



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	3
2. 网络拓扑	3
3. 地址规划	4
4. 配置步骤	4
4.1. 创建 VPC、子网	4
4.2. 创建安全组	6
4.3. 创建 FortiGate 实例	8
4.4. 创建弹性网卡	12
4.5. 访问 FortiGate	13
4.6. 重置密码	14
4.7. 格式化硬盘	14
4.8. 配置 FortiGate	15
4.9. 创建外部负载均衡器	19
4.10. 创建内部负载均衡器	22
4.11. 进站规则配置	23
4.12. 出站规则配置	26
5. 业务测试	31
6. HA 切换测试	31

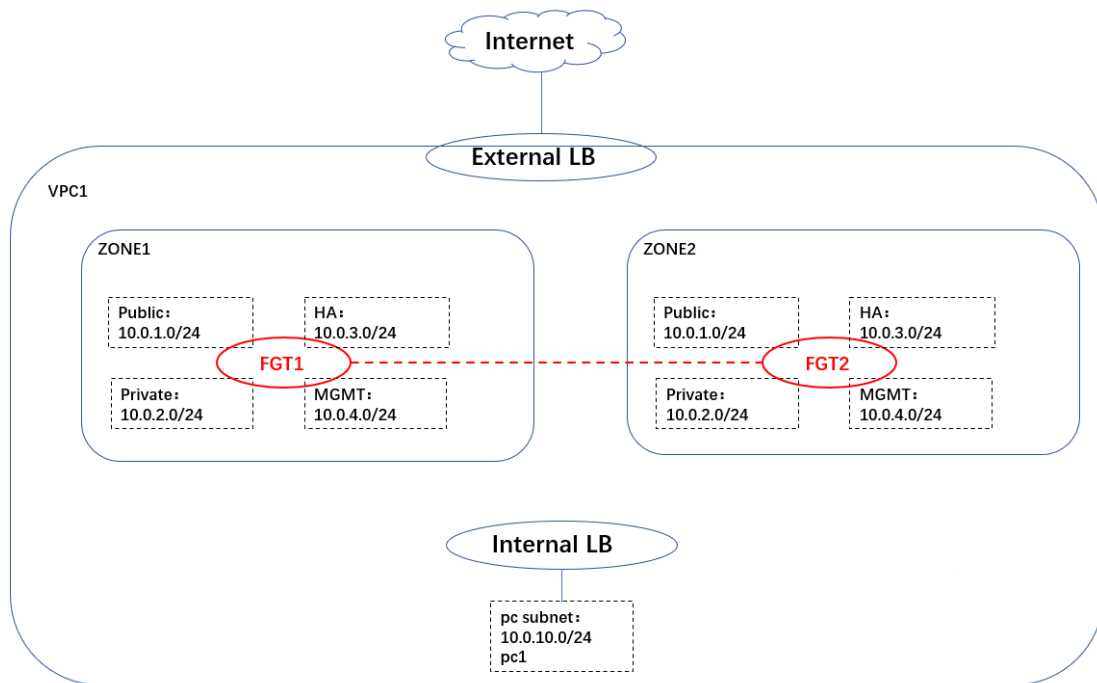
1. 介绍

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>



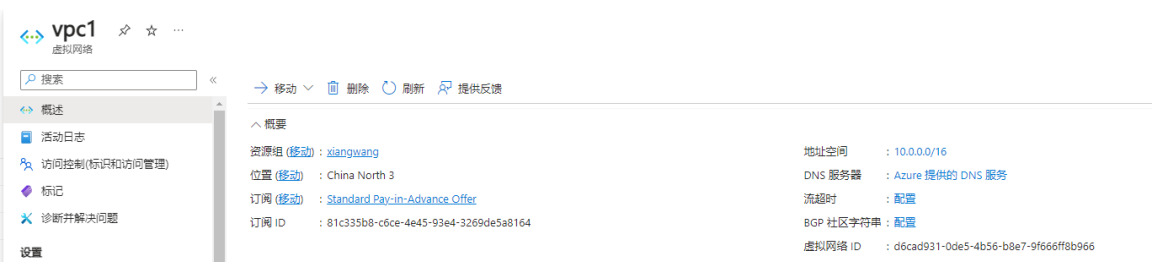
3. 地址规划

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

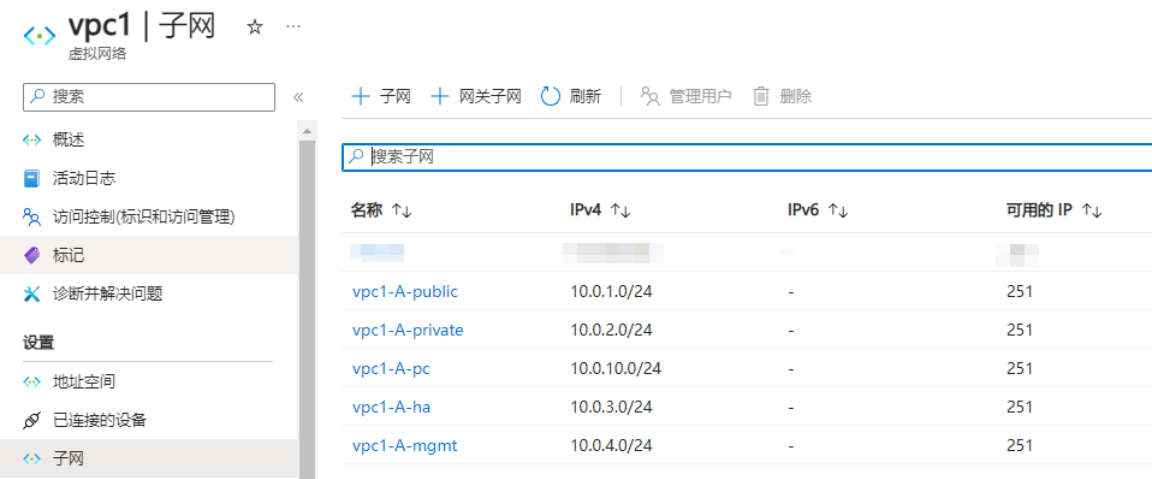
4. 配置步骤

4.1. 创建 VPC、子网

创建 VPC。



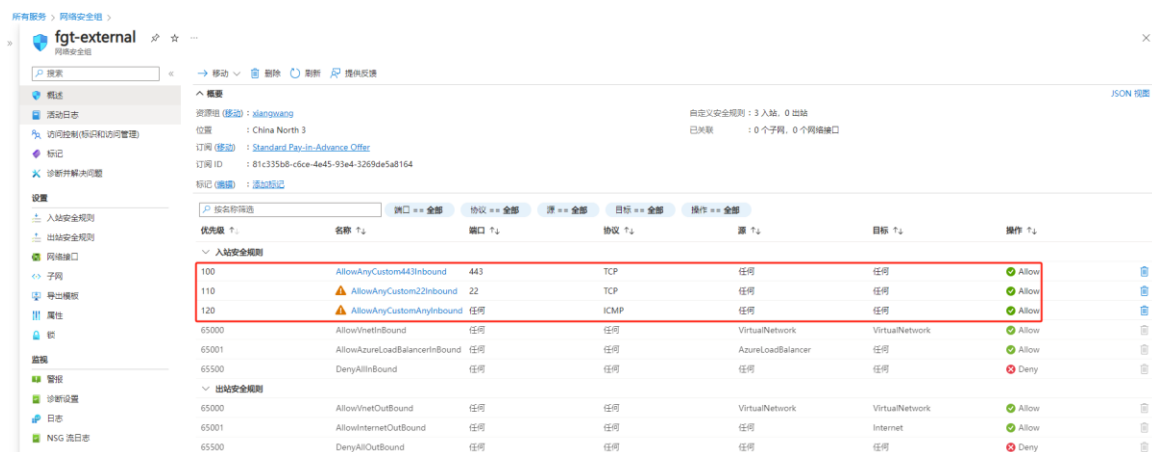
创建子网。



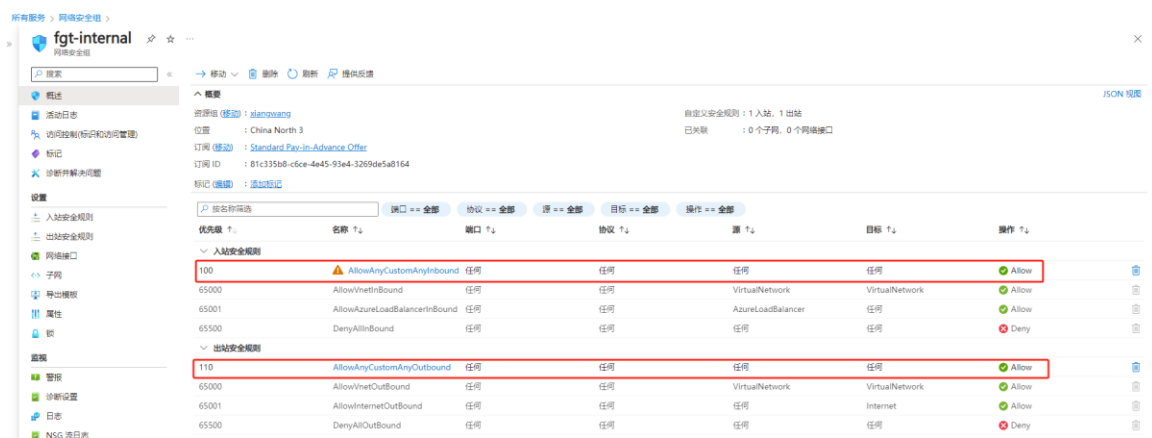
4.2. 创建安全组

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，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。

fgt-mgmt 网络安全组

搜索 移动 删除 刷新 提供反馈

概述 活动日志 访问控制(访问和访问管理) 标记 诊断并解决问题

