

知 F1000-X-G2/F100-X-G2系列防火墙策略路由配置案例（WEB）

策略路由 zhiliao_F03qD 2018-11-25 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

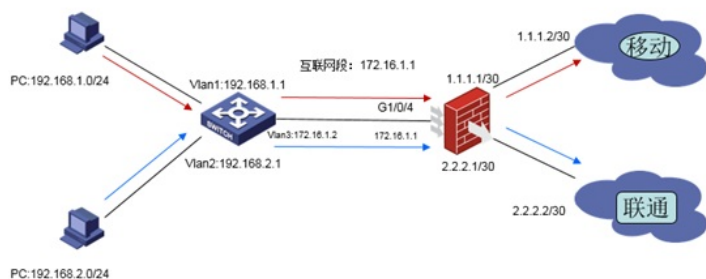
本案例适用于如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P1801版本上进行配置和验证的。

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，需要实现192.168.1.0网段走移动线路，192.168.2.0网段走联通车线。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

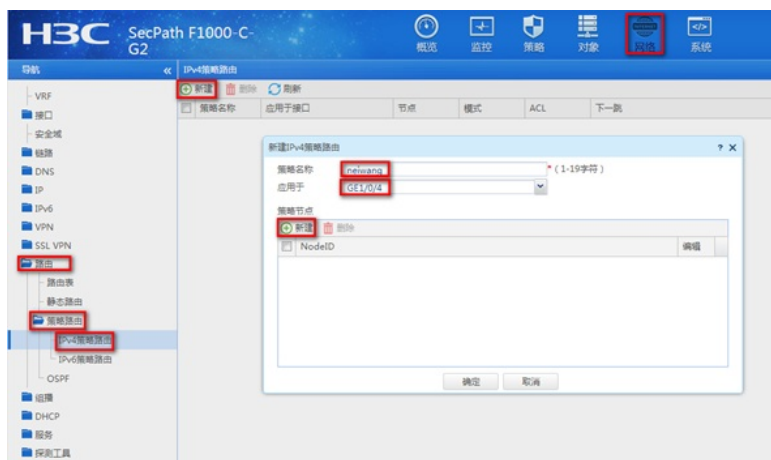
3 配置步骤

3.1 上网配置

