F10X0/F50X0系列两台防火墙采用公网固定地址方式搭建IPSEC VPN配置案例（主模式WEB配置）

IPSec VPN　zhiliao_FO3qD　2018-11-25 发表

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F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

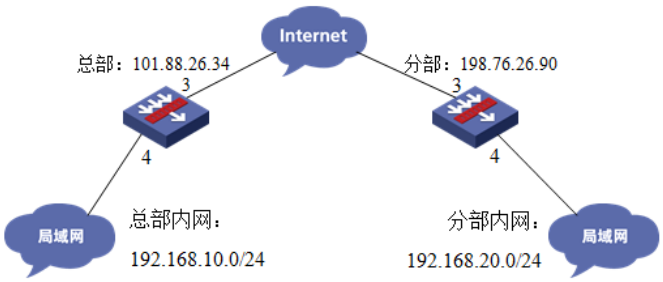
注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

总部和分部各有一台防火墙部署在互联网出口，因业务需要两端内网需要通过VPN相互访问。IP地址及接口规划如下表所示：

公司名称	外网接口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部	1/0/3	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部	1/0/3	198.76.26.90/30	198.76.26.89	1/0/4	192.168.20.0/24

2 组网图



配置步骤

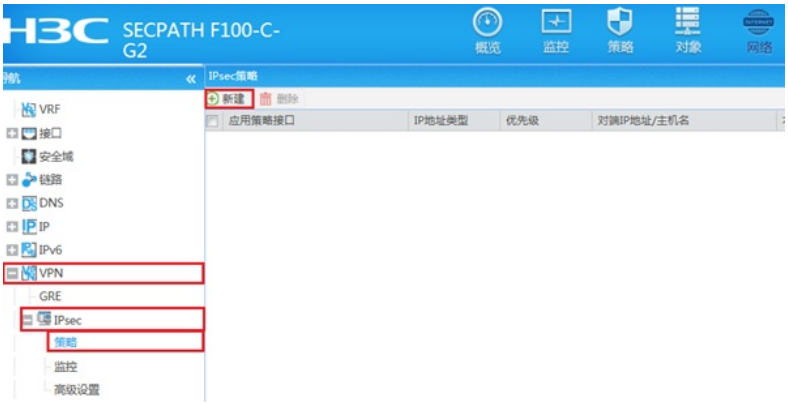
3 配置步骤

3.1 两端防火墙上网配置

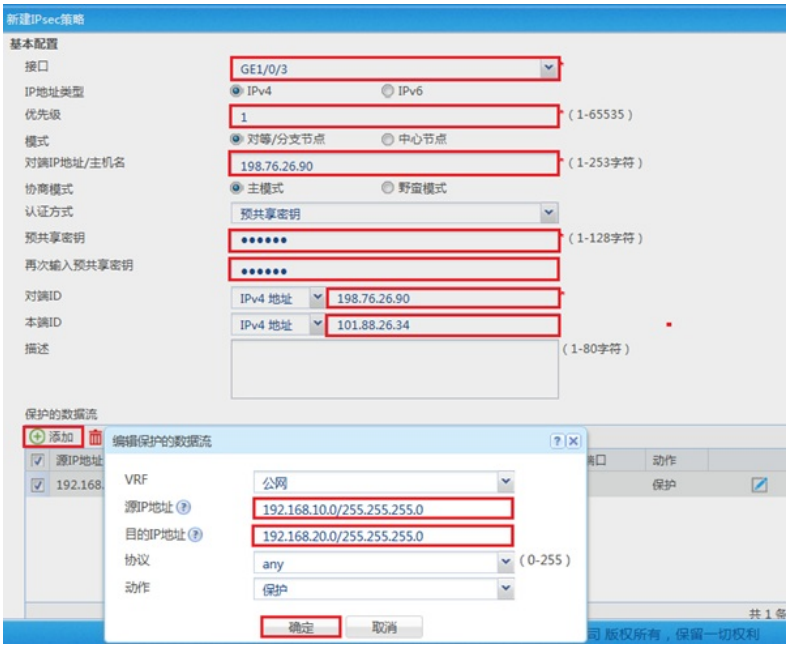
防火墙上网配置请参考“2.3.2 防火墙外网使用固定IP地址上网配置方法”进行配置，本文只针对IPSEC VPN配置进行介绍。

