ERG3 路由器对接华为路由器 IPSEC VPN（野蛮模式）

1 配置需求或说明

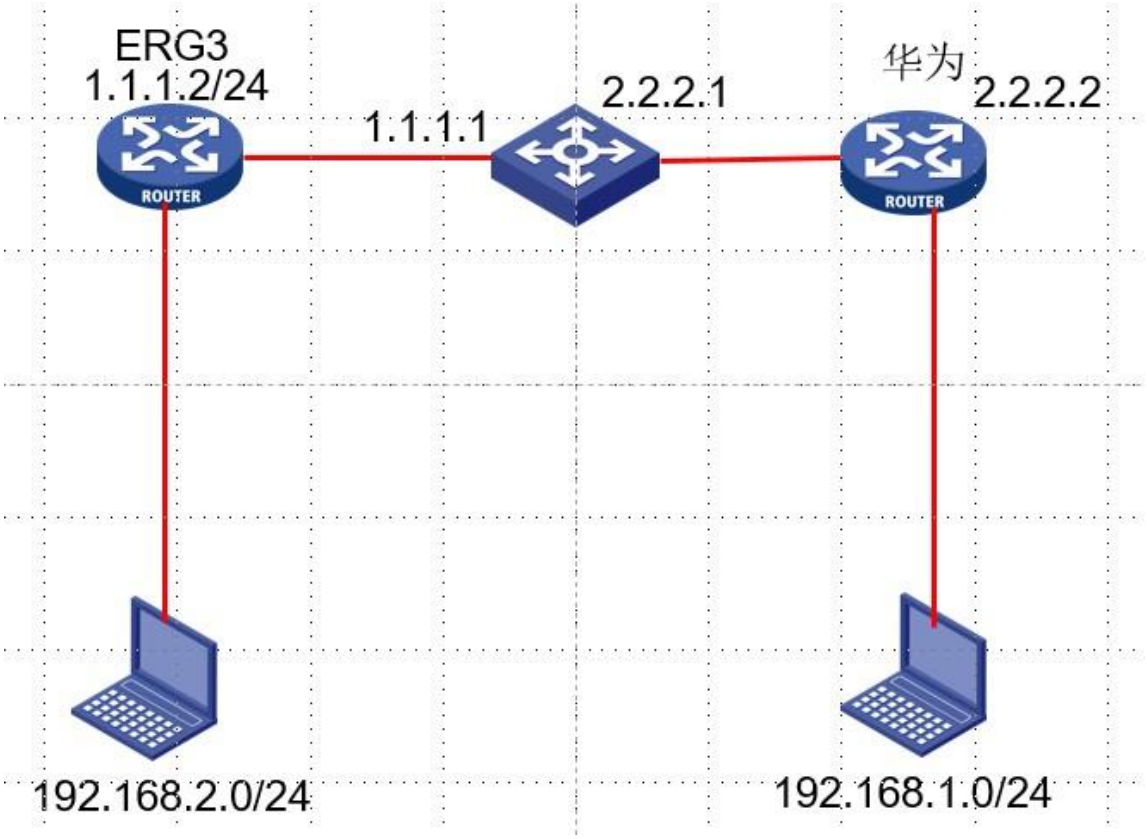
1.1 适用产品系列

本案例适用于 ERG3 系列路由器，华为 AR110-S 系列

1.2 配置需求及实现的效果

ERG3 和华为路由器分别作为企业网路的出口路由器，ERG3 有固定的公网地址，两个设备之间建立野蛮模式的 IPSEC VPN，ERG3 内网网段为 192.168.2.0/24，华为侧内网网段为 192.168.1.0/24 。

