结合 Azure 负载均衡器部署 FortiGate HA

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

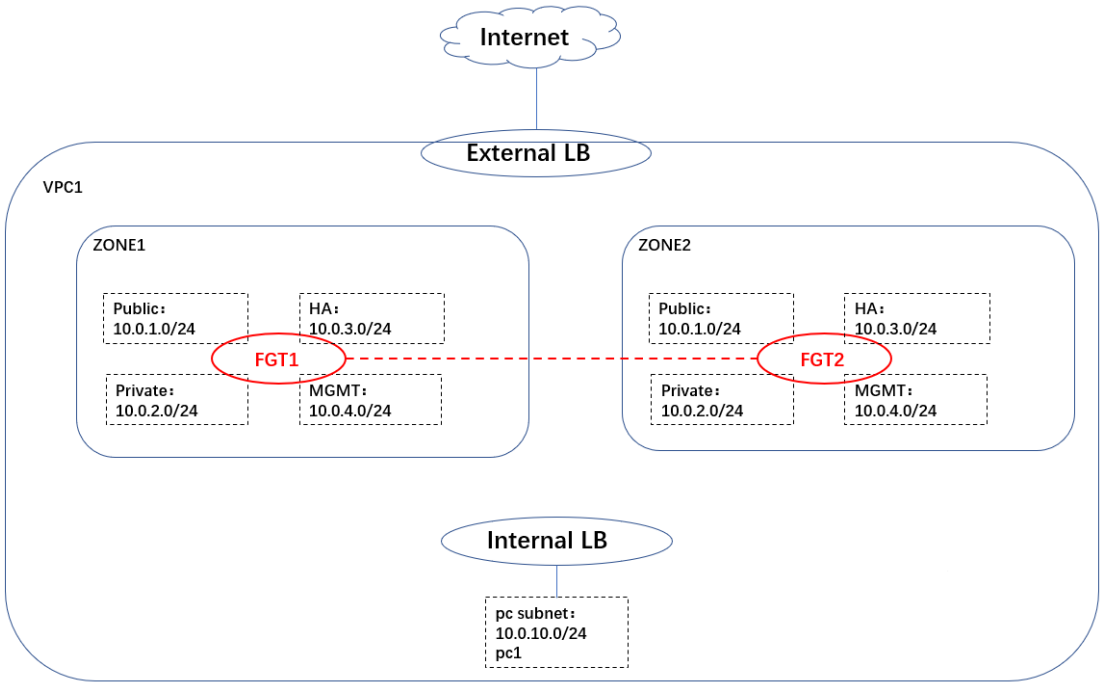
1. 介绍

本文档介绍如何在 Azure 部署 FortiGate HA，以提供统一的威胁管理安全解决方案，保护部署在 Azure 云中的各种应用负载。

2. 网络拓扑

在本方案中，通过 Azure LB 实现主备切换，External LB 向外网发布服务以及作为 Internet 出口，Internal LB 将内网数据转发到 FortiGate 实例上。这里将 FGT1 和 FGT2 部署在不同 AZ 中，FGT1 和 FGT2 的实例分别需要 4 块网卡，Port1 作为外网接口，Port2 作为内网接口，Port3 作为心跳接口，Port4 用于 HA 管理口。 Azure 每种实例规格查询链接如下：

https://learn.microsoft.com/en-us/azure/virtual-machines/fx-series



3. 地址规划

FGT1 地址规划（AZ-1a）	
Port	Azure primary address
Port1	10.0.1.4
Port2	10.0.2.4
Port3	10.0.3.4
Port4	10.0.4.4
FGT2 地址规划（AZ-1b）	
Port	Azure primary address
Port1	10.0.1.5
Port2	10.0.2.5
Port3	10.0.3.5
Port4	10.0.4.5
测试 PC	
PC 名称	测试地址
PC	10.0.10.10

4. 配置步骤

4.1. 创建 VPC、子网

创建 VPC。


vpc1
虚拟网络
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
移动
删除
刷新
提供反馈
概要
资源组 (移动) : xiangwang
位置 (移动) : China North 3
订阅 (移动) : Standard Pay-in-Advance Offer
订阅 ID : 81c335b8-c6ce-4e45-93e4-3269de5a8164
地址空间 : 10.0.0.0/16
DNS 服务器 : Azure 提供的 DNS 服务
流超时 : 配置
BGP 社区字符串 : 配置
虚拟网络 ID : d6cad931-0de5-4b56-b8e7-9f666ff8b966

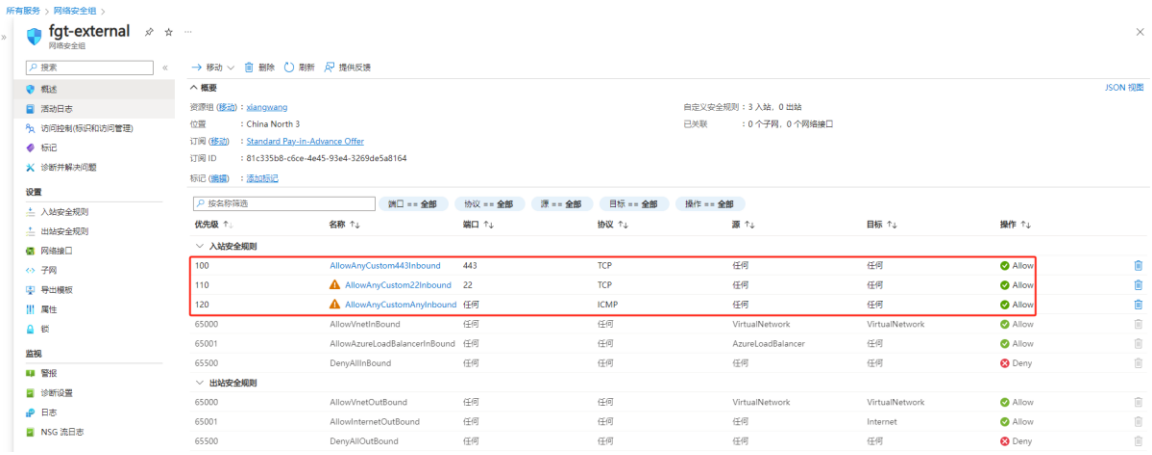
创建子网。


vpc1 | 子网
虚拟网络
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
地址空间
已连接的设备
子网
子网
网关子网
刷新
管理用户
删除
搜索子网
名称
IPv4
IPv6
可用的 IP
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
vpc1-A-ha 10.0.3.0/24 - 251
vpc1-A-mgmt 10.0.4.0/24 - 251