防火墙上网配置请参考“2.2.2 防火墙外网使用固定IP地址上网配置方法”进行配置，本文只针对策略路由配置进行介绍。

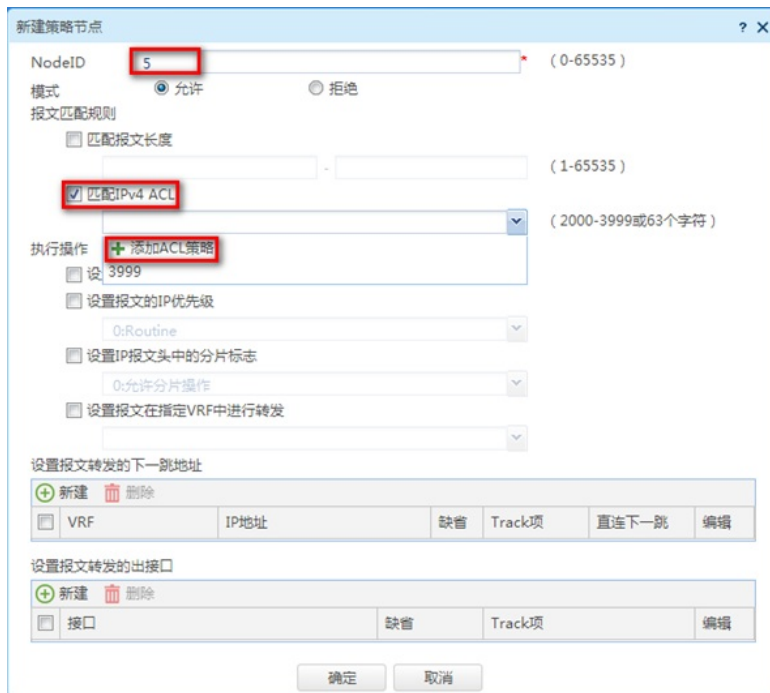
3.2 创建IPV4策略路由

#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“GE1/0/4”。



3.3 新建策略节点匹配移动数据

#在策略节点中点击“新建”，NodeID设置为“5”，勾选“匹配IPv4 ACL”后添加ACL策略。



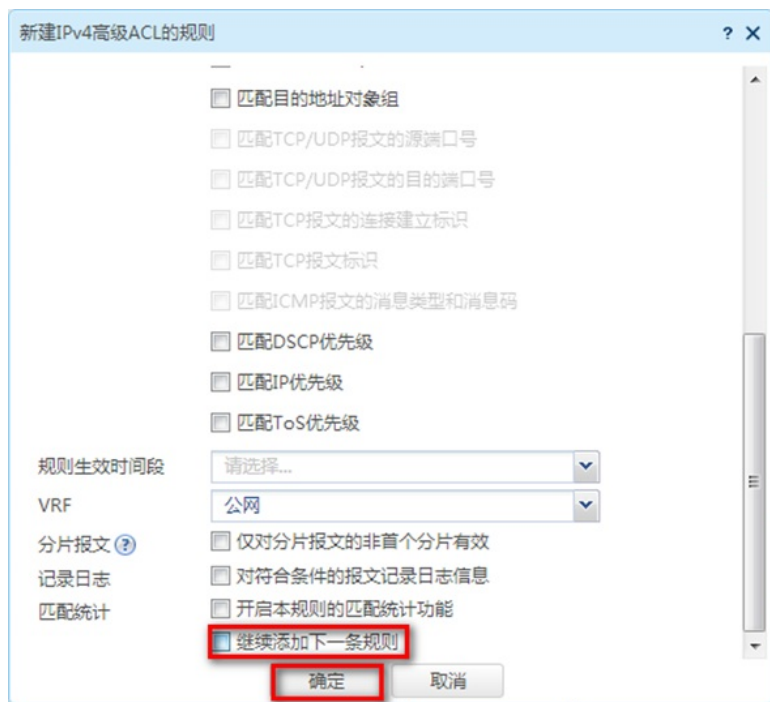
#类型选择“高级ACL”，ACL编号设置为3000然后点击确定。



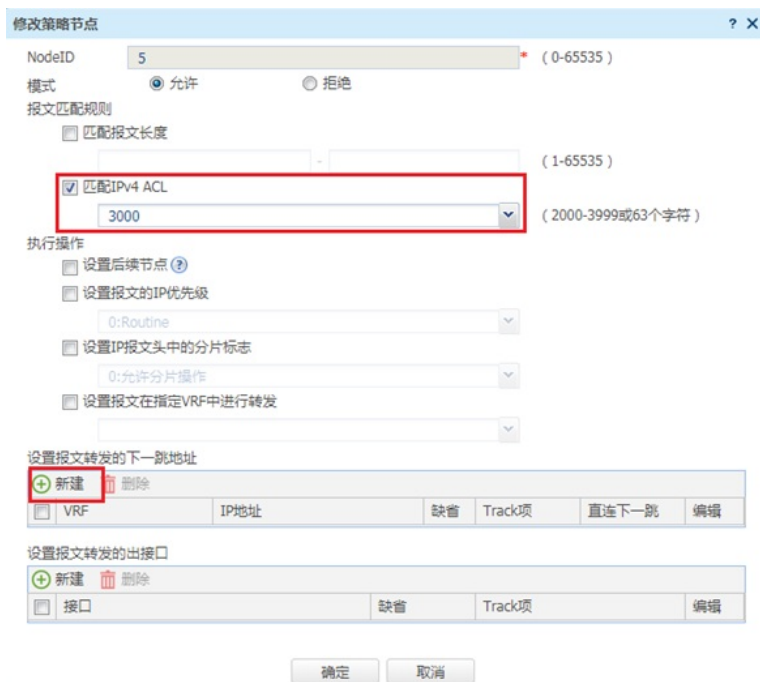
#在新弹窗中“IP协议类型选择”为IP，勾选匹配条件为“匹配源IP地址/通配符掩码”配置IP地址为192.168.1.0，设置反掩码为0.0.0.255后点击确定。