设置 入站安全规则 出站安全规则 网络接口 子网 导出模板 属性 标签 策略 管理 诊断设置 日志 NSG 流日志

名称: fgt-mgmt 位置: China North 3 订阅: Standard Pay-in-Advance Offer 订阅 ID: 81c335b8-c6ce-4e45-93e4-3269de5a8164 标记: 无标记

自定义安全规则: 3 入站, 0 出站 已关联: 0 个子网, 0 个网络接口

规则名称 优先级 名称 端口 协议 源 目标 操作

入站安全规则

规则名称	优先级	名称	端口	协议	源	目标	操作
100	100	AllowAnyCustom443Inbound	443	TCP	任何	任何	Allow
110	110	AllowAnyCustom22Inbound	22	TCP	任何	任何	Allow
120	120	AllowAnyCustomAnyInbound	任何	ICMP	任何	任何	Allow
65000	65000	AllowVnetInBound	任何	任何	VirtualNetwork	VirtualNetwork	Allow
65001	65001	AllowAzureLoadBalancerInBound	任何	任何	AzureLoadBalancer	任何	Allow
65500	65500	DenyAllInBound	任何	任何	任何	任何	Deny

出站安全规则

规则名称	优先级	名称	端口	协议	源	目标	操作
65000	65000	AllowVnetOutBound	任何	任何	VirtualNetwork	VirtualNetwork	Allow
65001	65001	AllowInternetOutBound	任何	任何	任何	Internet	Allow
65500	65500	DenyAllOutBound	任何	任何	任何	任何	Deny

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。

[主页](#) > [虚拟机](#) > [创建虚拟机](#) >

创建虚拟机 ...

