ERG2—MER路由器 IPSEC VPN配置(野蛮模式)

IPSec VPN 史晓虎 2020-01-17 发表

组网及说明

1 配置需求或说明

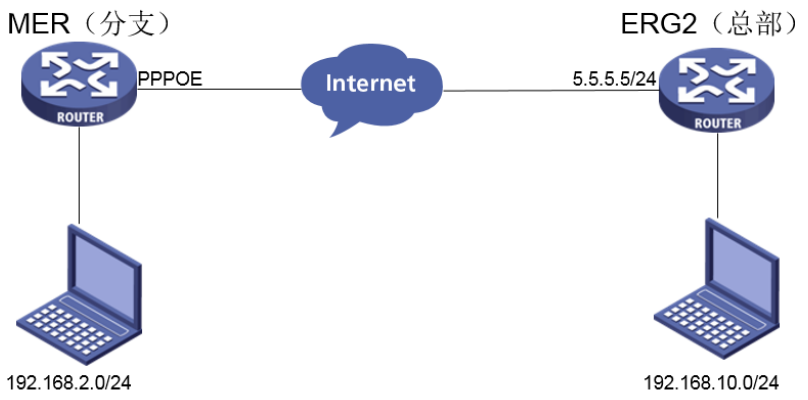
1.1适用产品系列

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

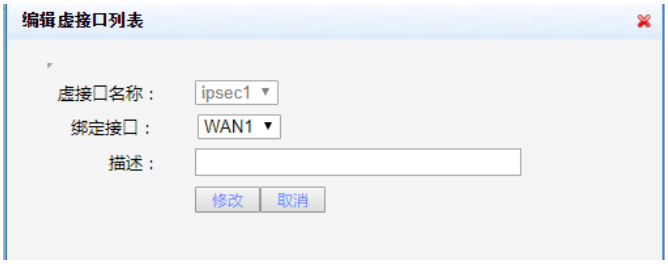


配置步骤

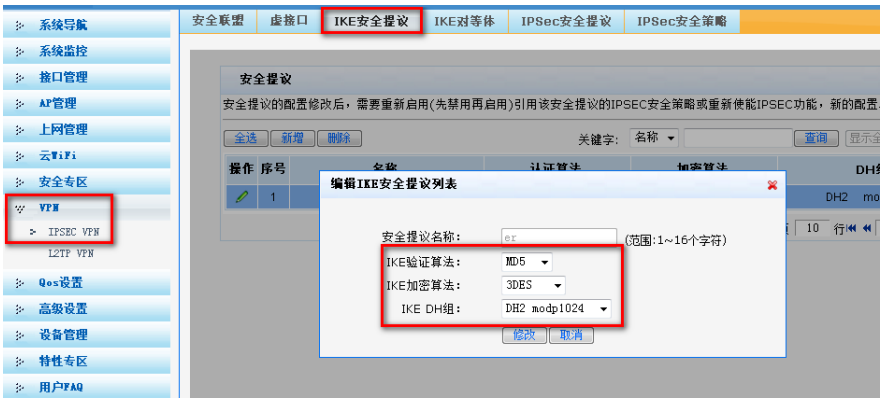
3 配置步骤

3.1配置ERG2路由器

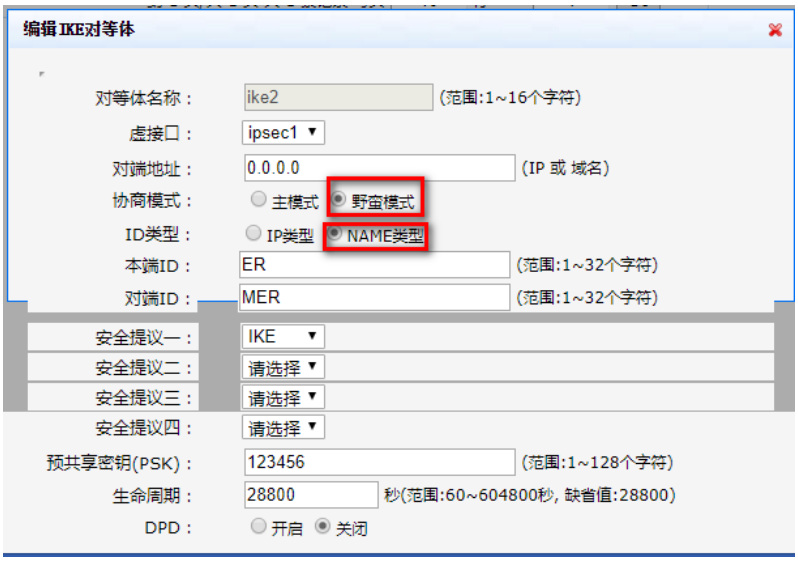
#选择【VPN】--【IPSEC VPN】--【虚接口】。单击【新增】按钮，将其与对应的出接口进行绑定，单击【增加】。



