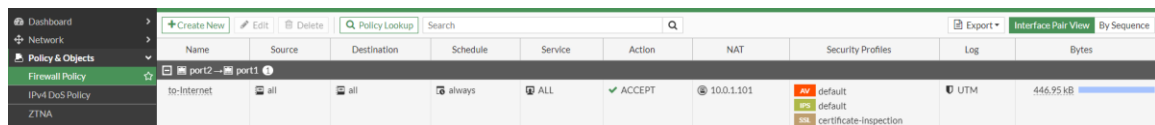
现在可以使用 FortiGate 实例 port4 关联的弹性 IP 进行访问，此时可以删除临时的 2 个弹性 IP。

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。

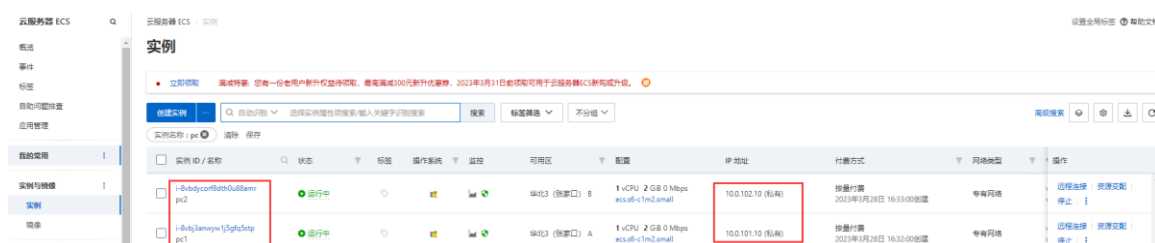


配置防火墙策略，会自动同步给 FGT2。



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。

The screenshot shows two parts of the FortiGate configuration interface. The top part shows the 'Virtual IP' configuration under 'Policy & Objects'. It lists two Virtual IPs: 'pc1-3389' and 'pc2-3389'. Both are mapped to the external address 100.1.101. The bottom part shows the 'Firewall Policy' configuration. It shows a policy named 'to-pc-3389' that allows traffic from 'all' sources to the 'pc1-3389' and 'pc2-3389' destinations. The action is set to 'ACCEPT' and the NAT is set to 'Disabled'.

Name	Details	Interfaces	Services	Ref.	Hit Count	Last Used
pc1-3389	100.1.101 → 10.0.101.10 (TCP: 10001 → 3389)	any		0	0	
pc2-3389	100.1.101 → 10.0.102.10 (TCP: 10002 → 3389)	any		0	0	

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
to-pc-3389	all	pc1-3389 pc2-3389	always	ALL	ACCEPT	Disabled	default default certificate-inspection	UTM	0 B

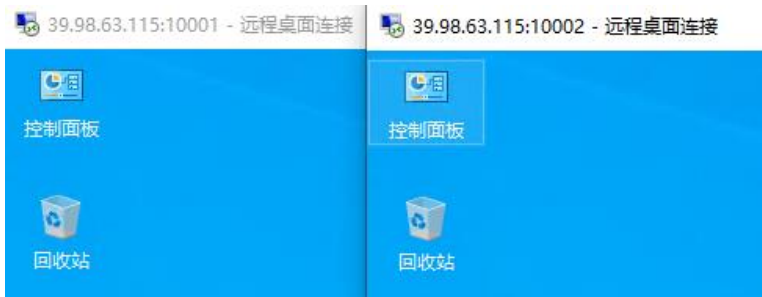
FortiGate 实例 port1 安全组 fgt-external 放通 10001, 10002 这两个对外的端口。

The screenshot shows the 'Security Group' configuration in the Alibaba Cloud ECS console. The security group is named 'sg-bb0c9yso-320-7020/fgt-external'. It has a VPC ID of 'vpc-bb0c9yso-4184420'. The configuration shows two inbound rules that are highlighted with red boxes. Both rules are 'Allow' rules with a priority of 1, allowing TCP traffic to the ports 10001 and 10002 from the source 0.0.0.0/0.