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 * ⓘ Standard Pay-in-Advance Offer

资源组 * ⓘ xiangwang
[新建](#)

实例详细信息

虚拟机名称 * ⓘ wxfgt1 ✓

区域 * ⓘ (Asia Pacific) China North 3

可用性选项 ⓘ 可用性区域

可用性区域 * ⓘ Zone 1

安全类型 ⓘ 标准

映像 * ⓘ Fortinet NGFW-FortiGate-7.0 (BYOL) - Gen1
[查看所有映像](#) | [配置 VM 生成](#)

大小 * ⓘ Standard_F4s - 4 vcpu、8 GiB 内存 (CN¥1,051.20/月)
[查看所有大小](#)

管理员帐户

身份验证类型 ⓘ
☐ SSH 公钥
☒ 密码

用户名 * ⓘ azureadmin ✓

密码 * ⓘ ✓

确认密码 * ⓘ ✓

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。

[主页](#) > [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 ⓘ

映像默认值(2 GiB) ▼

OS 磁盘类型 * ⓘ

高级 SSD (本地冗余存储) ▼

加密类型 *

(默认)使用平台管理的密钥进行静态加密 ▼

启用超级磁盘兼容性 ⓘ ☐

wxfgt1 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	wxfgt1_DataDisk_0	64	高级 SSD LRS	只读 ▼	 

[创建并附加新磁盘](#) [附加现有磁盘](#)

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

[主页](#) > [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

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 * ⓘ

vpc1

[新建](#)

子网 * ⓘ

vpc1-A-public (10.0.1.0/24)

[管理子网配置](#)

公用 IP ⓘ

(新) wxfgt1-ip

[新建](#)

NIC 网络安全组 ⓘ

☐ 无

☐ 基本

☒ 高级

i 此 VM 映像已预配置 NSG 规则

配置网络安全组 *

fgt-external

[新建](#)

启用加速网络 ⓘ

☐

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? ☐

查看实例当前配置，确认无误后点击“创建”。

[主页](#) > [虚拟机](#) >

创建虚拟机 ...

✓ 验证已通过

基本 磁盘 网络 管理 监视 高级 标记 查看 + 创建

基本

订阅	Standard Pay-in-Advance Offer
资源组	xiangwang
虚拟机名称	wxfgt1
区域	China North 3
可用性选项	可用性区域
可用性区域	1
安全类型	标准
映像	Fortinet NGFW-FortiGate-7.0 (BYOL) - Gen1
大小	Standard F4s (4 vcpu, 8 GiB 内存)
身份验证类型	密码
用户名	azureadmin

磁盘

OS 磁盘大小	映像默认值
OS 磁盘类型	高级 SSD LRS
使用托管的磁盘	是
数据磁盘	1
临时 OS 磁盘	否

网络

虚拟网络	vpc1
子网	vpc1-A-public (10.0.1.0/24)
公用 IP	(新) wxfgt1-ip

创建

< 上一步

下一步 >

[下载自动化模板](#)

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。

[主页](#) >

虚拟机 ...

FTNT (forti-partner-on-azure.com)

+ 创建 切换视图 管理视图 刷新 删除 导出至 CSV 打开查看 分配标记 开始 重新启动 停止 删除 维护

筛选任何字段... 订阅 等于 全部 类型 等于 全部 资源组 等于 全部 位置 等于 全部 添加过滤器

正在显示 1 到 12 条记录 (共 12 条)。

不运行分组 选择列表视图

☐	名称 ↑↓	类型 ↑↓	订阅 ↑↓	资源组 ↑↓	位置 ↑↓	状态 ↑↓	操作系统 ↑↓	大小 ↑↓	公共 IP 地址 ↑↓	磁盘 ↑↓	...
☐	wxfgt1	虚拟机	Standard Pay-in-Advan...	xiangwang	China North 3	正在运行	Linux	Standard_F4s	159.27.218.129	2	...
☐	wxfgt2	虚拟机	Standard Pay-in-Advan...	xiangwang	China North 3	正在运行	Linux	Standard_F4s	159.27.105.77	2	...

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

网络接口

正在显示 1 到 8 条记录 (共 8 条)。

名称 ↑	种类 ↑	虚拟网络	主要专... ↑	已附加到 ↑	资源组 ↑	位置 ↑	订购 ↑
 wxfgt1-port2	vpc1	10.0.2.4	 fgt-internal	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt1-port3	vpc1	10.0.3.4	 fgt-internal	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt1-port4	vpc1	10.0.4.4	 fgt-mgmt	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt1765_z1	vpc1	10.0.1.4	 wxfgt1	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt2-port2	vpc1	10.0.2.5	 fgt-internal	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt2-port3	vpc1	10.0.3.5	 fgt-internal	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt2-port4	vpc1	10.0.4.5	 fgt-mgmt	xiangwang	China North 3	Standard Pay-in-Advance Offer	
 wxfgt2970_z2	vpc1	10.0.1.5	 wxfgt2	xiangwang	China North 3	Standard Pay-in-Advance Offer	

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

所有服务 > 虚拟机 > wxfgt1

wxfgt1 | 网络

wxfgt1765_z1 wxfgt1-port2 wxfgt1-port3 wxfgt1-port4

IP 配置: ipv4config (主要)

网络接口: wxfgt1765_z1 有效安全规则

虚拟网络/子网: vpc1/vpc1-A-public NIC 公共 IP: 159.27.218.129 NIC 专用 IP: 10.0.1.4 更快的网络连接: 已禁用

所有服务 > 虚拟机 > wxfgt2

wxfgt2 | 网络

wxfgt2970_z2 wxfgt2-port2 wxfgt2-port3 wxfgt2-port4

IP 配置: ipconfig1 (主要)

网络接口: wxfgt2970_z2 有效安全规则

虚拟网络/子网: vpc1/vpc1-A-public NIC 公共 IP: 159.27.105.77 NIC 专用 IP: 10.0.1.5 更快的网络连接: 已禁用