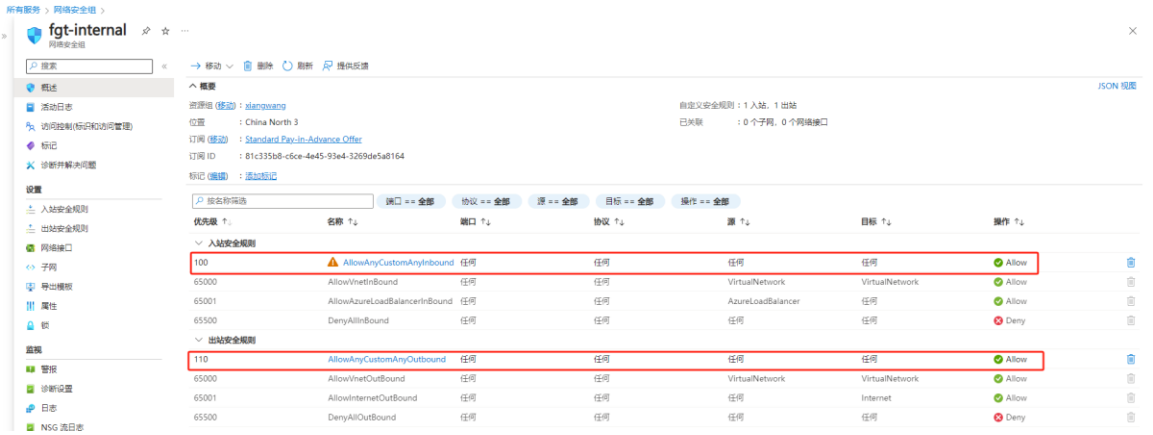
4.2. 创建安全组

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，可以和 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。

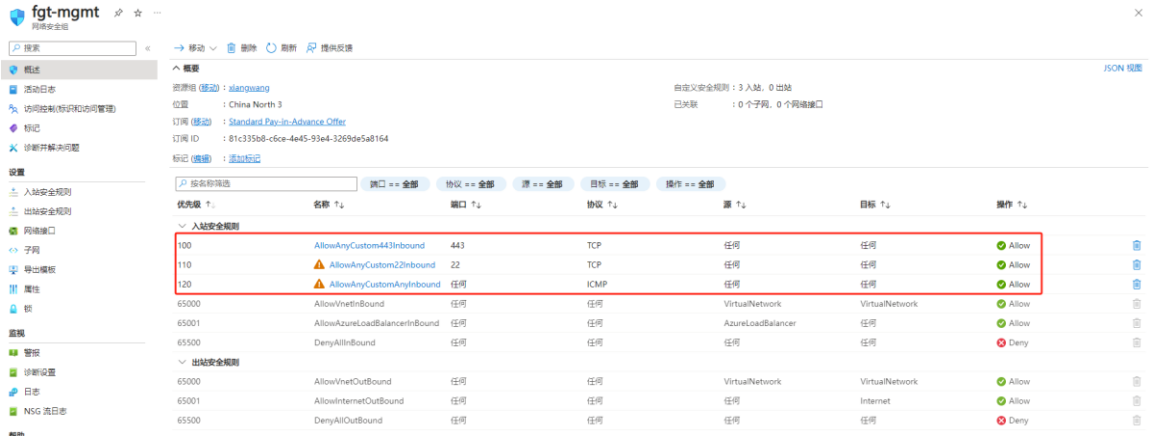
新建安全组 fgt-external，用于 port1。这里先放通管理所需的端口 HTTPS，SSH 和 ICMP。



再新建安全组 fgt-internal，用于 port2 和 port3，入站和出站安全规则放通所有。



新建安全组 fgt-mgmt，用于 port4，放通管理所需的端口 HTTPS，SSH 和 ICMP。



4.3. 创建 FortiGate 实例

创建两台 FortiGate 实例，一台位于 zone1，另一台位于 zone2，实例类型选择计算优化型 F4s。

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。

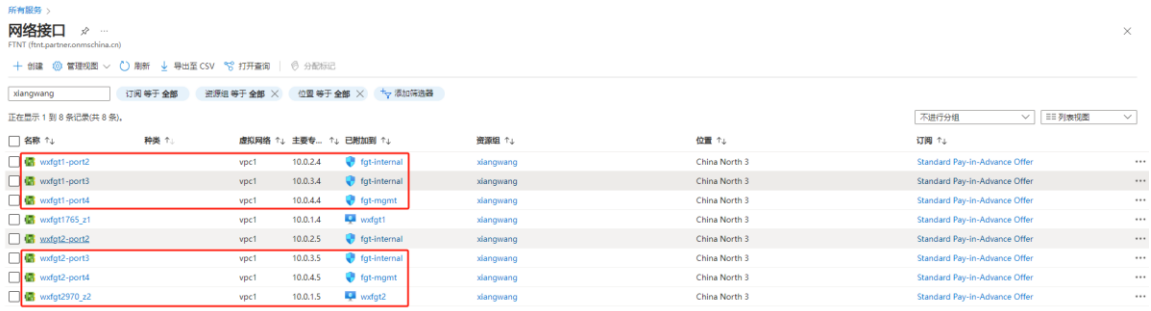
指定 FortiGate port1 接口的子网为 vpc1-A-public，及安全组，绑定公网 IP。

