

组网及说明

1 配置需求或说明

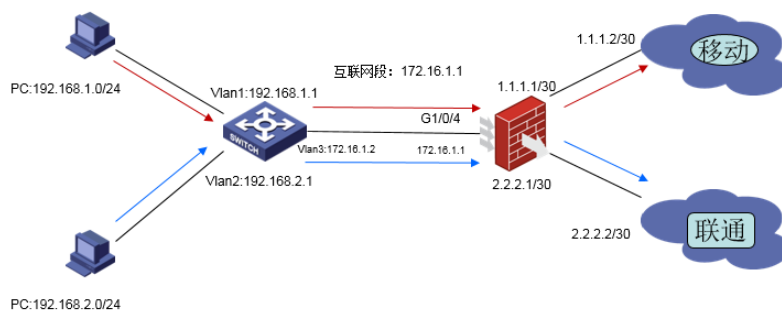
1.1 适用的产品系列

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

防火墙作为网络出口设备，外网有移动和联通两条线路。内网有192.168.1.0和192.168.2.0两个网段，要实现192.168.1.0网段走移动线路，192.168.2.0网段走联通车线路。当两条线路中的一条线路故障时数据可以通过正常链路转发。

2 组网图



配置步骤

3 上网配置

防火墙上网配置略，本文只针对策略路由配置进行介绍。

3.1 新建访问控制列表匹配移动和联通数据

创建ACL匹配需要由移动链路转发的数据

创建ACL 3000匹配192.168.1.0网段数据

```
system-view
```

```
[H3C]acl advanced 3000
```

```
[H3C-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255
```

```
[H3C-acl-ipv4-adv-3000]quit
```

创建ACL匹配需要由联通链路转发的数据

创建ACL 3001匹配192.168.2.0网段数据

```
[H3C]acl advanced 3001
```

```
[H3C-acl-ipv4-adv-3001]rule 0 permit ip source 192.168.2.0 0.0.0.255
```

```
[H3C-acl-ipv4-adv-3001]quit
```

3.2 创建策略路由

创建移动策略路由由节点

创建策略路由由neiwang节点5匹配192.168.1.0网段的数据由移动线路转发。

```
[H3C]policy-based-route neiwang node 5
```

```
[H3C-pbr-neiwang-5]if-match acl 3000
```

```
[H3C-pbr-neiwang-5]apply next-hop 1.1.1.2
```

```
[H3C-pbr-neiwang-5]quit
```

注：next-hop后的地址为移动线路的网关

创建移动策略路由由节点

创建策略路由由neiwang节点10匹配192.168.2.0网段的数据由联通线路转发。

```
[H3C]policy-based-route neiwang node 10
```

```
[H3C-pbr-neiwang-10]if-match acl 3001
```

```
[H3C-pbr-neiwang-10]apply next-hop 2.2.2.2
```

```
[H3C-pbr-neiwang-10]quit
```

注：next-hop后的地址为联通线路的网关

3.3 应用策略

在防火墙连接内网的接口GigabitEthernet 1/0/4口调用策略路由

```
[H3C]interface GigabitEthernet 1/0/4
```

```
[H3C-GigabitEthernet1/0/4]ip policy-based-route neiwang
```

```
[H3C-GigabitEthernet1/0/4]quit
```

注：策略路由必须调用在内网接口才能生效。

4 保存配置

```
[H3C]save force
```

配置关键点