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

所有服务 > 网络接口 > wxfgt1-port2

wxfgt1-port2 | IP 配置

IP 设置

启用 IP 转发: ☒

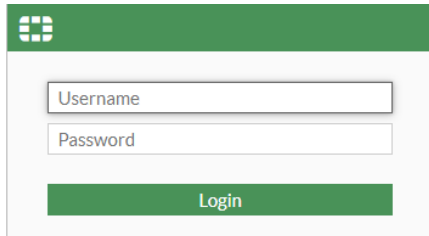
虚拟网络: vpc1

子网: vpc1-A-private (10.0.2.0/24) 249 个空闲 IP 地址

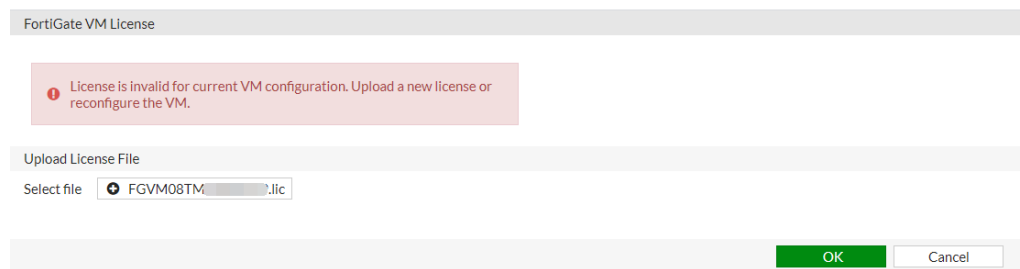
4.5. 访问 FortiGate

HTTPS 访问 FGT1，同理访问 FGT2：

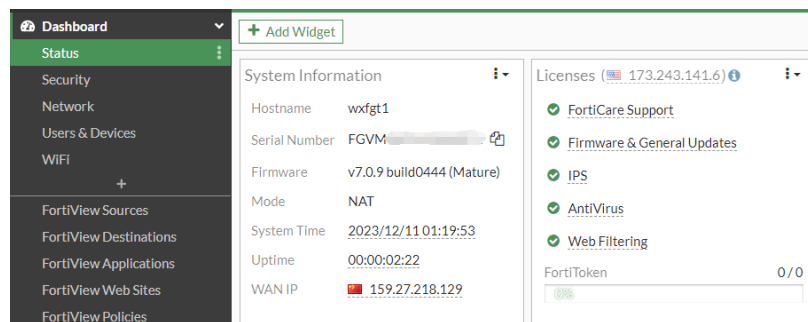
使用公网访问 FortiGate，账号和密码是创建 FortiGate 实例时填写的。

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' upload screen. At the top, there is a red error message: 'License is invalid for current VM configuration. Upload a new license or reconfigure the VM.' Below the error message, there is a section titled 'Upload License File'. It includes a 'Select file' button and a file name 'FGVM08TM...lic'. At the bottom right, there are 'OK' and 'Cancel' buttons.

