Azure 部署 FortiGate

版本	V1.0
时间	2023 年 12 月
作者	王祥
状态	已审核
反馈	support_cn@fortinet.com

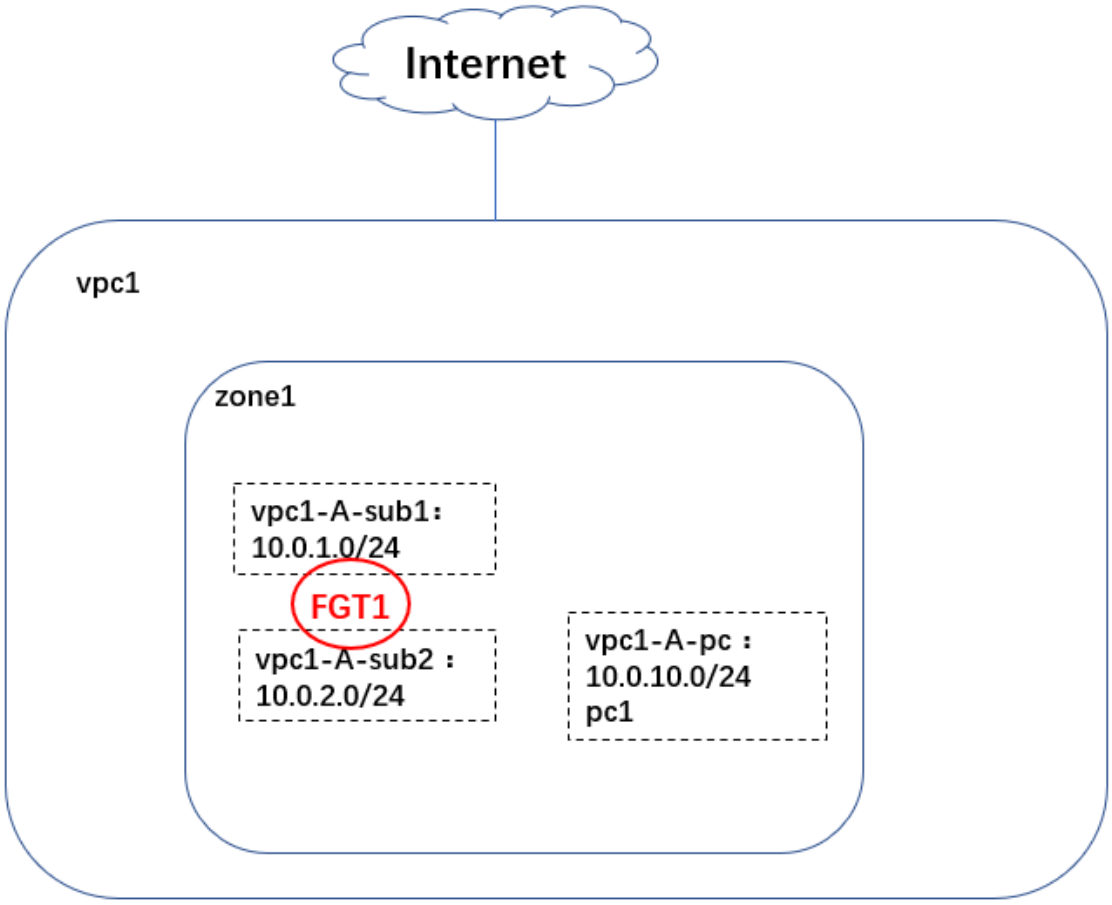
目录

1. 介绍 3
2. 网络拓扑 3
3. 配置步骤 4
3.1. 创建虚拟网络和子网 4
3.2. 创建安全组 6
3.3. 部署 FortiGate 8
3.4. 公网 IP 12
3.5. 网络接口 14
3.6. 创建路由表 16
3.7. 启动 IP 转发 17
3.8. 访问 FortiGate 17
3.9. 重置密码 19
3.10. 格式化硬盘 19
3.11. Console 查看 FortiGate 实例 20
3.12. FortiGate 配置源 NAT 21
3.13. FortiGate 配置目的 NAT 23
4. 业务测试 25

1. 介绍

本文档介绍如何在 Azure 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，保护部署在 Azure 中的各种应用负载。

