ERG2—MER路由器 IPSEC VPN野蛮模式配置

目录

ERG2—MER路由器 IPSEC VPN野蛮模式配置
1 配置需求或说明
1.1适用产品系列
1.2配置需求及实现的效果
2 组网图
3 配置步骤

3.1配置ERG2路由器
3.2配置MER路由器
3.3保存配置
3.4保存配置

1 配置需求或说明

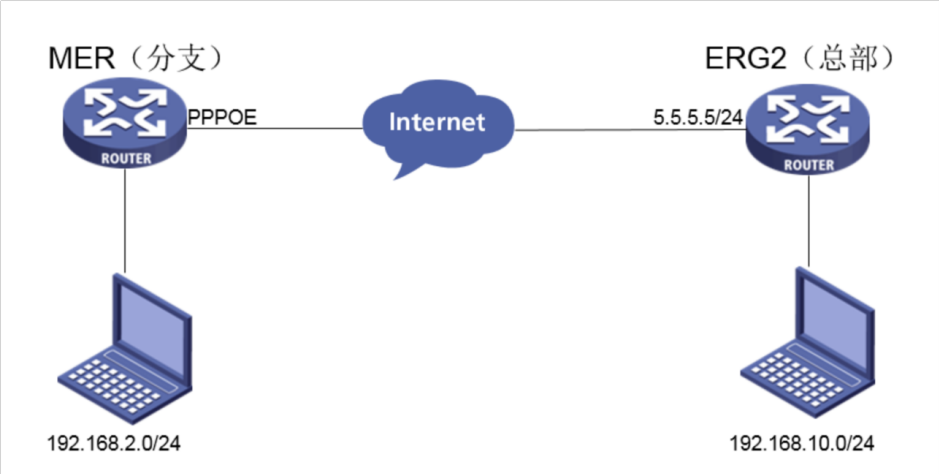
1.1适用产品系列

本案例适用于ERG2 产品系列路由器：ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等，MER系列路由器，如：MER3220、MER5200、MER8300。

1.2配置需求及实现的效果

在总部和分部之间分别建立安全隧道，对客户总部PC1所在的子网（192.168.10.0）与客户分支机构PC2所在的子网（192.168.2.0）之间的数据流进行安全保护。安全协议采用ESP协议，加密算法采用3DES，认证算法采用MD5，ERG2作为总部，MER作为分部。

