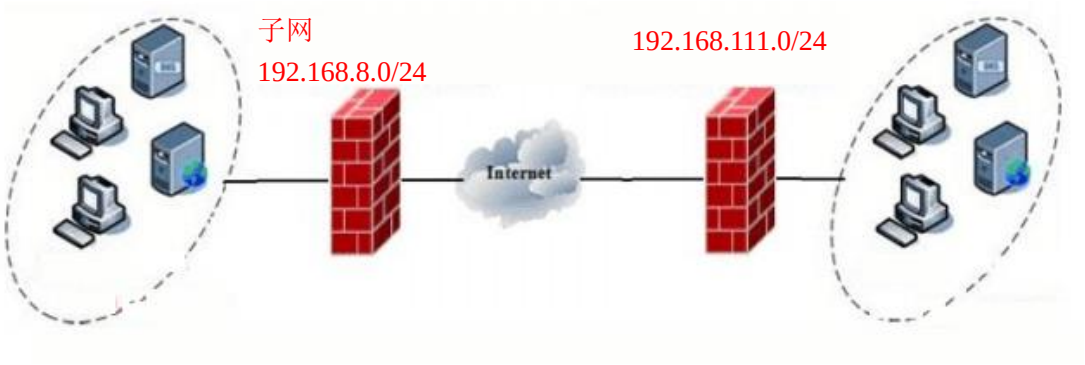
用户场景

企业通过 SonicWALL 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。

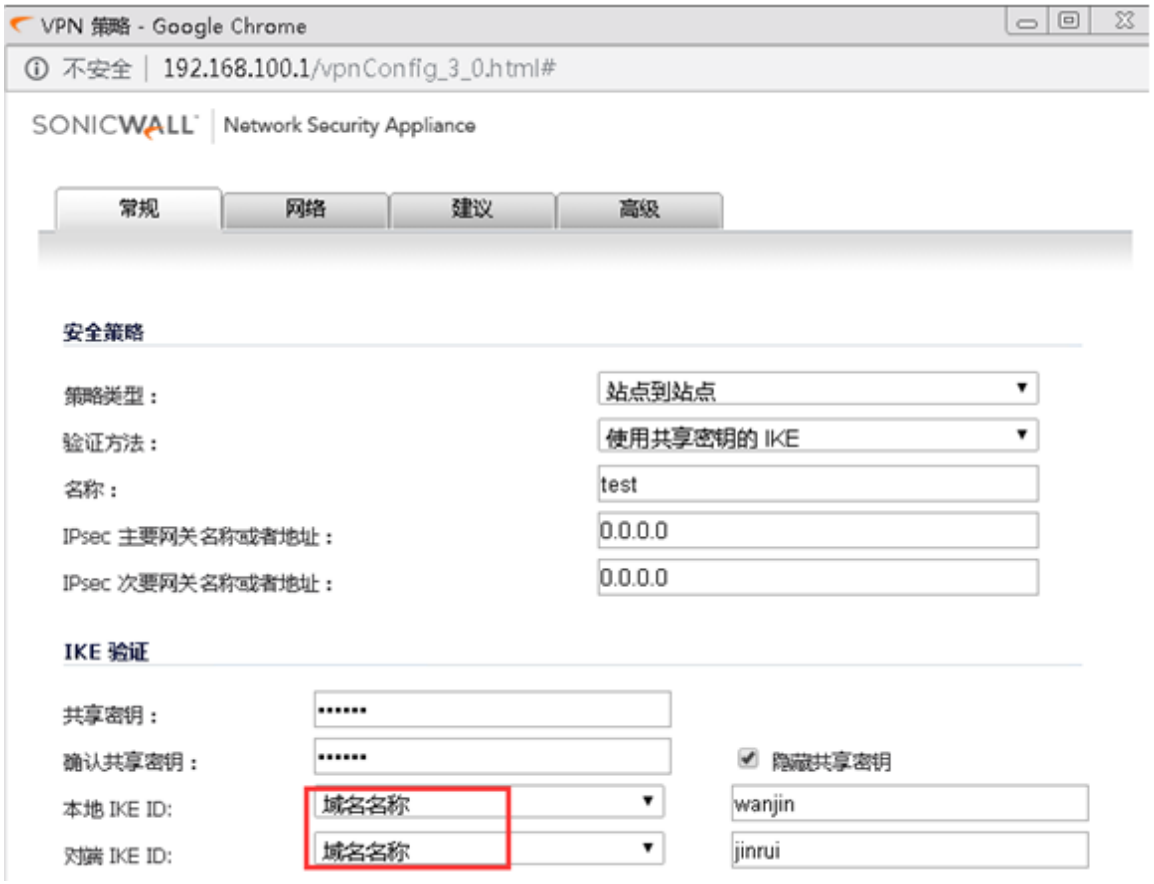
中心用网康设备，子网段 192.168.8.0/24

分支用启博设备，网段 192.168.111.0/24



启博设备配置

SonicWALL 设备配置


VPN 策略 - Google Chrome
不安全 | 192.168.100.1/vpnConfig_3_0.html#
SONICWALL Network Security Appliance
常规
网络
建议
高级
安全策略
策略类型：
站点到站点
验证方法：
使用共享密钥的 IKE
名称：
test
IPsec 主要网关名称或者地址：
0.0.0.0
IPsec 次要网关名称或者地址：
0.0.0.0
IKE 验证
共享密钥：
确认共享密钥：
隐藏共享密钥
本地 IKE ID:
域名名称
wanjin
对端 IKE ID:
域名名称
jinrui


SONICWALL Network Security Appliance
常规
网络
建议
高级
本地网络
从列表中选择本地网络
192.168.8.0
本地网络通过这个 VPN 隧道利用 DHCP 获得 IP 地址
任何地址
远程网络
使用该 VPN 隧道作为默认路由用于所有的网络流量
目标网络通过这个 VPN 隧道利用 DHCP 获得 IP 地址
从列表中选择目标网络
192.168.111.0


常规
网络
建议
高级
IKE (阶段 1) 建议
交换：
挑战模式
DH 群组：
群组 2
加密：
3DES
验证：
MD5
生存期（秒）：
28800
Ipsec (阶段 2) 建议
协议：
ESP
加密：
3DES
验证：
MD5
启用完全转发保密
生存期（秒）：
28800