2. 网络拓扑



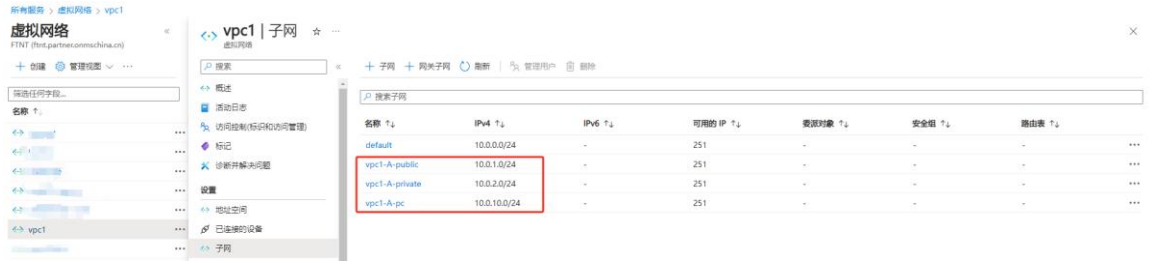
3. 配置步骤

3.1. 创建虚拟网络和子网

选择网络→ 虚拟网络，点击“创建”。

创建完成。

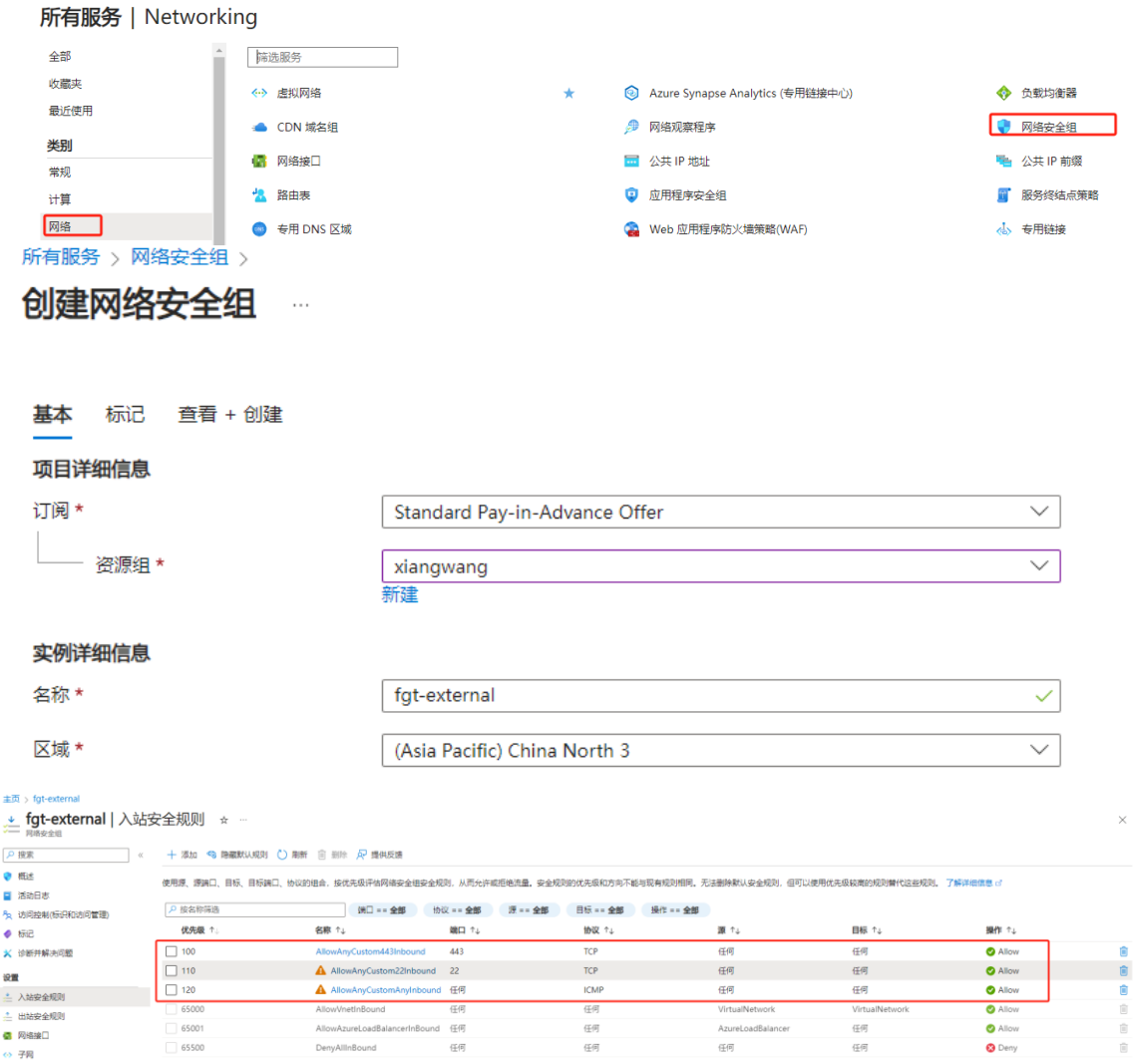
选择虚拟网络→ vpc1→ 子网，点击“子网”，创建子网。



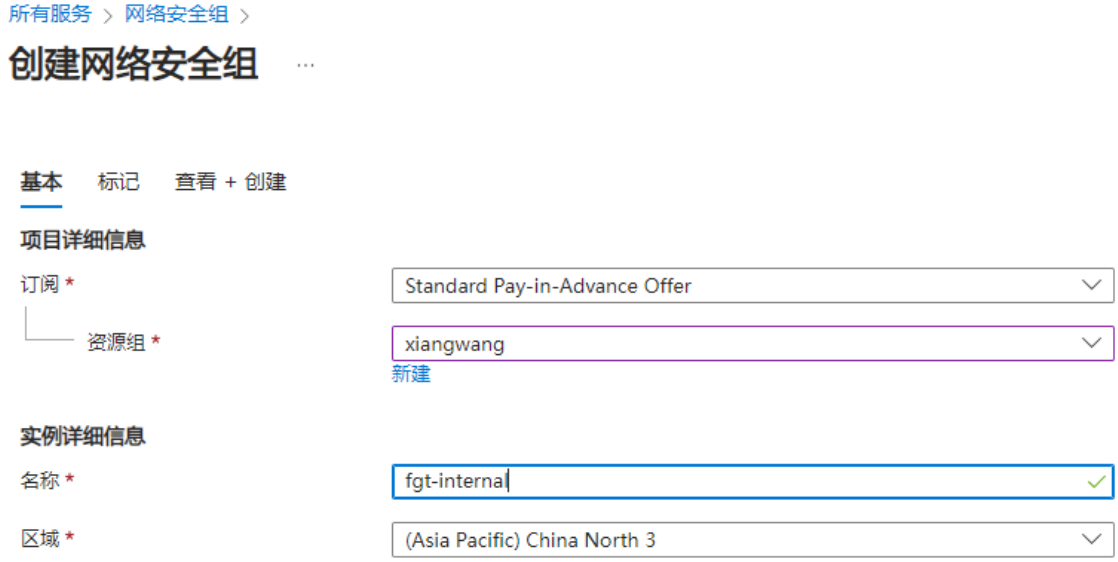
3. 2. 创建安全组

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“网络”→“网络安全组”→“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。

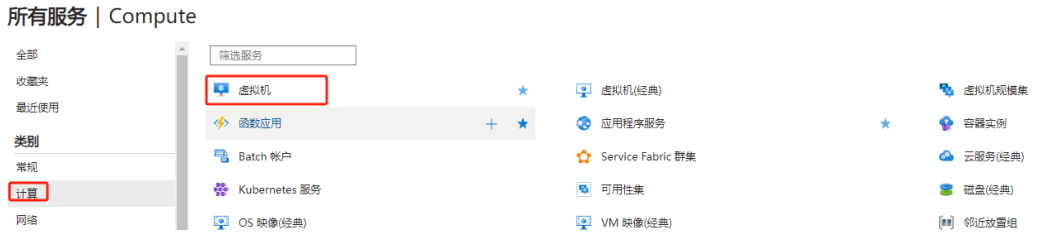


入站规则放通所有。

Azure 出站规则默认只允许 VirtualNetwork 到 VirtualNetwork、任何到 Internet 的访问，并没有允许 Internet 到 VirtualNetwork 的访问。因此如果外网通过 FortiGate VIP 访问内部 VM 则会被拒绝，这里新增一条任何到任何的全通策略。

