MER系列路由器和ERG2系列路由器对接 IPSEC VPN配置（主模式）

IPSec VPN　史晓虎　2020-09-04 发表

组网及说明

1 配置需求或说明

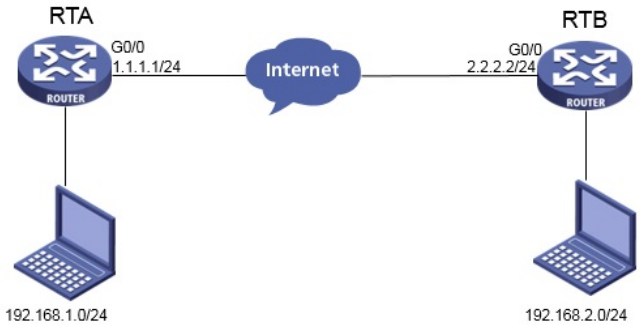
1.1 适用产品系列

本案例适用于MER3220、MER5200、MER8300路由器。

1.2 配置需求及实现的效果

Router A ERG2路由器和Router B MER路由器，在两者之间建立一个安全隧道，对客户分支机构A所在的子网（192.168.1.0/24）与客户分支机构B所在的子网（192.168.2.0/24）之间的数据流进行安全保护，实现两端子网终端通过IPsec VPN 隧道进行互访。

2 组网图



配置步骤

2 配置步骤

2.1 基本上网配置

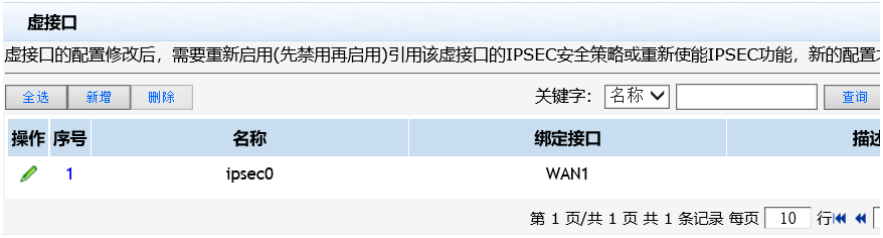
路由器基本上网配置省略，可参考 “MER系列路由器基本上网（静态IP）配置（V7）”案例。和ERG2上网案例。

