# ACG1000系列与ER路由器对接IPSEC VPN配置举例（适用于两端固定地址组网）

IPSec VPN　叶佳豪　2019-09-19 发表

## 组网及说明

**1 配置需求或说明**

**1.1 适用的产品系列**

本案例适用于软件平台为ACG1000系列应用控制网关：ACG10X0、ACG1000-AKXXX等。

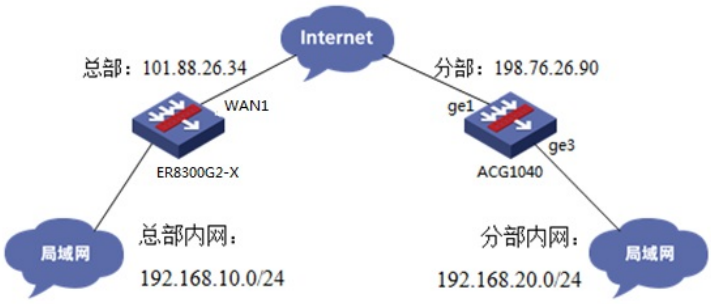
*注：本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。*

**1.2 配置需求及实现的效果**

因公司业务拓展需要将处于两地的公司网络通过IPSEC VPN连通，使总部和分部网络可以相互访问。IP地址及接口规划如下表所示：

| 公司名称 | 外网接口 | 公网地址/掩码 | 公网网关 | 内网接口 | 内网地址/掩码 |
|---|---|---|---|---|---|
| 总部（ER8300G2-X） | WAN1 | 101.88.26.34/30 | 101.88.26.33 | 1/0/4 | 192.168.10.0/24 |
| 分部（ACG1040） | ge1 | 198.76.26.90/30 | 198.76.26.89 | ge3 | 192.168.20.0/24 |

**2 组网图**




## 配置步骤

**3 配置步骤**

**3.1 两端配置上网配置**

本文档重点给出两台设备IPSEC VPN配置步骤，上网配置略。

**3.2 总部侧ER8300G2-X IPSEC VPN策略配置**

#在“VPN”>“IPSEC VPN”>“虚接口”中点击新增按钮，在新增虚接口中，虚接口名称设置为“ipsec0”，绑定的接口为WAN1。


#下一步“VPN”>“IPSEC VPN”>“IKE安全提议”中点击新增按钮，安全提议名称设置为“center”，IKE验证算法、IKE加密算法、IKE DH组参数一般使用系统默认即可。


#下一步“VPN”>“IPSEC VPN”>“IKE对等体”中点击新增按钮。


#在弹出的设置菜单中，对等体名称设置为“center”、虚接口选择为“ipsec0”、对端地址为“198.76.26.90”、协商模式选择为“主模式”、安全提议选择上一步中创建的“center”、预共享秘钥设置为“123456”，设置完成后点击确定完成IKE对等体设置。

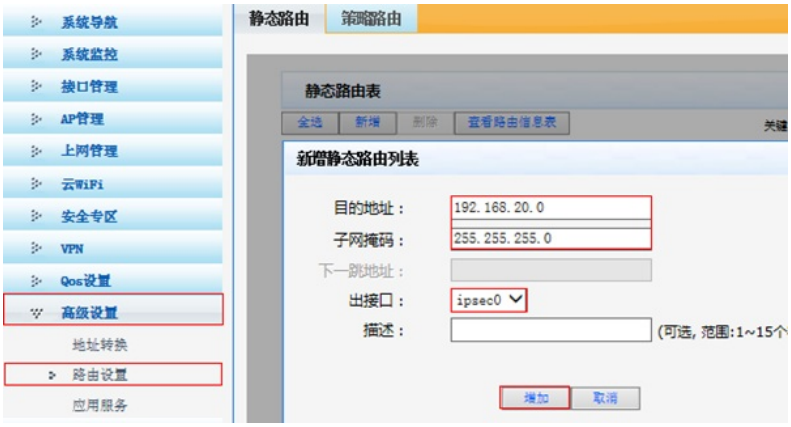

#下一步“VPN”>“IPSEC VPN”>“IPSEC安全提议”中点击新增按钮，安全提议名称设置为“center”，ESP验证算法、ESP加密算法参数一般使用系统默认即可。