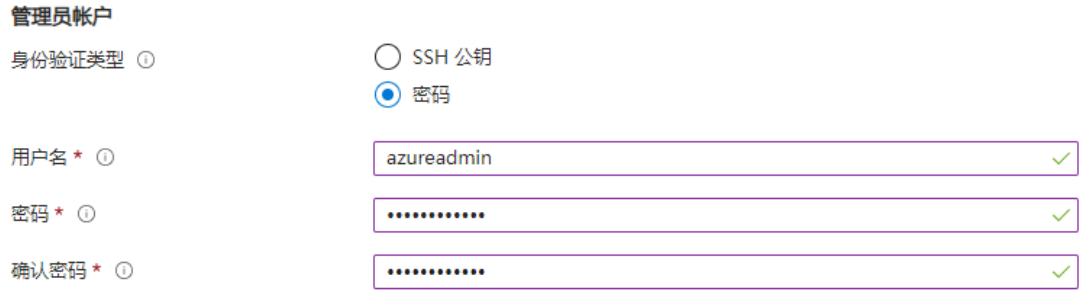
3.3. 部署 FortiGate

选择计算→虚拟机，点击“创建”。



实例类型请选择**计算优化型**，这里使用 F4s_v2，选择 FortiGate v7.0 的版本，所创建的虚拟网络，虚拟机，安全组，公网 IP 等都要在一个资源组内。

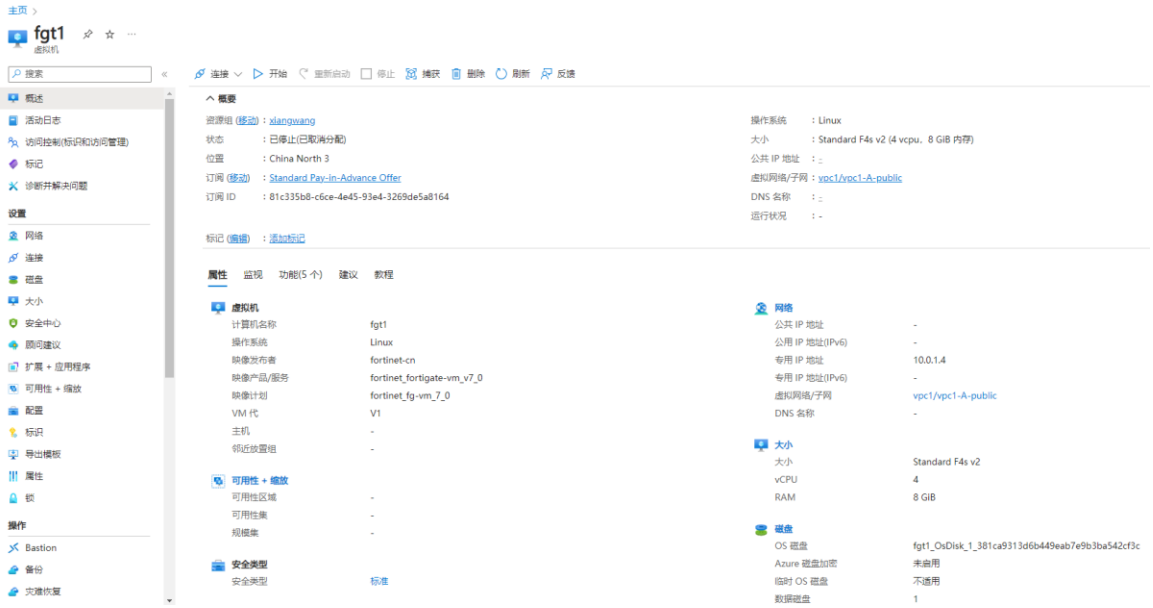
输入 FortiGate 实例的账号和密码



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。

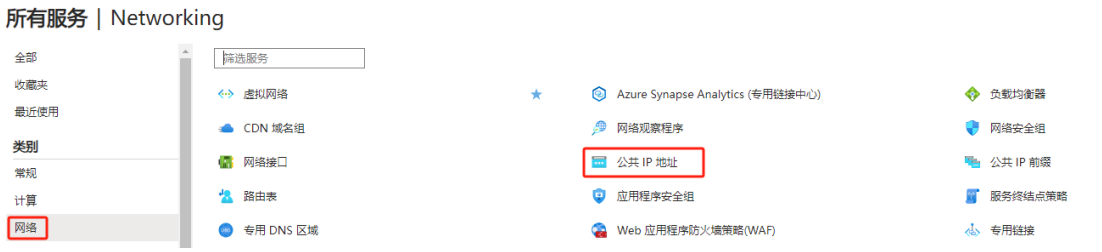
选择虚拟网络“vpc1”，及 port1 所在的子网“vpc1-A-public”，公网 IP 后续创建，先选择“无”，port1 的安全组选择 fgt-external。

部署完成。


主页 >
fgt1
虚拟机
搜索
概述
活动日志
访问控制(标识和访问管理)
标记
诊断并解决问题
设置
网络
连接
磁盘
大小
安全中心
顾问建议
扩展 + 应用程序
可用性 + 缩放
配置
标识
导出模板
属性
锁
操作
Bastion
备份
灾难恢复
连接
开始
重新启动
停止
捕获
删除
刷新
反馈
概要
资源组 (移动) : xiangwang
状态 : 已停止(已取消分配)
位置 : China North 3
订阅 (移动) : Standard Pay-In-Advance Offer
订阅 ID : 81c335b8-c6ce-4e45-93e4-3269de5a8164
操作系统 : Linux
大小 : Standard F4s v2 (4 vcpu，8 GiB 内存)
公共 IP 地址 : -
虚拟网络/子网 : vpc1/vpc1-A-public
DNS 名称 : -
运行状况 : -
标记 (编辑) : 添加标记
属性
监视
功能(5 个)
建议
教程
虚拟机
计算机名称 fgt1
操作系统 Linux
映像发布者 fortinet-cn
映像产品/服务 fortinet_fortigate-vm_v7_0
映像计划 fortinet_fg-vm_7_0
VM 代 V1
主机 -
邻近放置组 -
可用性 + 缩放
可用性区域 -
可用性集 -
规模集 -
安全类型
安全类型 标准
网络
公共 IP 地址 -
公用 IP 地址(IPv6) -
专用 IP 地址 10.0.1.4
专用 IP 地址(IPv6) -
虚拟网络/子网 vpc1/vpc1-A-public
DNS 名称 -
大小
大小 Standard F4s v2
vCPU 4
RAM 8 GiB
磁盘
OS 磁盘 fgt1_OsDisk_1_381ca9313d6b449eab7e9b3ba542cf3c
Azure 磁盘加密 未启用
临时 OS 磁盘 不适用
数据磁盘 1