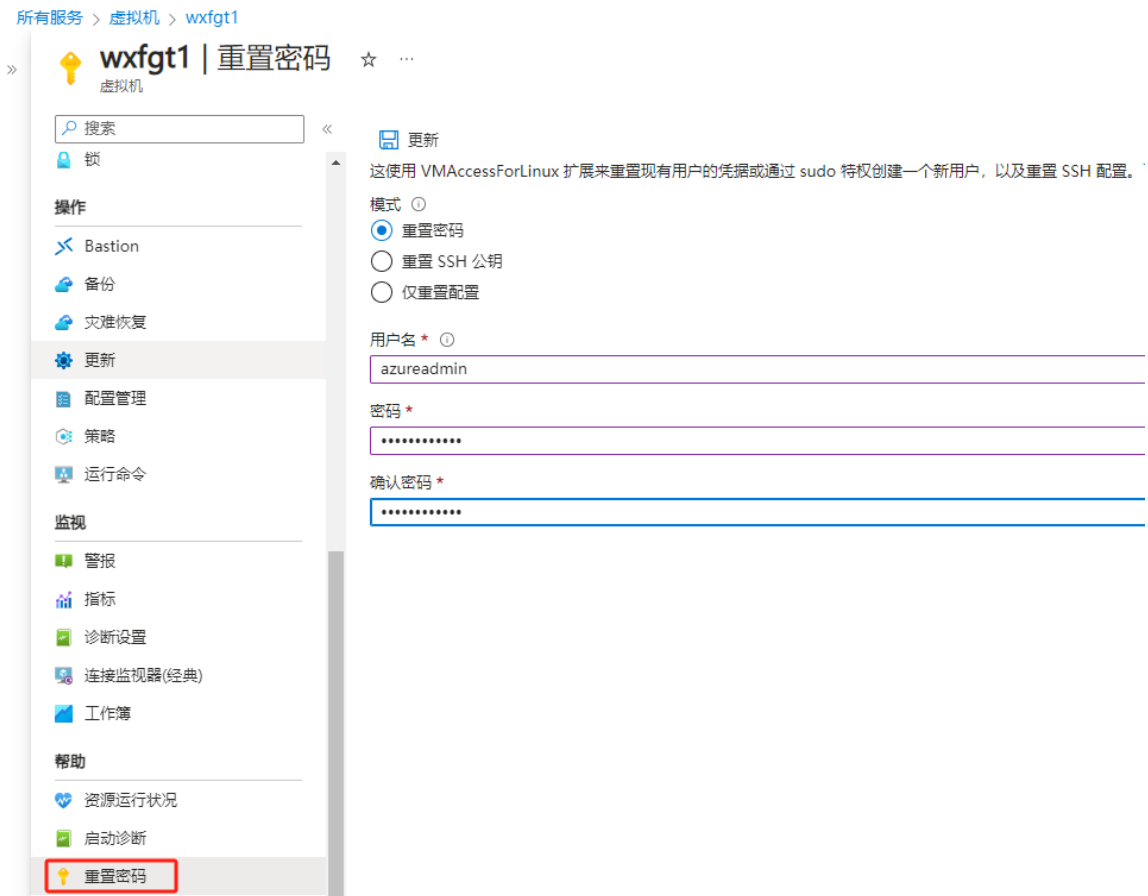
FortiGate 登录成功。

The image shows the FortiGate dashboard. On the left, there is a sidebar menu with options: Dashboard, Status, Security, Network, Users & Devices, WiFi, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, and FortiView Policies. The main area is divided into three sections: 'System Information' (Hostname: wxfgt1, Serial Number: FGVM..., Firmware: v7.0.9 build0444 (Mature), Mode: NAT, System Time: 2023/12/11 01:19:53, Uptime: 00:00:02:22, WAN IP: 159.27.218.129), 'Licenses' (173.243.141.6), and 'FortiToken' (0/0). The 'Licenses' section shows a list of licenses: FortiCare Support, Firmware & General Updates, IPS, AntiVirus, and Web Filtering.

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 # 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

