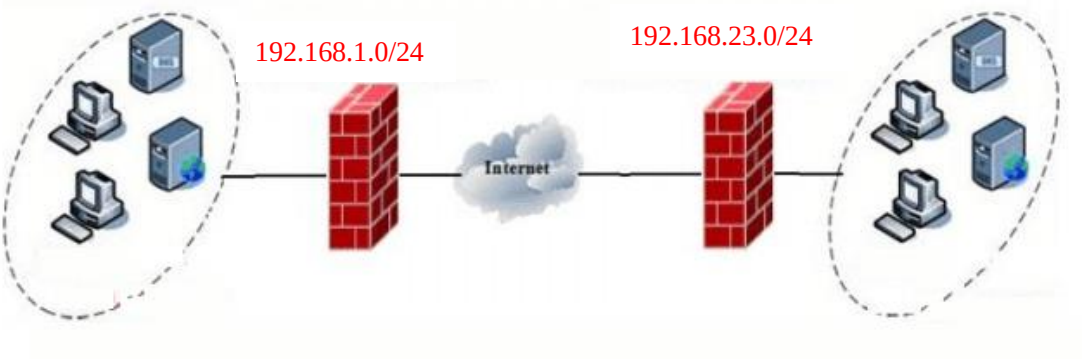
用户场景

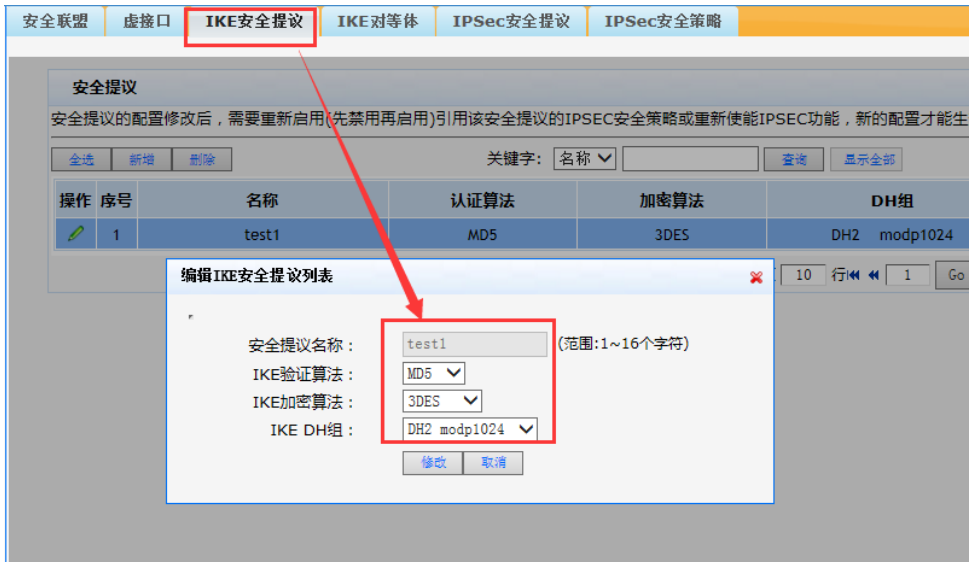
企业通过 H3C 和启博设备构建 VPN 通道，保证总部和分支机构的安全通信，均作为出口网关。