查看实例当前配置，确认无误后点击“创建”。

实例创建完成。同理创建 zone2 的 FortiGate 实例，在 Azure 中 zone1 和 zone2 可在相同的子网。

4. 4. 创建弹性网卡

分别创建 FortiGate 实例的其他三块网卡，并绑定对应的安全组



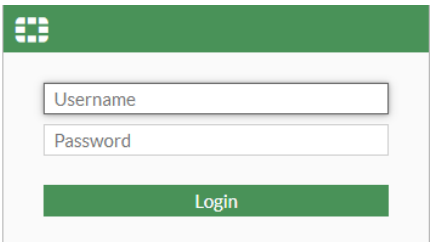
关闭 FortiGate 实例，将网卡依次绑定到 FortiGate 实例，绑定完成后再启动。

在两台 FortiGate 实例的 port1 和 port2 接口都开启“启用 IP 转发”。

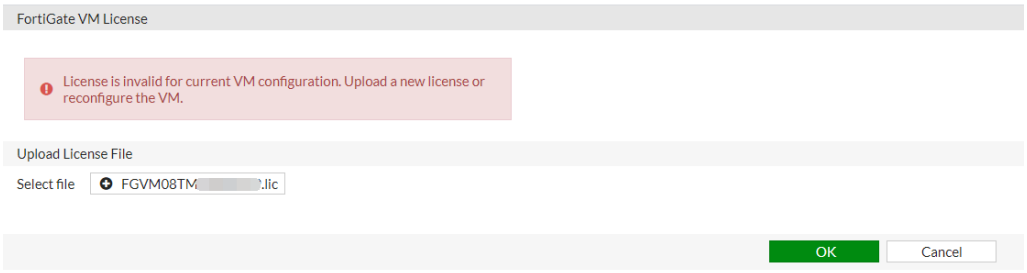
4.5. 访问 FortiGate

HTTPS 访问 FGT1，同理访问 FGT2：

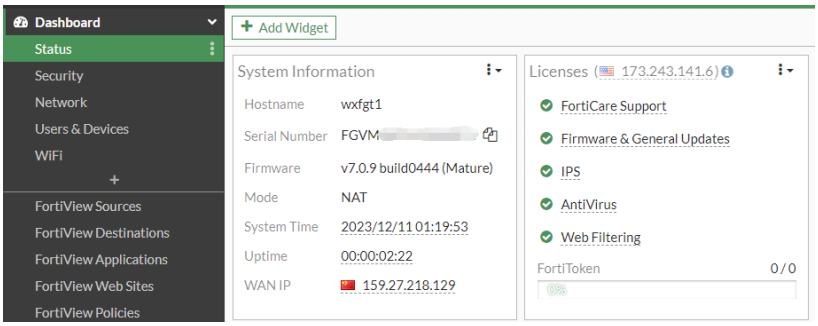
使用公网访问 FortiGate，账号和密码是创建 FortiGate 实例时填写的。