#下一步“VPN”>“IPSEC VPN”>“IPSEC安全策略”中点击新增按钮。


#在弹出的设置菜单中，安全策略名称设置为“center”、本地子网IP/掩码为“192.168.10.0/24”、 对端子网IP/掩码为“192.168.20.0/24”、对等体和安全策略选择之前创建的“center” ， 设置完成后点击新增。


#完成策略配置后开启IPSEC策略后点击应用按钮。


#下一步在“高级配置”>“路由配置”>“静态路由”中点击新增按钮，目的地址填写对端ACG内网网段地址、出接口设置为ipsec0，选择完成后点击增加完成配置。




### 3.3 分部侧IPSEC VPN策略配置

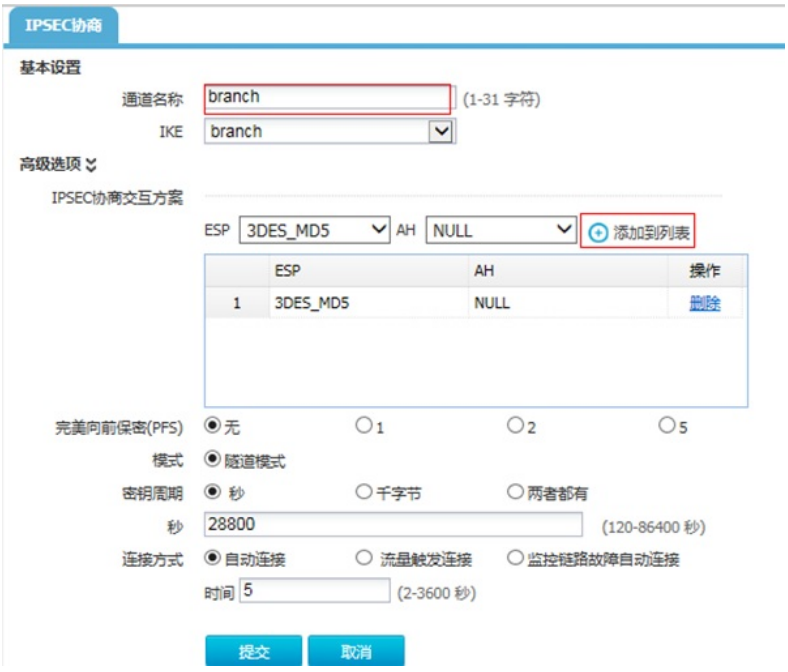
#在“VPN” >“IPsec-VPN”>“IPsec第三方对接” >“IPsec配置”中新建IKE对等体。