#在新弹窗中去勾选“继续添加下一条规则”点击确定。



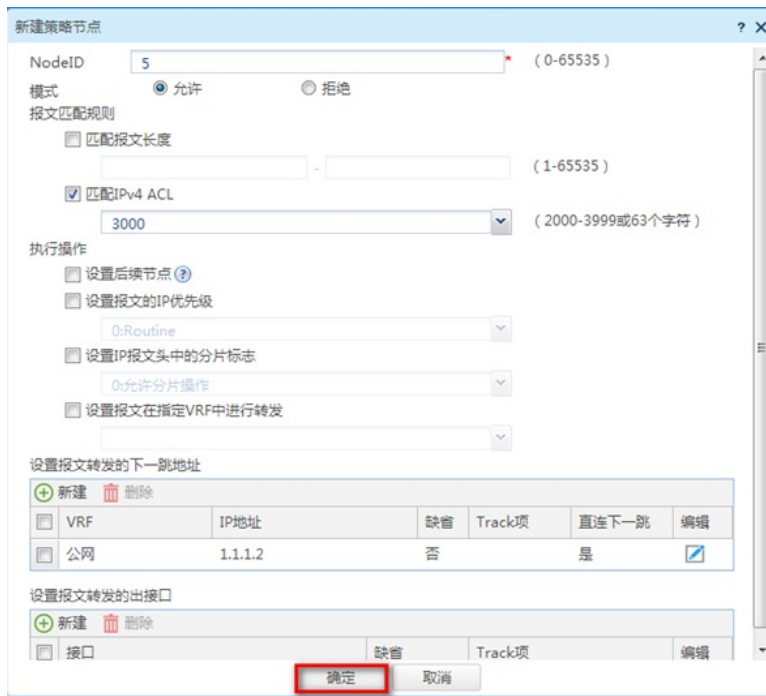
#确认匹配IPv4 ACL已经有访问控制列表时，在“设置报文转发的下一条地址”中点击新建。