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



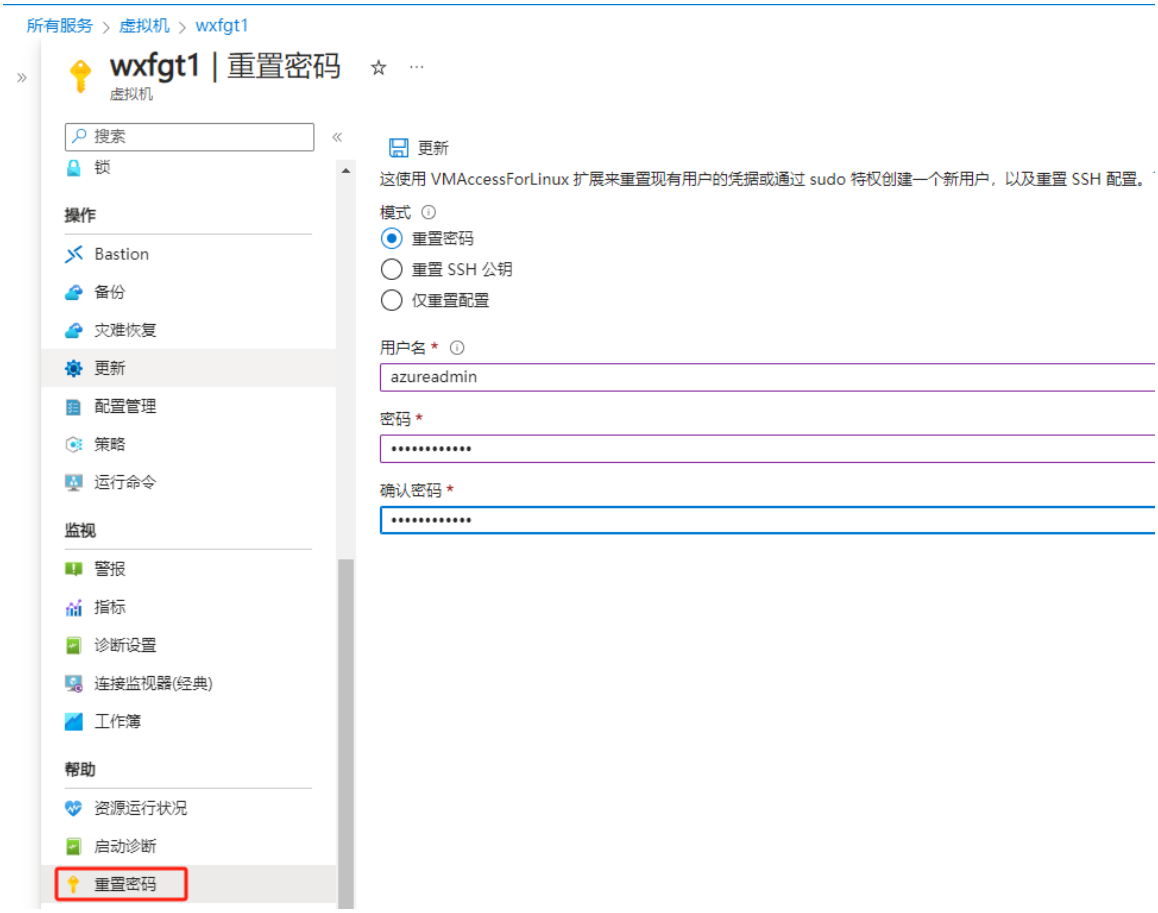
FortiGate 登录成功。



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。

4.6. 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。



4.7. 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[redacted] # 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
```

4.8. 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 10.0.1.1     #网关为所在子网的第 1 个 IP
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.2.1          #内网路由指向 port2 接口，网关为所在子网的第 1 个 IP
        set device "port2"
    next
end
config system interface
    edit "port1"
        set mode static
        set ip 10.0.1.4 255.255.255.0
        set allowaccess ping https ssh
    next
    edit "port2"
        set mode static
        set ip 10.0.2.4 255.255.255.0
        set allowaccess ping https
    next
    edit "port3"
        set mode static
        set ip 10.0.3.4 255.255.255.0
        set allowaccess ping
    next
    edit "port4"
        set mode static
        set ip 10.0.4.4 255.255.255.0
        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 FGT2 将无法访问。

```
config router static
    edit 1
        set gateway 10.0.1.1     #网关为所在子网的第 1 个 IP
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.2.1          #内网路由指向 port2 接口，网关为所在子网的第 1 个 IP
        set device "port2"
    next
end
config system interface
    edit "port1"
        set mode static
        set ip 10.0.1.5 255.255.255.0
        set allowaccess ping https ssh
    next
    edit "port2"
        set mode static
        set ip 10.0.2.5 255.255.255.0
        set allowaccess ping https
    next
    edit "port3"
        set mode static
        set ip 10.0.3.5 255.255.255.0
        set allowaccess ping
    next
    edit "port4"
        set mode static
        set ip 10.0.4.5 255.255.255.0
        set allowaccess ping https ssh
    next
end
config system global
    set admintimeout 50
    set hostname "FGT2"
    set timezone 55
end
```

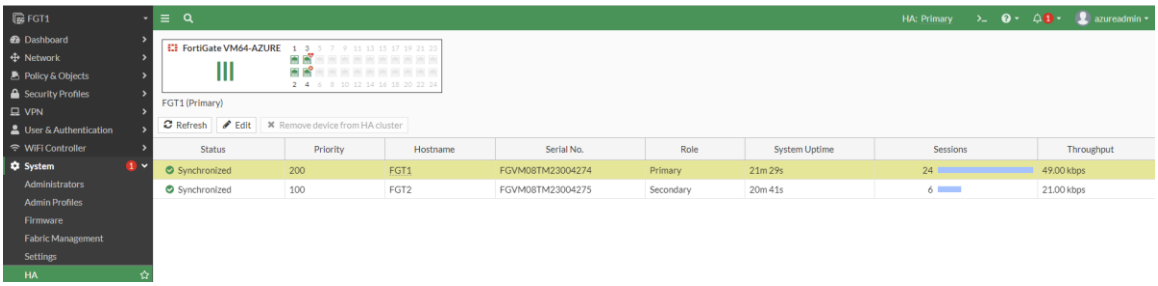
FGT1 HA 配置：

```
config system ha
    set group-name "FGTHA"
    set mode a-p
    set password fortinet
    set hbdev "port3" 50
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.4.1
        next
    end
    set override disable
    set priority 200
    set unicast-hb enable
    set unicast-hb-peerip 10.0.3.5
end
```

FGT2 HA 配置：

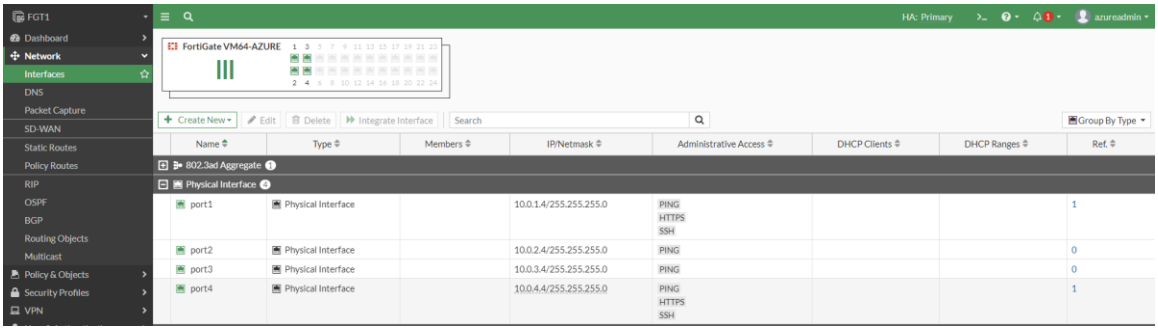
```
config system ha
    set group-name "FGTHA"
    set mode a-p
    set password fortinet
    set hbdev "port3" 50
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.4.1
        next
    end
    set override disable
    set priority 100
    set unicast-hb enable
    set unicast-hb-peerip 10.0.3.4
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。