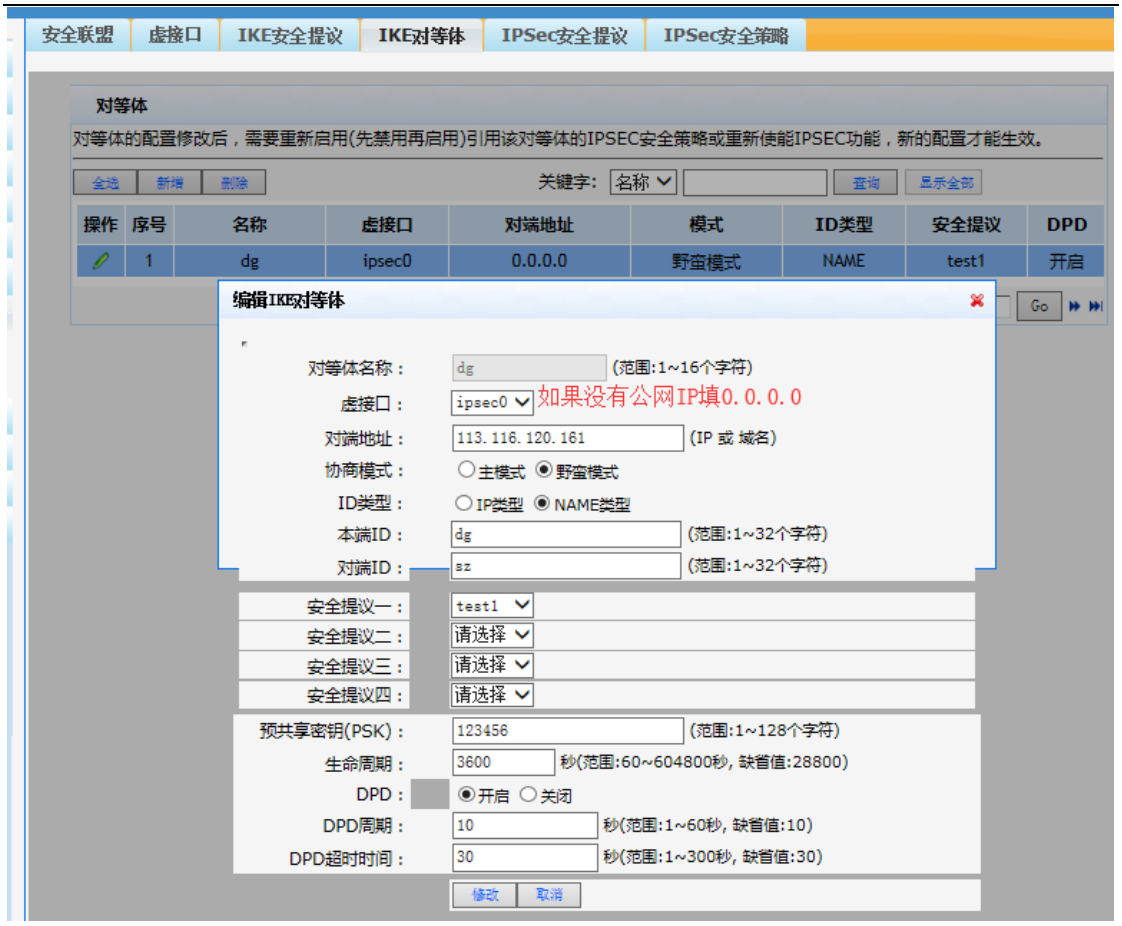
中心用 H3C 设备，网段 92.168.1.0/24

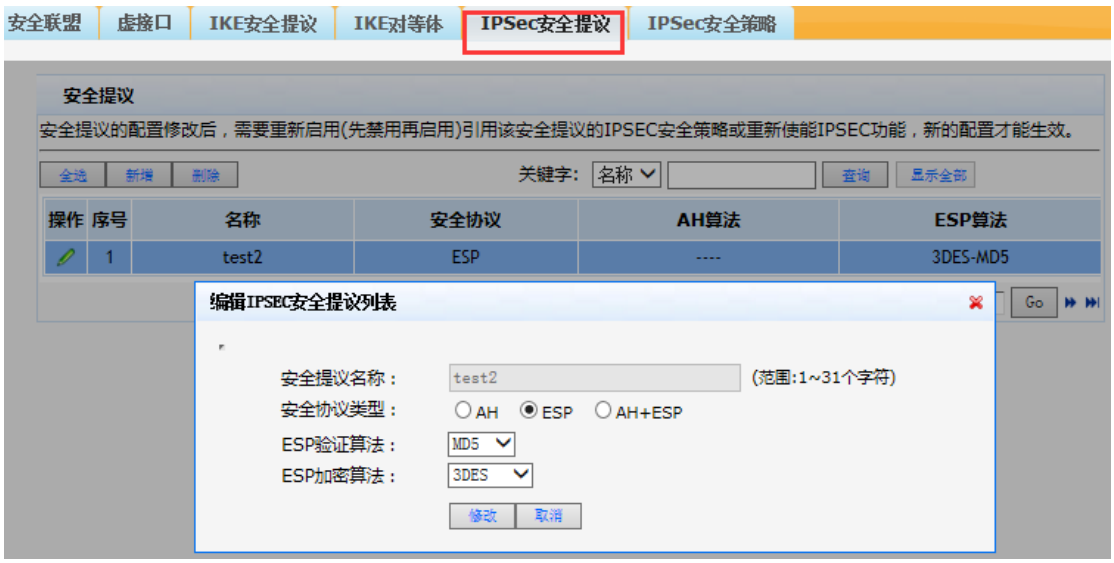
分支用启博设备，网段 192.168.23.0/24

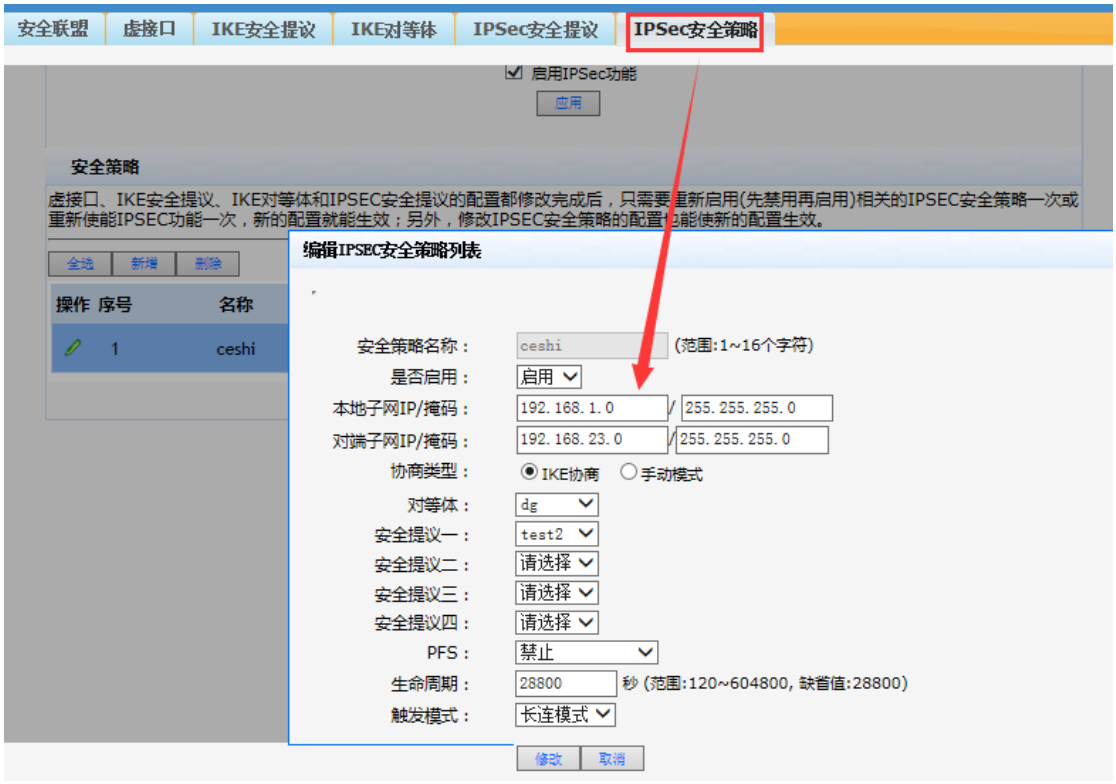


H3C 作为网关，主要参数设置如下




安全联盟
虚接口
IKE安全提议
IKE对等体
IPSec安全提议
IPSec安全策略
对等体
对等体的配置修改后，需要重新启用(先禁用再启用)引用该对等体的IPSEC安全策略或重新使能IPSEC功能，新的配置才能生效。
全选
新增
删除
关键字:
名称
查询
显示全部
操作 序号 名称 虚接口 对端地址 模式 ID类型 安全提议 DPD
1 dg ipsec0 0.0.0.0 野蛮模式 NAME test1 开启
Go
编辑IKE对等体
对等体名称：
dg
(范围:1~16个字符)
虚接口：
ipsec0
如果没有公网IP填0.0.0.0
对端地址：
113.116.120.161
(IP 或 域名)
协商模式：
主模式
野蛮模式
ID类型：
IP类型
NAME类型
本端ID：
dg
(范围:1~32个字符)
对端ID：
sz
