

知 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。

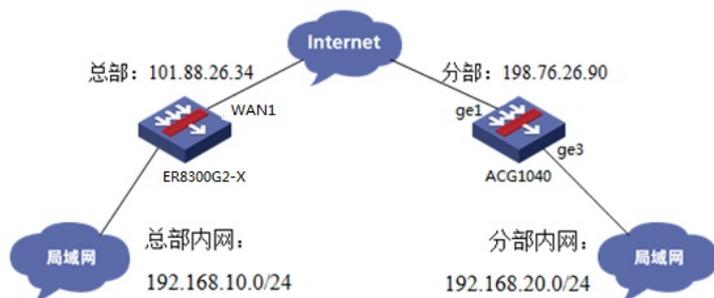
注：本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。

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”、预共享密钥设置为“123456”，设置完成后点击确定完成IKE对等体设置。



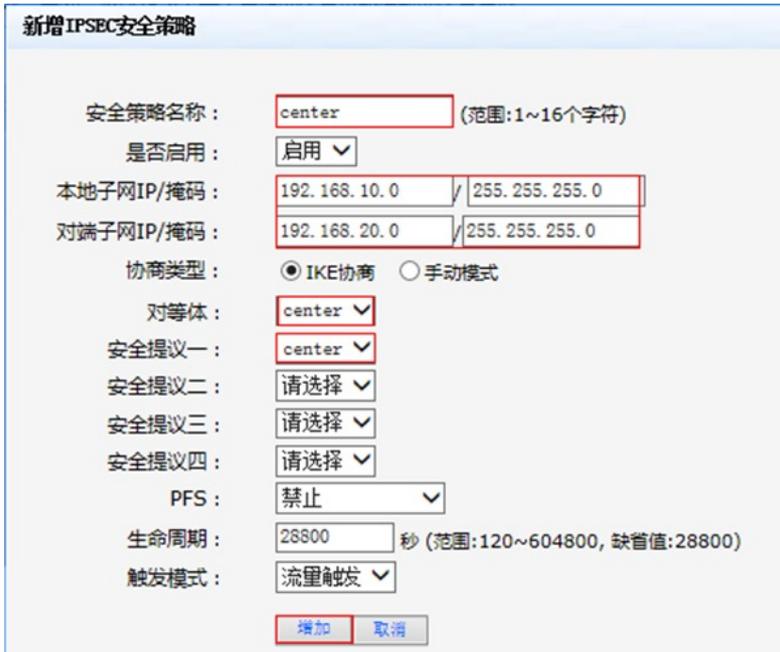
#下一步“VPN”>“IPSEC VPN”>“IPSEC安全提议”中点击新增按钮，安全提议名称设置为“center”，ESP验证算法、ESP加密算法参数一般使用系统默认即可。



#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。

基本设置

网关名称 (1-31 字符)

本地源接口 本地源IP地址 无

对端网关

IP地址

模式 野蛮模式 主模式(ID保护)

认证方式

预共享密钥 (6-39 字符)

高级选项

IKE协商交互方案

加密算法 认证

加密算法	认证	操作
1 3DES	MD5	<input type="button" value="删除"/>

DH组 1 2 5

密钥周期 (120-86400 秒)

NAT穿越连接频率 (10-900 秒)

本地ID 无 FQDN U-FQDN IP地址

对端ID 无 FQDN U-FQDN IP地址

#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。

IPSEC协商

基本设置

通道名称 (1-31 字符)

IKE

高级选项

IPSEC协商交互方案

ESP AH

ESP	AH	操作
1 3DES_MD5	NULL	<input type="button" value="删除"/>

完美向前保密(PFS) 无 1 2 5

模式 隧道模式

密钥周期 秒 千字节 两者都有

秒 (120-86400 秒)

连接方式 自动连接 流量触发连接 监控链路故障自动连接

时间 (2-3600 秒)

#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。

IPsec隧道接口

IPsec接口: tunnel 0 (0-1023)

IPv4地址: (例如: 192.168.1.1/24)

IPsec: branch

地址项目: 192.168.20.0/24 - 192.168.10.0/24 (例如: 192.168.1.1/24-192.168.2.1/24) 添加到列表

源地址	目的地址	操作
1 192.168.20.0/24	192.168.10.0/24	删除

提交 取消

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

静态路由

目的地址: 192.168.10.0

子网掩码: 255.255.255.0

下一跳/出口: 下一跳 出口

出口: tunnel0 (tunnel、pppoe接口，黑洞路由)

权重: 1 (1-255)

距离: 1 (1-255)

地址探测: -

提交 取消

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。

```
C:\Users\lfw1769>ping 192.168.10.2

正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126

192.168.10.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

查看总部侧IPSEC安全联盟情况:

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		
安全联盟SA							
通过安全联盟SA，IPSec能够对不同的数据流提供不同级别的安全保护。在这里可以查询到相应隧道当前状态，了解隧道建立的各个参数。							
刷新							
名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
center	in	198.76.26.90 =>101.88.26.34	----	----	0x5b5d2f1d	3DES_3DES	192.168.20.0/24 =>192.168.10.0/24
center	out	101.88.26.34 =>198.76.26.90	----	----	0x796ad0a	3DES_3DES	192.168.10.0/24 =>192.168.20.0/24

#分部侧设备查看IPSEC连接状态:

IKE连接情况:

名称	对端网关	本地网关	状态	过期时间/s
1 <input type="checkbox"/> branch	101.88.26.34	198.76.26.90	连接	85788

IPSEC连接情况:



Item	Value
ID	1185
名称	branch
本地网关	198.76.26.90
对端网关	101.88.26.34
状态	连接
源网络	192.168.20.0/24
目的网络	192.168.10.0/24
ESP SAs	
ESP SA life(seconds)	28138/28800
ESP SA life(kilobytes)	0/0/0
ESP inbound SPI	127315210
ESP outbound SPI	1532833565
ESP encapsulation	tunnel
ESP ENC ALGO	3des
ESP AUTH ALGO	md5
AH SAs	
AH SA life(seconds)	

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