



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

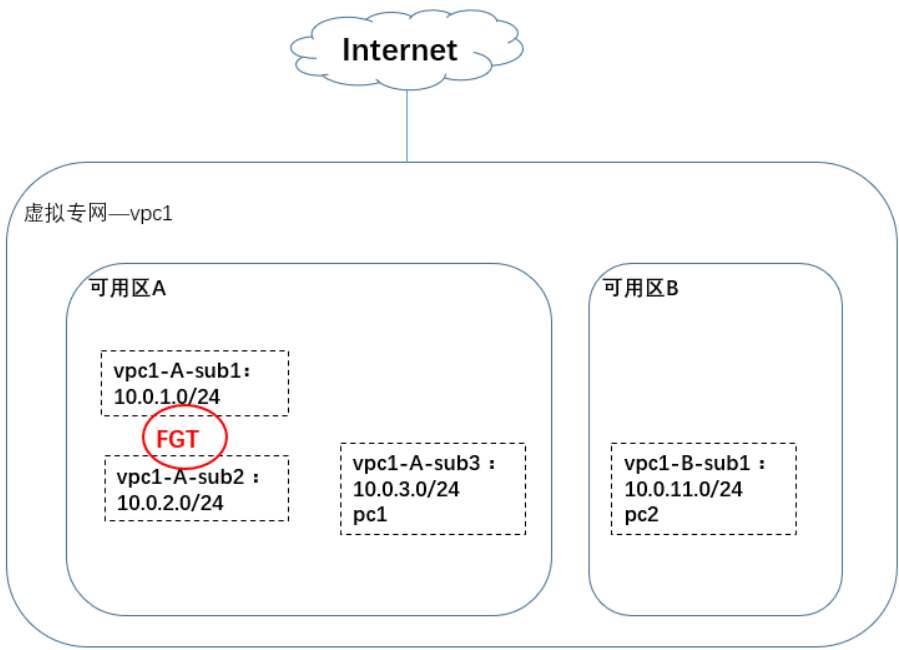
目录

1. 介绍	3
2. 网络拓扑	3
3. 地址规划	3
4. 配置步骤	4
4.1. 创建专有网络和交换机	4
4.2. 创建安全组	6
4.3. 部署 FortiGate	7
4.4. 创建弹性网卡	11
4.5. 弹性 IP	13
4.6. 阿里云路由表	14
4.7. 访问 FortiGate	19
4.8. 格式化硬盘	21
4.9. Console 查看 FortiGate 实例	21
4.10. FortiGate 配置源 NAT	22
4.11. FortiGate 配置目的 NAT	24
5. 业务测试	25

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”。

专有网络

概览

专有网络

交换机

路由表

VPC前端列表

IPv4网关

NAT网关

VPC对等连接

终端节点

终端节点服务

网络智能服务

高可用虚拟IP

DHCP选项集

公网访问

弹性公网IP

Anycast弹性公网IP

共享带宽

共享流量包

IPv6网关

IPv6地址段名称

专有网络 / 专有网络 / 创建专有网络

← 创建专有网络

专有网络

地域

华北2（北京）

* 名称

vpc1

4/128

* IPv4网段

建议使用RFC私网地址作为专有网络的网段如 10.0.0.0/8 , 172.16.0.0/12 , 192.168.0.0/16 。 网段配置建议

10.0.0.0/16

一旦创建成功，网段不能修改

IPv6网段

不分配

描述

0/256

资源组

默认资源组

高级配置

是否开启IPv4网关能力

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。

名称	可用区	IPv4网段	网段配置建议	操作
vpc1-a-sub1	张家口 可用区A	10.0.0.0/24	请确保有至少3个可用IP地址	删除
vpc1-a-sub2	张家口 可用区A	10.0.0.0/24	请确保有至少3个可用IP地址	删除
vpc1-a-sub3	张家口 可用区A	10.0.0.0/24	请确保有至少3个可用IP地址	删除
vpc1-b-sub1	张家口 可用区B	10.0.0.0/24	请确保有至少3个可用IP地址	删除

创建完成。

专有网络

概述

专有网络

交换机

路由表

VPC子网列表

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关

NAT网关流量包

专有网络 / 专有网络

什么是专有网络

专有网络

网络智能服务正在火热公测中！核心功能如下，欢迎免费试用。
实例诊断：检测实例配置和运行状态，一键诊断异常并智能修复。
流量分析：洞察网络流量和性能分析，网络拓扑和压测场景复现。
流量分析：监测网络流量异常，及时发现并分析原因。

创建专有网络

高级筛选

请输入关键字进行搜索

高级搜索

重置

刷新

关联规则 应用 vpc1 X 清空搜索条件

实例ID名称	标签	网络	IPv4网络	状态	默认专有网络	路由表	交换机	云服务商	资源组	操作
vpc-bt9phududy4t184z9f-vpc1		10.0.0.0/16	开通IPv4	可用 未绑定云企业网	否	1	4	9	默认资源组	添加云产品 编辑
创建专有网络										