#设置IP地址为移动外网线路的网关地址1.1.1.2后点击确定。

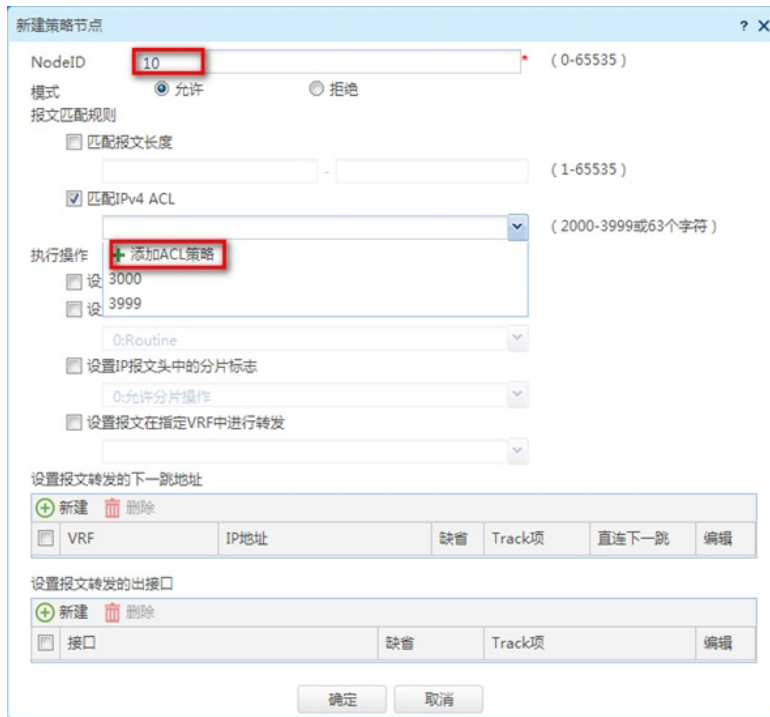


#策略全部配置完成后点击确定完成对移动链路的配置。

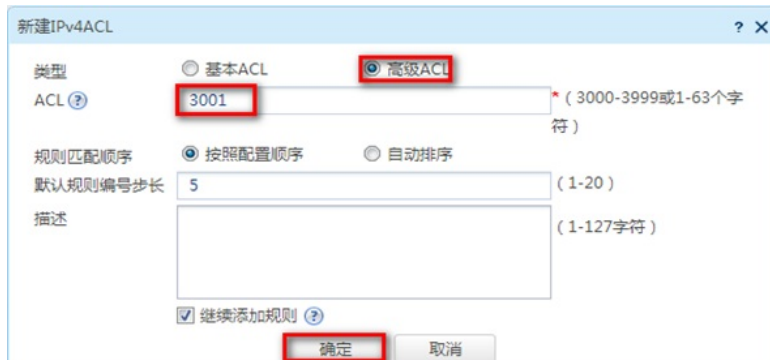


3.4 新建策略节点匹配联通线路

#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。



#类型选择“高级ACL”，ACL编号设置为3001然后点击确定。



#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。

新建IPv4高级ACL的规则

ACL编号: 3001 (3000-3999或1-63个字符)

规则编号: 自动编号 (0-65534)

描述: (1-127字符)

动作: 允许 拒绝

IP协议类型: 请选择... (0-256, 256代表任意ip)

匹配条件 匹配源IP地址/通配符掩码
 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报文的端口号

192.168.2.0 / 0.0.0.255

确定 取消

#在新弹窗中去勾选“继续添加下一条规则”点击确定。

新建IPv4高级ACL的规则

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
 继续添加下一条规则

确定 取消

#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。

新建策略节点

NodeID: 10 (0-65535)

模式: 允许 拒绝

报文匹配规则

匹配报文长度 (1-65535)

匹配IPv4 ACL (2000-3999或63个字符)

3001

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	直连下一跳	编辑

设置报文转发的出接口

新建 删除

接口	缺省	Track项	编辑

确定 取消

#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。

报文转发的下一跳地址

VRF: 公网

IP地址: 2.2.2.2

缺省: 否

Track项: (1-1024)

直连下一跳: 是

确定 取消

#策略全部配置完成后点击确定完成对联通链路的配置。

新建策略节点

NodeID: 10 (0-65535)

模式: 允许 拒绝

报文匹配规则

匹配报文长度 (1-65535)

匹配IPv4 ACL (2000-3999或63个字符)

3001

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	直连下一跳	编辑
公网	2.2.2.2	否		是	<input checked="" type="checkbox"/>

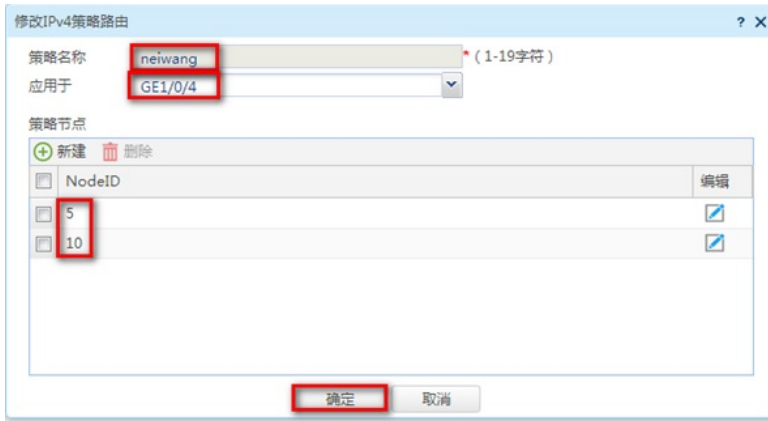
设置报文转发的出接口

新建 删除

接口	缺省	Track项	编辑

确定 取消

最后在IPv4策略中点击确定完成策略配置。



3.5 保存配置



配置关键点