

## 一 实验需求

本案例适用小贝优选全系列防火墙，针对防火墙有多个出口，对内网的流量进行策略路由，使得流量按照策略转发。

## 二 组网图



## 三、操作过程

### 3.1 配置防火墙上网

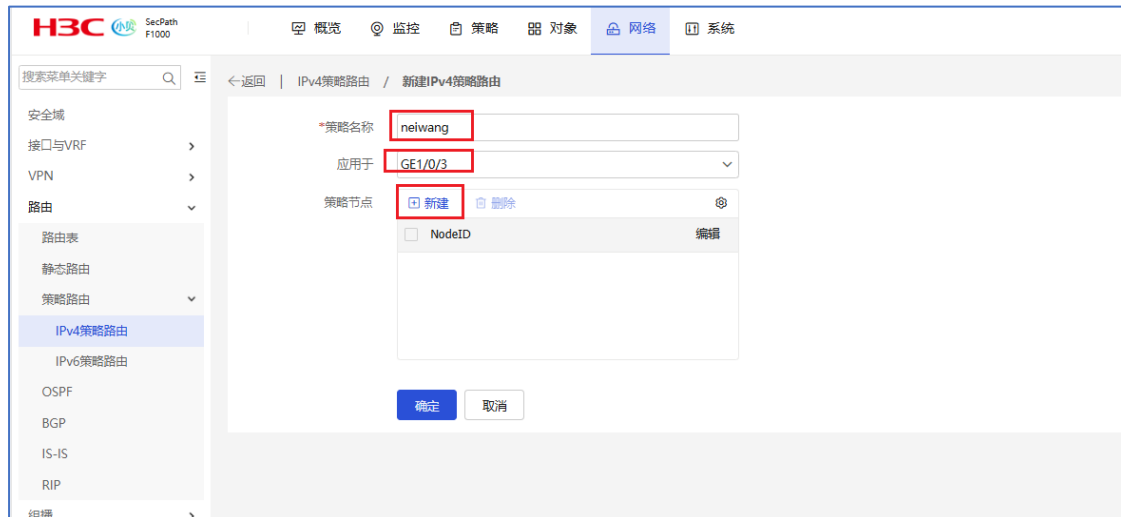
该操作步骤请按照防火墙固定上网配置进行部署

### 3.2 配置策略路由

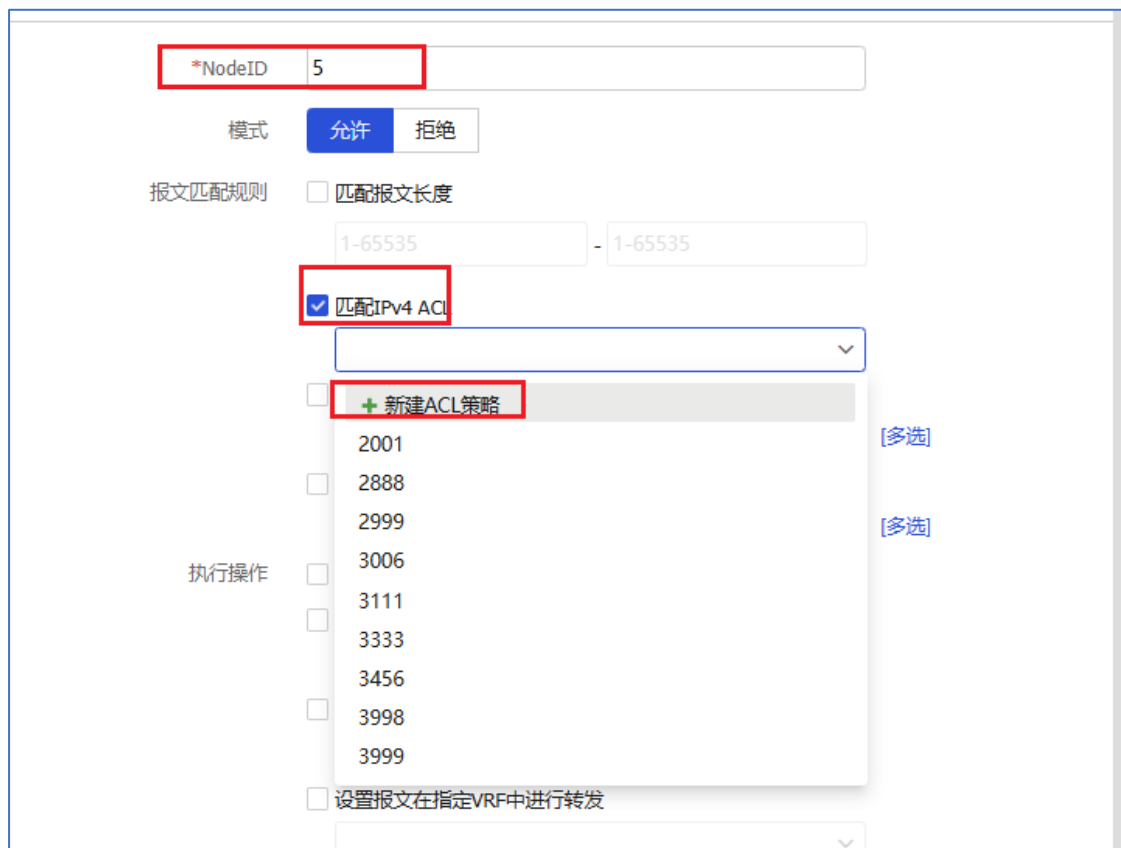
#### 3.2.1 创建策略路由

在【网络】>【路由】>【策略路由】>【IPV4 策略路由】中点击“新建”，策略名称设置为“neiwang” 应用于“GE1/0/3”。





### 3.2.2 新建策略节点匹配移动数据



新建IPv4ACL

类型 ☐ 基本ACL ☒ 高级ACL

\*ACL ①

规则匹配顺序 ☒ 按照配置顺序 ☐ 自动排序

默认规则编号步长

描述

在新弹窗中“IP 协议类型选择”为 IP，勾选匹配条件为“匹配源 IP 地址/通配符掩码”配置 IP 地址为 192.168.1.0，设置反掩码为 0.0.0.255 后点击确定

新建IPv4高级ACL的规则

?

×

ACL编号

3000

\*规则编号

0-65534

☒ 自动编号

描述

1-127字符

动作

允许

拒绝

\*IP协议类型

256

▼

匹配条件?

☒ 匹配源IP地址/通配符掩码

192.168.1.0

/

0.0.0.255

☐ 匹配源地址对象组

☐ 匹配目的IP地址/通配符掩码

☐ 匹配目的地址对象组

☐ 匹配TCP/UDP报文的源端口号

☐ 匹配TCP/UDP报文的目的端口号

☐ 匹配TCP报文的连接建立标识

☐ 匹配TCP报文标识

☐ 匹配ICMP报文的消息类型和消息码

☐ 匹配DSCP优先级

☐ 匹配IP优先级

☐ 匹配ToS优先级

规则生效时间段

请选择...

▼

VRF

公网

▼

分片报文?

☐ 仅对分片报文的非首个分片有效

确认匹配 IPv4 ACL 已经有访问控制列表时，在“设置报文转发的下一条地址”中点击新建

\*NodeID

5

模式

允许

拒绝

报文匹配规则

☐ 匹配报文长度

1-65535

-

1-65535

☒ 匹配IPv4 ACL

3000

▼

☐ 匹配服务对象组

▼

[多选]

☐ 匹配应用组

▼

[多选]

执行操作

☐ 设置后续节点 ?

☐ 设置报文的IP优先级

0:Routine

▼

☐ 设置IP报文头中的分片标志

0:允许分片操作

▼

☐ 设置报文在指定VRF中进行转发

▼

设置报文转发的下一跳地址

+ 新建

删除

☐ VRF