1/1

专有网络

概述

专有网络

交换机

路由表

VPC子网列表

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关

NAT网关流量包

专有网络 / 交换机

如何创建交换机

创建交换机

高级搜索

Q vpc1

高级搜索

重置

刷新

实例ID名称	专有网络	标签	状态	IPv4网络	可用IP数	IPv4网络	默认交换机	可用区	路由表	操作
vsw-bt9t7tg72a7mrewo13g-vpc1-b-sub1	vpc-bt9phududy4t184z9f-vpc1		可用	10.0.1.0/24	252	开通IPv4	否	张家口 可用区 B	vrb-bt9odadw0t86kz9f	创建 删除
vsw-bt9t7m9p49h2moupyzp1-vpc1-A-sub3	vpc-bt9phududy4t184z9f-vpc1		可用	10.0.0.0/24	252	开通IPv4	否	张家口 可用区 A	vrb-bt9odadw0t86kz9f	创建 删除
vsw-bt9amtd8qz7uqwy5j-vpc1-A-sub2	vpc-bt9phududy4t184z9f-vpc1		可用	10.0.0.0/24	252	开通IPv4	否	张家口 可用区 A	vrb-bt9odadw0t86kz9f	创建 删除
vsw-bt9pzh2ndudw5am4f-vpc1-A-sub1	vpc-bt9phududy4t184z9f-vpc1		可用	10.0.1.0/24	252	开通IPv4	否	张家口 可用区 A	vrb-bt9odadw0t86kz9f	创建 删除
创建交换机										