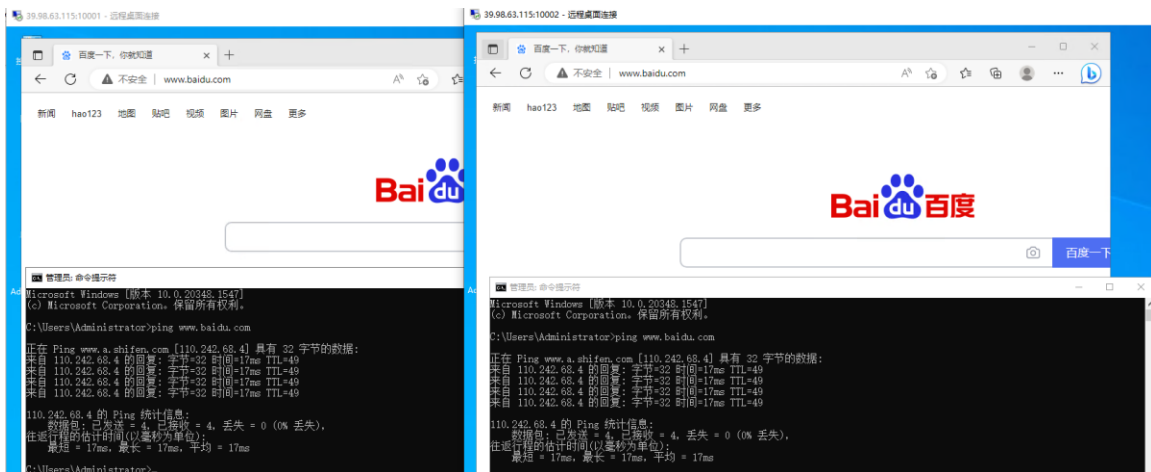
规则策略	优先级	协议类型	端口范围	授权对象	描述	创建时间	操作
允许	1	自定义 TCP	目的: 10001/10001	源: 0.0.0.0/0		2023年3月28日 16:49:30	编辑 复制 删除
允许	1	自定义 TCP	目的: 10002/10002	源: 0.0.0.0/0		2023年3月28日 16:49:20	编辑 复制 删除
允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0		2023年2月16日 16:21:58	编辑 复制 删除
允许	1	自定义 TCP	目的: 22/22	源: 0.0.0.0/0		2023年2月16日 16:21:58	编辑 复制 删除
允许	1	全部 ICMP(IPv4)	目的: -1/-1	源: 0.0.0.0/0		2023年2月16日 16:21:58	编辑 复制 删除

5. 业务测试

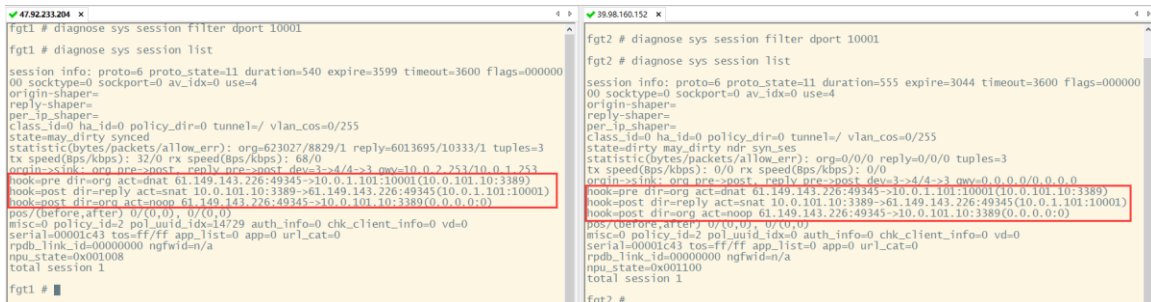
远程桌面访问两台 PC 正常。



两台 PC 访问外网正常。



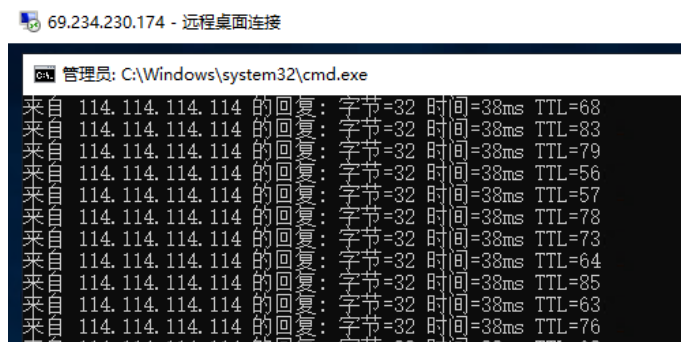
会话同步正常。



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。



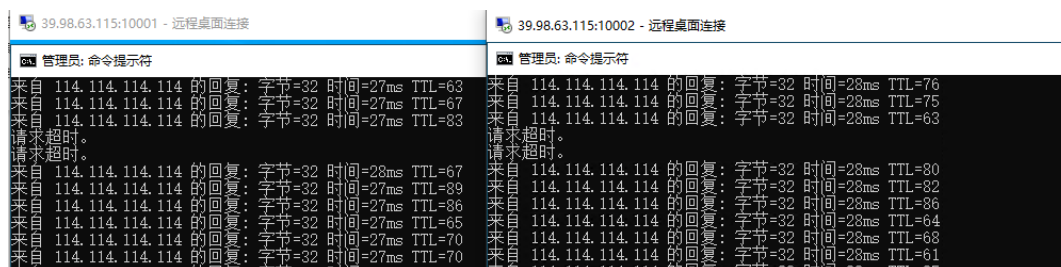
HA 切换前，FGT1 是主，FGT2 是备：

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-8vbhgyf9hq0zabd9dqun, 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。

The screenshot shows the Alibaba Cloud console interface for managing route tables. The left sidebar contains navigation options like '专有网络' (VPC), '路由表' (Route Table), and 'VPC 路由表' (VPC Route Table). The main content area displays the details of the selected route table 'vtb-8vb0mwemacy0vssqf746i'. The '路由表基本属性' (Route Table Basic Properties) section shows the route table ID, name, and creation time. The '路由表路由条目' (Route Table Route Entries) section shows a list of route entries. A new route entry is being added with the destination '0.0.0.0/0', the next hop 'vtb-8vb0mwemacy0vssqf746i', and the interface 'fgt2-port2'. The status is 'Available'.