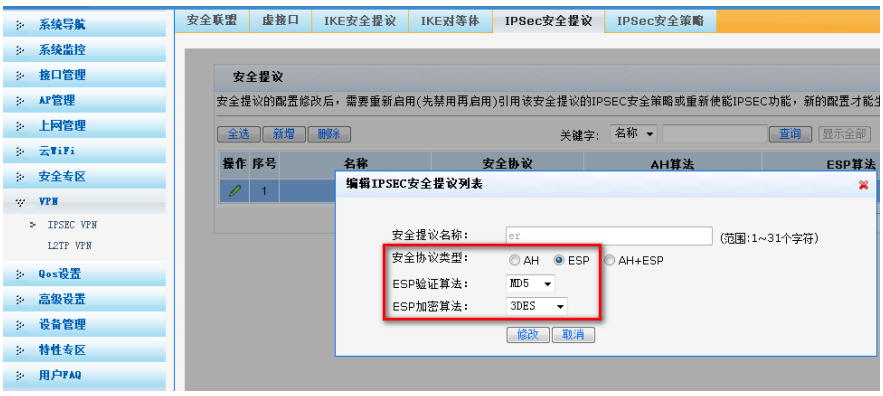
#选择【VPN】--【IPSEC VPN】--【IKE安全提议】。单击【新增】按钮，设置验证算法和加密算法分别为MD5、3DES，DH组选择DH2，单击【增加】。



#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】。

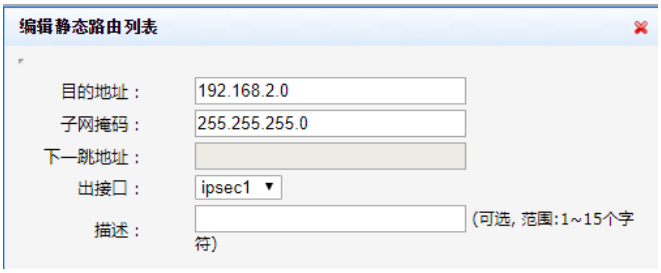


#选择【VPN】--【IPSEC VPN】--【IPSEC安全提议】。单击【新增】，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击【增加】。



#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】。

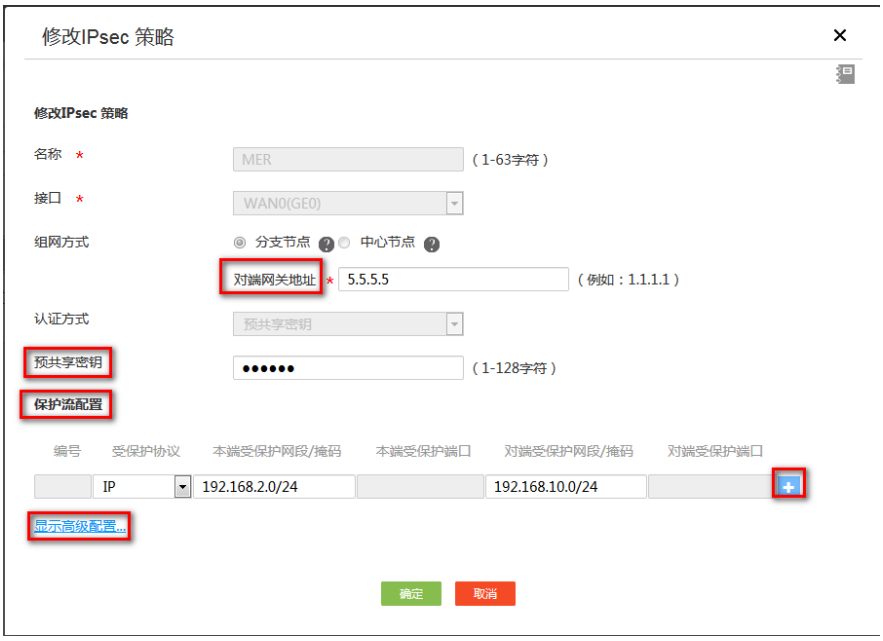
#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择【高级设置】--【路由设置】--【静态路由】，单击【新增】，目的地址填写 192.168.2.0，出接口选择ipsec1。



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。

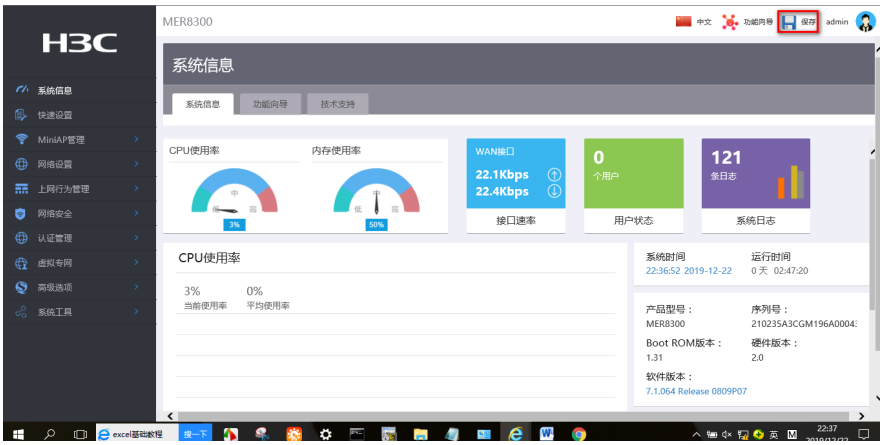
#选择分支节点，对端地址填写5.5.5.5，预共享秘钥为123456，保证两端秘钥一致，配置保护流，本端地址为192.168.2.0/24，对端地址为192.168.10.0/24，并点击高级设置进行下一步设置。



#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。

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
ipsec2	in	4.4.4.4 =>5.5.5.5	----	----	0xb5c15050	3DES_MD5	192.168.2.0/24 =>192.168.10.0/24
ipsec2	out	5.5.5.5 =>4.4.4.4	----	----	0xdbca08f2	3DES_MD5	192.168.10.0/24 =>192.168.2.0/24

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

配置关键点