



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

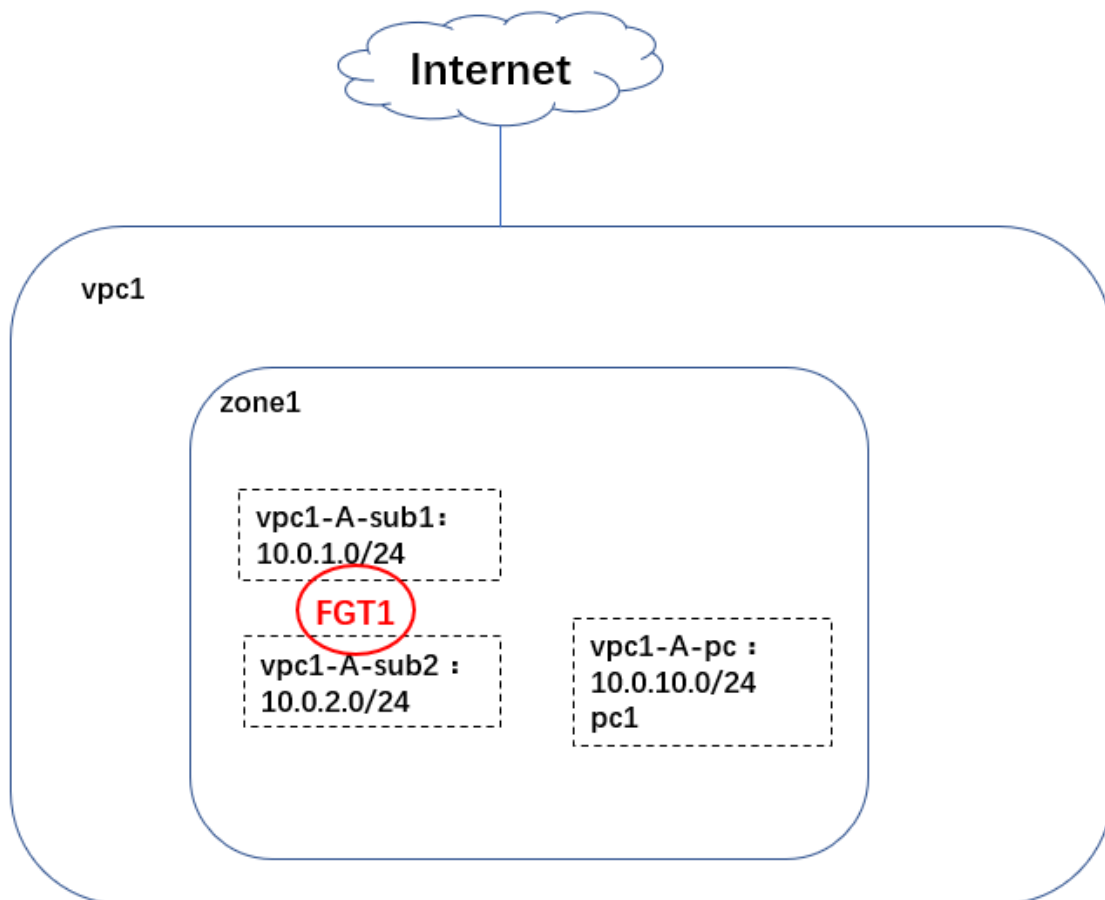
目录

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”。



所有服务 > 虚拟网络 >

创建虚拟网络 ...

基本信息 安全性 IP 地址 标记 查看 + 创建

使用所需的 IPv4 和 IPv6 地址及子网配置虚拟网络地址空间。 [了解详细信息](#)

使用一个或多个 IPv4 或 IPv6 地址范围定义虚拟网络的地址空间。创建子网以将虚拟网络地址空间分段为较小的范围，供应用程序使用。将资源部署到子网时，Azure 会从子网为资源分配 IP 地址。 [了解更多](#)

添加 IPv4 地址空间 | v

10.0.0.0/16
删除地址空间

/16 个(共 65,536 个地址) v

10.0.0.0 - 10.0.255.255 (65536 个地址)

+ 添加子网

子网	IP 地址范围	大小	NAT 网关
default	10.0.0.0 - 10.0.0.255	/24 个(共 256 个地址)	-

创建完成。

The screenshot shows the 'vpc1' configuration page in the Azure portal. The left sidebar contains navigation options like '概述', '活动日志', '访问控制', '标记', '诊断并解决问题', '设置', '地址空间', and '已连接的设备'. The main content area displays details for the virtual network, including its name 'vpc1', location 'China North 3', and subscription ID. A '地址空间' (Address Space) section shows the configured address range '10.0.0.0/16'.