3.4. 公网 IP

选择网络→公网 IP 地址，创建公网 IP。



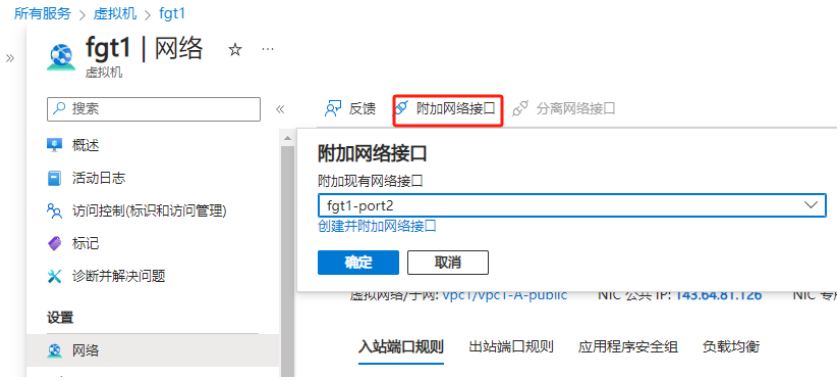
FortiGate 实例 port1 接口的网卡名称是 fgt1615，将公网 IP 关联到该网卡。

3. 5. 网络接口

FortiGate 实例当前只有一个接口 port1，再增加一个网络接口，作为 FortiGate port2 接口。选择网络→网络接口，创建网络接口。

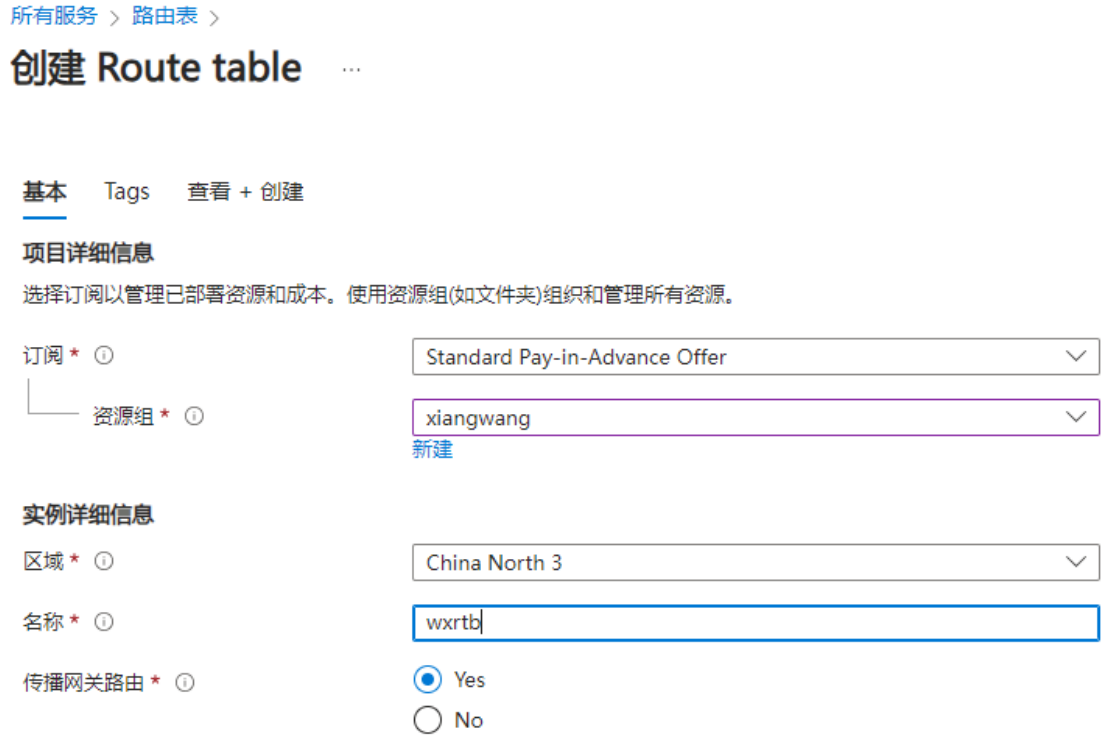
Port2 所在的子网是 vpc1-A-private，安全组是 fgt-internal。

Azure 绑定网卡需要先停止 FortiGate 实例，然后绑定新创建的网卡，再启动实例。

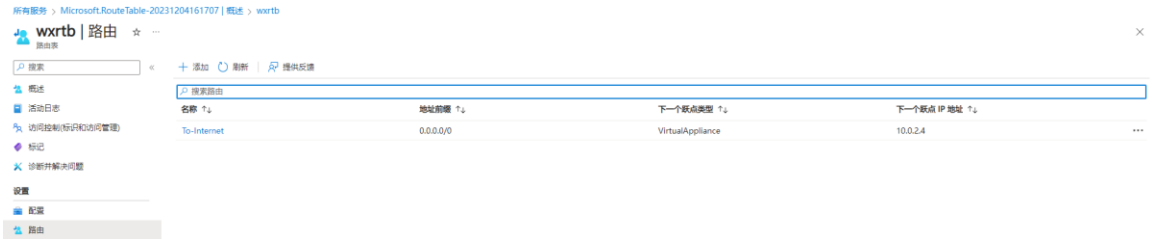


3. 6. 创建路由表

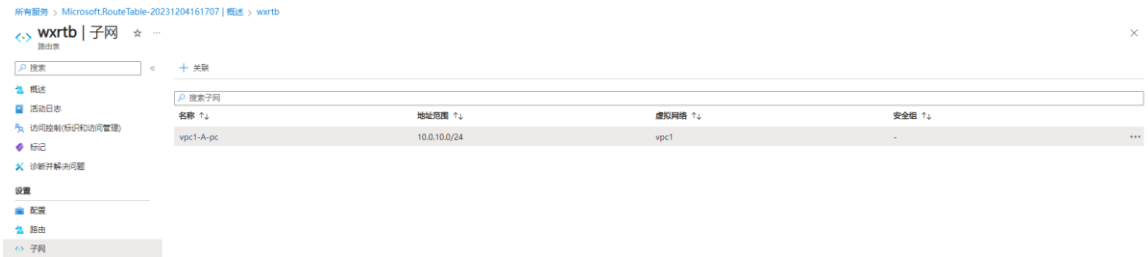
新建路由表用于内网 PC 通过 FortiGate 实例出去。



添加路由，网关 IP 是 FortiGate 实例 port2 接口的 IP



关联 PC 所在的子网。



3.7. 启动 IP 转发

在 FortiGate 实例 port1 和 port2 所在的网卡上都开启 IP 转发。

3.8. 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。

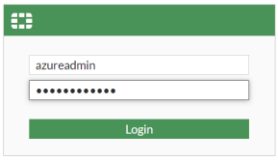
在没有备案之前可以通过修改 FortiGate 的 HTTPS 的登录端口来解决，通过 SSH 登录 FortiGate 修改 HTTPS 端口号。这样就可以通过 GUI 访问 FortiGate。