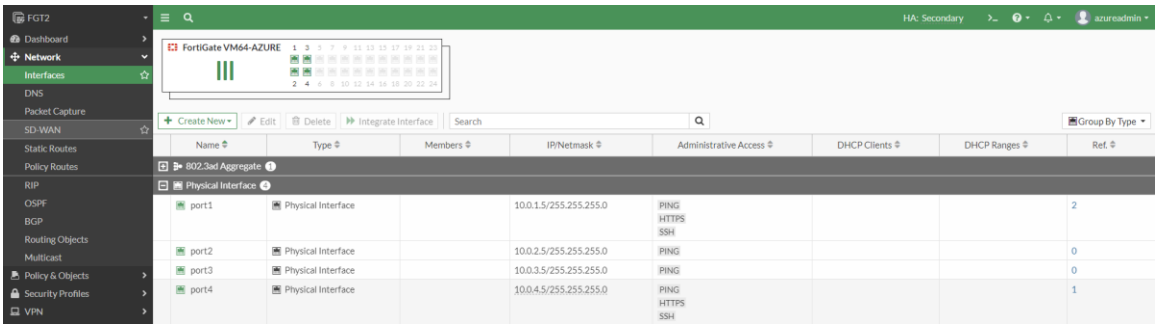


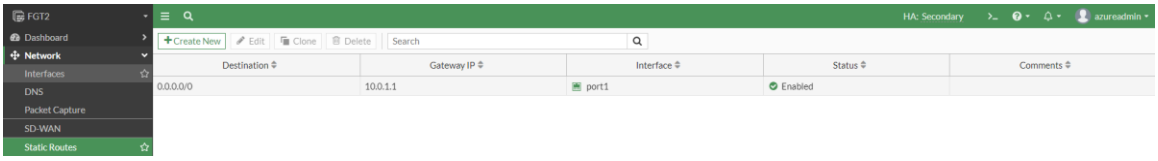
将两台 FortiGate port1 接口绑定的公网 IP 解绑，然后绑定到 port4 接口上，通过 port4 接口管理 FortiGate。