选择虚拟网络 → vpc1 → 子网，点击“子网”，创建子网。

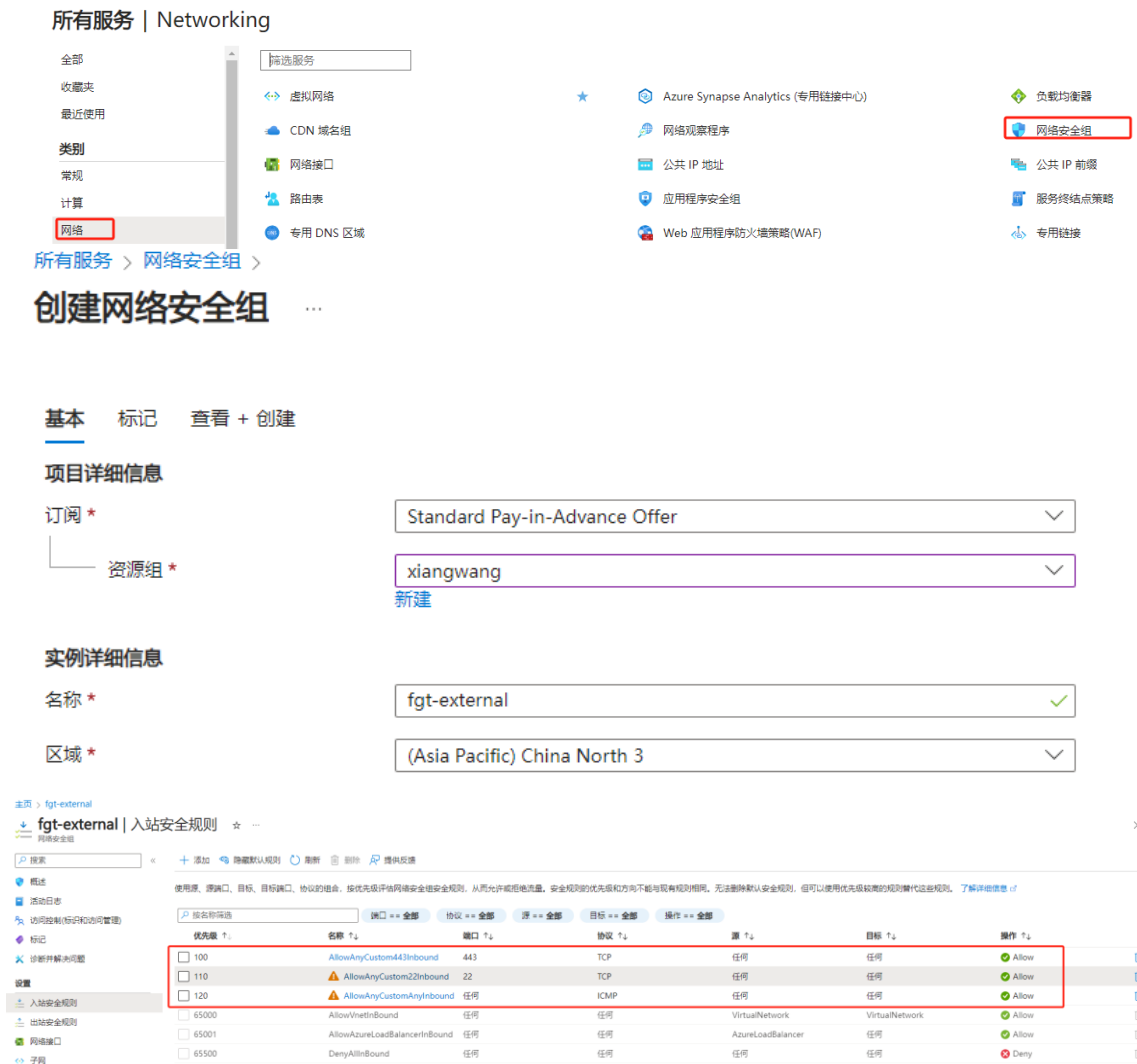
The screenshot shows the 'Subnets' page for the virtual network 'vpc1'. A table lists the subnets created:

名称	IPv4 子网	IPv6 子网	可用的 IP 子网	资源对象	安全组	路由表
default	10.0.0.0/24	-	251	-	-	...
vpc1-A-public	10.0.1.0/24	-	251	-	-	...
vpc1-A-private	10.0.2.0/24	-	251	-	-	...
vpc1-A-pc	10.0.10.0/24	-	251	-	-	...

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。

所有服务 > 网络安全组 >

创建网络安全组 ...