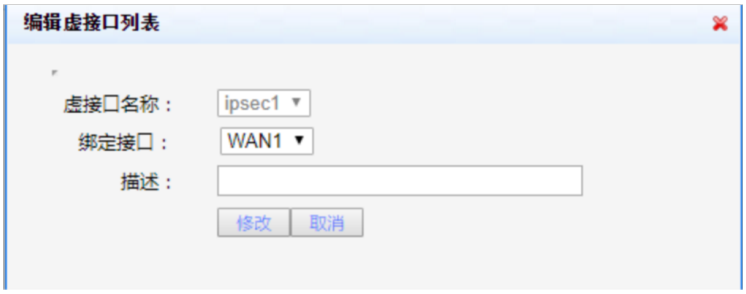
2 组网图



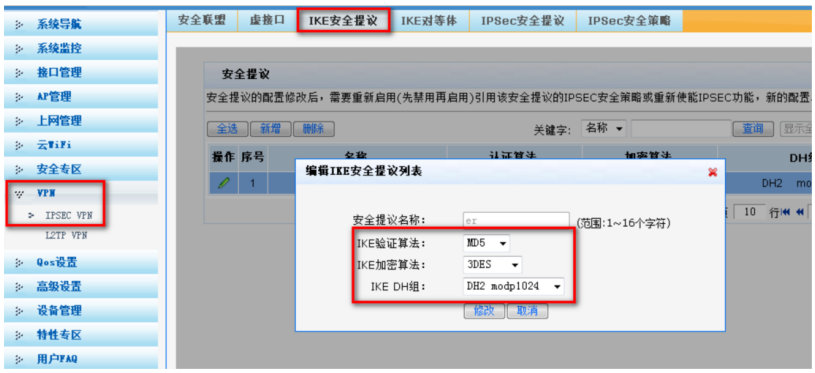
3 配置步骤

3.1配置ERG2路由器

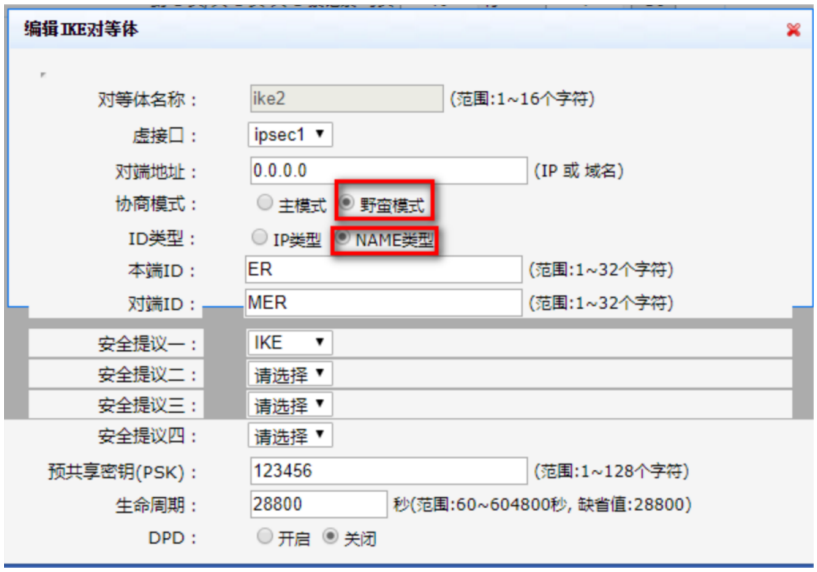
#选择【VPN】--【IPSEC VPN】--【虚接口】。单击【新增】按钮，将其与对应的出接口进行绑定，单击【增加】。



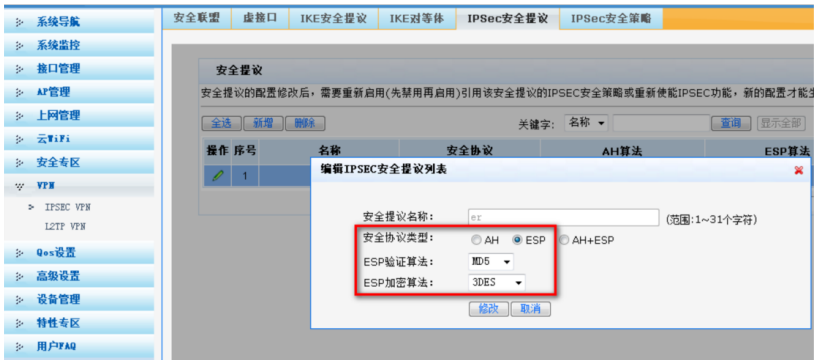
#选择【VPN】--【IPSEC VPN】--【IKE安全提议】。单击【新增】按钮，设置验证算法和加密算法分别为MD5、3DES，DH组选择DH2，单击【增加】。



#选择【VPN】--【IPSEC VPN】--【IKE对等体】。单击【新增】按钮，选择野蛮模式，选择对应的虚接口，对端地址填写0.0.0.0。在“ID类型”选择NAME，本端ID为ER，对端ID为MSR，预共享秘钥填写123456，保证两端秘钥一致，单击【增加】。


编辑IKE对等体
对等体名称：
ike2
(范围:1~16个字符)
虚接口：
ipsec1
对端地址：
0.0.0.0
(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：
ER
(范围:1~32个字符)
对端ID：
MER
(范围:1~32个字符)
安全提议一：
IKE
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：
28800
秒(范围:60~604800秒，缺省值:28800)
DPD：
开启
关闭

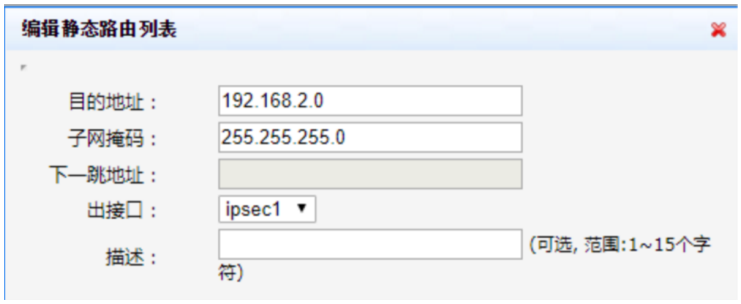
#选择【VPN】--【IPSEC VPN】--【IPSEC安全提议】。单击【新增】，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击【增加】。



#选择【VPN】--【IPSEC VPN】--【IPSEC安全策略】。选中“启用IPSec功能”复选框，单击【应用】按钮生效。单击【新增】按钮，本端子网192.168.10.0/24，对端子网192.168.2.0/24，并选择协商类型，对等体，安全提议，单击【增加】。


编辑IPSEC安全策略列表
安全策略名称：
ipsec2
(范围:1~16个字符)
是否启用：
启用
本地子网IP/掩码：
192.168.10.0
/
255.255.255.0
对端子网IP/掩码：
192.168.2.0
/255.255.255.0
协商类型：
IKE协商
手动模式
对等体：
ike2
安全提议一：
IPSEC
安全提议二：
请选择
安全提议三：
请选择
安全提议四：
请选择
PFS：
DH1 modp768
生命周期：
28800
秒 (范围:120~604800, 缺省值:28800)
触发模式：
流量触发