2 组网图



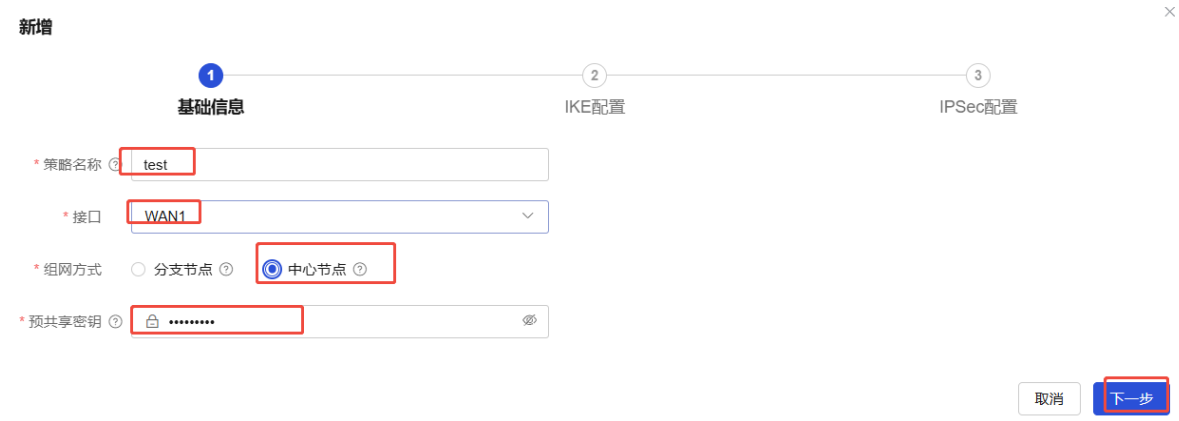
3 配置步骤

3.1 配置 ERG3

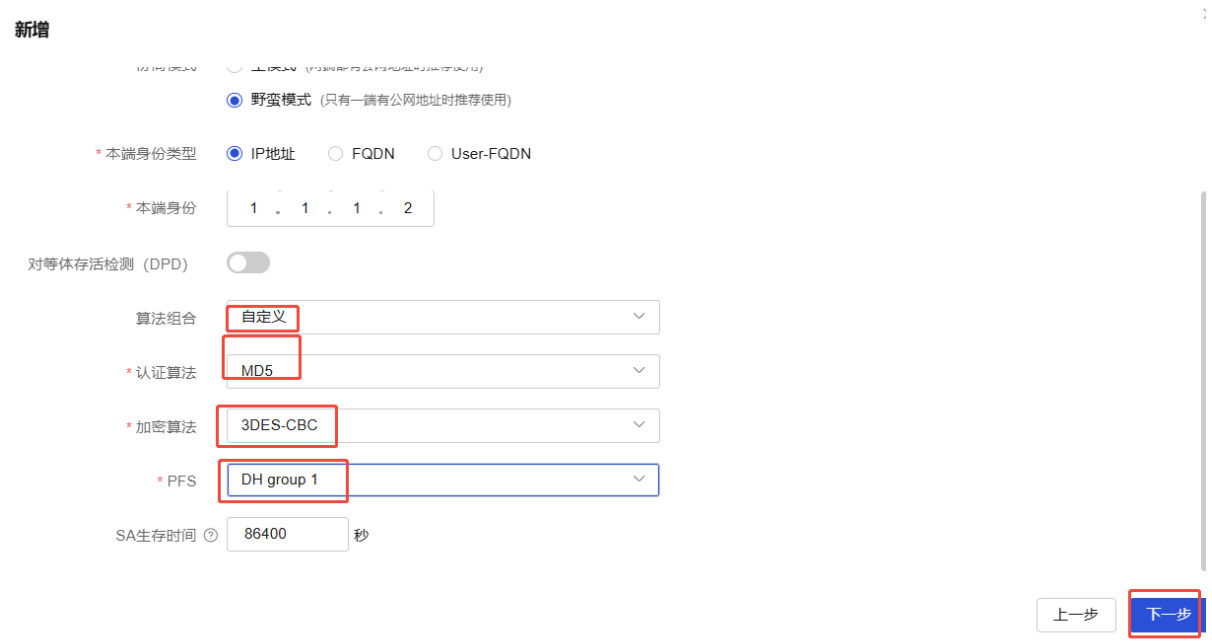
#正常配置内网口和外网口地址(此处省略，可以参考配置上网的案例)