#基本设置中网关名称设置为“branch”、对端网关地址为101.88.26.34、模式设置为主模式、预共享秘

钥与ER8300设置一致为“123456”、IKE协商交互方案加密算法为3DES，认证算法为MD5，点击添加到列表、DH组选择“2”后点击提交完成配置。

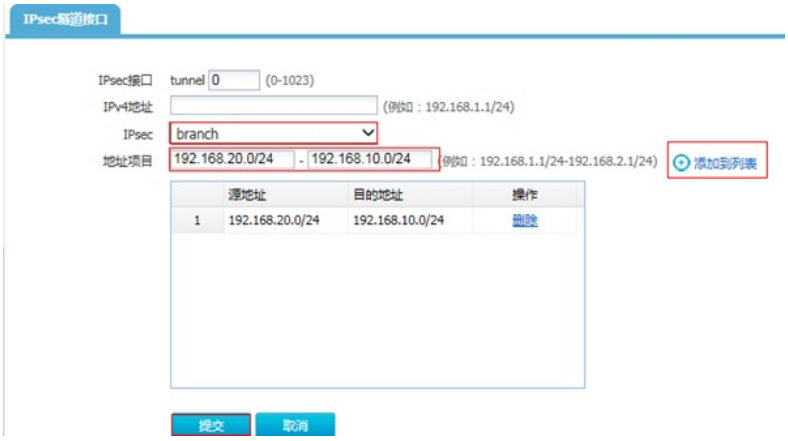

#新建IPsec安全提议。


#设置通道名称为“branch”，IKE对等体调用“branch”，ESP加密和认证算法设置为3DES_MD5H后点击添加到列表，设置完成后点击提交按钮。




#在“VPN” >“IPsec-VPN”>“IPsec第三方对接” >“IPsec隧道接口”中点击新建。


#IPsec选择之前创建的“branch”，地址选项中添加本地子网到对端子网的规则后点击添加到列表，注意：Tunnel口的IPV4地址不需要填写。



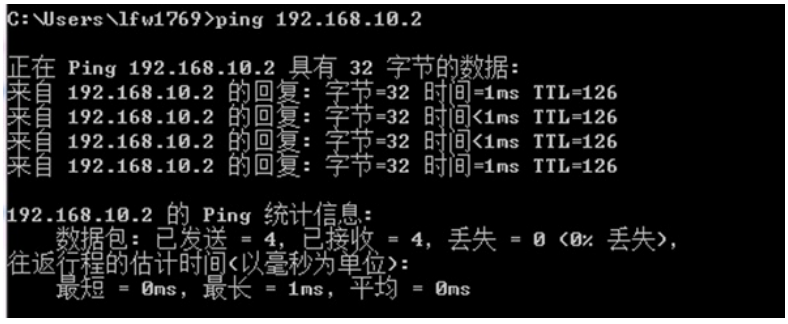

#在 “网络配置” >“路由”>“静态路由”中填写去往对端内网的路由，出接口为tunnel0接口。


### 3.4 配置保存

#在设备管理界面右上角点击配置保存，保存当前配置。


### 3.5 结果测试

#分支侧电脑可以与总部侧电脑正常通信，下图为Ping测试结果。

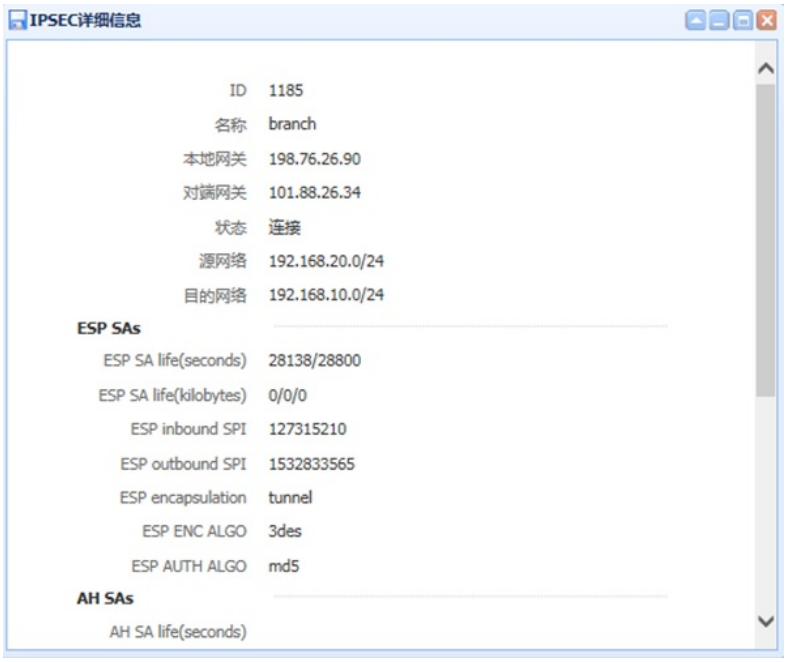



查看总部侧IPSEC安全联盟情况：


#分部侧设备查看IPSEC连接状态：

IKE连接情况：

IPSEC连接情况：




### 3.6 常见问题

#### 3.6.1 当使用ER2100设备配置IPSEC VPN时没有配置静态路由的位置怎么处理?

ER2100定位为分支设备，因此设备不支持填写静态路由。使用此设备进行IPSEC VPN配置时无需添加到ipsec接口的静态路由就可以和对端建立IPSEC隧道。

#### 3.6.2 IPSEC隧道中的Tunnel接口地址是做什么使用的?

Tunnel接口地址是为GRE OVER IPSEC VPN隧道配置GRE两端地址准备的，只做IPSEC VPN此地址不需要添加。

#### 3.6.3 ER路由器与ACG设备是否可以通过野蛮模式建立IPSEC VPN?

实际测试不支持。

配置关键点