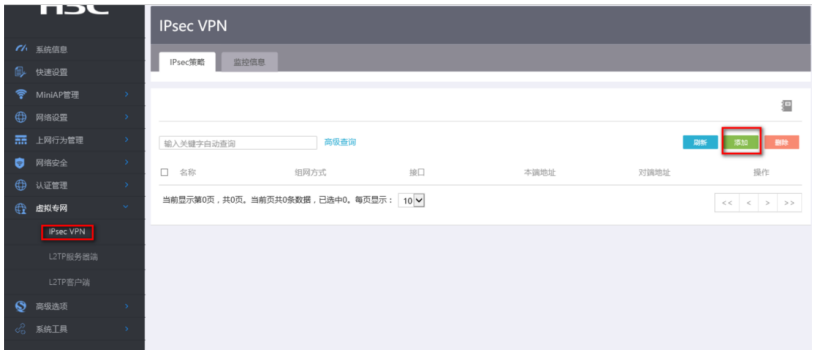
#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择【高级设置】--【路由设置】--【静态路由】，单击【新增】，目的地址填写192.168.2.0，出接口选择ipsec1。



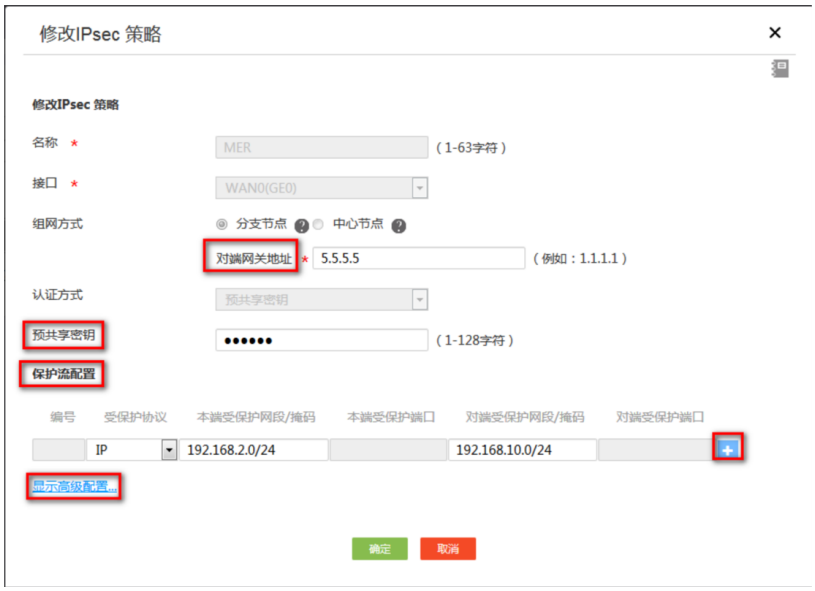
3.2配置MER路由器

#选择【虚拟专网】--【IPsec VPN】--【IPsec策略】单击【添加】按钮

。



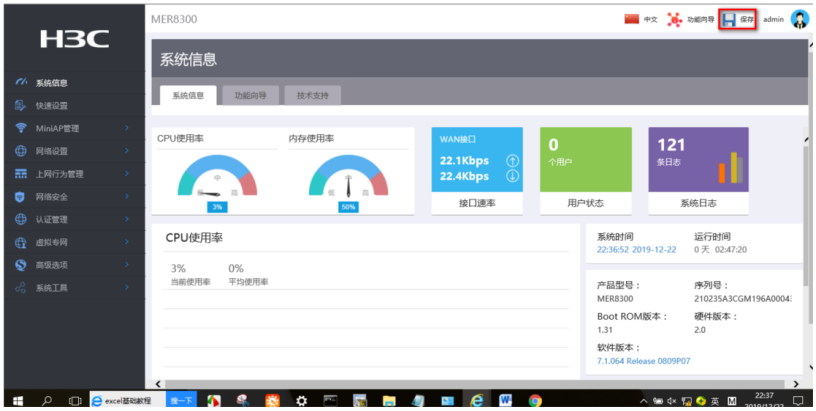
#选择分支节点，对端地址填写5.5.5.5，预共享秘钥为123456，保证两端秘钥一致，配置保护流，本端地址为192.168.2.0/24，对端地址为192.168.10.0/24，并点击高级设置进行下一步设置。


修改IPsec 策略
修改IPsec 策略
名称 *
MER
(1-63字符)
接口 *
WAN0(GE0)
组网方式
分支节点
中心节点
对端网关地址 *
5.5.5.5
(例如：1.1.1.1)
认证方式
预共享密钥
预共享密钥
(1-128字符)
保护流配置
编号
受保护协议
本端受保护网段/掩码
本端受保护端口
对端受保护网段/掩码
对端受保护端口
IP
192.168.2.0/24
192.168.10.0/24
显示高级配置...
确定
取消

#IKE配置，协商模式选择野蛮模式，本端身份类型选择FQDN，填写MER，对端身份类型选择IP地址，填写5.5.5.5，认证算法，加密算法，PFS分部为MD5，3DES-CBC，DH2，保证与ERG2侧一致。

#IPsec配置，安全协议选择ESP，认证算法MD5，加密算法3DES-CBC，PFS为Group1，算法保证与ERG2保持一致。

3.3保存配置



3.4验证配置

#ERG2侧，点击【VPN】--【IPSEC VPN】--【安全联盟】，查看ipsec隧道信息。

#MER侧，点击【虚拟专网】--【IPsec VPN】--【监控信息】，查看ipsec隧道信息。