#点击虚拟专网—ipsec—ipsec 策略—新增

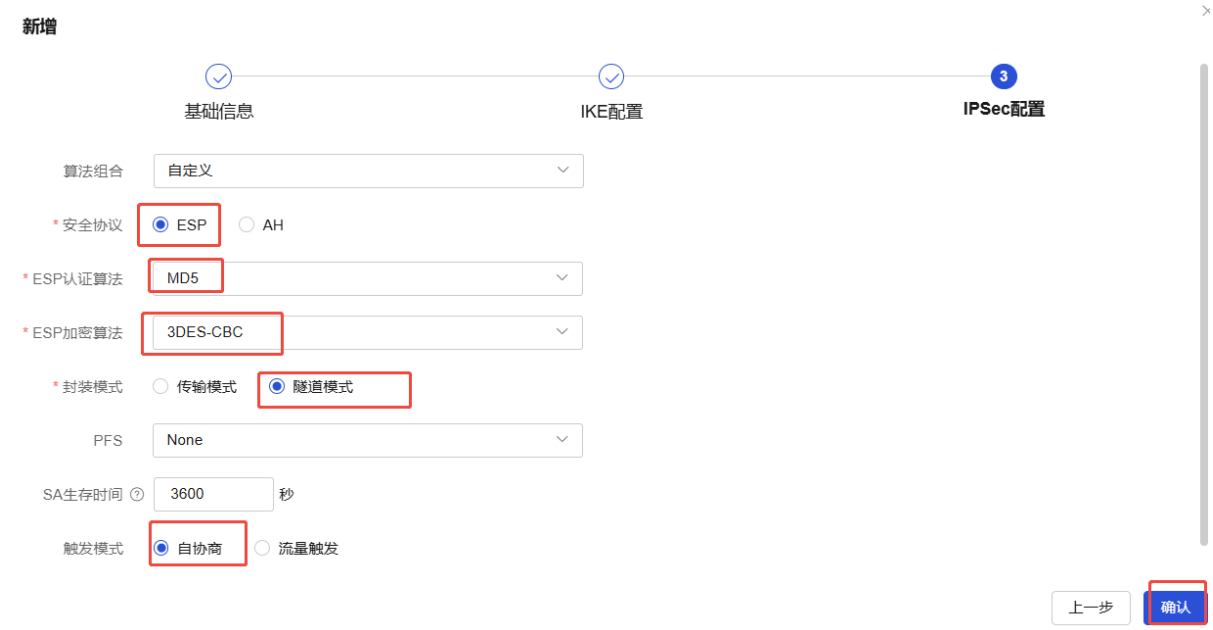
#配置策略名称为 test，接口选择外网口 wan1，组网方式选择中心节点，预共享密钥，配置完成后点击下一步



#配置 IKE，IKE 版本选择 V1，协商模式选择野蛮模式，两端身份类型都选择 IP 地址，算法组合选择自定义，配置加密算法为 3DES-CBC，认证算法为 MD5，PFS 选择 DH group1（两端的算法要保持一致），配置完成后点击下一步