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

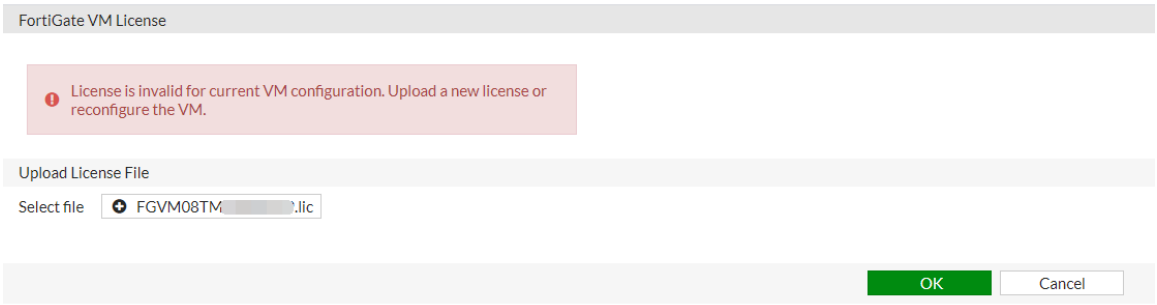
这里使用的 Azure 账号已经备案，可以使用 443 端口。

HTTPS 访问 FortiGate：

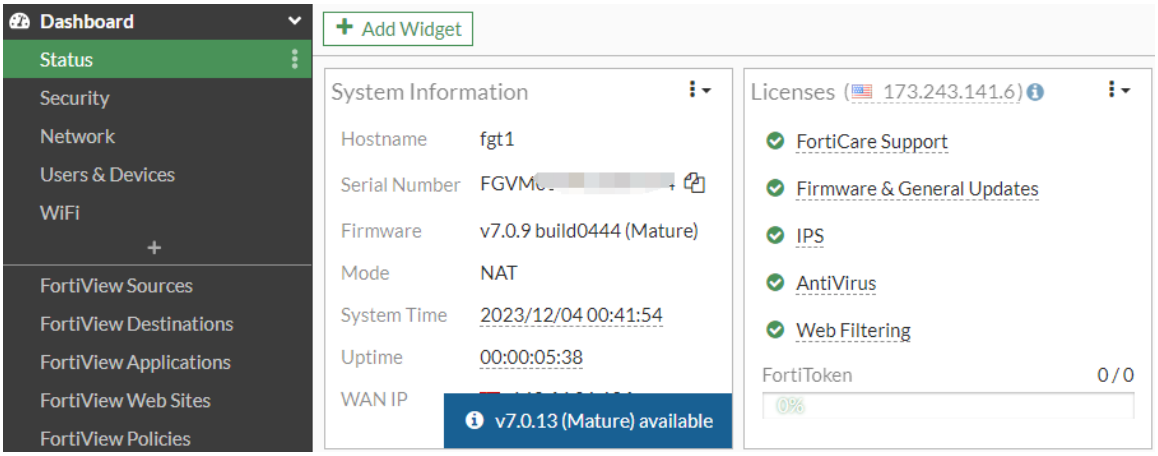
使用 https:// 143.64.81.126（弹性 IP）访问 FortiGate，账号和密码是创建 FortiGate 实例时填写的。



