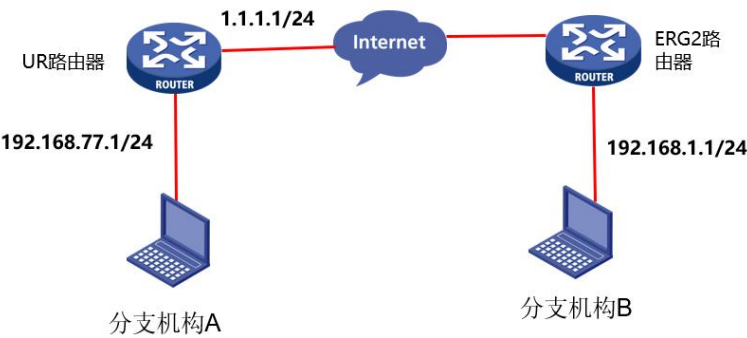


一 实验需求

两端路由为 UR 和 ERG2 路由器，在两者之间建立一个安全隧道，对客户分支机构 A 所在的子网（192.168.1.0/24）与客户分支机构 B 所在的子网（192.168.77.1/24）之间的数据流进行安全保护，实现两端子网终端通过 IPsec VPN 隧道进行互访。（本案例适用 UR 所有系列路由器）

二 组网图

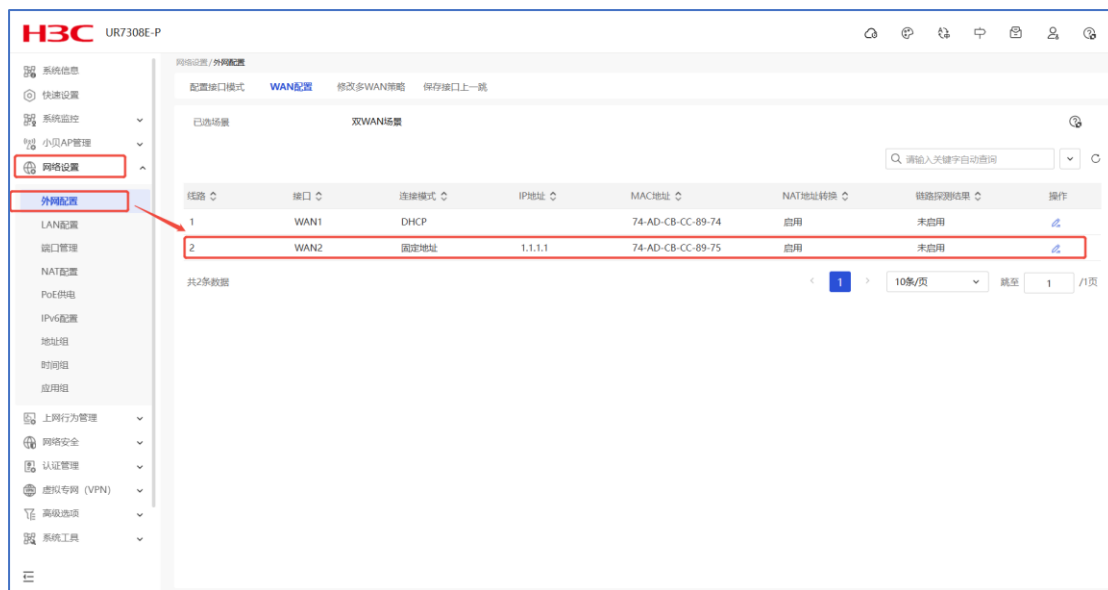


三 配置步骤

3.1 登录 UR 的 web 界面，配置外网

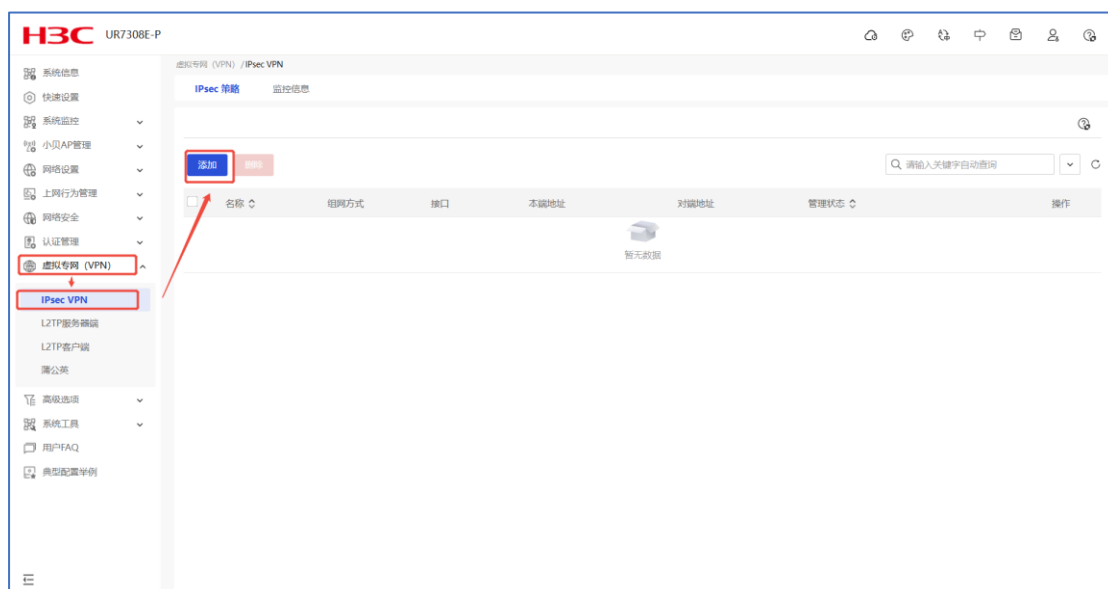
【网络设置】--【外网配置】--【WAN 配置】



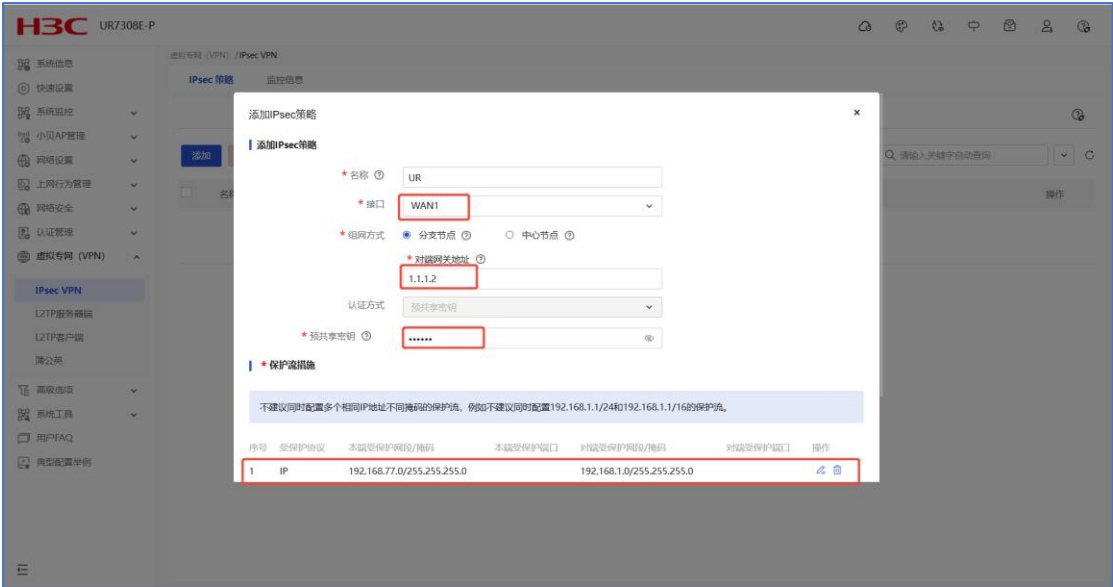