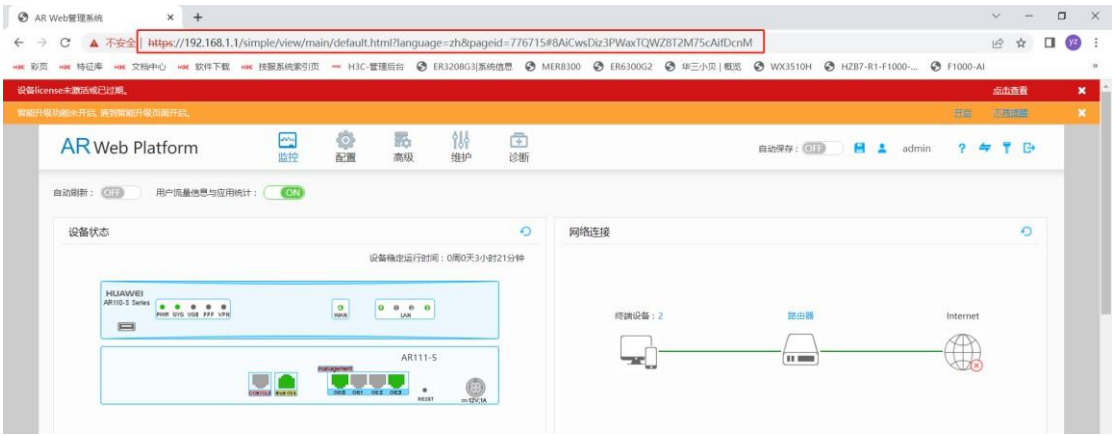
#配置 ipsec,算法组合自定义，安全协议选择 ESP，认证算法为 MD5，加密算法为 3DES-CBC，封装模式选择隧道模式，触发模式选择自协商，配置完成后点击确认