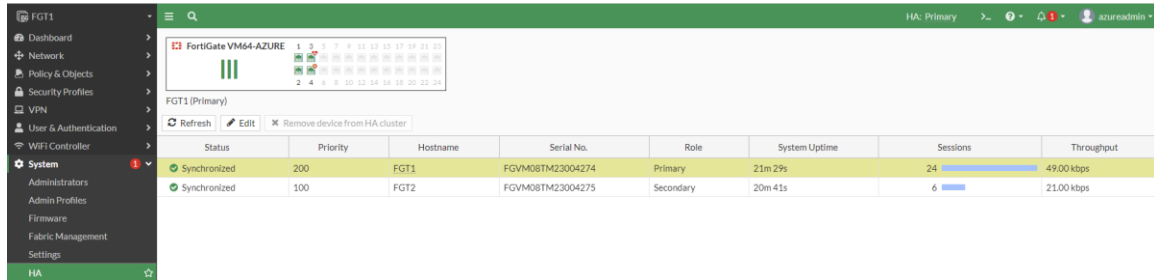
FGT1 HA 配置:

```
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。

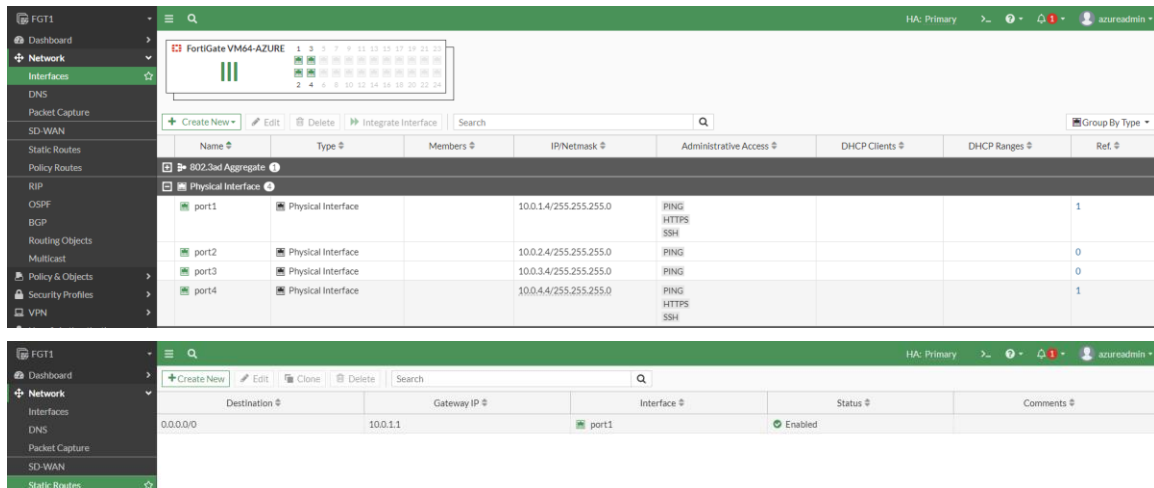


The screenshot shows the FortiGate HA status page. At the top, there's a status bar for 'FortiGate VM64-AZURE' with a green 'HA: Primary' indicator. Below it, a table lists the HA members:

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	200	FGT1	FGVM08TM23004274	Primary	21m 29s	24	49.00 kbps
Synchronized	100	FGT2	FGVM08TM23004275	Secondary	20m 41s	6	21.00 kbps

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：



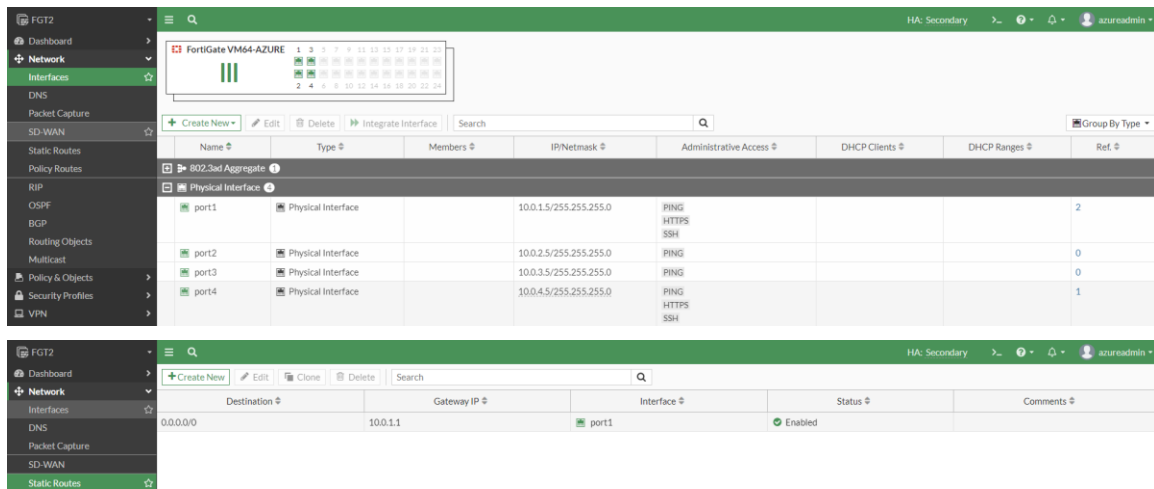
The screenshot shows the FortiGate FGT1 configuration page. The 'Interfaces' section lists four physical interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
port1	Physical Interface		100.1.4/255.255.255.0	PING, HTTPS, SSH			1
port2	Physical Interface		100.2.4/255.255.255.0	PING			0
port3	Physical Interface		100.3.4/255.255.255.0	PING			0
port4	Physical Interface		100.4.4/255.255.255.0	PING, HTTPS, SSH			1

The 'Static Routes' section shows a single route:

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	100.1.1	port1	Enabled	

FGT2 接口 IP 及路由：



The screenshot shows the FortiGate FGT2 configuration page. The 'Interfaces' section lists four physical interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
port1	Physical Interface		100.1.5/255.255.255.0	PING, HTTPS, SSH			2
port2	Physical Interface		100.2.5/255.255.255.0	PING			0
port3	Physical Interface		100.3.5/255.255.255.0	PING			0
port4	Physical Interface		100.4.5/255.255.255.0	PING, HTTPS, SSH			1

The 'Static Routes' section shows a single route:

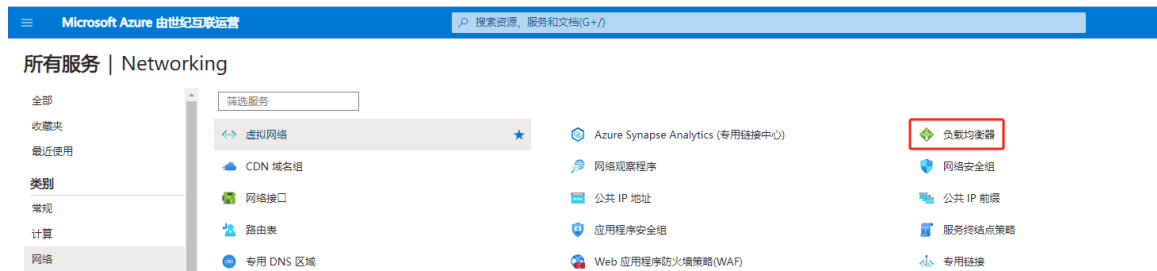
Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	100.1.1	port1	Enabled	

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，进站规则和出站规则可后续再配置。

所有服务 >

创建负载均衡器 ...

基本 前端 IP 配置 后端池 进站规则 出站规则 标记 查看 + 创建

后端池是负载均衡器可向其发送流量的资源集合。后端池只能包含虚拟机、虚拟机规模集和容器。

+ 添加后端池

名称	虚拟网络	资源名称	网络接口	IP 地址	可用性区域
fgt-pool					
fgt-pool	vpc1	WXFGT1	wxfgt1765_z1	10.0.14	1
fgt-pool	vpc1	WXFGT2	wxfgt2970_z2	10.0.15	2

创建完成。

所有服务 >

wxfgt-external-ip 负载均衡器

☆ ☆ ...

搜索

移动 删除 刷新 提供反馈

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

前端 IP 配置

后端池

概要

资源组 (移动) : xiangwang

位置 : China North 3

订阅 (移动) : Standard Pay-in-Advance Offer