每页显示 50

1

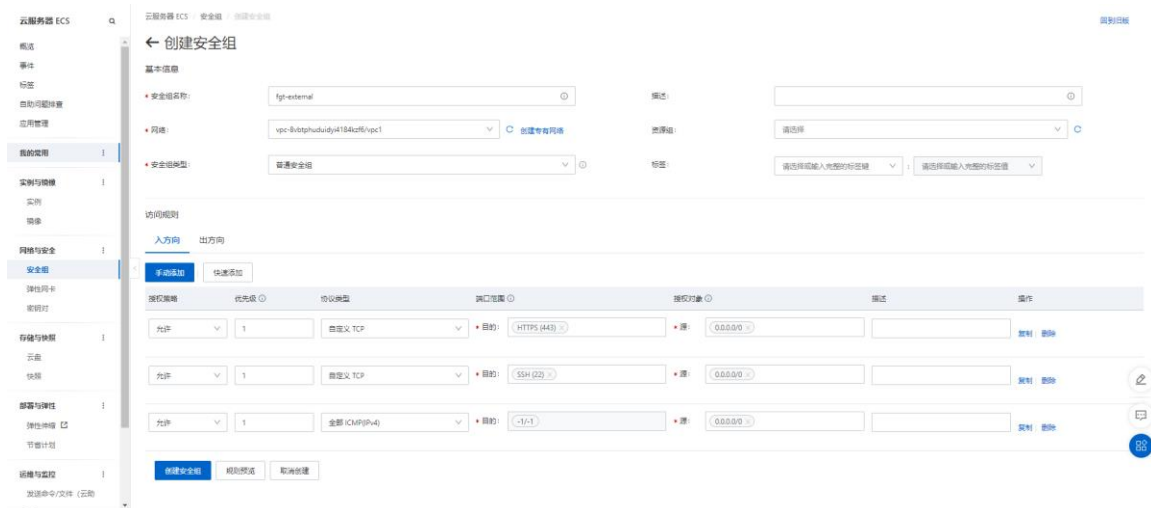
前一页

后一页

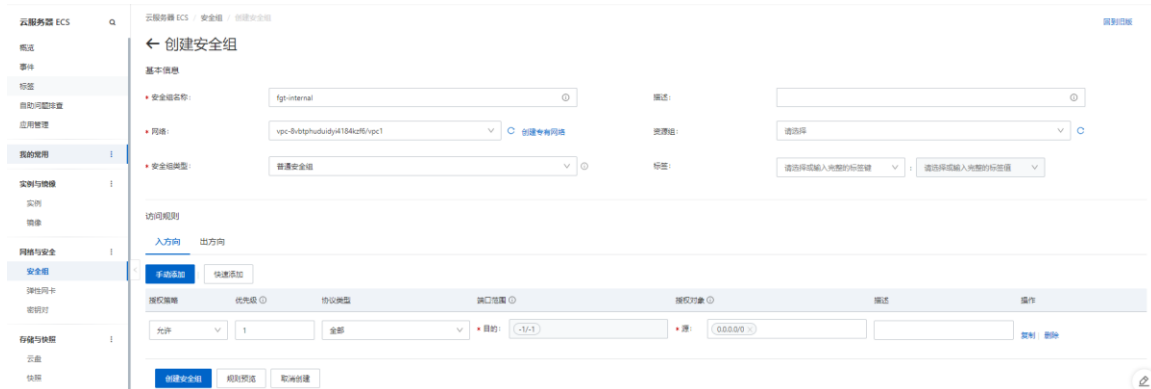
4.2. 创建安全组

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，

The screenshot shows the configuration options for creating an ECS instance. The 'Payment Type' (付费类型) section has three options: 'Subscription' (包年包月) selected, 'Pay-as-you-go' (按量付费), and 'Spot Instance' (抢占式实例). The 'Region' (地域) section shows 'China East 2 (Shanghai)' (华东 2 (上海)) selected, with 'China North 3 (Zhangjiakou)' (华北 3 (张家口)) and 'China East 1 (Hangzhou)' (华东 1 (杭州)) also visible. The 'Network and Availability Zone' (网络及可用区) section shows 'vpc1 / vpc-8vbtphuduidyi4184kzfb' selected for the VPC, and 'vpc1-A-Sub0 / vsw-8vbyarh2lndw8iw5avn4f | China North 3 Availability Zone A | CIDR: 10.0.1.0/24' selected for the Subnet. The 'Specify Private IP Address' (指定主网卡主私网IP地址) checkbox is checked, and the IP address '10.0.1.10' is entered in the input field.

“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。

FortiGate

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
☐ 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-计算型	intel	¥0.821/时
☐ 计算平衡增强型 c6e	ecs.c6e.2xlarge	8 vCPU		☐ X86 计算-内存型	intel	¥1.642/时
☐ 计算平衡增强型 c6e	ecs.c6e.4xlarge	16 vCPU		☐ X86 计算-通用算力型	intel	¥3.283/时
☐ 计算平衡增强型 c6e	ecs.c6e.8xlarge	32 vCPU		☐ X86 计算-大数据型	intel	¥6.567/时
☐ 计算平衡增强型 c6e	ecs.c6e.13xlarge	52 vCPU		☐ X86 计算-本地 SSD	intel	¥10.671/时
☐ 计算平衡增强型 c6e	ecs.c6e.26xlarge	104 vCPU		☐ X86 计算-高主频型	intel	¥21.342/时
☐ 计算型 c6	ecs.c6.large	2 vCPU		☐ X86 计算-共享型	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

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

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

FortiGate

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 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 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 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 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 使用		
本产品许可方式为BYOL, 需自行导入License。Fortinet FortiGate...		

共有7条

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)	☐ 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)	☒ 系统默认分配设备名 ☒ 随实例释放 ☐ 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。

FortiGate

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

[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”。

▲ 高级选项 (选填)

[实例名称](#) | [描述](#) | [主机名](#) | [有序后缀](#) | [实例RAM角色](#) | [元数据访问模式](#) | [自定义数据](#) | [资源组](#) | [部署集](#) | [专有宿主主机](#) | [私有池类型](#)

实例名称

fgt

3 / 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](#)

实例创建完成，实例 id 是 i-8vbcxzu0ao830f6jk7pe。

云服务器 ECS

Q

云服务器 ECS / 实例

实例

概览

事件

标签

自助问题库

应用管理

我的资源

实例与镜像

实例

设置与帮助

帮助文档

创建实例

Q 自动识别

选择实例属性模板/输入关键字识别模板

搜索

标签筛选

不分组

高级搜索

Q

+

+

+

+

实例 ID: i-8vbcxzu0ao830f6jk7pe

选择

保存

☐

实例 ID / 名称

Q

状态

▼

标签

操作系统

▼

监控

可用区

▼

配置

IP 地址

付费方式

▼

网络类型

▼

操作

☐

i-8vbcxzu0ao830f6jk7pe
fgt

运行中

华北2 (张家口)

A

4 vCPU 8 GB 0 Mbps
ecs.g6.large

10.0.1.10 (私有)

按量付费
2023年2月16日 16:40:00创建

专有网络

远程连接

快速入门

停止

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 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。

弹性网卡ID	弹性网卡名称	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-8vcs5f8easfc160i356x	fgt-port2		辅助网卡	可用	未绑定实例	10.0.2.10(主私网IP)	vpc-8b7phududy4184zr6 vsw-8ybomtdhgz7ujrey5q	张家口 可用区A	sg-8vbdcoafcy5l3rce27	管理辅助私网IP 修改安全组 绑定实例