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



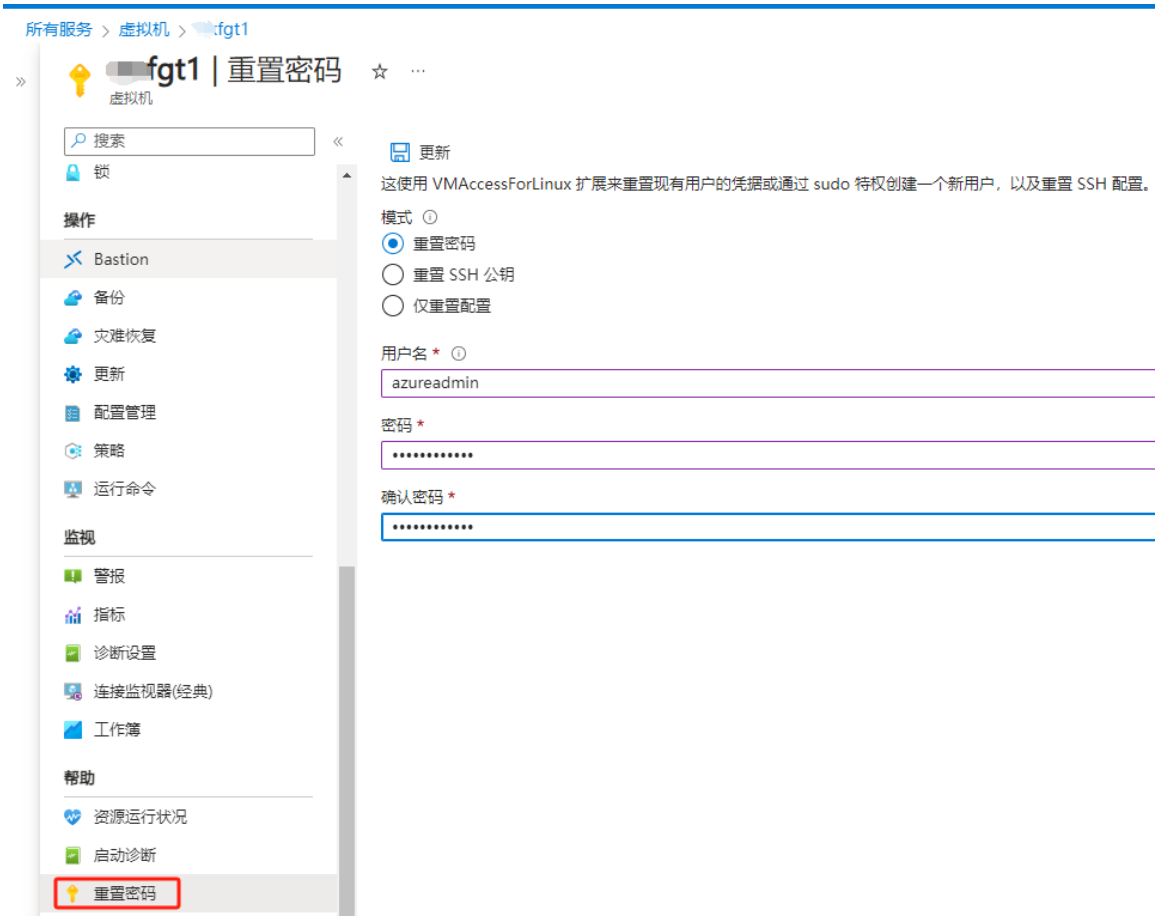
FortiGate 登录成功。



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。

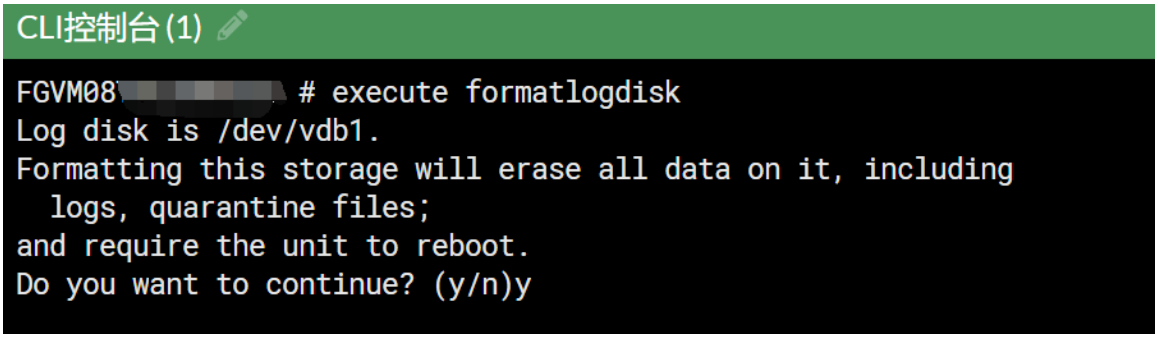
3.9. 重置密码

当执行“execute factoryreset keepvmlicense”，部署 FortiGate 实例的密码也会移除，因此需要通过重置密码来恢复之前设定的账号和密码。