3.2 配置 ipsec

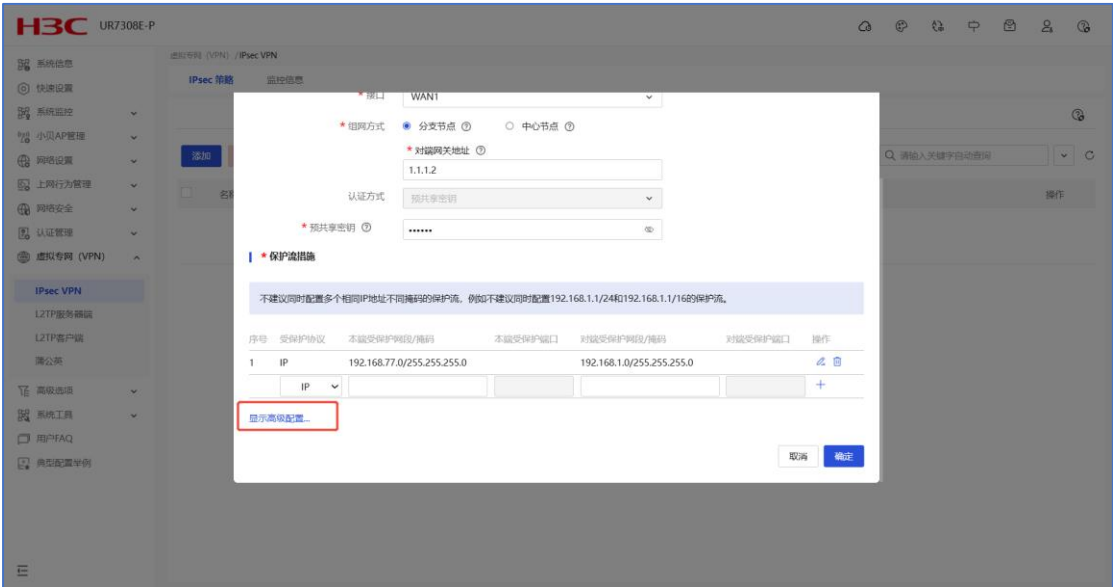
【虚拟专网】--【ipsec vpn】点击添加



选择 wan 口，配置对端网关地址，预共享密钥以及感兴趣流



点击显示高级配置



配置 IKE 参数，这里的算法组合可选择默认推荐也可根据实际情况自定义配置

高级配置

IKE配置

IPsec配置

IKE 版本
V1

协商模式
主模式

本端身份类型
IP地址
1.1.1.1
(例如: 1.1.1.1)

* 对端身份类型
IP地址
1.1.1.2
(例如: 1.1.1.1)

对等体存活检测 (DPD)
☐ 开启
☒ 关闭

算法组合
推荐

AES128-SHA1-GROUP1 (设备厂商默认)
AES128-SHA1-GROUP2 (Windows7 默认)

SA生存时间
86400
秒 (60-604800, 缺省值为86400)

配置 IPsec 参数，这里的算法组合可选择默认推荐也可根据实际情况自定义配置

H3C UR7308E-P

系统信息
快速设置
系统监控
小页AP管理
网络设置
上网行为管理
网络安全
虚拟专网 (VPN)
IPsec VPN
L2TP服务端
L2TP客户端
蒲公英
高级选项
系统工具
用户FAQ
典型配置示例

虚拟专网 (VPN) / IPsec VPN
IPsec 策略
策略信息

高级配置

IKE配置

IPsec配置

算法组合
推荐

ESP-SHA1-3DES (推荐)
ESP-SHA1-AES128 (Windows7 默认)
ESP-SHA1-AES256 (推荐)

* 封装模式
☐ 传输模式
☒ 隧道模式

PFS
禁止

基于时间的SA生存时间
3600
秒 (600-604800, 缺省值为3600)