基本 标记 查看 + 创建

项目详细信息

订阅 * Standard Pay-in-Advance Offer

资源组 * xiangwang
新建

实例详细信息

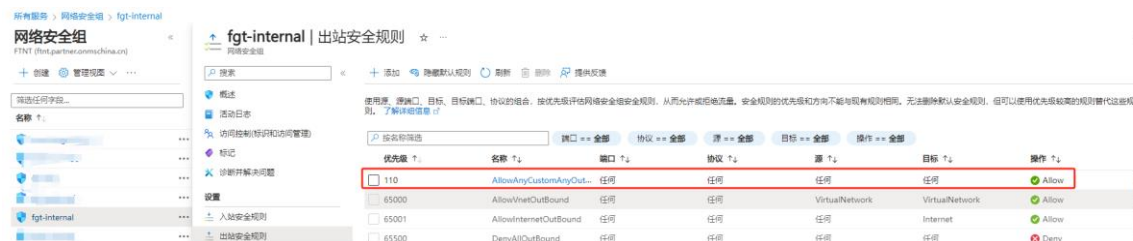
名称 * fgt-internal

区域 * (Asia Pacific) China North 3

进站规则放通所有。

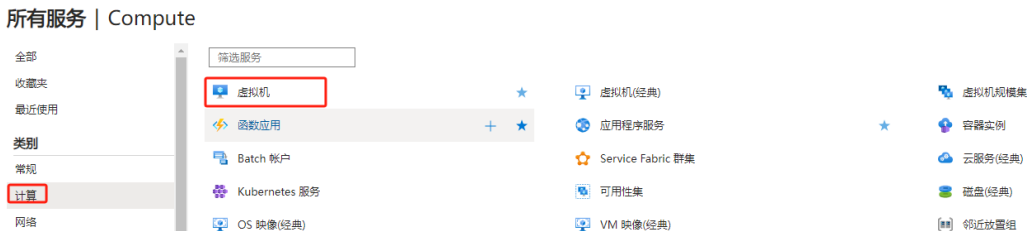


Azure 出站规则默认只允许 VirtualNetwork 到 VirtualNetwork、任何到 Internet 的访问,并没有允许 Internet 到 VirtualNetwork 的访问。因此如果外网通过 FortiGate VIP 访问内部 VM 则会被拒绝,这里新增一条任何到任何的全通策略。



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。

[所有服务](#) > [虚拟机](#) >

创建虚拟机 ...

[基本](#) [磁盘](#) [网络](#) [管理](#) [监视](#) [高级](#) [标记](#) [查看 + 创建](#)

创建运行 Linux 或 Windows 的虚拟机。从 Azure 市场中选择映像，或使用自定义的映像。完成“基本信息”选项卡，然后通过“查看+创建”，使用默认参数来设置虚拟机，或查看每个选项卡，全部实施自定义。 [了解详细信息](#)

项目详细信息

选择订阅以管理已部署资源和成本。使用资源组(如文件夹)组织和管理所有资源。

订阅 * ①

资源组 * ① [新建](#)

实例详细信息

虚拟机名称 * ① ✓

区域 * ①

可用性选项 ①

安全类型 ①

映像 * ① [查看所有映像](#) | [配置 VM 生成](#)

大小 * ① [查看所有大小](#)

输入 FortiGate 实例的账号和密码

管理员帐户

身份验证类型 ^① SSH 公钥 密码

用户名 * ^① ✓

密码 * ^① ✓

确认密码 * ^① ✓

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。

[所有服务](#) > [虚拟机](#) >

创建虚拟机 ...

基本 **磁盘** 网络 管理 监视 高级 标记 查看 + 创建

Azure VM 具有一个操作系统磁盘和一个用于短期存储的临时磁盘。可附加其他数据磁盘。VM 的大小决定可使用的存储类型和允许使用的数据磁盘数量。 [了解更多信息](#)

磁盘选项

OS 磁盘大小 ^① ▾

OS 磁盘类型 * ^① ▾

加密类型 * ▾

启用超级磁盘兼容性 ^① 对于所选的 VM 大小 Standard_F4s_v2，超级磁盘在一个或多个可用性区域 2,3 中受支持。

fgt1 的数据磁盘

可以添加和配置虚拟机的其他数据磁盘或附加现有磁盘。此 VM 还附带的临时磁盘。

L...	名称	大小(GiB)	磁盘类型	主机缓存
0	fgt1_DataDisk_0	64	高级 SSD LRS	只读 ▾  

[创建并附加新磁盘](#) [附加现有磁盘](#)

∨ 高级

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。

[所有服务](#) > [虚拟机](#) >

创建虚拟机 ...

通过配置网络接口卡(NIC)设置来定义虚拟机的网络连接。你可通过安全组规则来控制端口、入站连接和出站连接，也可采用现有负载均衡解决方案。 [了解更多信息](#)

网络接口

创建虚拟机时，Azure 门户会创建一个网络接口。

虚拟网络 * ①	<input type="text" value="vpc1"/> ▼ 新建
子网 * ①	<input type="text" value="vpc1-A-public (10.0.1.0/24)"/> ▼ 管理子网配置
公用 IP ①	<input type="text" value="无"/> ▼ 新建
NIC 网络安全组 ①	<input type="radio"/> 无 <input type="radio"/> 基本 <input checked="" type="radio"/> 高级

i 此 VM 映像已预配置 NSG 规则

配置网络安全组 *	<input type="text" value="fgt-external"/> ▼ 新建
-----------	--

启用加速网络 ①	<input type="checkbox"/>	所选的映像不支持加速网络。
----------	--------------------------	---------------

负载均衡

可将此虚拟机放在现有 Azure 负载均衡解决方案的后端池中。 [了解更多信息](#)

是否将此虚拟机置于现有负载均衡解决方案之后?