FGT1 接口 IP 及路由：



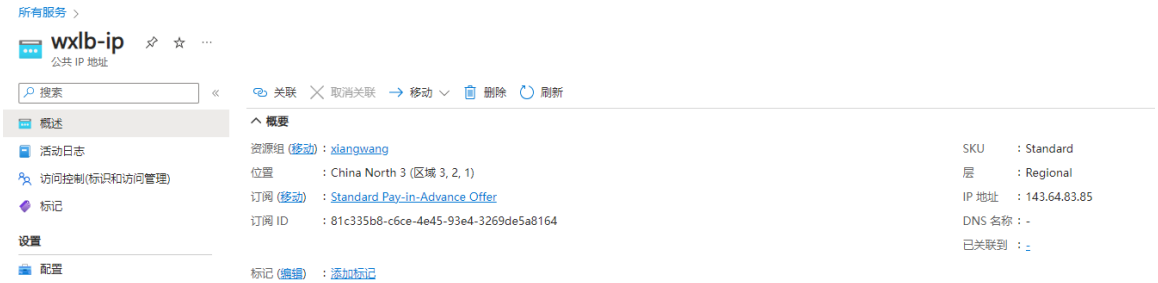
FGT2 接口 IP 及路由：



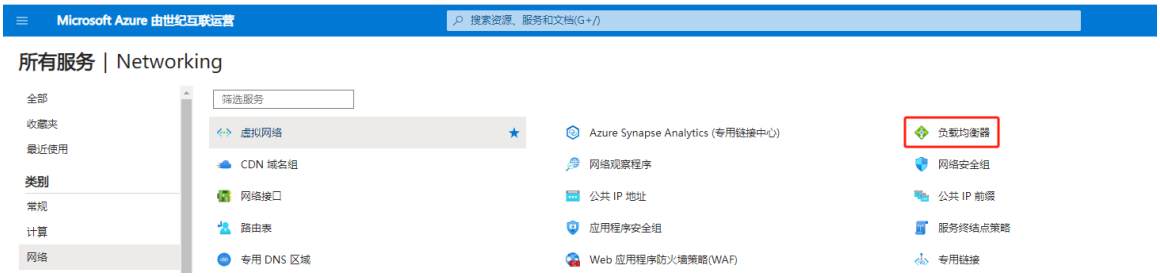


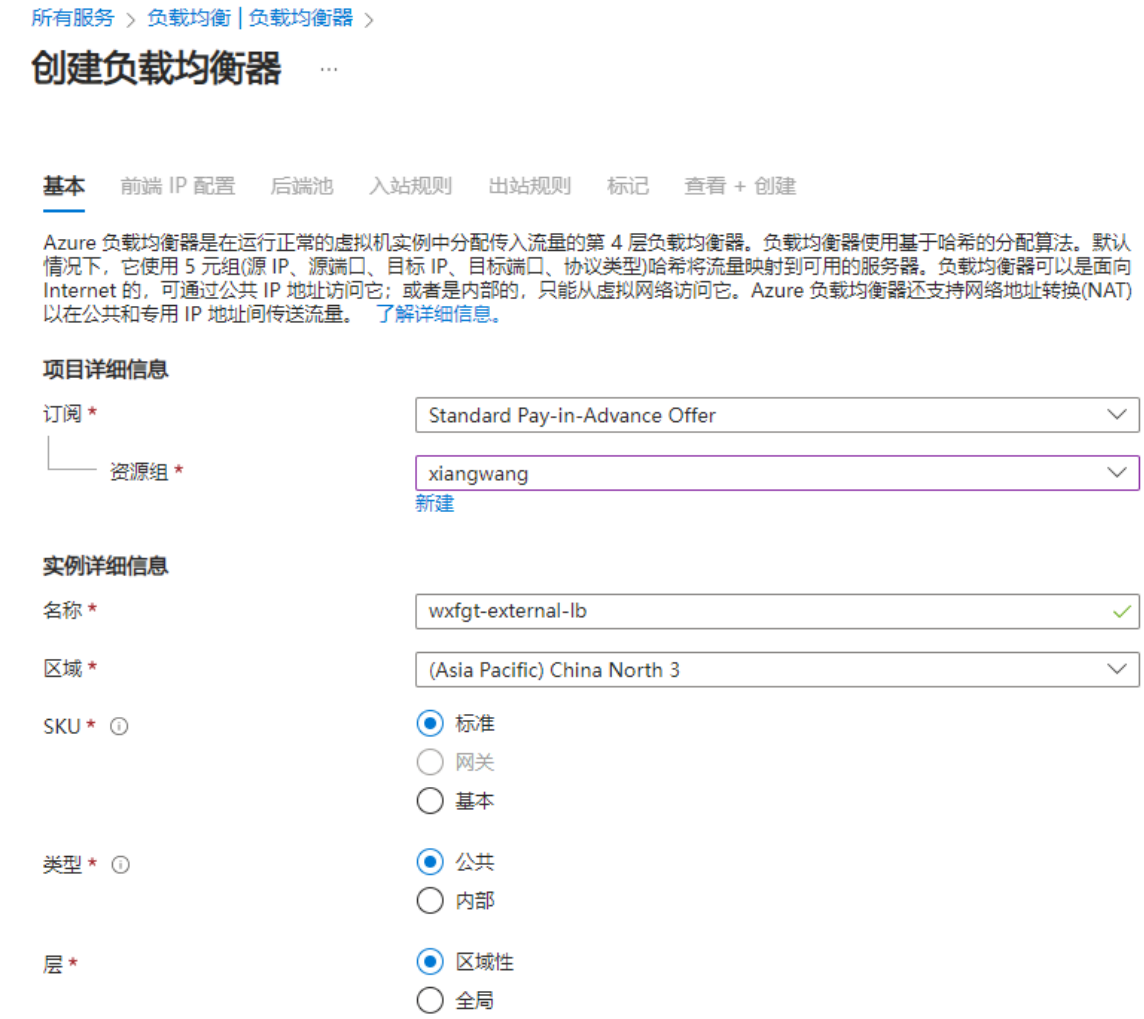
4. 9. 创建外部负载均衡器

创建一个公网 IP 用于绑定外部负载均衡器。



选择 网络→负载均衡器，点击创建。




所有服务 > 负载均衡 | 负载均衡器 >
创建负载均衡器 ...
基本 前端 IP 配置 后端池 入站规则 出站规则 标记 查看 + 创建
Azure 负载均衡器是在运行正常的虚拟机实例中分配传入流量的第 4 层负载均衡器。负载均衡器使用基于哈希的分配算法。默认情况下，它使用 5 元组(源 IP、源端口、目标 IP、目标端口、协议类型)哈希将流量映射到可用的服务器。负载均衡器可以是面向 Internet 的，可通过公共 IP 地址访问它；或者是内部的，只能从虚拟网络访问它。Azure 负载均衡器还支持网络地址转换(NAT)以在公共和专用 IP 地址间传送流量。 了解详细信息。
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 *
wxfgt-external-lb
区域 *
(Asia Pacific) China North 3
SKU *
标准
网关
基本
类型 *
公共
内部
层 *
区域性
全局

创建前端 IP 池。


所有服务 >
创建负载均衡器 ...
基本 前端 IP 配置 后端池 入站规则 出站规则 标记 查看 + 创建
前端 IP 配置是在负载均衡、入站 NAT 和出站规则中定义的用于入站和/或出站通信的 IP 地址。
添加前端 IP 配置
名称
IP 地址
wxlb-public-ip-pool
wxlb-ip (143.64.83.85)