IP地址

缺省

Track项

直连...

编辑

设置报文转发的出接口

+ 新建

删除

☐ 接口

缺省

Track项

编辑

报文转发的下一跳地址

\*VRF

公网

▼

\*IP地址

1.1.1.2

缺省

否

▼

Track项 ?

▼

直连下一跳

是

▼

策略全部配置完成后点击确定完成对移动链路的配置。

\*NodeID 5

模式 **允许** 拒绝

报文匹配规则 ☐ 匹配报文长度

1-65535 - 1-65535

☒ 匹配IPv4 ACL

3000

☐ 匹配服务对象组

[多选]

☐ 匹配应用组

[多选]

执行操作 ☐ 设置后续节点 ②

☐ 设置报文的IP优先级

0:Routine

☐ 设置IP报文头中的分片标志

0:允许分片操作

☐ 设置报文在指定VRF中进行转发

设置报文转发的下一跳地址

| + 新建                     |     | 删除      |    |        |       |    |
|--------------------------|-----|---------|----|--------|-------|----|
| <input type="checkbox"/> | VRF | IP地址    | 缺省 | Track项 | 直连... | 编辑 |
| <input type="checkbox"/> | 公网  | 1.1.1.2 | 否  | 是      |       |    |

设置报文转发的出接口

| + 新建                     |    | 删除 |        |    |  |  |
|--------------------------|----|----|--------|----|--|--|
| <input type="checkbox"/> | 接口 | 缺省 | Track项 | 编辑 |  |  |

取消

确定

### 3.2.3 新建策略节点匹配联通线路

在策略节点中点击“新建”，NodeID 设置为“10”，勾选“匹配 IPv4 ACL”后添加 ACL 策略。

新建策略节点

\*NodeID 10

模式 允许 拒绝

报文匹配规则 ☐ 匹配报文长度 1-65535 - 1-65535

☒ 匹配IPv4 ACL

+ 新建ACL策略

2001 [多选]

2888

2999 [多选]

3000

3006

3111

3333

3456

3998

执行操作

类型选择“高级 ACL”，ACL 编号设置为 3001 然后点击确定。

新建IPv4ACL

类型

基本ACL

高级ACL

\*ACL ?