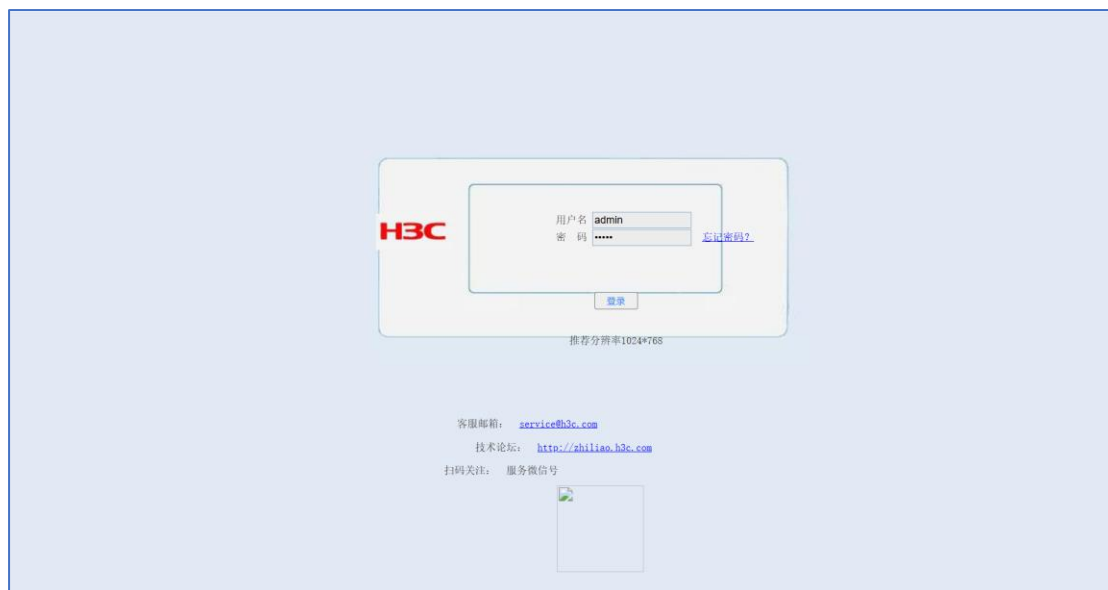
基于流量的生存时间
1843200
千字节 (2560-4294967295, 缺省值)