将网卡绑定到 fgt 实例中。

FortiGate



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。

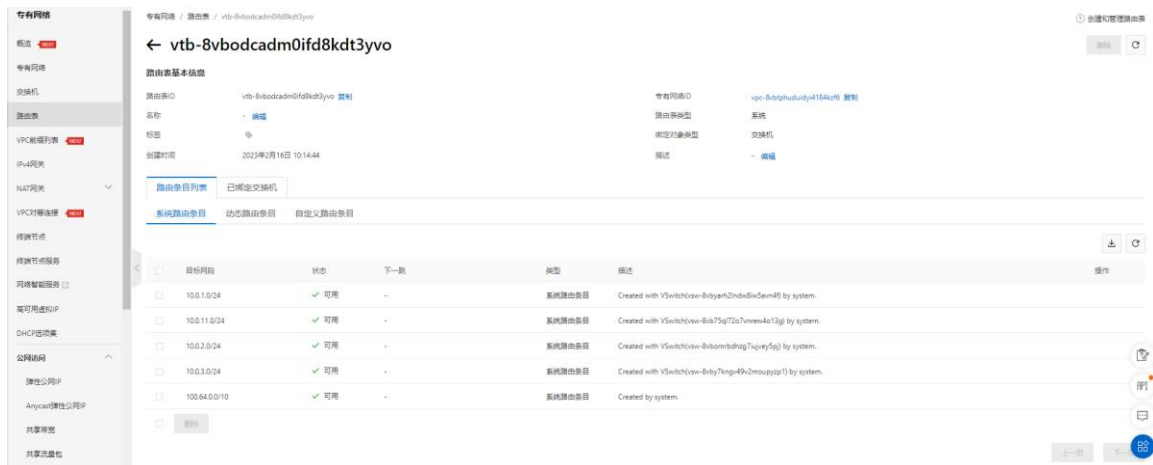


绑定成功。



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。

专有网络

概览 NEW

专有网络

交换机

路由表

VPC前缀列表 NEW

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关 NEW

NAT网关资源包

VPC对等连接 NEW

终端节点

终端节点服务

网络智能服务

专有网络 / 路由表 / 创建路由表

← 创建路由表

资源组

全部

专有网络

vpc1/vpc-8vbtphudidy4184kzf6

绑定对象类型

☒ 交换机
用于交换机流量的路由策略控制。

☐ 边界网关
用于边界网关入方向流量的路由策略控制。

* 名称

vpc1-public-rtb 15/128

描述

0/256

确定

取消

关联 fgt 实例 port1 接口的交换机。

专有网络

概览 NEW

专有网络

交换机

路由表

VPC前缀列表 NEW

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关 NEW

NAT网关资源包

VPC对等连接 NEW

终端节点

终端节点服务

网络智能服务

专有网络 / 路由表 / vtb-8vbm3x7ogle8mgcrpu609

← vtb-8vbm3x7ogle8mgcrpu609

路由表基本信息

路由表ID

vtb-8vbm3x7ogle8mgcrpu609

名称

vpc1-public-rtb

标签

🏷️

创建时间

2023年2月16日 17:39:29

专有网络ID

vpc-8vbtphudidy4184kzf6

路由表类型

自定义

绑定对象类型

交换机

描述

📝

路由条目列表

已绑定交换机

新建交换机

	状态	目标网段	操作
☐ 交换机			
☐ vsw-8vbyarh2indw8v5awm4f vpc1-4-sub-1	🔄 绑定中	10.0.1.0/24	编辑
☐ 路由			

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。

专有网络

概览 NEW

专有网络

交换机

路由表

VPC前缀列表 NEW

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关 NEW

NAT网关资源包

VPC对等连接 NEW

终端节点

终端节点服务

网络智能服务

虚拟专用网络

DHCP服务器

专有网络 / 路由表 / vtb-8vbm3x7ogle8mgcrpu609

← vtb-8vbm3x7ogle8mgcrpu609

路由表基本信息

路由表ID

vtb-8vbm3x7ogle8mgcrpu609

名称

vpc1-public-rtb

标签

🏷️

创建时间

2023年2月16日 17:39:29

专有网络ID

vpc-8vbtphudidy4184kzf6

路由表类型

自定义

绑定对象类型

交换机

描述

📝

路由条目列表

已绑定交换机

系统路由条目

动态路由条目

自定义路由条目

	目标网段	状态	下一跳	类型	描述	操作
☐	10.0.1.0/24	✓ 可用	-	系统路由条目	Created with VSwitch(vsw-8vbyarh2indw8v5awm4f) by system.	
☐	10.0.11.0/24	✓ 可用	-	系统路由条目	Created with VSwitch(vsw-8vbyarh2indw8v5awm4f) by system.	
☐	10.0.2.0/24	✓ 可用	-	系统路由条目	Created with VSwitch(vsw-8vbyarh2indw8v5awm4f) by system.	
☐	10.0.3.0/24	✓ 可用	-	系统路由条目	Created with VSwitch(vsw-8vbyarh2indw8v5awm4f) by system.	
☐	100.64.0.0/10	✓ 可用	-	系统路由条目	Created by system.	
☐						