3.2 总部侧IPSEC VPN策略配置

#在“网络”>“VPN”>“策略”中点击新建。

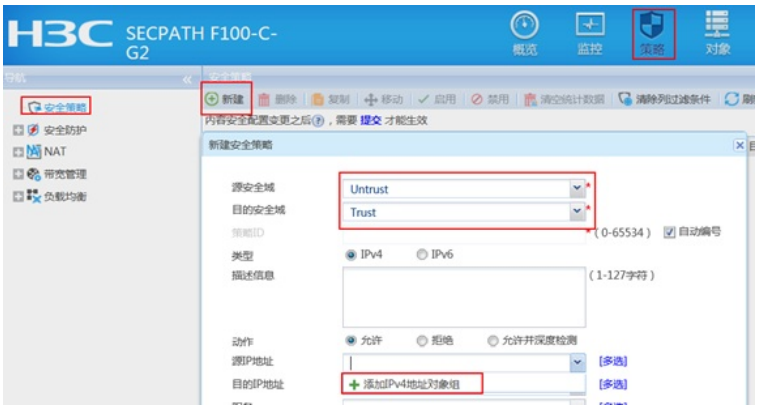


#在“基本配置”中“接口”选择接入外网的1/0/3接口，“优先级”设置为1（优先级代表了策略匹配顺序，当存在多条VPN隧道时需要对各VPN隧道优先级进行设置），“认证方式”选择域共享密钥，建立VPN两端隧道的域共享密钥必须一致。对端ID设置对IP地址即分公司公网地址，本端ID默认为本端公网接口IP地址。在保护的数据流中添加源为总部内网网段192.168.10.0/24，目的IP地址为分部内网网段192.168.20.0/24。

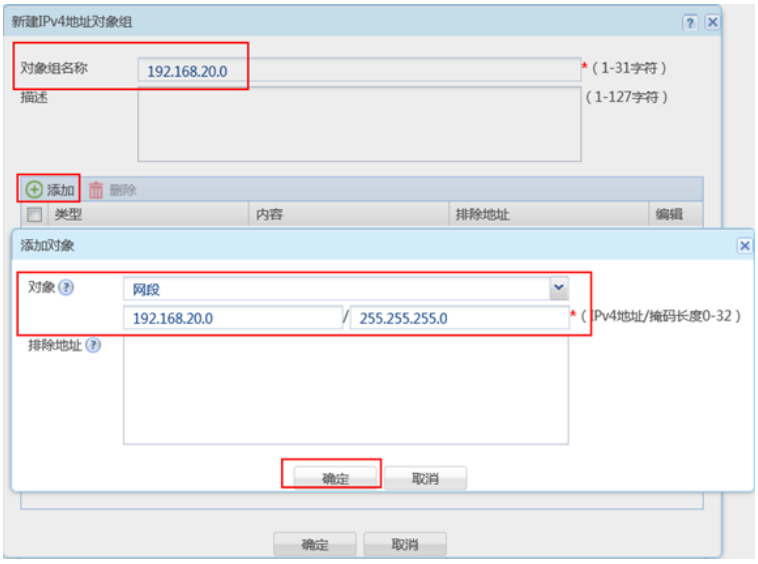


3.3 总部侧配置安全策略，放通IPSEC感兴趣流的数据策略

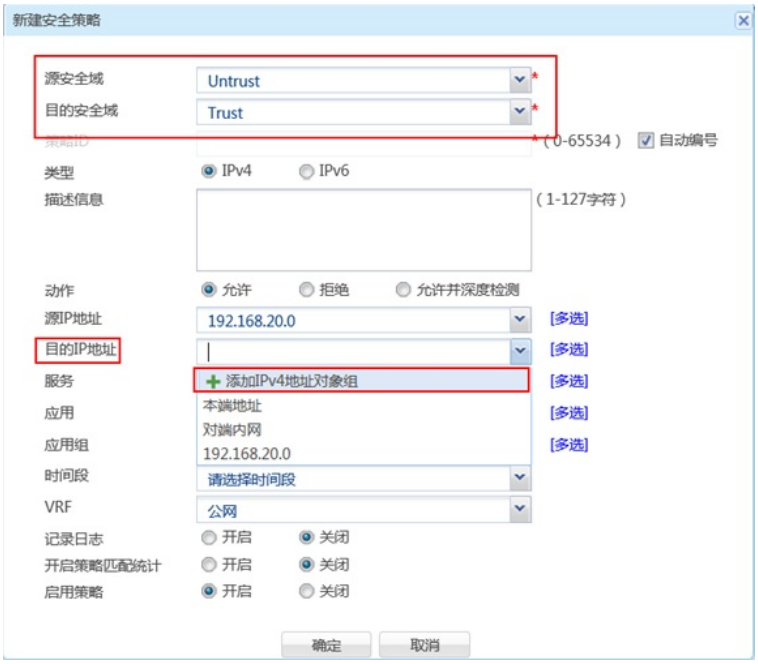
#在“策略”>“安全策略”>点击“新建”，“源IP地址”中点击“添加IPV4地址对象组”



