

## 组网及说明

### 1 配置需求及说明

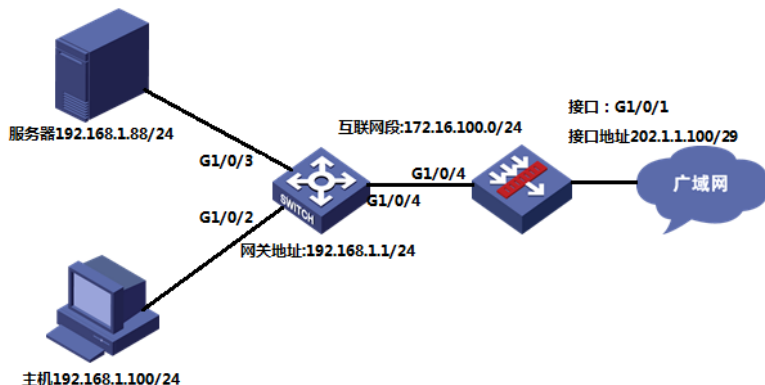
#### 1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

#### 1.2 配置需求及实现的效果

防火墙部署在互联网出口，内网有一台OA服务器通过防火墙发布了8081端口，并且外网用户访问对应服务正常。目前需要实现内网用户也能通过公网地址去访问内部服务器的需求。

### 2 组网图



## 配置步骤

### 3 配置步骤

#### 3.1 配置内部服务器映射（端口映射）

#在外网口填写运营商提供的公网地址，掩码，配置映射，映射端口8081，服务器地址192.168.1.88

```
system-view
[H3C] interface GigabitEthernet1/0/1
[H3C-GigabitEthernet1/0/1] ip add 202.1.1.100 255.255.255.248
[H3C-GigabitEthernet1/0/1] nat server protocol tcp global 202.1.1.100 8081 inside 192.168.1.88 8081
[H3C-GigabitEthernet1/0/1] quit
```

#在内网口配置映射,填写内网网关地址以及配置Nat Hairpin

```
[H3C] interface GigabitEthernet1/0/4
[H3C-GigabitEthernet1/0/4] ip add 172.16.100.1 255.255.255.0
[H3C-GigabitEthernet1/0/4] nat hairpin enable
[H3C-GigabitEthernet1/0/4] quit
```

Nat Hairpin功能简介: 通过在内网侧接口上使能NAT hairpin功能, 可以实现内网用户使用NAT地址访问内网服务器或内网其它用户。NAT hairpin功能需要与内部服务器 (nat server)、出方向动态地址转换 (nat outbound) 或出方向静态地址转换 (nat static outbound) 配合工作, 且这些配置所在的接口必须在同一个接口板, 否则NAT hairpin功能无法正常工作。

#### 3.2 配置策略

#创建地址对象组, 地址对象组名称为OA服务器

```
[H3C] object-group ip address OA服务器
[H3C-obj-grp-ip-OA服务器] network host address 192.168.1.88
[H3C-obj-grp-ip-OA服务器] quit
```

#创建服务对象组, 服务对象组名称为8081端口, 目的端口8081

```
[H3C] object-group service 8081端口
[H3C-obj-grp-service-8081端口] service tcp destination eq 8081
[H3C-obj-grp-service-8081端口] quit
```

#创建IPv4对象策略, 策略名称为OA服务器, 放通目的地址为192.168.1.88的8081端口

```
[H3C] object-policy ip OA服务器
[H3C-object-policy-ip-OA服务器] rule 0 pass destination-ip 192.168.1.88 service 8081端口
```

#创建安全策略, 源安全域为Untrust目的安全域为Trust, 应用创建的IPv4对象策略

```
[H3C] zone-pair security source Untrust destination Trust
[H3C-zone-pair-security-Untrust-Trust] object-policy apply ip OA服务器
```

```
[H3C-zone-pair-security-Untrust-Trust]quit
#创建IPv4对象策略, 策略名称为互通,规则为允许
[H3C]object-policy ip 互通
[H3C-zone-pair-security-互通]rule pass
[H3C-zone-pair-security-互通]quit
#创建安全策略, 源安全域为Trust目的安全域为Trust, 放通内网到内部服务器的访问数据
[H3C]zone-pair security source Trust destination Trust
[H3C-zone-pair-security-Trust-Trust]object-policy apply ip 互通
[H3C-zone-pair-security-Trust-Trust]quit
```

#### 4 保存配置

```
[H3C]save force
```

配置关键点