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。

专有网络

概览 NEW

专有网络

交换机

路由表

VPC前缀列表 NEW

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关 NEW

NAT网关资源包

VPC对等连接 NEW

终端节点

终端节点服务

网络智能服务

专有网络 / 路由表 / 创建路由表

← 创建路由表

资源组

全部

专有网络

vpc1/vpc-8vbtphuidiyi4184kzf6

绑定对象类型

☒ 交换机
用于交换机流量的路由策略控制。

☐ 边界网关
用于边界网关入方向流量的路由策略控制。

* 名称

vpc1-private-rtb 16/128

描述

0/256

确定 取消

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

专有网络

概览 NEW

专有网络

交换机

路由表

VPC前缀列表 NEW

IPv4网关

NAT网关

公网NAT网关

VPC NAT网关 NEW

NAT网关资源包

VPC对等连接 NEW

终端节点

终端节点服务

网络智能服务

可用区及IP

专有网络 / 路由表 / vtb-8vboo4j56w0q2rldq7112

← vtb-8vboo4j56w0q2rldq7112

路由表基本信息

路由表ID

vtb-8vboo4j56w0q2rldq7112 复制

专有网络ID

vpc-8vbtphuidiyi4184kzf6 复制

名称

vpc1-private-rtb 编辑

路由表类型

自定义

标签

无

绑定对象类型

交换机

创建时间

2023年2月16日 17:47:09

描述

编辑

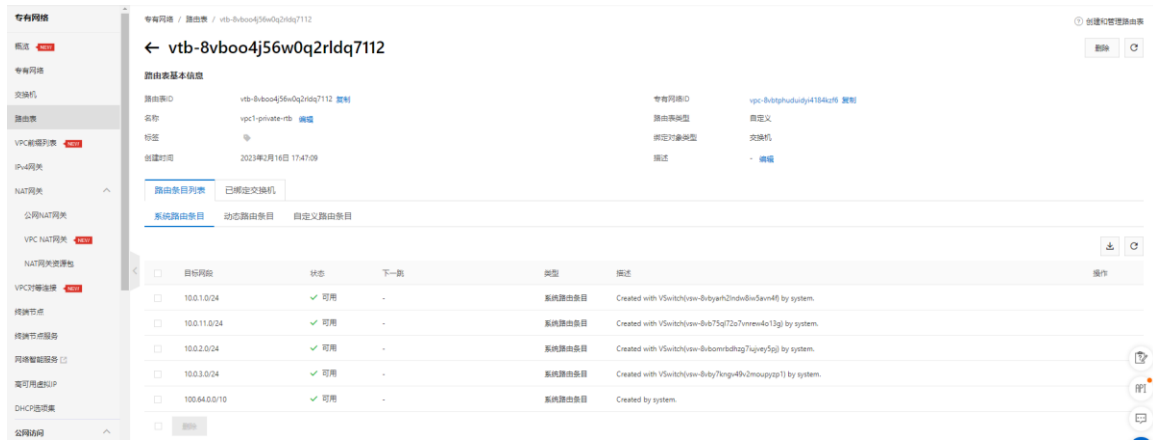
路由表条目列表

已绑定交换机

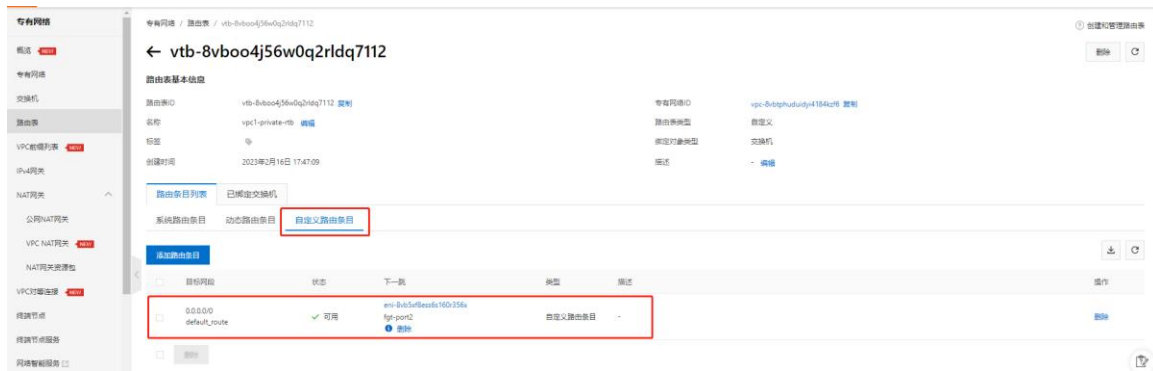
绑定交换机

交换机	状态	目标网段	操作
☐ vsw-8vbtphuidiyi4184kzf6-vpc1-8-sub1	正在配置中	10.0.11.0/24	解除
☐ vsw-8vbtphuidiyi4184kzf6-vpc1-4-sub3	可用	10.0.3.0/24	解除
☐ vsw-8vbtphuidiyi4184kzf6-vpc1-4-sub2	可用	10.0.2.0/24	解除
☐ 新增			