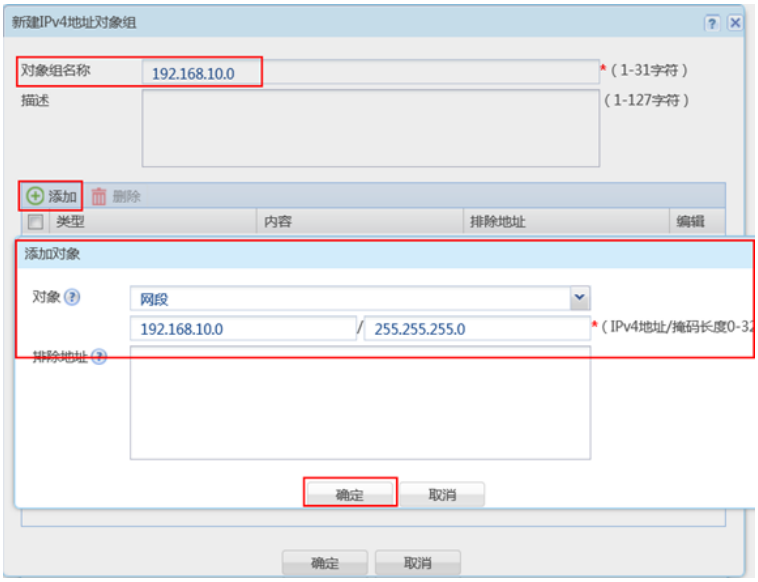
#配置对象组名称为“192.168.20.0”，点击“添加”，对象地址为192.168.20.0网段，为分支内网段地址



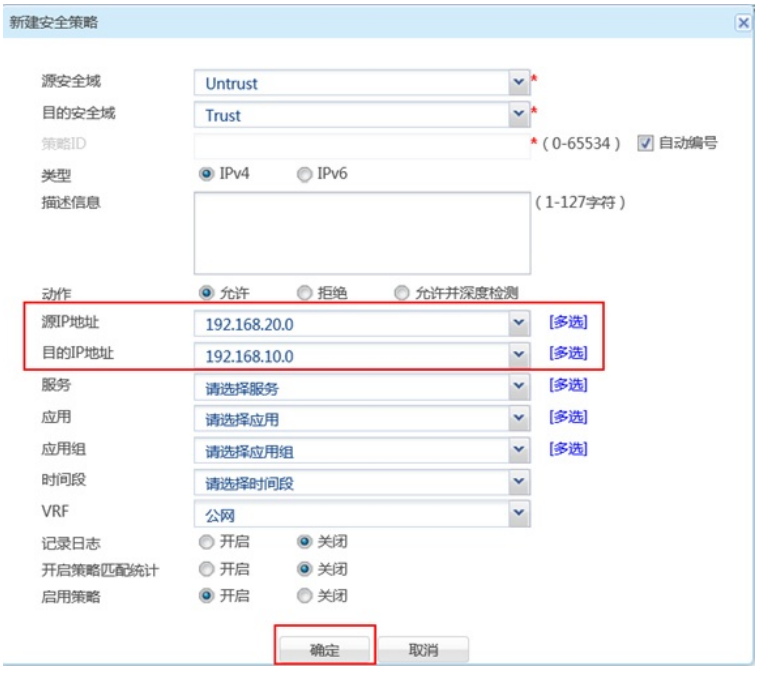
#在“策略”>“安全策略”>点击“新建”，“目的IP地址”中点击“添加IPV4地址对象组”