2.2 配置IPSEC VPN

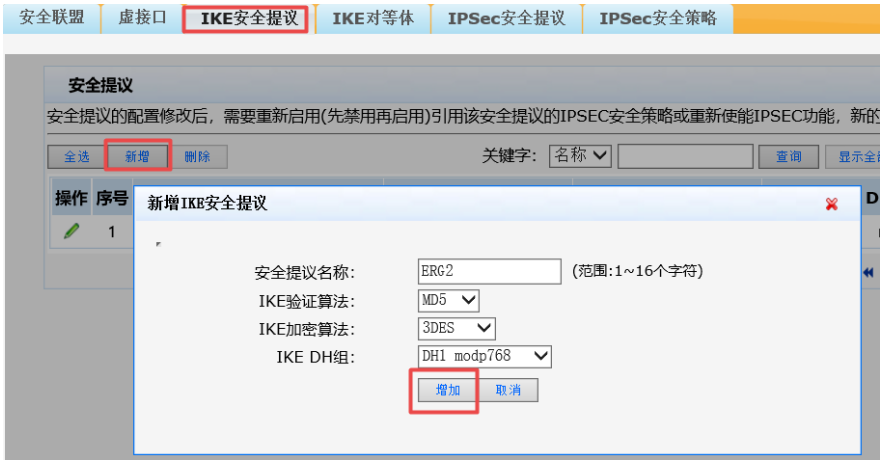
2.2.1 配置ERG2 Router A

单击【VPN】--【IPsec VPN】--【虚接口】，点击【新增】

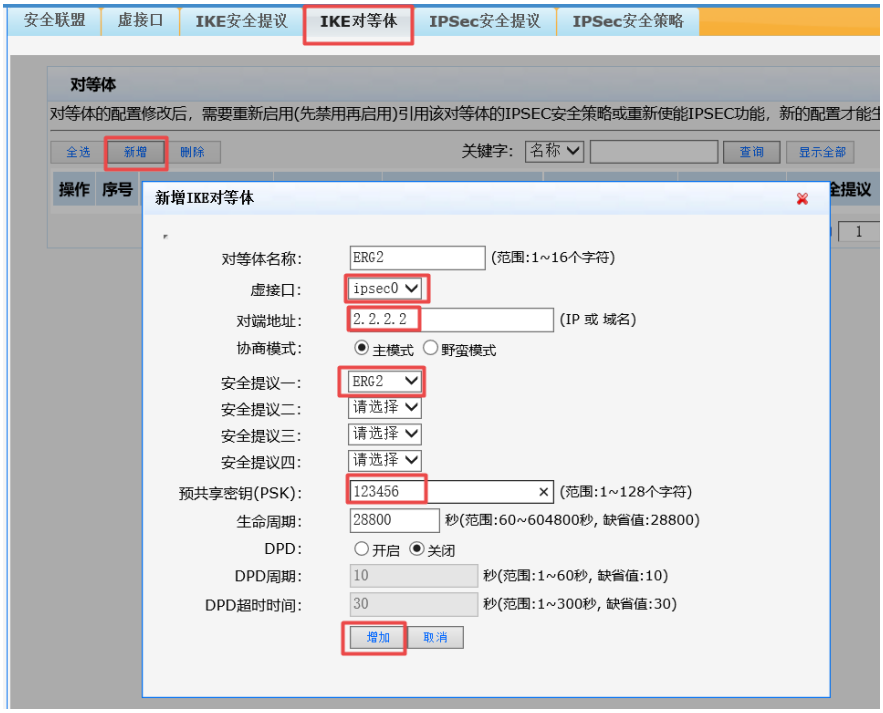
虚接口名称选择【ipsec0】，绑定接口选择【WAN1】，点击【增加】



#配置IKE安全提议 点击【新增】，验证算法选择【MD5】，加密算法选择【3DES】，DH组选择【DH1】,点击【增加】

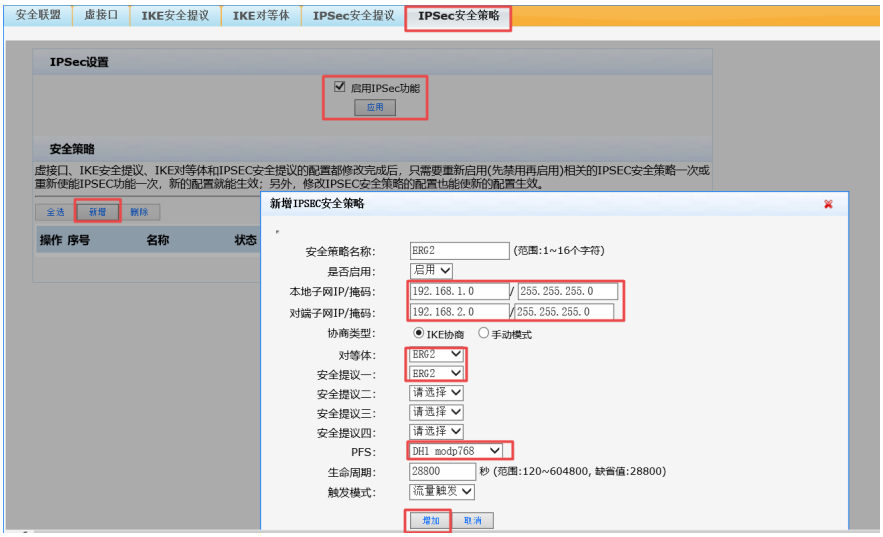


#配置IKE对等体 点击【新增】，虚接口选择【ipsec0】，对端地址填【2.2.2.2】，协商，模式选择【主模式】，安全提议一选择【ERG2】，预共享密钥填【123456】，点击【增加】