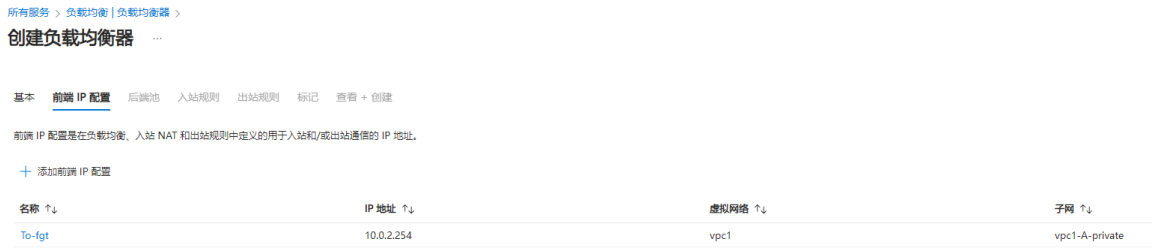
创建后端池，并点击创建，入站规则和出站规则可后续再配置。

创建完成。

4. 10. 创建内部负载均衡器

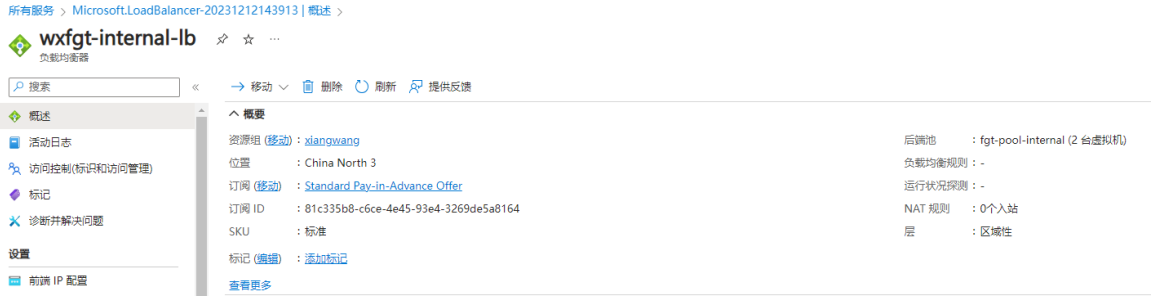
选择 网络→负载均衡器，点击创建。

创建前端 IP 池。



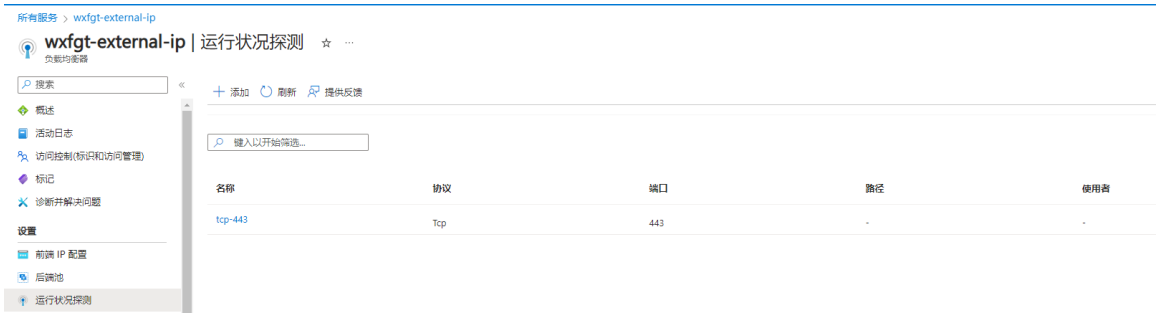
创建后端池关联 FortiGate 实例 port2 接口。

创建完成。



4. 11. 入站规则配置

创建运行状况探测以检查 FortiGate 是否正常工作，这里探测 FortiGate port1 接口的 TCP 443 端口，FortiGate port1 接口已开启 HTTPS。



创建负载均衡规则，将 tcp 8080 端口映射到 FortiGate 实例的 8080 端口。

所有服务 > wxfgt-external-ip | 负载均衡规则 >

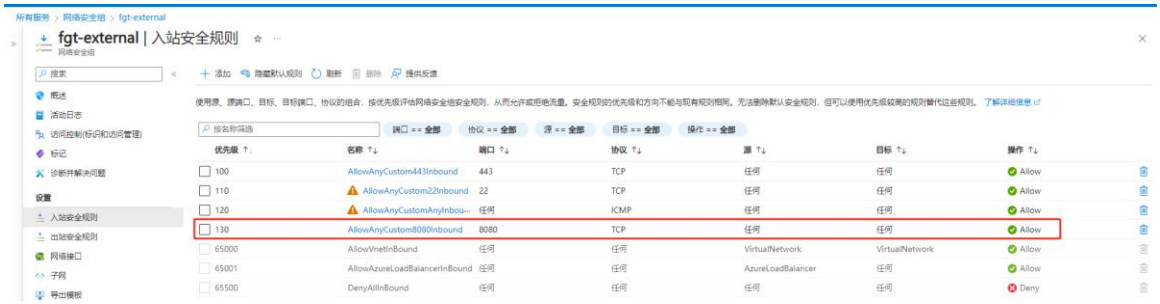
添加负载均衡规则

wxfgt-external-ip

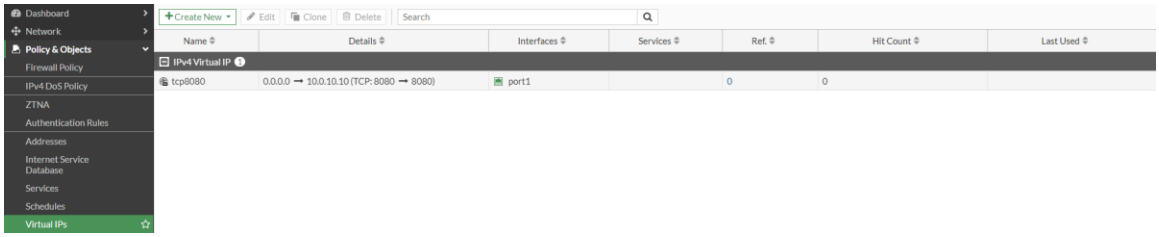
负载均衡规则跨一组后端池实例分布发送到选定 IP 地址和端口组合的传入流量。只有运行状况探测视为正常运行的后端实例才能收到新流量。

名称 *	web8080
IP 版本 *	IPv4 / IPv6
前端 IP 地址 *	wxlb-public-ip-pool (143.64.83.85)
后端池 *	fgt-pool
协议	TCP / UDP
端口 *	8080
后端端口 *	8080
运行状况探测 *	tcp-443 (TCP:443) 新建
会话持续性	无
空闲超时(分钟) *	4
启用 TCP 重置	
启用浮动 IP	
出站源网络地址转换(SNAT)	(建议)使用出站规则为后端池成员提供对 Internet 的访问权限。 了解详细信息。 / 使用默认端口分配为后端池成员提供一组最少的 SNAT 端口。不建议这样做，因为它可能导致 SNAT 端口耗尽。 了解详细信息。

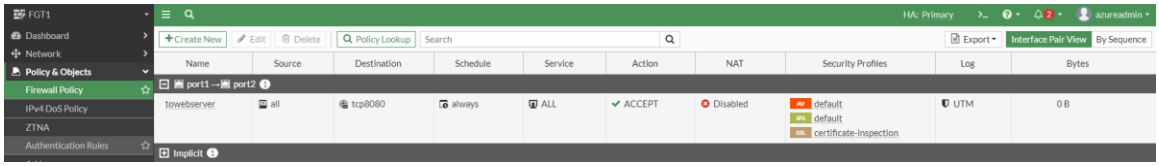
配置 fgt-external 安全组允许 8080 端口到达 FortiGate port1 接口。



登录 FortiGate，使用 VIP 将 8080 端口映射到内网 PC。由于两台 FortiGate port1 接口 IP 是不一样的，因此这里 external ip 应该使用 0.0.0.0。