订阅 ID : 81c335b8-c6ce-4e45-93e4-3269de5a8164

SKU : 标准

标记 (编辑) : 添加标记

查看更多

后端池 : fgt-pool (2 台虚拟机)

负载均衡规则 : -

运行状况探测 : -

NAT 规则 : 0个进站

层 : 区域性

4. 10. 创建内部负载均衡器

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-internal-lb

区域 *

(Asia Pacific) China North 3

SKU * ①

☒ 标准

☐ 网关

☐ 基本

类型 * ①

☐ 公共

☒ 内部

层 *

☒ 区域性

☐ 全局

创建前端 IP 池。

[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

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。

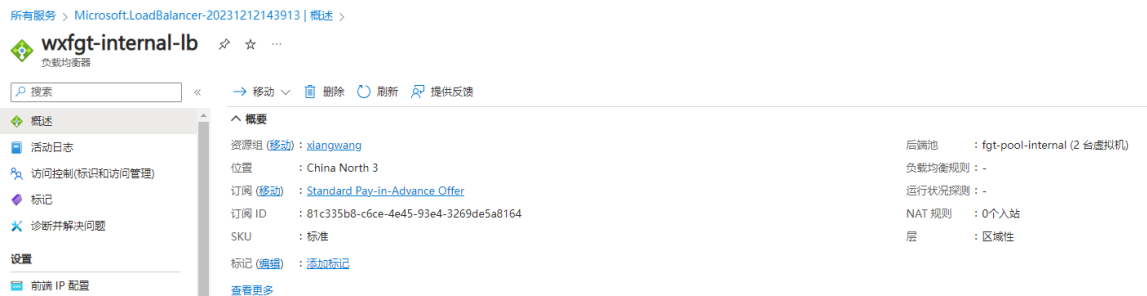
+ 添加前端 IP 配置

名称 ↑↓	IP 地址 ↑↓	虚拟网络 ↑↓	子网 ↑↓
To-fgt	10.0.2.254	vpc1	vpc1-A-private

创建后端池关联 FortiGate 实例 port2 接口。

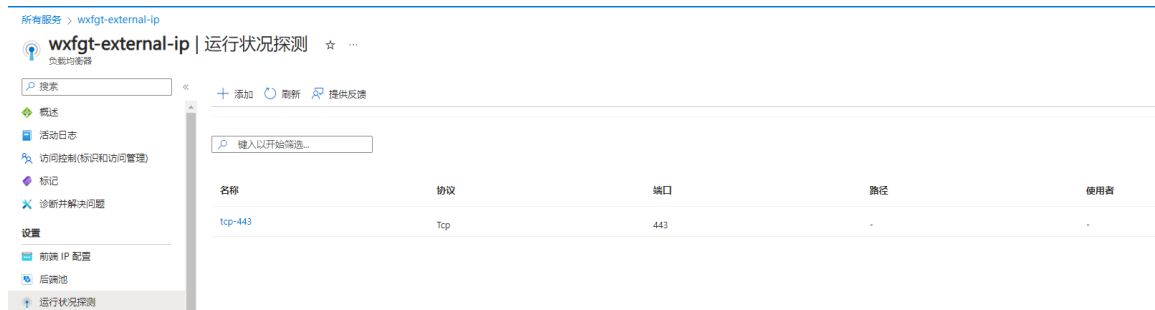


创建完成。



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。



所有服务 > wxfgt-external-ip | 运行状况探测 >

添加运行状况探测

wxfgt-external-ip

① 运行状况探测用于检查后端池实例的状态。如果运行状况探测无法从后端实例获取响应，则在运行状况探测再次成功之前，将不会向该后端实例发送新的连接。

名称 *	tcp-443
协议 *	TCP
端口 * ①	443
间隔(秒) * ①	5
使用者 * ①	未使用

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

wxfgt-external-ip | 负载均衡规则

负载均衡规则

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

前端 IP 配置

后端池

运行状况探测

负载均衡规则

+ 添加 刷新 删除

负载均衡规则用于定义如何向后端池中的所有实例分发传入流量。负载均衡规则将给定的前端 IP 配置和端口映射到多个后端 IP 地址和端口。例如，在端口 80 上创建的规则，用于平衡 Web 流量的负载。[了解详细信息。](#)

按名称筛选...

☐ 名称 TL	协议 TL	后端池 TL	运行状况探测 TL	
☐ web8080	TCP/8080	fgt-pool	tcp-443	

[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 * ①	wxdlb-public-ip-pool (143.64.83.85)
后端池 * ①	fgt-pool
协议	☒ TCP ☐ UDP
端口 *	8080
后端端口 * ①	8080
运行状况探测 * ①	tcp-443 (TCP:443)
会话持续性 ①	无
空闲超时(分钟) * ①	4
启用 TCP 重置	☐
启用浮动 IP ①	☐
出站源网络地址转换(SNAT) ①	☒ (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。

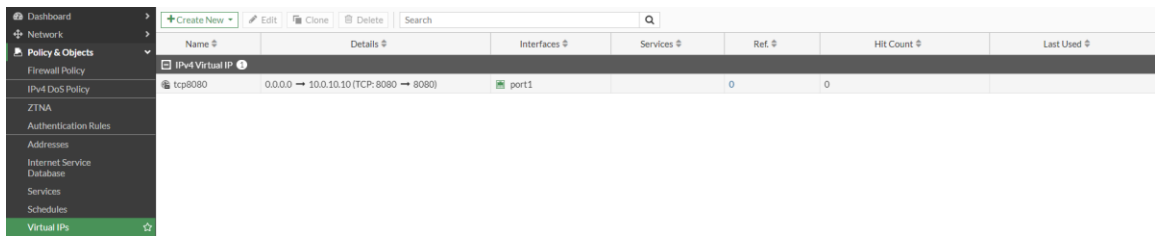
所有服务 > 网络安全组 > fgt-external

fgt-external | 入站安全规则

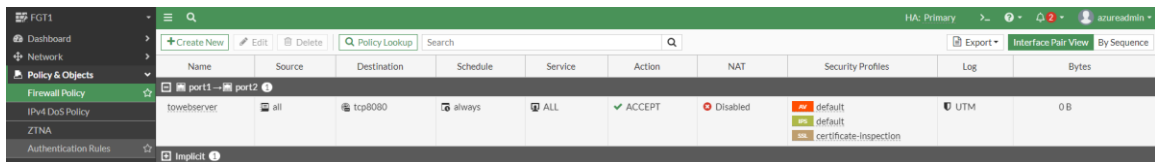
使用源、目标、目标端口、协议的组合，按优先级评估网络安全安全规则，从而允许或拒绝流量。安全规则的优先级和方向不能与现有规则相同。无法删除默认安全规则，但可以使用优先级较高的规则替代这些规则。[了解详细信息。](#)

优先级 ↑	名称 ↑	端口 ↑	协议 ↑	源 ↑	目标 ↑	操作 ↑
☐ 100	AllowAnyCustom443Inbound	443	TCP	任何	任何	允许
☐ 110	AllowAnyCustom22Inbound	22	TCP	任何	任何	允许
☐ 120	AllowAnyCustomAnyInbound	任何	ICMP	任何	任何	允许
☒ 130	AllowAnyCustom8080Inbound	8080	TCP	任何	任何	允许
☐ 65000	AllowVnetInbound	任何	任何	VirtualNetwork	VirtualNetwork	允许
☐ 65001	AllowAzureLoadBalancerInbound	任何	任何	AzureLoadBalancer	任何	允许
☐ 65500	DenyAllInbound	任何	任何	任何	任何	拒绝

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。

所有服务 > 负载均衡 | 负载均衡器 > wxfgt-internal-lb