3.2 配置华为设备

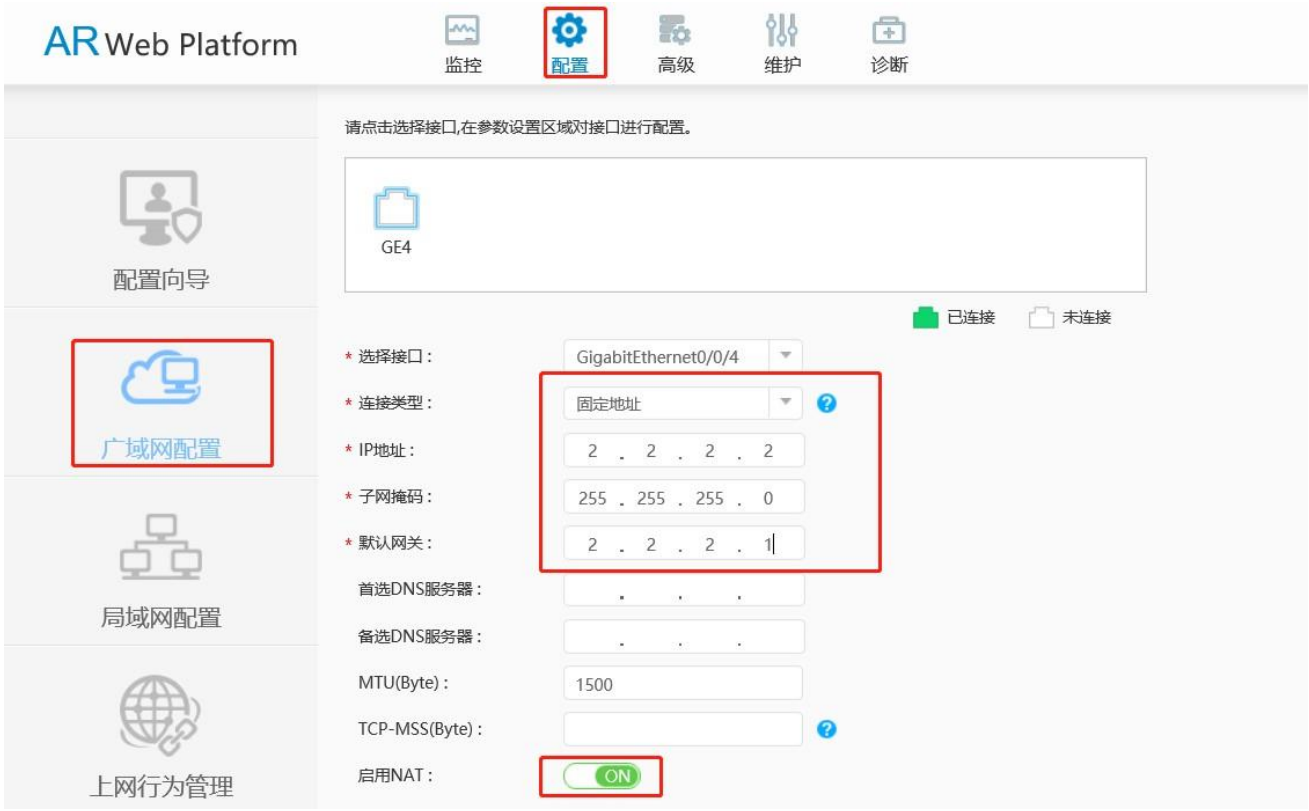
3. 2. 1 登录设备

电脑连接设备的 LAN 口，自动获取地址，默认登录地址为 192.168.1.1



3.2.2 配置外网

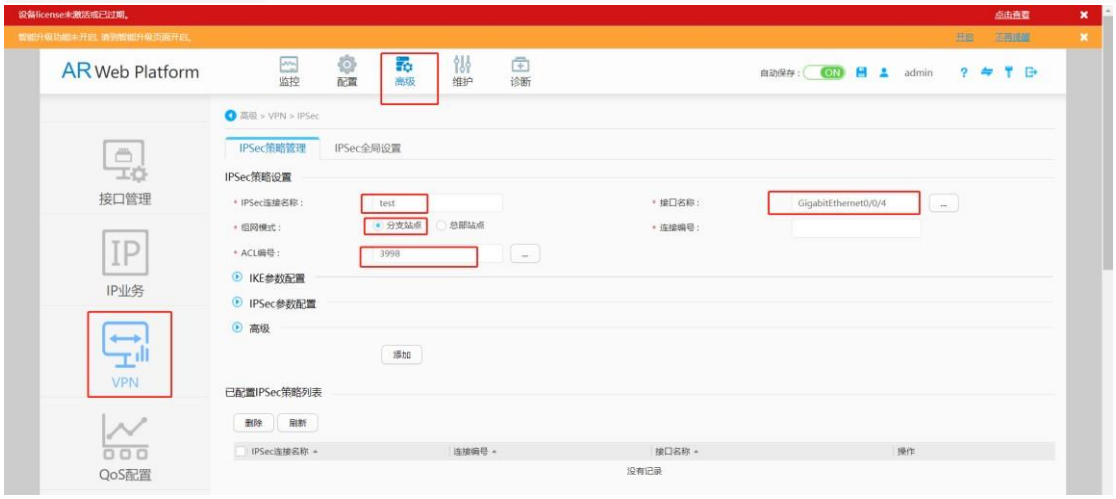
【配置】--【广域网配置】--固定外网口地址