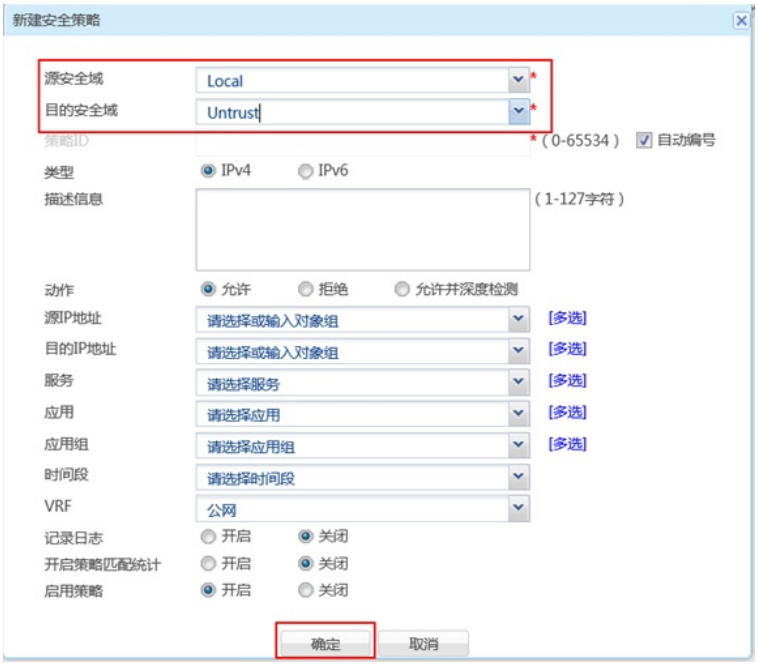
#配置对象组名称为“192.168.10.0”，点击“添加”，对象地址为192.168.10.0网段，为总部内网网段地址