wxfgt-internal-lb | 运行状况探测

负载均衡器

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

前端 IP 配置

后端池

运行状况探测

+ 添加

刷新

提供反馈

键入以开始筛选...

名称	协议	端口	路径	使用者
tcp-443	Tcp	443	-	-

所有服务 > 负载均衡 | 负载均衡器 > wxfgt-internal-lb | 运行状况探测 >

添加运行状况探测

wxfgt-internal-lb

运行状况探测用于检查后端池实例的状态。如果运行状况探测无法从后端实例获取响应，则在运行状况探测再次成功之前，将不会向该后端实例发送新的连接。

名称 *

tcp-443

协议 *

TCP

端口 * ①

443

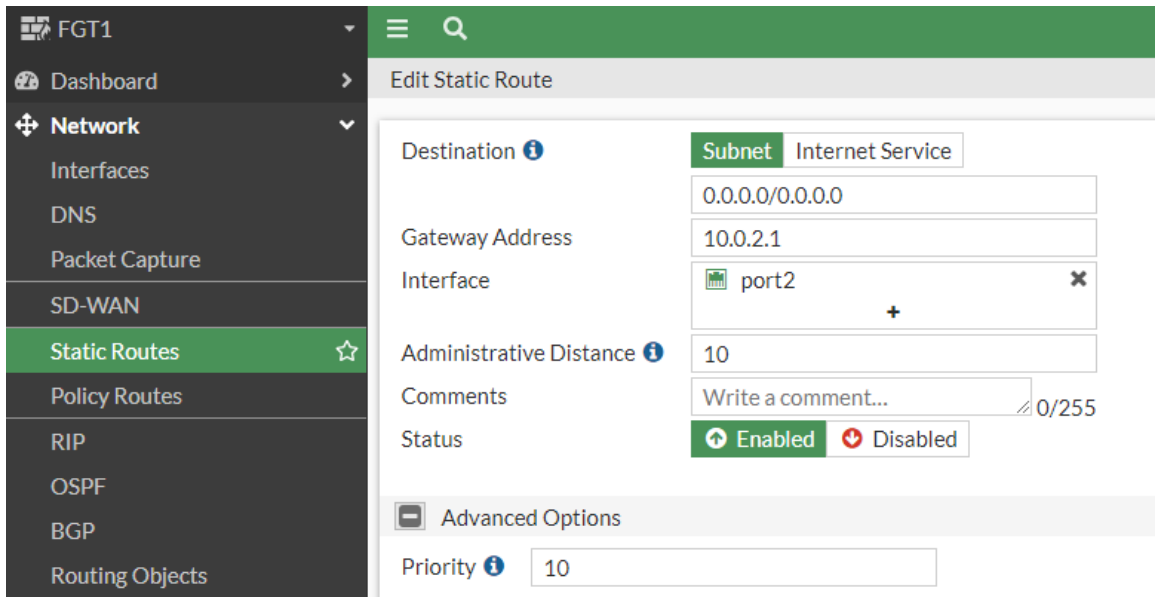
间隔(秒) * ①

5

使用者 * ①

未使用

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。



Destination	Gateway IP	Interface	Status	Distance	Priority
0.0.0.0/0	10.0.1.1	port1	Enabled	10	1
10.0.0.0/16	10.0.2.1	port2	Enabled	10	1
0.0.0.0/0	10.0.2.1	port2	Enabled	10	10

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。



所有服务 > 负载均衡 | 负载均衡器 > wxfgt-internal-lb | 负载均衡规则 >

添加负载均衡规则

wxfgt-internal-lb

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 *	Outbound
IP 版本 *	☒ IPv4 ☐ IPv6
前端 IP 地址 * ①	To-fgt (10.0.2.254)
后端池 * ①	fgt-pool-internal
高可用性端口 ①	☒
运行状况探测 * ①	tcp-443 (TCP:443)
会话持续性 ①	无
空闲超时(分钟) * ①	4
启用 TCP 重置	☐
启用浮动 IP ①	☐

配置 FortiGate 出站策略。

The screenshot shows the FortiGate Web UI configuration page for a Firewall Policy. The policy is named 'port1 -> port2' and is configured to allow traffic from 'To-Internet' to 'all' destinations. The action is set to 'ACCEPT' and the policy is enabled. The security profiles include 'default', 'default', and 'certificate-inspection'. The log is set to 'UTM' and the bytes are set to '0B'.

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

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。

The screenshot shows the Azure Portal configuration page for an Outbound Rule named 'Outbound'. The rule is configured to allow traffic from 'wxlb-public-ip-pool' to 'fgt-pool (2 个实例)' on port 31992. The rule is enabled and the action is set to 'Allow'.

名称: Outbound

前端 IP 地址: wxlb-public-ip-pool

后端: fgt-pool (2 个实例)

协议: All

每个实例的端口数: 31992

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 * ①

已选择 1 项

协议

☒ All

☐ TCP

☐ UDP

空闲超时(分钟) ①

4

最大值: 100

TCP 重置 ①

☒ 已启用

☐ 已禁用

后端池 * ①

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 ①

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 ①

31992

可用的前端端口

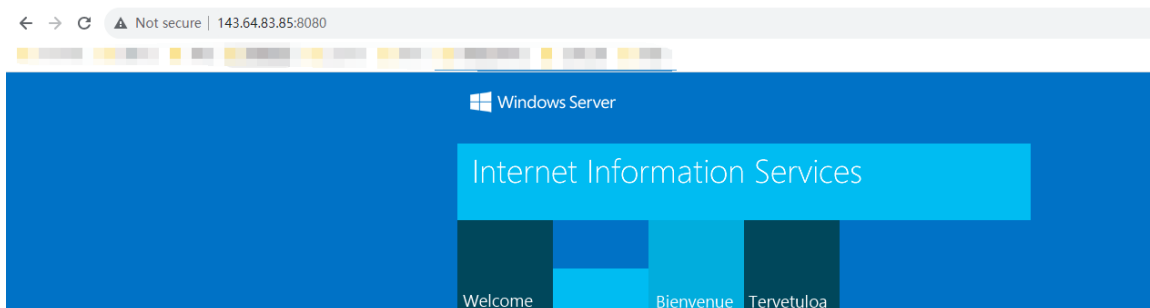
63992

最大后端实例数 * ①

2

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。