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
```

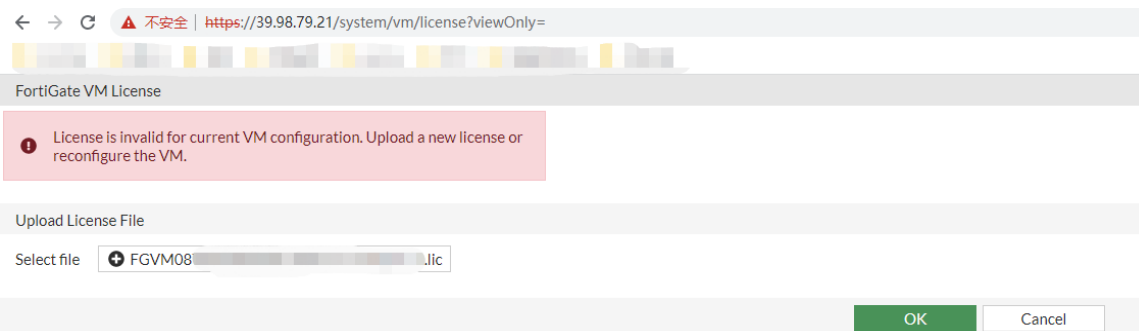
这里使用的阿里云账号已经备案,可以使用 443 端口。

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。

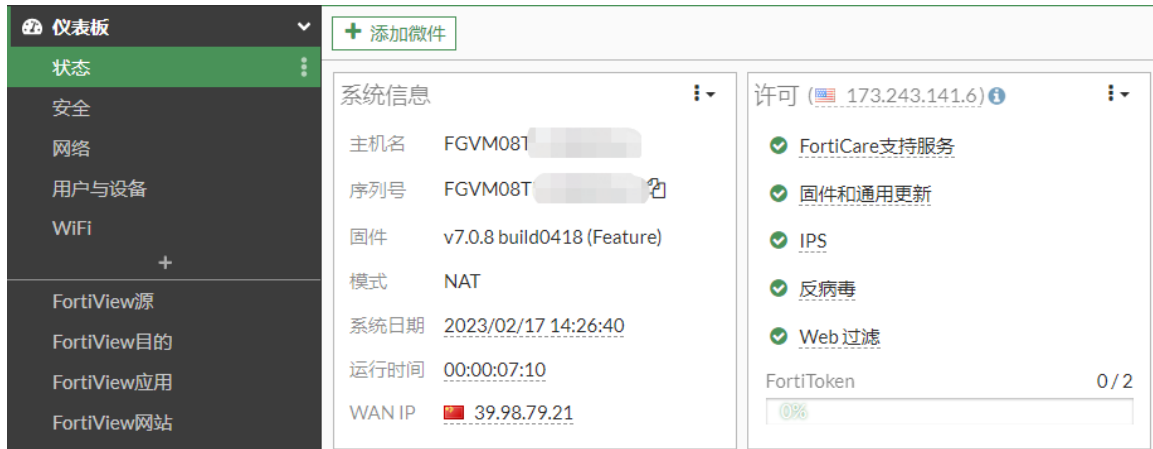


登录后, 请先上传购买好的 license, 导入 license 会重启 FortiGate。



FortiGate

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。

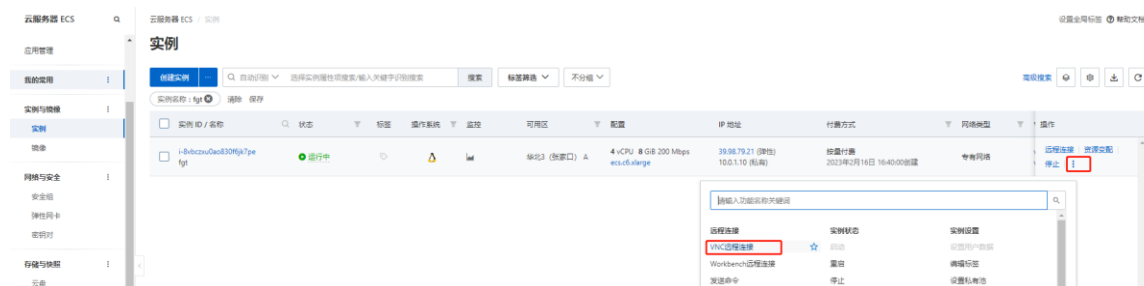
4.8. 格式化硬盘

执行 `execute formatlogdisk` 格式化记录日志的硬盘。

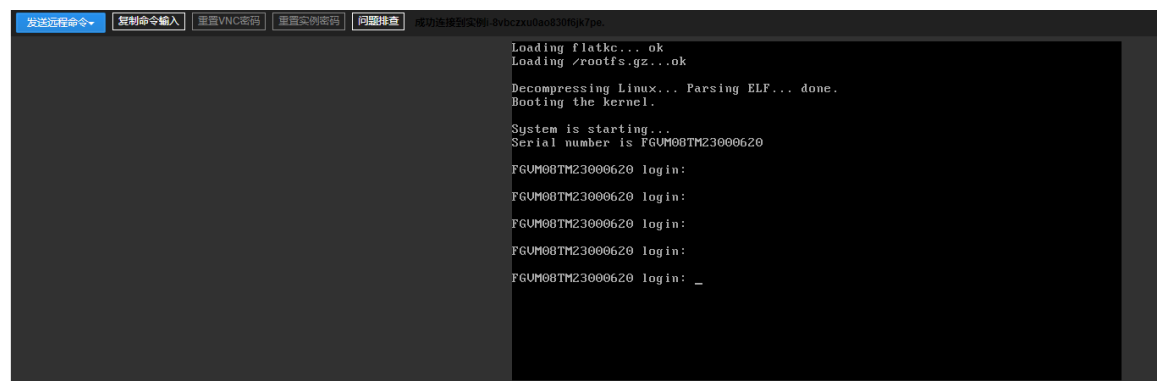
```
CLI控制台 (1)
FGVM08 # execute formatlogdisk
Log disk is /dev/vdb1.
Formatting this storage will erase all data on it, including
logs, quarantine files;
and require the unit to reboot.
Do you want to continue? (y/n)y
```

4.9. Console 查看 FortiGate 实例

在实例右侧，点击，选择“VNC 远程连接”

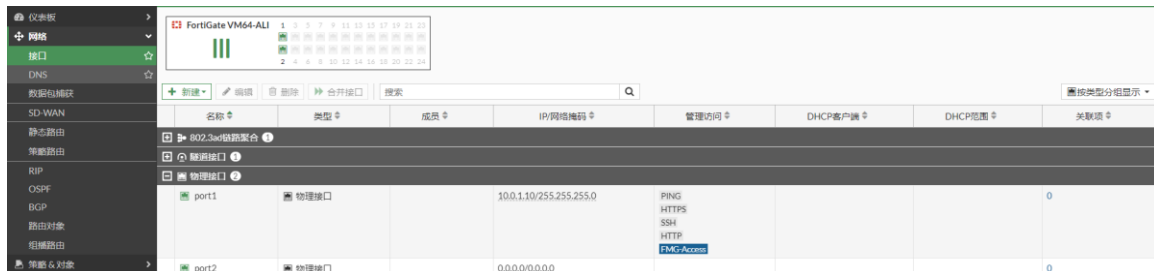


在 VNC 界面敲回车，可以查看到 fgt 实例的 console。



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：



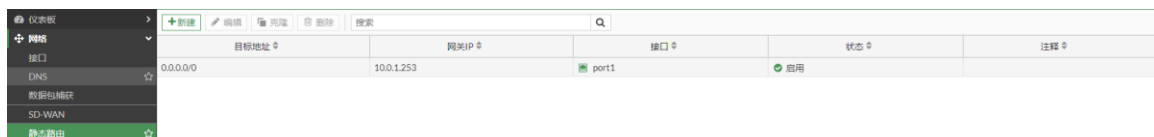
名称	类型	成员	IP/网络掩码	管理访问	DHCP客户端	DHCP范围	关联设备
port1	物理接口		10.0.1.10/255.255.255.0	PING HTTPS SSH HTTP TMCAccess			0
port2	物理接口		0.0.0.0/0.0.0.0				0