#最后确认一下“源IP地址”为对端内网所在对象组，“目的IP地址”为本端内网地址所在对象组，确定即可

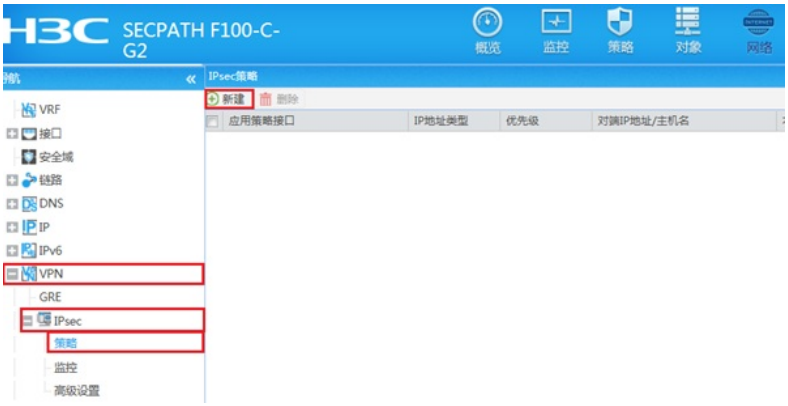


3.4 总部侧配置安全策略，放通Untrust到Local，和Local到Utrust的策略，用于建立IPSEC 隧道

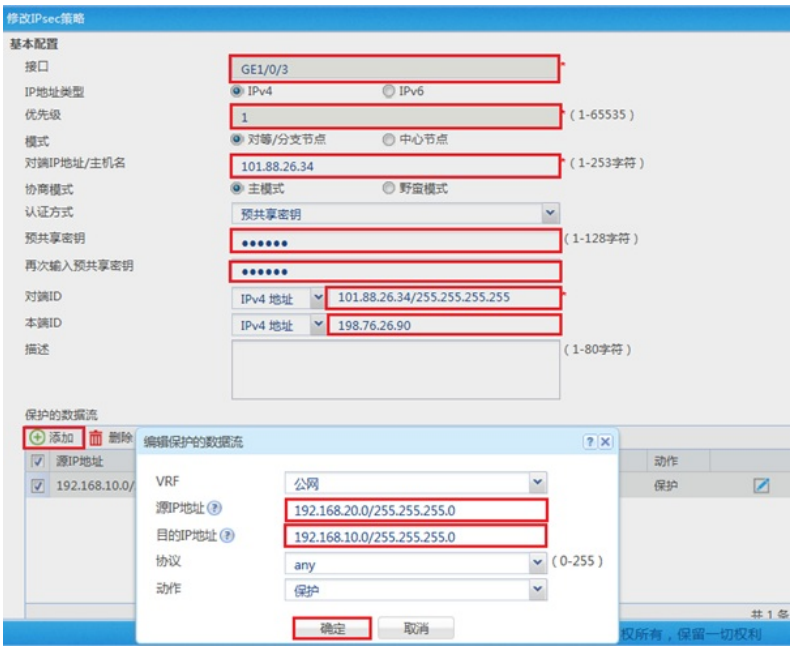


3.5 分部侧IPSEC VPN策略配置

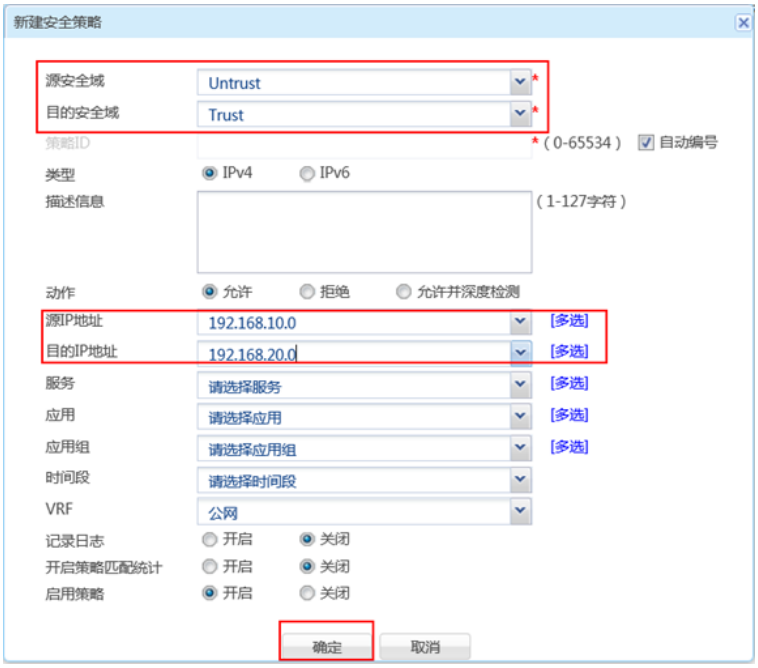
#在“网络”>“VPN”>“策略”中点击新建。



#在“基本配置”中“接口”选择接入外网的1/0/3接口，“优先级”设置为1（优先级代表了策略匹配顺序，当存在多条VPN隧道时需要对各VPN隧道优先级进行设置），“认证方式”选择域共享密钥，建立VPN两端隧道的域共享密钥必须一致。对端ID设置对IP地址即分公司公网地址，本端ID默认为本端公网接口IP地址。在保护的数据流中添加源为分部内网网段192.168.20.0/24，目的IP地址为总部内网网段192.168.10.0/24。



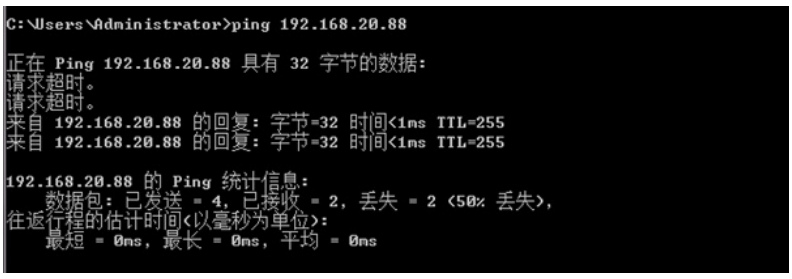
3.6 分部侧安全策略和总部的配置方法类似，只需将IPSEC的感兴趣流的源和目的IP反过来写即可。