3001

规则匹配顺序

按照配置顺序

自动排序

默认规则编号步长

5

描述

1-127字符

取消

确定

确定并添加规则 ?

在新弹窗中“IP 协议类型选择”为 IP，勾选匹配条件为“匹配源 IP 地址/通配符掩码”配置 IP 地址为 192.168.2.0，设置反掩码为 0.0.0.255 后点击确定

ACL编号

3001

\*规则编号

0-65534

☒ 自动编号

描述

1-127字符

动作

允许

拒绝

\*IP协议类型

256

匹配条件 ?

☒ 匹配源IP地址/通配符掩码

192.168.2.0

/ 0.0.0.255

☐ 匹配源地址对象组☐ 匹配目的IP地址/通配符掩码☐ 匹配目的地址对象组☐ 匹配TCP/UDP报文的源端口号☐ 匹配TCP/UDP报文的目的端口号☐ 匹配TCP报文的连接建立标识☐ 匹配TCP报文标识☐ 匹配ICMP报文的消息类型和消息码☐ 匹配DSCP优先级☐ 匹配IP优先级☐ 匹配ToS优先级

规则生效时间段

请选择...

VRF

公网

分片报文 ?

☐ 仅对分片报文的非首个分片有效

记录日志

☐ 对符合条件的报文记录日志信息

匹配统计

☐ 开启本规则的匹配统计功能

确认匹配 IPv4 ACL 已经有访问控制列表时，在“设置报文转发的下一条地址”中点击新建。

\*NodeID10

模式

允许

拒绝

报文匹配规则

☐ 匹配报文长度

1-65535

-

1-65535

☒ 匹配IPv4 ACL

3001

☐ 匹配服务对象组

[多选]

☐ 匹配应用组

[多选]

执行操作

☐ 设置后续节点 ②

☐ 设置报文的IP优先级

0:Routine

☐ 设置IP报文头中的分片标志

0:允许分片操作

☐ 设置报文在指定VRF中进行转发

设置报文转发的下一跳地址

+ 新建

删除

| <input type="checkbox"/> VRF | IP地址 | 缺省 | Track项 | 直连... | 编辑 |
|------------------------------|------|----|--------|-------|----|
|------------------------------|------|----|--------|-------|----|

设置报文转发的出接口

+ 新建

删除

| <input type="checkbox"/> 接口 | 缺省 | Track项 | 编辑 |
|-----------------------------|----|--------|----|
|-----------------------------|----|--------|----|

设置 IP 地址为联通外网线路的网关地址 2.2.2.2 后点击确定

\*NodeID10

模式

允许

拒绝

报文匹配规则

☐ 匹配报文长度

1-65535-1-65535

☒ 匹配IPv4 ACL

3001

☐ 匹配服务对象组

[多选]

☐ 匹配应用组

[多选]

执行操作

☐ 设置后续节点

☐ 设置报文的IP优先级

0:Routine

☐ 设置IP报文头中的分片标志

0:允许分片操作

☐ 设置报文在指定VRF中进行转发

设置报文转发的下一跳地址

+ 新建

删除

| <input type="checkbox"/> | VRF | IP地址    | 缺省 | Track项 | 直连... | 编辑 |
|--------------------------|-----|---------|----|--------|-------|----|
| <input type="checkbox"/> | 公网  | 2.2.2.2 | 否  | 是      |       |    |

设置报文转发的出接口

+ 新建

删除

| <input type="checkbox"/> | 接口 | 缺省 | Track项 | 编辑 |
|--------------------------|----|----|--------|----|
|--------------------------|----|----|--------|----|

最后在 IPv4 策略中点击确定完成策略配置

← 返回 | IPv4策略路由 / 新建IPv4策略路由

\*策略名称

neiwang

应用于

GE1/0/3

策略节点

新建

删除

☐

NodeID

编辑

☐

5

☐

10

确定

取消

## 保存配置

|                                                |         |         |     |  |  |  |  |  |  |  |
|------------------------------------------------|---------|---------|-----|--|--|--|--|--|--|--|
| H3C                                            |         |         |     |  |  |  |  |  |  |  |
| 策略路由                                           |         |         |     |  |  |  |  |  |  |  |
| 策略名称 策略子接口 节点 模式 报文长度 ACL 服务对象组 应用组 下一跳 出接口 编辑 |         |         |     |  |  |  |  |  |  |  |
| <input type="checkbox"/>                       | neiwang | GE1/0/3 | * 2 |  |  |  |  |  |  |  |