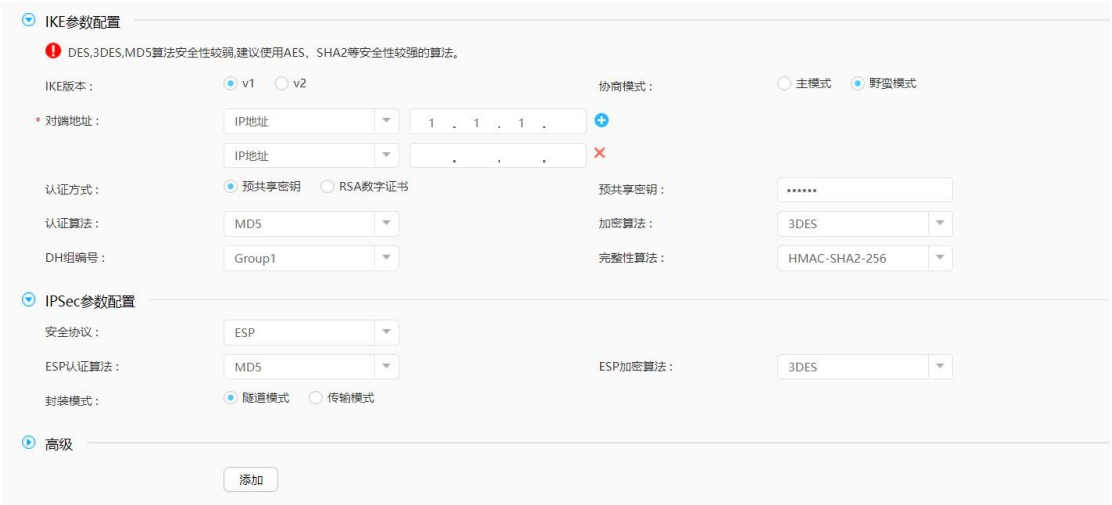


3.2.3 配置 IPSEC VPN

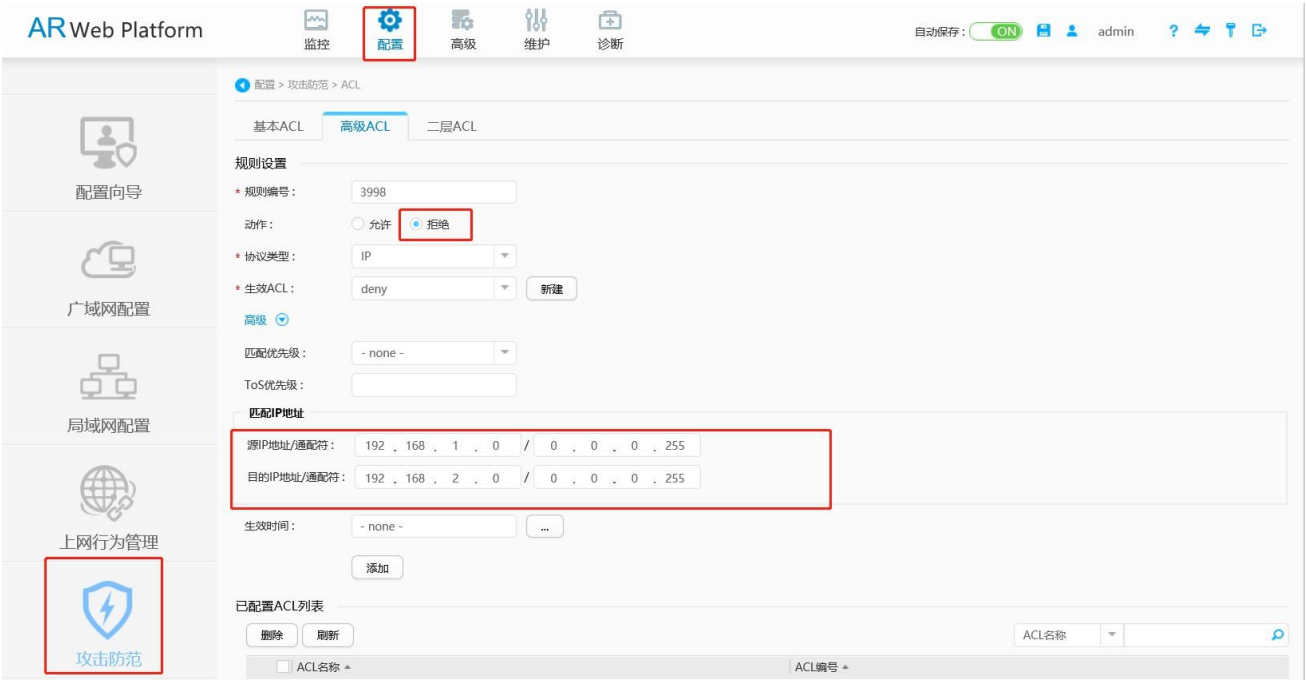
【高级】--【VPN】--【IPSEC 策略管理】先在 ACL 处创建 ACL 3999，然后在 IPSEC 里面调用