部署完成。

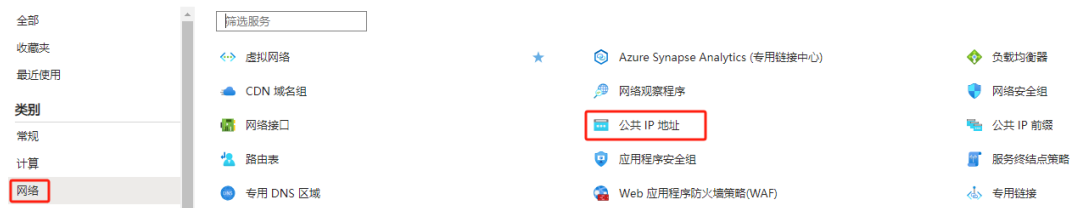
The screenshot displays the Azure portal interface for a virtual machine named 'fgt1'. The left-hand navigation pane includes sections for '概述' (Overview), '设置' (Settings), and '操作' (Operations). The main content area is divided into several sections:

- 概要 (Summary):**
 - 资源组 (Resource Group): xiangwang
 - 状态 (Status): 已停止 (已取消分配) (Stopped (Deallocated))
 - 位置 (Location): China North 3
 - 订购 (Offer): Standard Pay-In-Advance Offer
 - 订购 ID (Order ID): 81c335b8-c6ce-4e45-93e4-3269de5a8164
 - 操作系统 (OS): Linux
 - 大小 (Size): Standard F4s v2 (4 vcpu, 8 GiB 内存)
 - 公共 IP 地址 (Public IP): -
 - 虚拟网络/子网 (Virtual Network/Subnet): vpc1/vpc1-A-public
 - DNS 名称 (DNS Name): -
 - 运行状况 (Health): 1 -
- 属性 (Properties):**
 - 虚拟机 (Virtual Machine):**
 - 计算机名称 (Computer Name): fgt1
 - 操作系统 (OS): Linux
 - 映像发布者 (Image Publisher): fortinet-cn
 - 映像产品/服务 (Image Product/Service): fortinet_fortigate-vm_v7_0
 - 映像计划 (Image Plan): fortinet_fg-vm_7_0
 - VM 代 (VM Gen): V1
 - 主机 (Host): -
 - 邻近放置组 (Proximity Placement Group): -
 - 可用性 + 缩放 (Availability + Scaling):**
 - 可用性区域 (Availability Zone): -
 - 可用性集 (Availability Set): -
 - 规模集 (Scale Set): -
 - 安全类型 (Security Type):**
 - 安全类型 (Security Type): 标准 (Standard)
- 网络 (Network):**
 - 公共 IP 地址 (Public IP): -
 - 公用 IP 地址 (IPv6) (Public IP (IPv6)): -
 - 专用 IP 地址 (Private IP): 10.0.1.4
 - 专用 IP 地址 (IPv6) (Private IP (IPv6)): -
 - 虚拟网络/子网 (Virtual Network/Subnet): vpc1/vpc1-A-public
 - DNS 名称 (DNS Name): -
- 大小 (Size):**
 - 大小 (Size): Standard F4s v2
 - vCPU: 4
 - RAM: 8 GiB
- 磁盘 (Disks):**
 - OS 磁盘 (OS Disk): fgt1_OsDisk_1_381ca9313d6b449eab7e9b3ba542cf3c
 - Azure 磁盘加密 (Azure Disk Encryption): 未启用 (Not Enabled)
 - 临时 OS 磁盘 (Temporary OS Disk): 不适用 (Not Applicable)
 - 数据磁盘 (Data Disk): 1

3.4. 公网 IP

选择网络→公网 IP 地址，创建公网 IP。

所有服务 | Networking



所有服务 > 公共 IP 地址 >

创建公共 IP 地址 ...

基本信息 标记 审阅 + 创建

创建公共 IP 地址。将其与虚拟机或其他 Azure 资源相关联。Internet 资源通过公共 IP 地址与 Azure 资源通信。 [了解详细信息。](#)

项目详细信息

选择订阅以管理已部署的资源 and 成本。使用资源组 (如文件夹) 来整理和管理所有资源。

订阅 ⓘ *

资源组 ⓘ * [新建](#)

实例详细信息

区域 ⓘ *

配置详细信息

名称 *

IP 版本 * ⓘ IPv4 IPv6

SKU * ⓘ 标准 基本

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

主页 > fgt1

fgt1 | 网络 ☆ ... 虚拟机

搜索 << 反馈 附加网络接口 分离网络接口

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

fgt1615

IP 配置 ①
ipconfig1 (主要)

网络接口: **fgt1615** 有效安全规则
虚拟网络/子网: [vpc1/vpc1-A-public](#) NIC 公共 IP: - NIC 专用 IP: 10.0.1.4