```
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。



目标地址	网关IP	接口	状态	注释
0.0.0.0	10.0.1.253	port1	启用	

修改 port1 ip 的配置为手动。

FortiGate

The screenshot shows the 'Edit' configuration page for the 'port1' interface. The left sidebar contains navigation options like 'Dashboard', 'Network', 'Interface', 'DNS', 'Data Capture', 'SD-WAN', 'Static Route', 'Policy Route', 'RIP', 'OSPF', 'BGP', 'Route Object', 'Route Map', 'Policy & Object', 'Security Configuration', and 'VPN'. The main configuration area includes fields for 'Name' (port1), 'Alias', 'Type' (Physical Interface), 'VRF ID' (0), and 'Role' (Undefined). Under the 'Address' section, 'Interface Mode' is set to 'Manual', 'IP/Network Mask' is '10.0.1.10/255.255.255.0', and 'Additional IP Address' is disabled. The 'Management Access' section shows 'IPv4' with 'HTTPS', 'FMG-Access', and 'FTM' checked, and 'HTTP', 'SSH', 'RADIUS Accounting', 'PING', 'SNMP', and 'Security Fabric Connection' unchecked.

同样设置 port2 接口的 IP。

The screenshot shows the 'Edit' configuration page for the 'port2' interface. The configuration is similar to port1, but 'Interface Mode' includes 'Single Arm Sniff' in addition to 'Manual'. The 'Management Access' section shows 'IPv4' with 'HTTP' and 'SSH' checked, while 'HTTPS', 'FMG-Access', 'FTM', 'RADIUS Accounting', 'PING', 'SNMP', and 'Security Fabric Connection' are unchecked.

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。

目标地址	源地址	网关 IP	接口	状态	注释
0.0.0.0/0		10.0.1.253	port1	启用	
10.0.0/16		10.0.2.253	port2	启用	

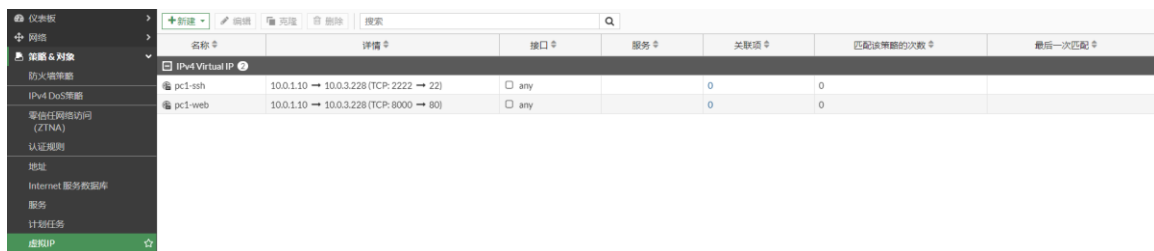
配置防火墙策略。

名称	源地址	目的地址	计划任务	服务	动作	NAT	安全配置	流量日志	字节数
To-Internet	all	all	always	ALL	接受	启用	av default ips default certificate-inspection	UTM	0B