3.7 测试VPN是否连通

在总部或者分部内网中任意找一台电脑访问对端网络资源。

举例：在总支侧电脑ping分部侧电脑，IPSEC初始建立时会丢1-2个包，建立后通信正常。

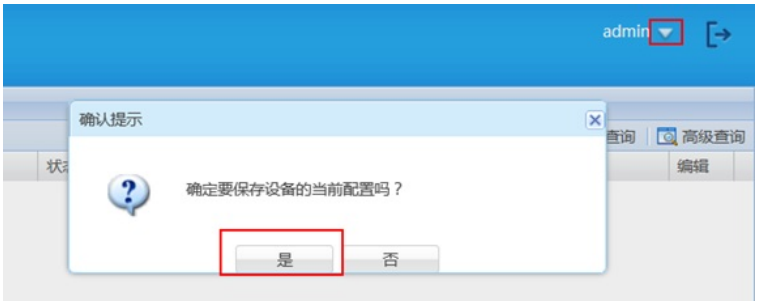


3.8 查看IPSEC监控信息

在“网络”>“VPN”>“IPsec”>“监控”中查看对到信息，如果有隧道信息就说明VPN已经正常建立，如果没有隧道信息就说明VPN未建立成功。

3.9 保存配置

在设备右上角选择“保存”选项，点击“是”完成配置。

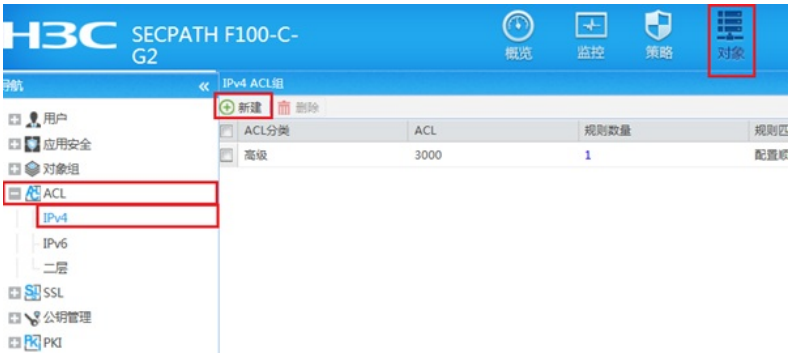


4 注意事项

4.1 外网接口配置动态地址转换导致VPN无法建立问题

在配置IPSEC VPN时需要注意外网口配置地址转换时一定要排除掉VPN的感兴趣流，因为NAT转换在接口出方向优先于IPSEC策略，如果不修改会导致数据先经过NAT地址转换后无法匹配兴趣流。

在“对象”>“ACL”>“IPv4”中点击新建按钮。



#在“类型”中选择高级ACL，ACL编号输入3999。

#以总部防火墙为例，动作选择拒绝，IP协议类型选择拒绝，匹配条件匹配总部侧内网到分部侧内网的网段（在分部侧防火墙匹配条件取反）后点击确定添加下一条策略。

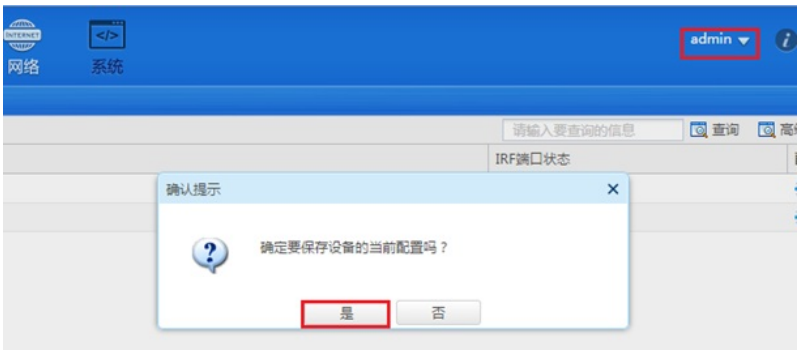
#不需要改变此页面配置，可以直接点击确定按钮。当有多个网段访问VPN的需求时，需要先添加拒绝的策略，再添加全部允许的策略。

#在“策略”>“NAT”>“NAT动态转换”>“策略配置”中点击新建按钮。接口选择外网接口，ACL选择之前创建的3999，转换后地址选择接口IP地址。

注意：如果配置策略中已经存在动态转换策略，请在此策略的基础上添加或者更换ACL选项。该操作可能导致断网请谨慎操作。

4.2 保存配置

在设备右上角选择“保存”选项，点击“是”完成配置。



配置关键点