进站端口规则 出站端口规则 应用程序安全组 负载均衡

网络安全组 **fgt-external** (附加到网络接口: **fgt1615**)
影响 0 个子网, 1 个网络接口

优先级	名称
100	AllowAnyCustom443Inbound
110	⚠ AllowAnyCustom22Inbound
120	⚠ AllowAnyCustomAnyInbound
65000	AllowVnetInBound
65001	AllowAzureLoadBalancerInBound
65500	DenyAllInBound

wxfgt-port1 公网 IP 地址

关联公共 IP 地址

选择此公共 IP 地址要关联的资源。

资源类型
网络接口
网络接口
fgt1615
资源池: vlangwang

概述
活动日志
访问控制(标识和访问管理)
标记
设置
配置
导出模板

名称: wxfgt-port1
SKU: Standard
层: Regional
IP 地址: 143.64.81.126
DNS 名称: -
已关联到: 1

资源组 (链接): [vlangwang](#)
位置: China North 3 (区域 3, 2, 1)
订购 (链接): [Standard Pay-in-Advance Offer](#)
订购 ID: 81c335b8-c5ce-4e45-93e4-3269d548164
标记 (链接): [添加标记](#)
查看步骤

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。

[所有服务](#) > [网络接口](#) >

创建网络接口 ...

基本 标记 查看 + 创建

创建一个网络接口, 并将其附加到虚拟机。网络接口使虚拟机能够与 Internet、Azure 和本地资源进行通信。
[详细了解网络接口](#)

项目详细信息

订阅 *

资源组 * [新建](#)

实例详细信息

名称 * ✓

区域 *

虚拟网络 * [编辑虚拟网络](#)

子网 * [编辑子网](#) 10.0.2.0 - 10.0.2.255 (256 个地址)

专用 IP 地址分配 动态 静态

网络安全组

专用 IP 地址(IPv6)

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。

所有服务 > 路由表 >

创建 Route table ...

基本 Tags 查看 + 创建

项目详细信息

选择订阅以管理已部署资源和成本。使用资源组(如文件夹)组织和管理所有资源。

订阅 * ⓘ

资源组 * ⓘ
新建

实例详细信息

区域 * ⓘ

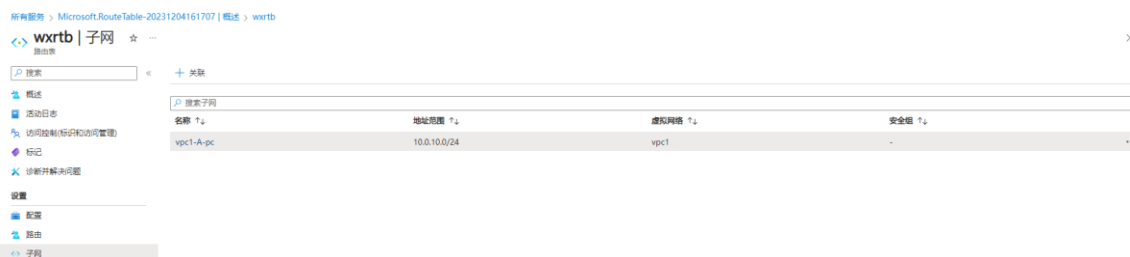
名称 * ⓘ

传播网关路由 * ⓘ Yes No

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。

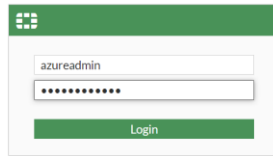
在没有备案之前可以通过修改 FortiGate 的 HTTPS 的登录端口来解决,通过 SSH 登录 FortiGate 修改 HTTPS 端口号。这样就可以通过 GUI 访问 FortiGate。

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

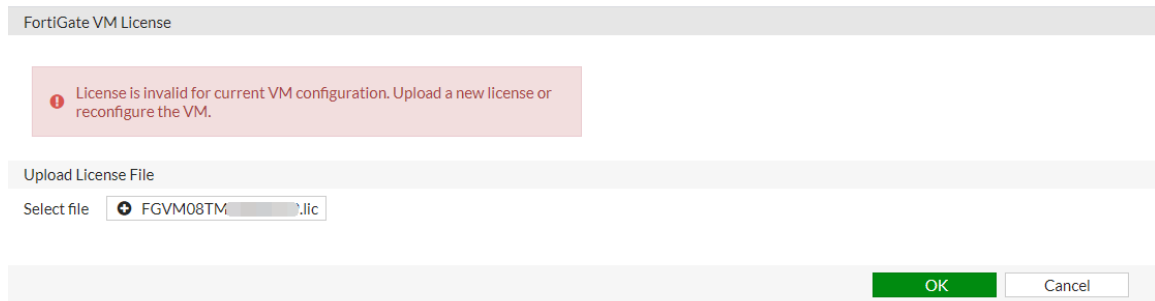
这里使用的 Azure 账号已经备案,可以使用 443 端口。

HTTPS 访问 FortiGate:

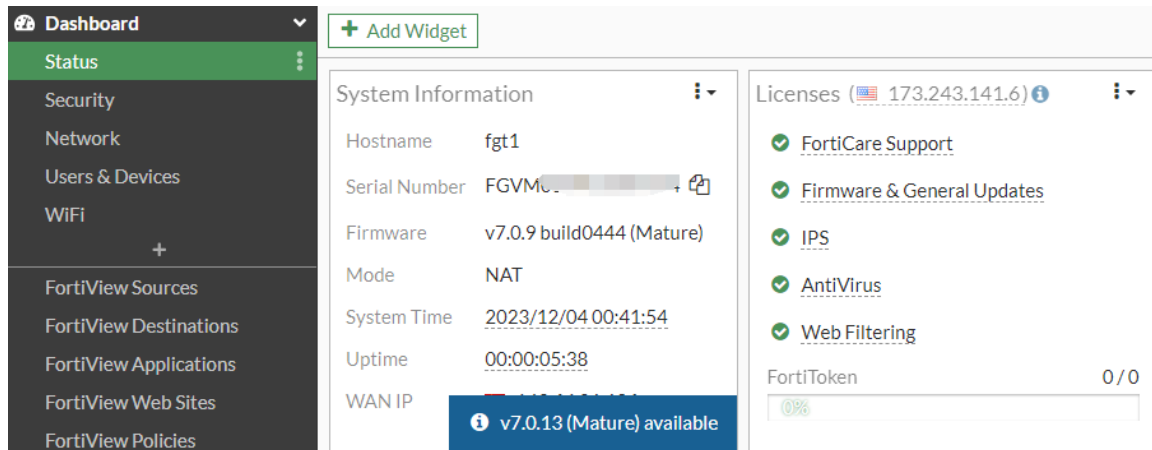
使用 [https:// 143.64.81.126](https://143.64.81.126) (弹性 IP) 访问 FortiGate, 账号和密码是创建 FortiGate 实例时填写的。



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



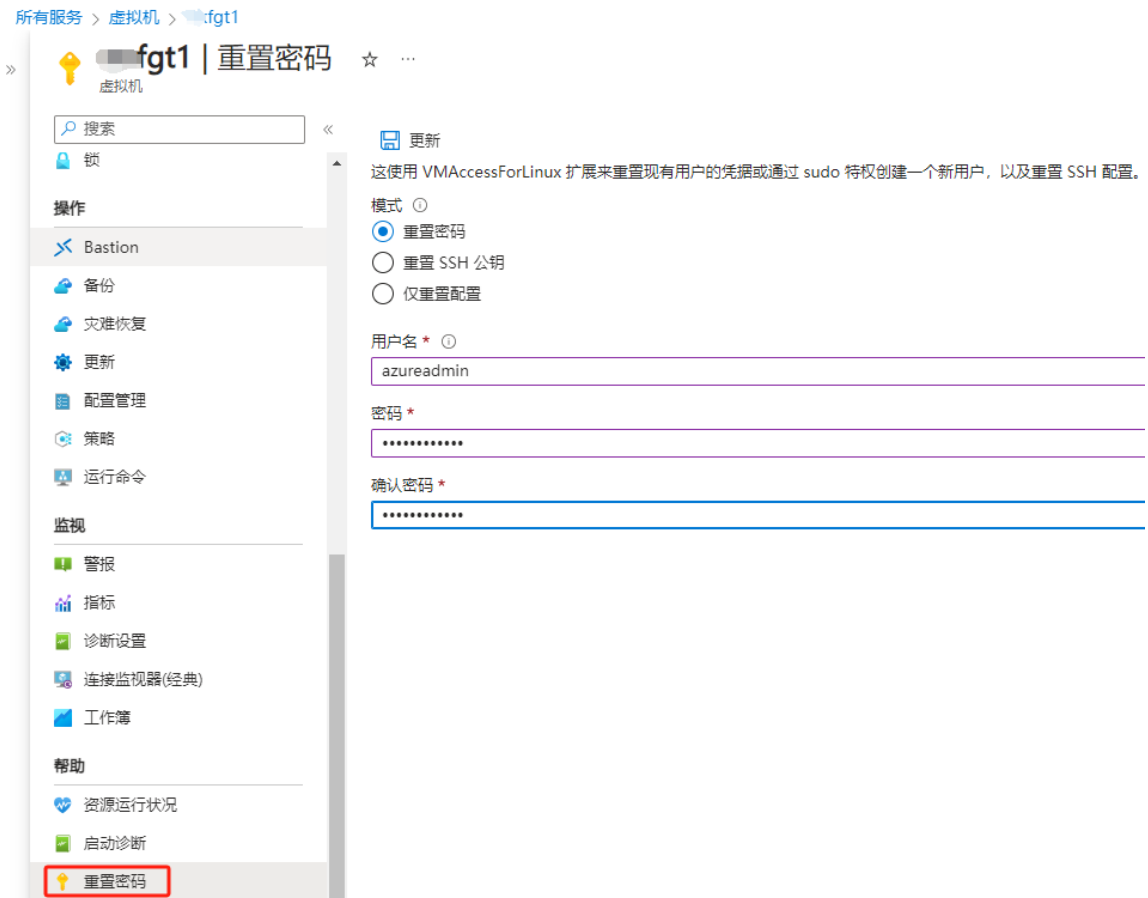
FortiGate 登录成功。



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。

```
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
```

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。

所有服务 > 虚拟机 > fgt1

>> fgt1 | 串行控制台 ...