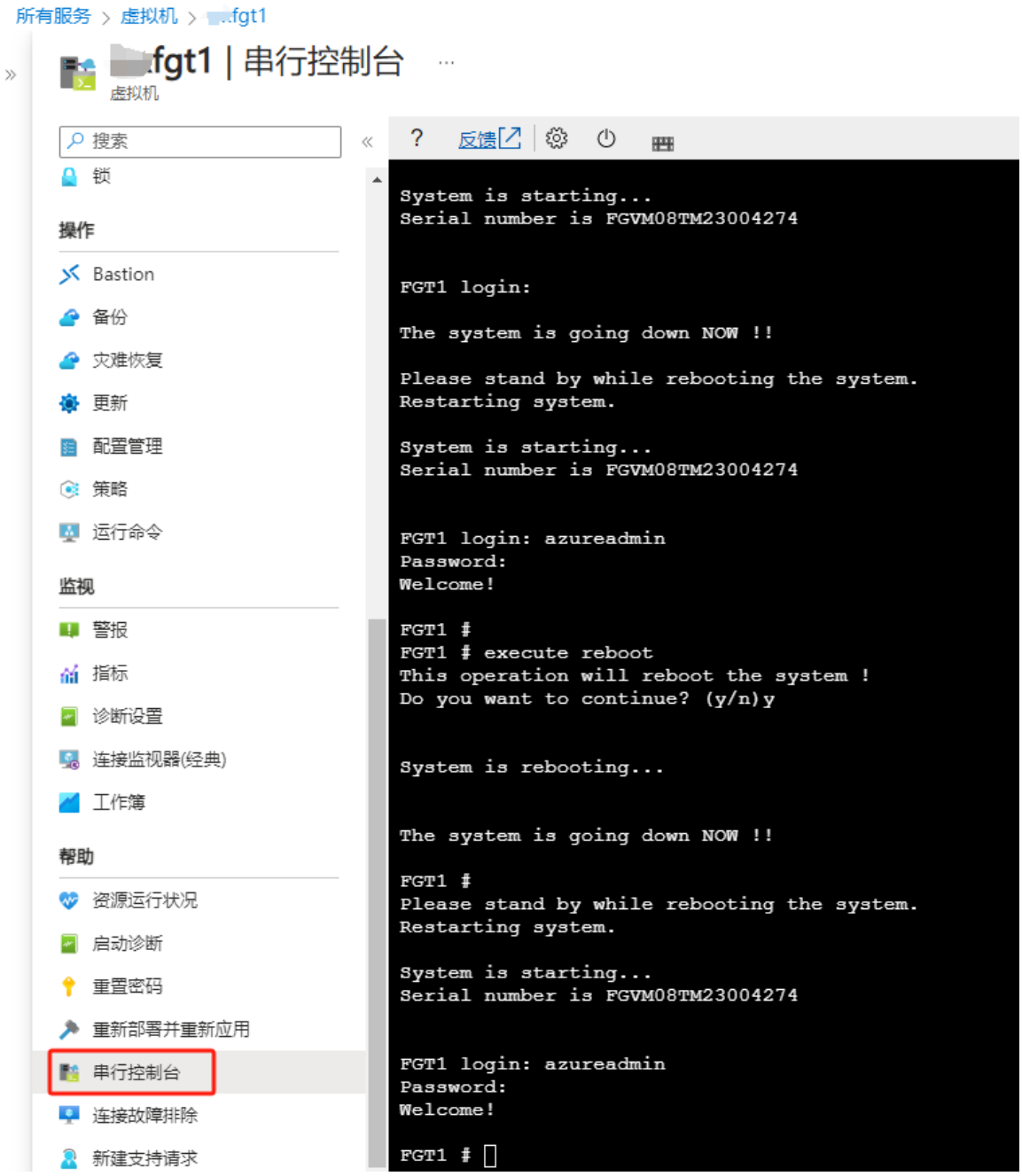
3.10. 格式化硬盘

执行 execute formatlogdisk 格式化记录日志的硬盘。



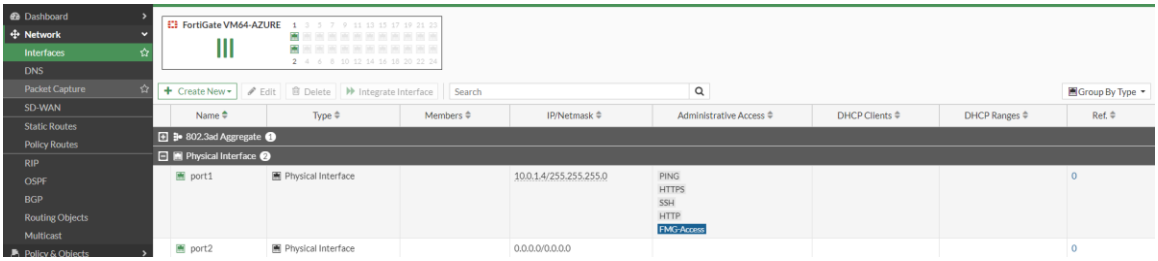
3.11. Console 查看 FortiGate 实例

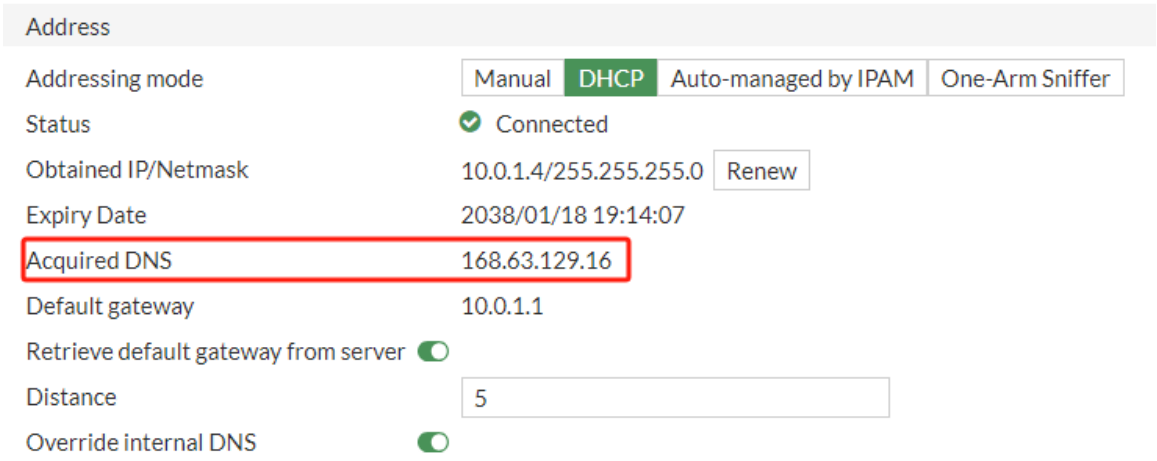
可通过点击虚拟机下“串行控制台”进入 FortiGate 实例的 console。



3.12. FortiGate 配置源 NAT

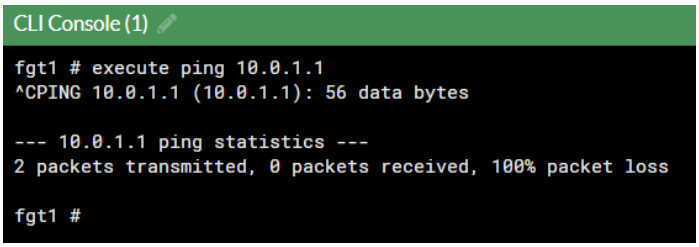
FortiGate 默认会 DHCP 获取 Azure 分配的地址、DNS、路由表如下：





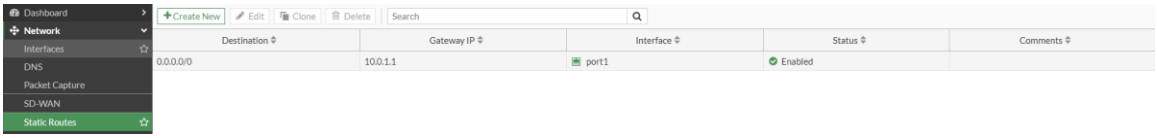

```
fgt1 # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS 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 10.0.1.1, port1, [1/0]
C       10.0.1.0/24 is directly connected, port1
```