触发模式
自动协商模式

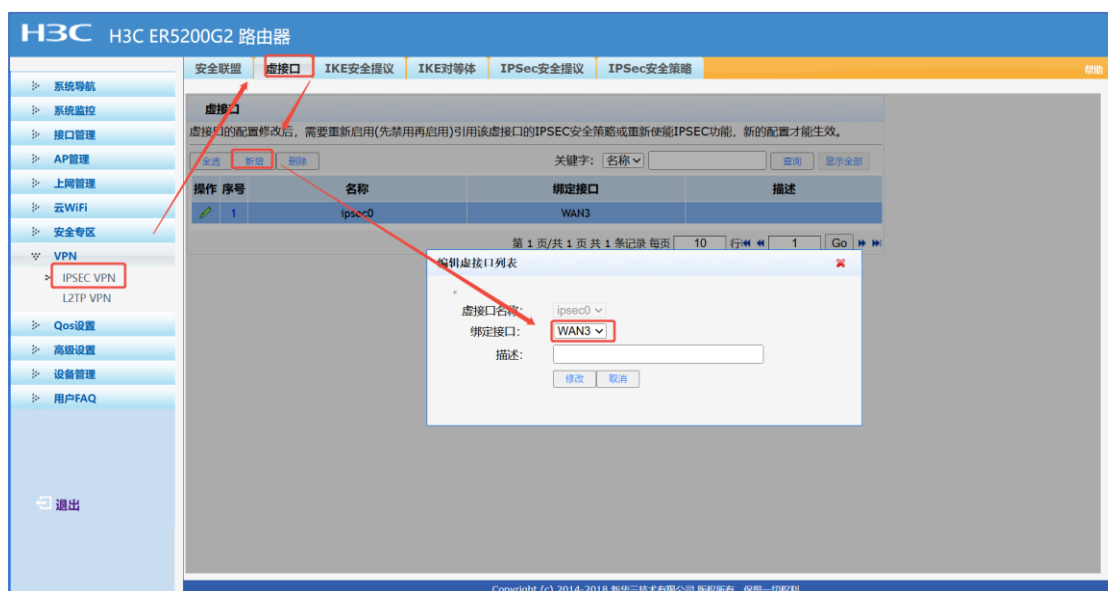
返回基本设置

3.3 配置 ERG2 端

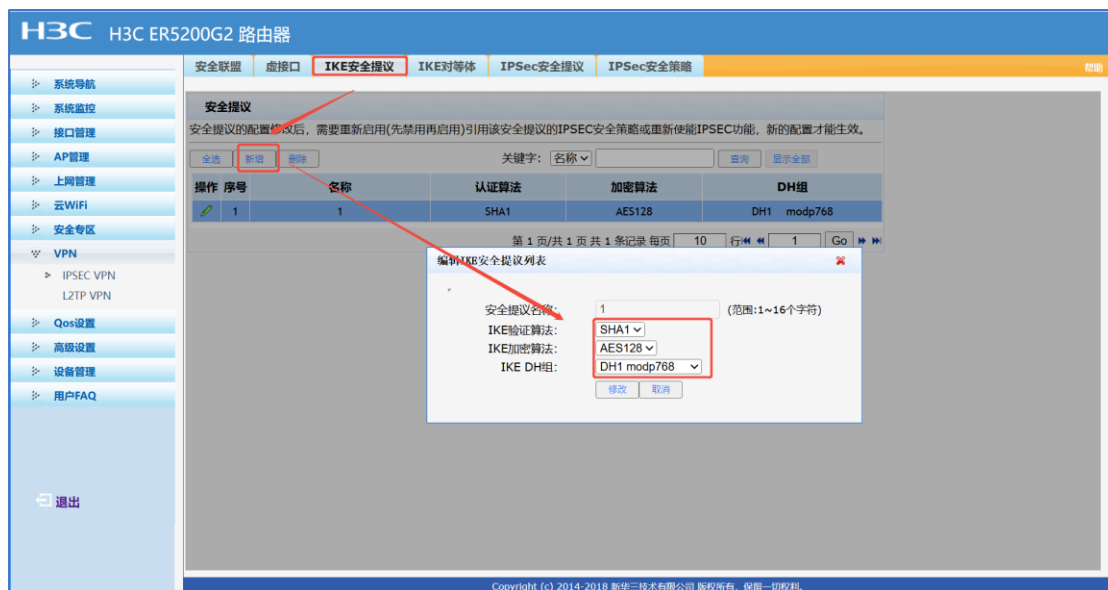
进入设备 web 界面



单击【VPN】--【VPN 设置】--【虚接口】，点击【新增】，绑定对应的 WAN 口



配置 IKE 安全提议，单击【VPN】--【VPN 设置】--【IKE 安全提议】，点击【新增】，配置 IKE 安全提议的各个参数：安全提议名称、IKE 验证算法、IKE 加密算法、IKE DH 组，如下图配置。



配置 IKE 对等体



配置 IPSec 安全提议



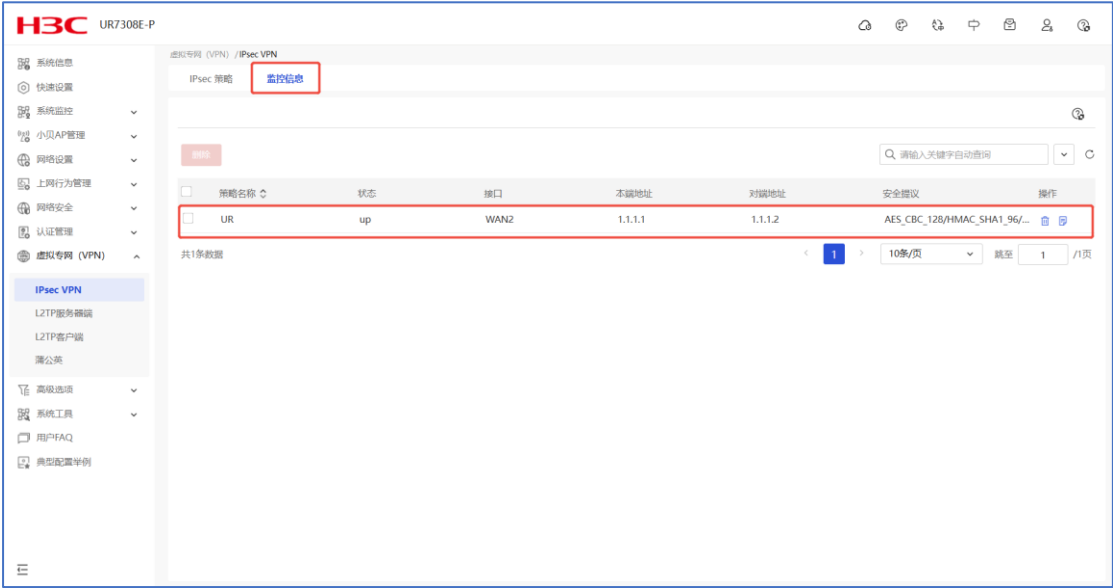
配置 IPSEC 安全策略，添加感兴趣流



注意: 修改了 IPSEC 相关参数, 需要将启用 IPsec 功能勾去掉应用再重新勾上应用使能, 否则 IPsecVPN 无法起来。

四 实验结果

查看隧道建立成功



两边内网也可互通