虚拟机

搜索

锁

操作

- Bastion
- 备份
- 灾难恢复
- 更新
- 配置管理
- 策略
- 运行命令

监视

- 警报
- 指标
- 诊断设置
- 连接监视器(经典)
- 工作簿

帮助

- 资源运行状况
- 启动诊断
- 重置密码
- 重新部署并重新应用
- 串行控制台**
- 连接故障排除
- 新建支持请求

```
? 反馈 设置 电源 帮助
System is starting...
Serial number is FGVM08TM23004274

FGT1 login:

The system is going down NOW !!
Please stand by while rebooting the system.
Restarting system.

System is starting...
Serial number is FGVM08TM23004274

FGT1 login: azureadmin
Password:
Welcome!

FGT1 #
FGT1 # execute reboot
This operation will reboot the system !
Do you want to continue? (y/n)y

System is rebooting...

The system is going down NOW !!

FGT1 #
Please stand by while rebooting the system.
Restarting system.

System is starting...
Serial number is FGVM08TM23004274

FGT1 login: azureadmin
Password:
Welcome!

FGT1 #
```

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：

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
port1	Physical Interface		10.0.1.4/255.255.255.0	PING HTTPS SSH HTTP FMG Access			0
port2	Physical Interface		0.0.0.0/0.0.0.0				0

Address

Addressing mode: Manual DHCP Auto-managed by IPAM One-Arm Sniffer

Status: Connected

Obtained IP/Netmask: 10.0.1.4/255.255.255.0

Expiry Date: 2038/01/18 19:14:07

Acquired DNS: 168.63.129.16

Default gateway: 10.0.1.1

Retrieve default gateway from server:

Distance:

Override internal DNS:

```

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。

```

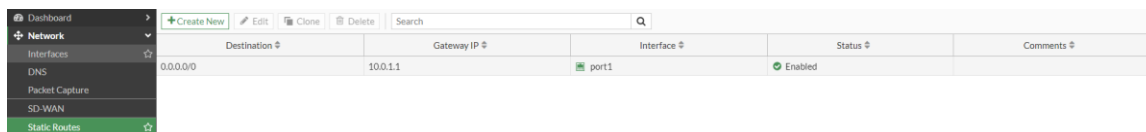
CLI Console (1)
fgt1 # execute ping 10.0.1.1
^CPING 10.0.1.1 (10.0.1.1): 56 data bytes

--- 10.0.1.1 ping statistics ---
2 packets transmitted, 0 packets received, 100% packet loss