AR Web Platform
监控
配置
高级
维护
诊断
自动保存：ON
配置向导
广域网配置
局域网配置
上网行为管理
攻击防范
配置 > 攻击防范 > ACL
基本ACL
高级ACL
二层ACL
规则设置
* 规则编号：3999
动作：允许 拒绝
* 协议类型：IP
* 生效ACL：permit
新建
高级
匹配优先级：- none -
ToS优先级：
匹配IP地址
源IP地址/通配符：192 . 168 . 1 . 0 / 0 . 0 . 0 . 255
目的IP地址/通配符：192 . 168 . 2 . 0 / 0 . 0 . 0 . 255
生效时间：- none -
添加
已配置ACL列表
删除
刷新
ACL名称
ACL编号

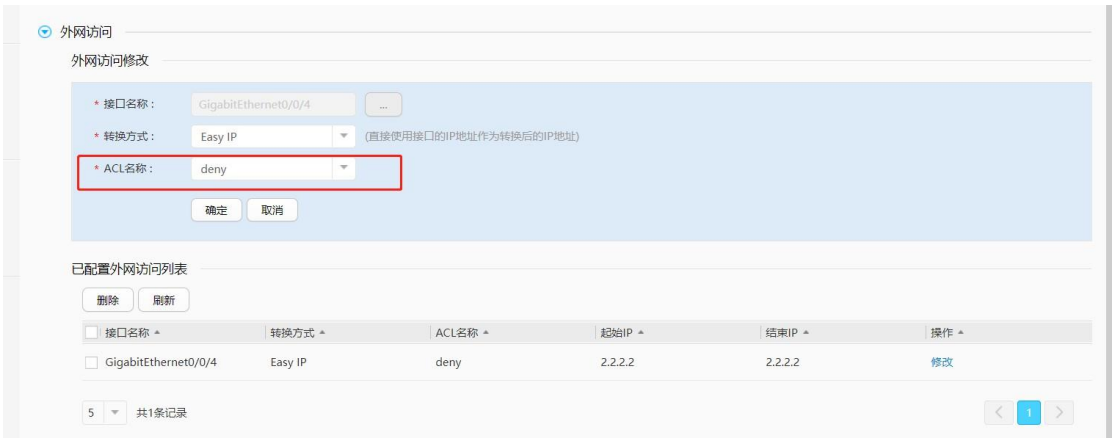

AR Web Platform
监控
配置
高级
维护
诊断
admin
接口管理
IP业务
VPN
QoS配置
IPSec策略管理
IPSec全局设置
IPSec策略设置
* IPSec连接名称：test
* 组网模式：分支站点 总部站点
* ACL编号：3998
* 接口名称：GigabitEthernet0/0/4
* 连接编号：
IKE参数配置
IPSec参数配置
高级
添加
已配置IPSec策略列表
删除
刷新
IPSec连接名称
连接编号
接口名称
操作
没有记录


IKE参数配置
DES,3DES,MD5算法安全性较弱,建议使用AES、SHA2等安全性较强的算法。
IKE版本：v1 v2
协商模式：主模式 野蛮模式
* 对端地址：IP地址 1 . 1 . 1 .
IP地址
认证方式：预共享密钥 RSA数字证书
预共享密钥：
认证算法：MD5
加密算法：3DES
DH组编号：Group1
完整性算法：HMAC-SHA2-256
IPSec参数配置
安全协议：ESP
ESP认证算法：MD5
ESP加密算法：3DES
封装模式：隧道模式 传输模式
高级
添加

【配置】--【攻击防范】--【ACL】，配置拒绝的 ACL



外网口拒绝 ACL



3.3 结果验证

华为侧 ping 测试：

```
C:\windows\system32\cmd.exe - ping 192.168.2.1 -t
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
```

3.4 保存配置

默认都是自动保存