(范围:1~32个字符)
安全提议一：
test1
安全提议二：
请选择
安全提议三：
请选择
安全提议四：
请选择
预共享密钥(PSK)：
123456
(范围:1~128个字符)
生命周期：
3600
秒(范围:60~604800秒，缺省值:28800)
DPD：
开启
关闭
DPD周期：
10
秒(范围:1~60秒，缺省值:10)
DPD超时时间：
30
秒(范围:1~300秒，缺省值:30)
修改
取消


安全联盟
虚接口
IKE安全提议
IKE对等体
IPSec安全提议
IPSec安全策略
安全提议
安全提议的配置修改后，需要重新启用(先禁用再启用)引用该安全提议的IPSEC安全策略或重新使能IPSEC功能，新的配置才能生效。
全选
新增
删除
关键字:
名称
查询
显示全部
操作 序号 名称 安全协议 AH算法 ESP算法
1 test2 ESP ---- 3DES-MD5
Go
编辑IPSEC安全提议列表
安全提议名称：
test2
(范围:1~31个字符)
安全协议类型：
AH
ESP
AH+ESP
ESP验证算法：
MD5
ESP加密算法：
3DES
修改
取消



组网成功之后，可以看到两边的信息

添加静态路由

MR-1300 作为网关上网，的所有配置参数（当二级路由和透明模式也可以的）

组网成功之后会显示建立