fgt1 #
    
```

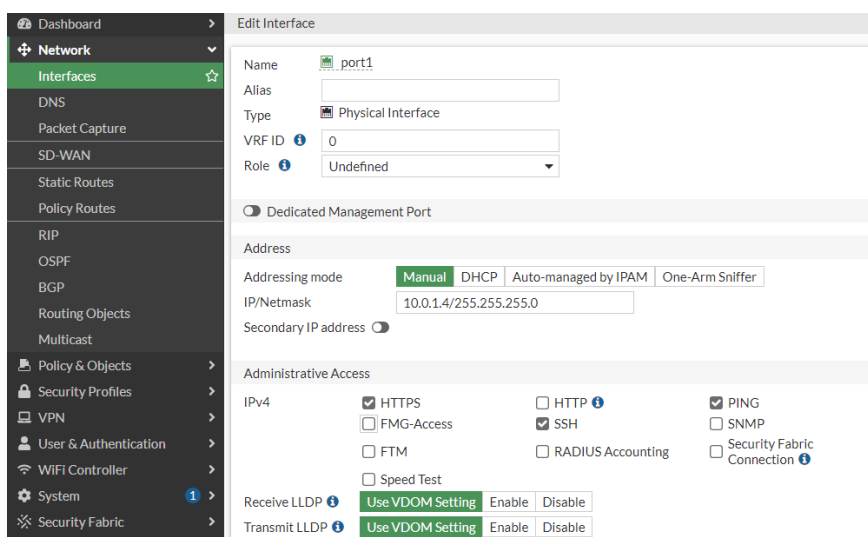
Port2 接口是附加的弹性接口，接口 ip 默认是静态配置。这里将 port1 的接口 IP 也从 DHCP 改为静态配置，并添加默认的路由。

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。



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.0.1.1	port1	Enabled	

修改 port1 IP 的配置为手动。



Edit Interface

Name: port1
Alias:
Type: Physical Interface
VRF ID: 0
Role: Undefined

Dedicated Management Port

Address

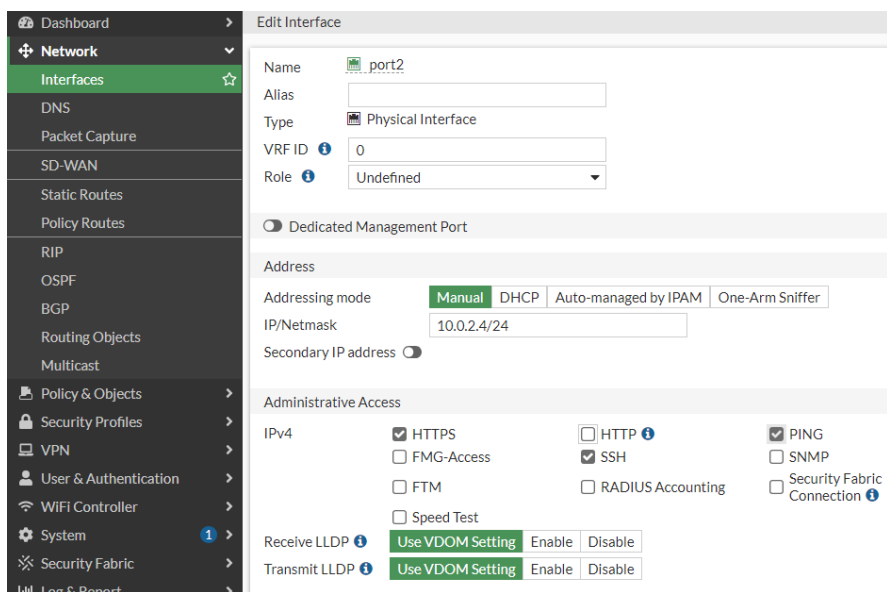
Addressing mode: **Manual** | DHCP | Auto-managed by IPAM | One-Arm Sniffer
IP/Netmask: 10.0.1.4/255.255.255.0
Secondary IP address:

Administrative Access

IPv4: HTTPS | HTTP | PING
 FMG-Access | SSH | SNMP
 FTM | RADIUS Accounting | Security Fabric Connection
 Speed Test

Receive LLDP: Use VDOM Setting | Enable | Disable
Transmit LLDP: Use VDOM Setting | Enable | Disable

同样设置 port2 接口的 IP。



Edit Interface

Name: port2
Alias:
Type: Physical Interface
VRF ID: 0
Role: Undefined

Dedicated Management Port

Address

Addressing mode: **Manual** | DHCP | Auto-managed by IPAM | One-Arm Sniffer
IP/Netmask: 10.0.2.4/24
Secondary IP address:

Administrative Access

IPv4: HTTPS | HTTP | PING
 FMG-Access | SSH | SNMP
 FTM | RADIUS Accounting | Security Fabric Connection
 Speed Test

Receive LLDP: Use VDOM Setting | Enable | Disable
Transmit LLDP: Use VDOM Setting | Enable | Disable

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。

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.0.1.1	port1	Enabled
10.0.0.0/16	10.0.2.1	port2	Enabled

修改 FortiGate DNS 为 Azure 的 DNS。

配置防火墙策略。

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
test	port2	port1	always	ALL	ACCEPT	Enabled	default, default, certificate-inspection	UTM	0B

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) :

Name	Details	Interfaces	Services	Ref.	Hit Count	Last Used
pc1-rdp	10.0.1.4 -> 10.0.10.4 (TCP:3389 -> 3389)	any		0	0	

配置防火墙策略调用 VIP:

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	
port1 -> port2	port1	port2								
IPV4 DoS Policy	ip-pc1	all	pc1-rdp	always	ALL	ACCEPT	Disabled	no-Inspection	UTM	0 B
ZTNA	port2 -> port1									
Authentication Rules	Implicit									

在 fgt-external 安全组中放通 3389 端口。

fgt-external | 入站安全规则

使用源、源端口、目标、目标端口、协议的组合，按优先级评估网络安全组安全规则，从而允许或拒绝流量。安全规则的优先级和方向不能与现有规则相同，无法删除默认安全规则，但可以使用优先级较高的规则替代这些规则。 [了解详情](#)

优先级	名称	端口	协议	源	目标	操作
100	AllowAnyCustom443Inbo...	443	TCP	任何	任何	Allow
110	AllowAnyCustom22In...	22	TCP	任何	任何	Allow
120	AllowAnyCustomAnyI...	任何	ICMP	任何	任何	Allow
130	AllowAnyCustom3389Inb...	3389	TCP	任何	任何	Allow
65000	AllowVnetInBound	任何	任何	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	任何	任何	AzureLoadBalancer	任何	Allow
65500	DenyAllInBound	任何	任何	任何	任何	Deny

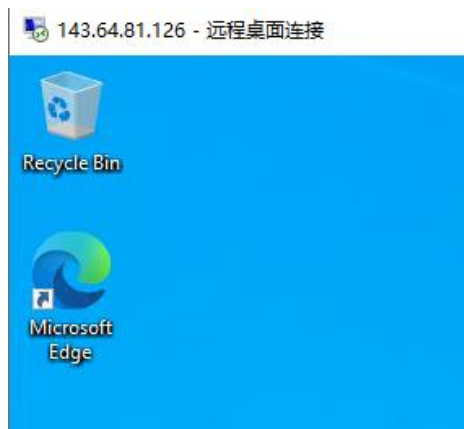
4. 业务测试

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