4.11. FortiGate 配置目的 NAT

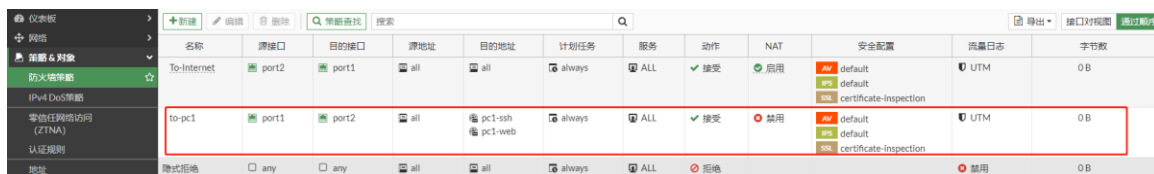
使用 **port1** 接口的地址做目的 NAT:

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。



名称	详情	接口	服务	关联项	匹配该策略的次数	最后一次匹配
pc1-ssh	10.0.1.10 → 10.0.3.228 (TCP: 2222 → 22)	☐ any		0	0	
pc1-web	10.0.1.10 → 10.0.3.228 (TCP: 8000 → 80)	☐ any		0	0	

配置防火墙策略。



名称	源接口	目的接口	源地址	目的地址	计划任务	服务	动作	NAT	安全配置	流量日志	字节数
To-Internet	port2	port1	all	all	always	ALL	接受	启用	default default certificate-inspection	UTM	0 B
to-pc1	port1	port2	all	pc1-ssh pc1-web	always	ALL	接受	禁用	default default certificate-inspection	UTM	0 B
隐式拒绝	☐ any	☐ any	all	all	always	ALL	拒绝			禁用	0 B

fgt 实例安全组放通 8000 和 2222 端口。

FortiGate

云服务商 ECS / 安全组 / sg-b6bngjrd0u320u7tcd9l fgt-external

← fgt-external vpc1/vpc-b6bphududj4l84kz96

使用默认策略规则管理安全组规则管理的政策，查看最佳实践

安全组规则

安全组实例列表

安全组内弹性网卡

基本信息

安全组ID(名称): sg-b6bngjrd0u320u7tcd9l fgt-external

网络: vpc-b6bphududj4l84kz96

安全组类型: 普通安全组

组内流量策略: 组内互连 [设置组内流量](#)

描述: 类源组:

标签:

访问规则 导入安全组规则 导出 搜索规则

入方向 出方向

快速添加 输入端口或策略ID的对象进行搜索 不会并

操作策略	优先级	协议类型	端口范围	操作对象	描述	创建时间	操作
☐ 允许	1	自定义 TCP	目的: 2222/2222	源: 0.0.0.0/0		2023年2月17日 16:30:29	编辑 复制 删除
☐ 允许	1	自定义 TCP	目的: 8000/8000	源: 0.0.0.0/0		2023年2月17日 16:30:22	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

☐ 删除

5. 业务测试

测试的 PC 如下

云服务商 ECS / 实例

应用管理

实例

快速添加

搜索 输入实例名称或ID/标签/名称/关键字进行搜索

实例名称: pc2 清除 保存

实例ID/名称	状态	标签	操作策略	监控	可用区	配置	IP地址	付费方式	网络类型	操作
i-b6b74d8hazouk8ct-pc2	运行中				华北3 (张家口) B	2 vCPU 4 GiB 0 Mbps ecs.4f1-c1m2.large	10.0.11.238 (私网)	按量付费 2023年2月17日 16:30:00创建	专有网络	启动/关机 续费/变配 停止
i-b6b74d8hazouk8ct-pc1	运行中				华北3 (张家口) A	2 vCPU 4 GiB 0 Mbps ecs.4f1-c1m2.large	10.0.3.228 (私网)	按量付费 2023年2月16日 10:58:00创建	专有网络	启动/关机 续费/变配 停止

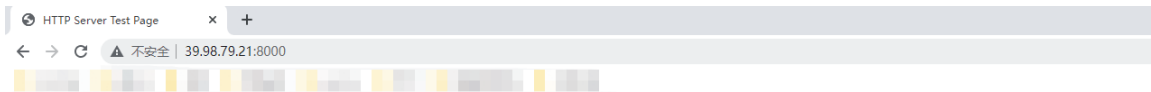
目的 NAT 测试:

ssh 39.98.79.21 2222 访问正常。

FortiGate

```
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](http://39.98.79.21:8000) 访问正常。



Welcome to HTTP Server Test Page!

If you see this page, the httpd web server is successfully installed and working. Further configuration is required.

Thank you for using apache httpd.

源 NAT 测试:

pc1 ping www.baidu.com 正常

FortiGate

```

root@pc1:~ x 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:~ x ecs-user@pc2:~ x
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 ~]$

```