配置防火墙策略。

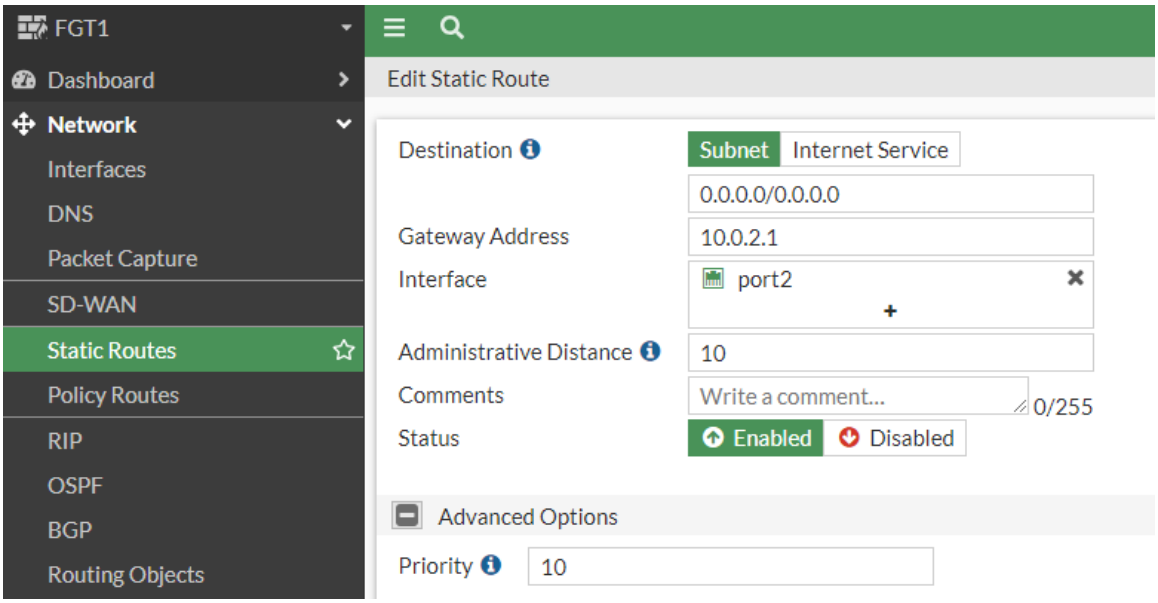


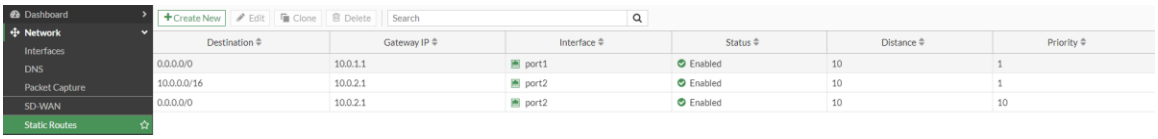
4.12. 出站规则配置

在 Azure 新建路由表，将内网 PC 的默认路由的出口指向内部负载均衡器 wxfgt-internal-lb。

配置内部负载均衡器出站规则。创建运行状况探测以检查 FortiGate 是否正常工作，这里探测 FortiGate port2 接口的 TCP 443 端口，FortiGate port2 接口已开启 HTTPS。

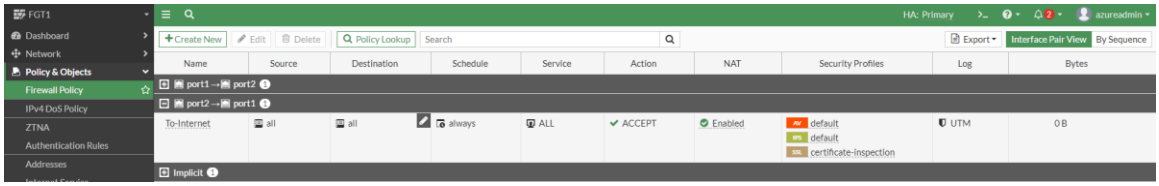
Azure 负载均衡器探测的源地址是公网 IP，因此需要在 port2 接口增加一条 0.0.0.0/0 浮动路由以响应 Azure 的探测，该路由的优先级低于 port1 接口的默认路由。





配置负载均衡规则，勾选“高可用性端口”，此选项作用类似链路负载均衡。

配置 FortiGate 出站策略。

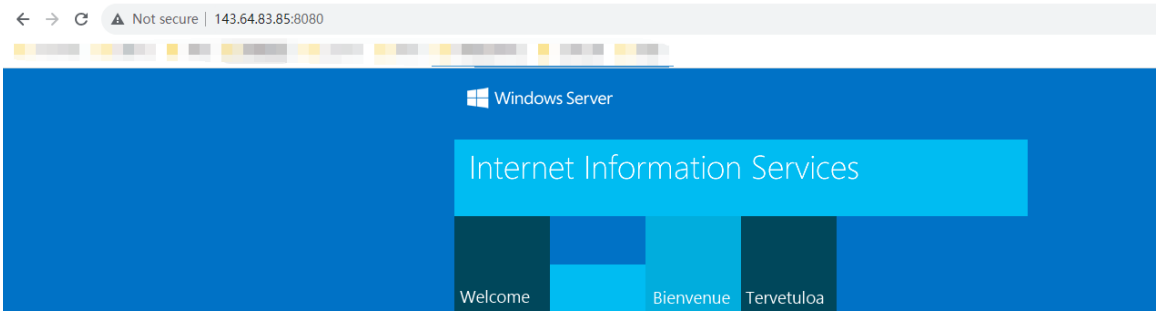


FortiGate 实例没有绑定公网 IP，因此需要通过外部负载均衡器的出站规则访问公网。


主页 > wxfgt-external-ip | 出站规则 >
添加出站规则
wxfgt-external-ip
名称 *
Outbound
IP 版本 *
IPv4
IPv6
前端 IP 地址 *
已选择 1 项
协议
All
TCP
UDP
空闲超时(分钟)
4
最大值: 100
TCP 重置
已启用
已禁用
后端池 *
fgt-pool (2 个实例)
端口分配
Azure 根据前端 IP 地址和后端池实例的数量，自动分配用于源网络地址转换(SNAT)的出站端口数。 详细了解出站连接
端口分配
手动选择出站端口数
出站端口
选择依据 *
最大后端实例数
每个实例的端口数
31992
可用的前端端口
63992
最大后端实例数 *
2
添加
提供反馈

5. 业务测试

访问负载均衡器发布的 8080 端口正常。



内网 PC 访问外网正常。

6. HA 切换测试

重启主 FortiGate，切换时间取决于负载均衡器的健康检查，大概 10s 左右（负载均衡器不支持 ping），再次访问 http://143.64.83.85:8080/正常。