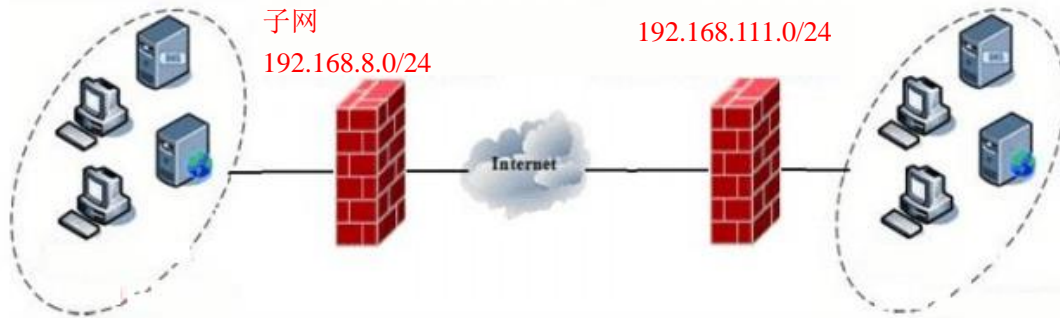


## 用户场景

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

网络 转发规则 第三方互联 VPN 路由功能 EPN 无线 上网行为管理 防火墙 系统管理 状态

添加IPSEC连接

类型	Net-to-Net虚拟专用网
IPSEC功能	<input checked="" type="radio"/> 客户端 <input type="radio"/> 服务端
名称	towanjin
启用	<input checked="" type="checkbox"/>
本端WAN接口	默认
本端子网	192.168.111.0/24
本端标志符	@jinrui
对端地址	
对端子网	192.168.8.0/24
对端标志符	@wanjin
启用DPD检测	<input checked="" type="checkbox"/>
时间间隔	60 (秒)
超时时间	60 (秒)
操作	restart
第一阶段	加密 3DES 完整性 MD5 DH小组 组2(1024) 生命周期 1 小时
第二阶段	加密 3DES 完整性 MD5 生命周期 8 小时
模式	野蛮模式
会话密钥向前加密(PFS)	<input type="checkbox"/>
使用预共享密钥:	123456

保存 取消

## SonicWALL 设备配置

启博官网: <http://www.vpnsoft.net>

联系电话: 0755-82195178

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：

验证方法：

名称：

IPsec 主要网关名称或者地址：

IPsec 次要网关名称或者地址：

### IKE 验证

共享密钥：

确认共享密钥：

隐藏共享密钥

本地 IKE ID：

对端 IKE ID：

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

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

常规

网络

建议

高级

### IKE (阶段 1) 建议

交换：	<input type="text" value="挑战模式"/>
DH 群组：	<input type="text" value="群组 2"/>
加密：	<input type="text" value="3DES"/>
验证：	<input type="text" value="MD5"/>
生存期 (秒)：	<input type="text" value="28800"/>

### Ipssec (阶段 2) 建议

协议：	<input type="text" value="ESP"/>
加密：	<input type="text" value="3DES"/>
验证：	<input type="text" value="MD5"/>
<input type="checkbox"/> 启用完全转发保密	
生存期 (秒)：	<input type="text" value="28800"/>