Azure 的虚拟网关不能被 ping 通。

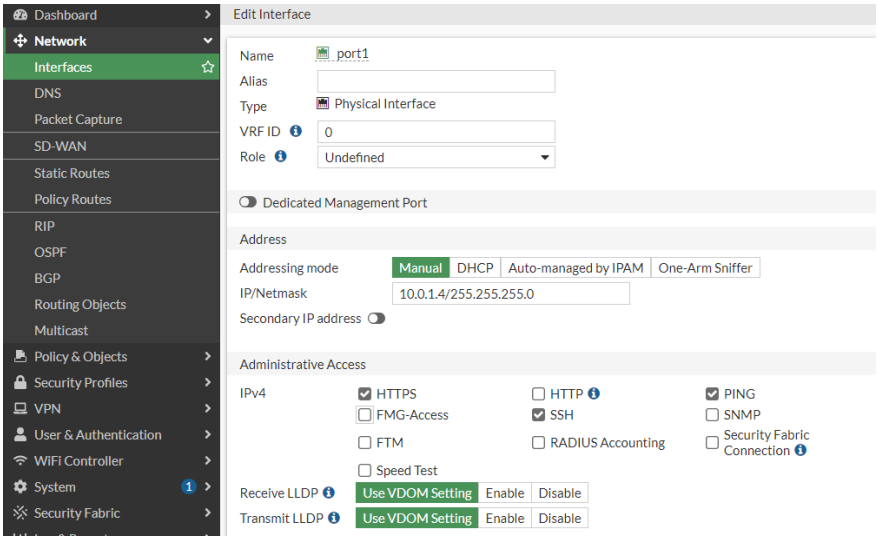


Port2 接口是附加的弹性接口，接口 ip 默认是静态配置。这里将 port1 的接口 IP 也从 DHCP 改为静态配置，并添加默认的路由。

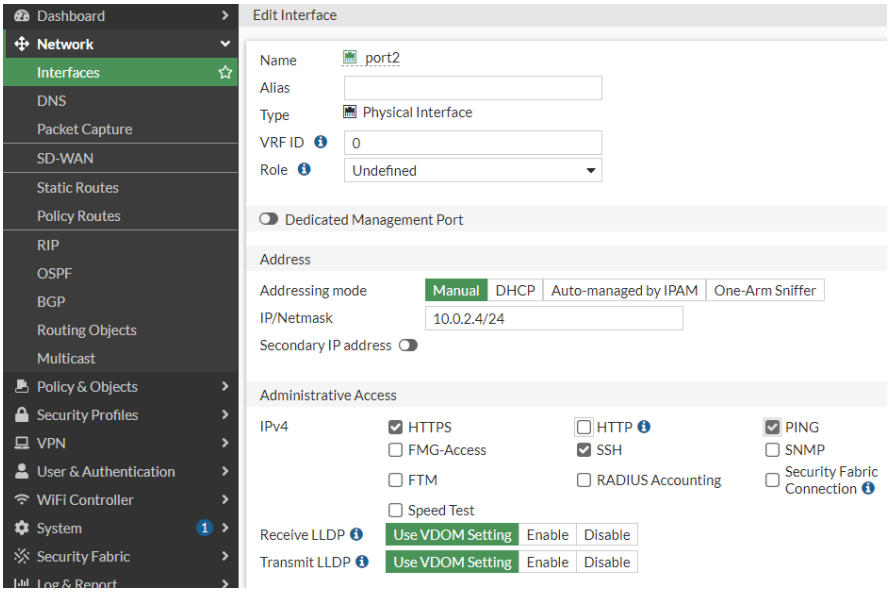
先配置默认路由，网关与 DHCP 获取的网关一致，避免 port1 接口改为静态配置 IP 后无法管理。



修改 port1 IP 的配置为手动。

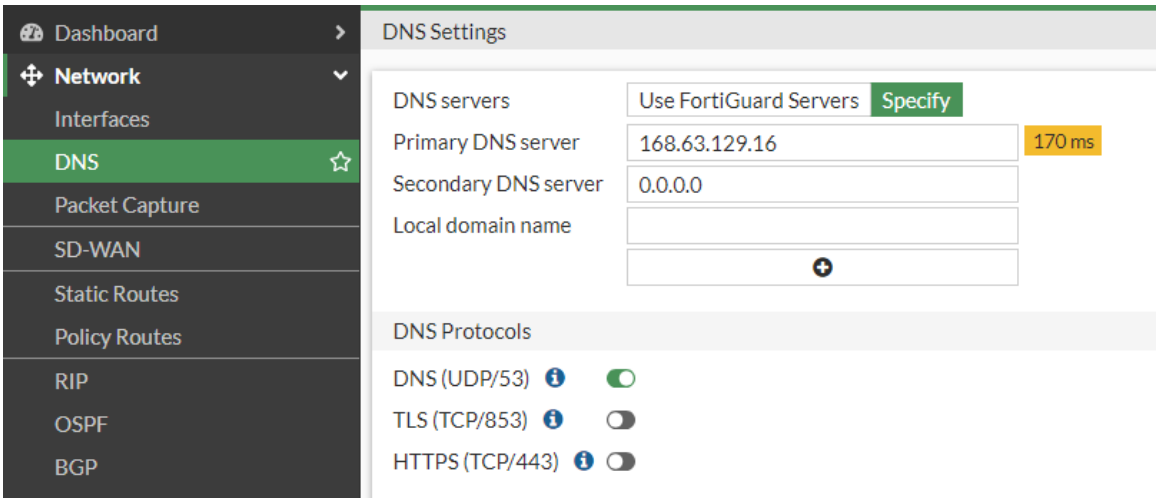


同样设置 port2 接口的 IP。

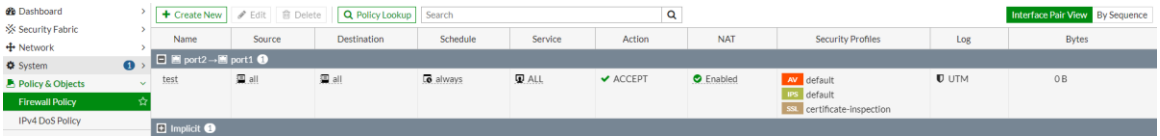


配置 10.0.0.0/16 的内部路由指向 port2 所有子网的虚拟网关 10.0.2.1，虚拟网关是该子网的第 1 个地址。

修改 FortiGate DNS 为 Azure 的 DNS。



配置防火墙策略。

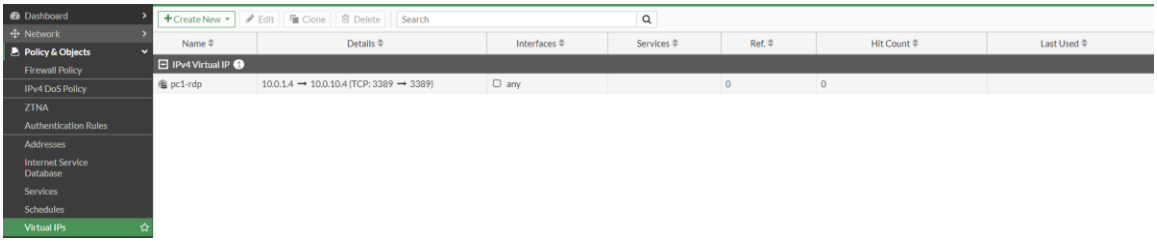


3.13. FortiGate 配置目的 NAT

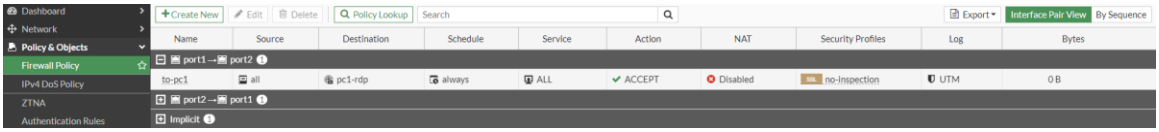
可以使用 port1 接口的地址做目的 NAT，也可以分配一个单独的 IP 来做目的 NAT。

这里使用 port1 接口的地址做目的 NAT：

配置 VIP，external 地址是 10.0.1.4，internal 地址是 10.0.10.4（新建的测试 PC）：



配置防火墙策略调用 VIP：



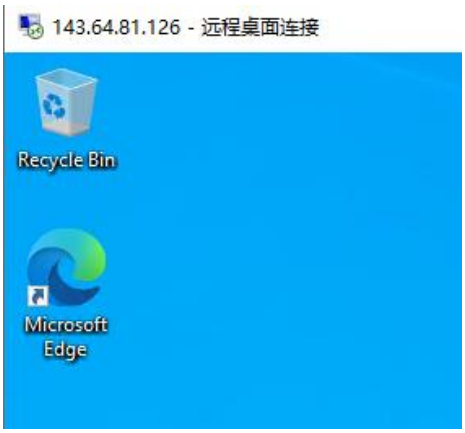
在 fgt-external 安全组中放通 3389 端口。

4. 业务测试

测试的 PC 如下

目的 NAT 测试：

RDP 143.64.81.126 访问正常。



源 NAT 测试：

ping 223.5.5.5 正常