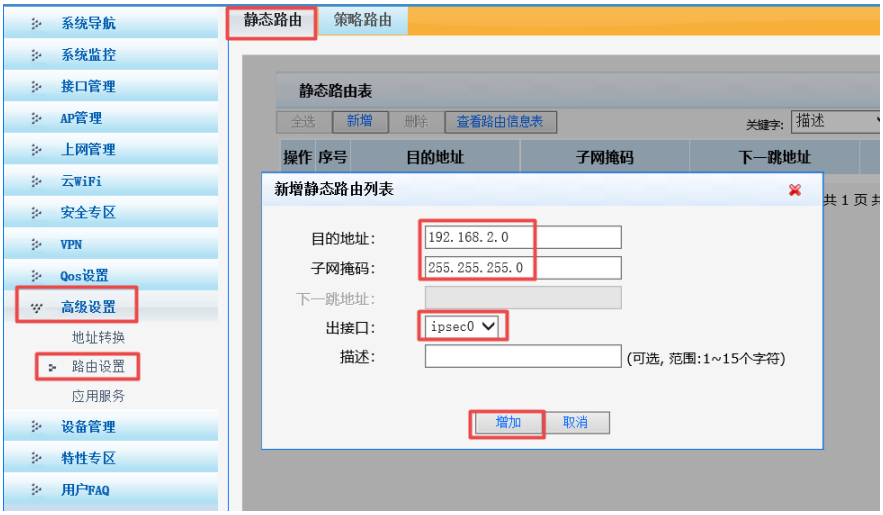


#配置IPSEC安全提议 点击【新增】，安全协议类型选择【ESP】，验证算法选择【MD5】，加密算法选择【3DES】，点击【增加】

#配置IPSEC安全策略本地子网IP填写【192.168.1.0/255.255.255.0】，对端子网IP填【192.168.2.0/255.255.255.0】，协商类型选择【IKE协商】，对等体选择【ERG2】，安全提议一选择【ERG2】，PFS选择【DH1】，点击【增加】

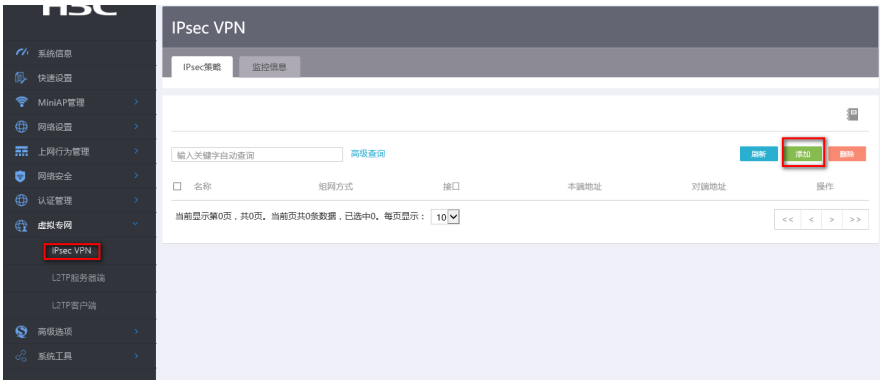


#配置静态路由 选择【高级设置】，选择【路由设置】，静态路由点击【新增】，目的地址填【192.168.2.0】，子网掩码填【255.255.255.0】，出接口选择【ipsec0】

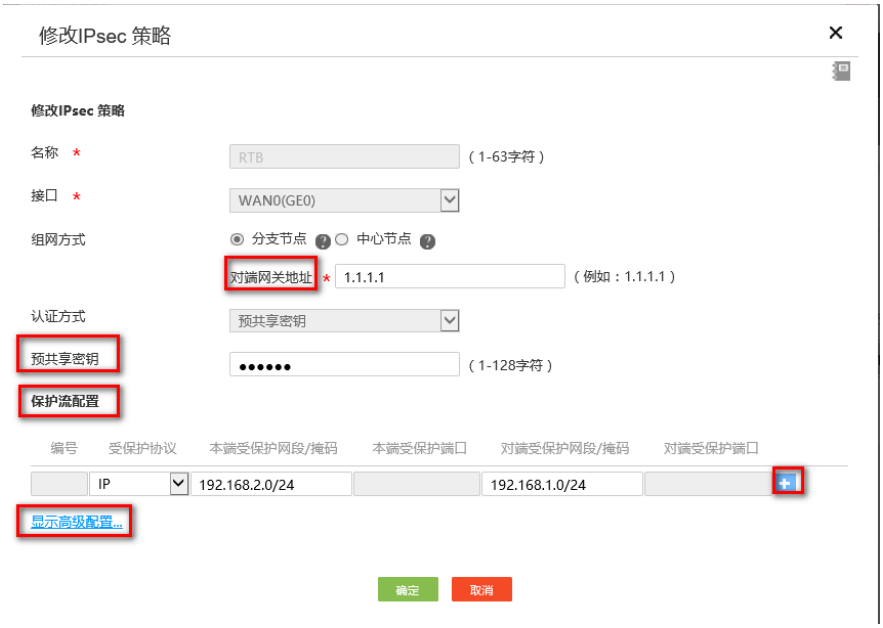


3.2.2 配置MER Router B

#单击【虚拟专网】--【IPsec VPN】--【IPsec策略】，点击【添加】



#选择分支节点，对端网关地址填写对端公网地址，预共享秘钥保证两端一致123456，添加两端的保护流，本端受保护网段192.168.2.0/24，对端受保护网段192.168.1.0/24。

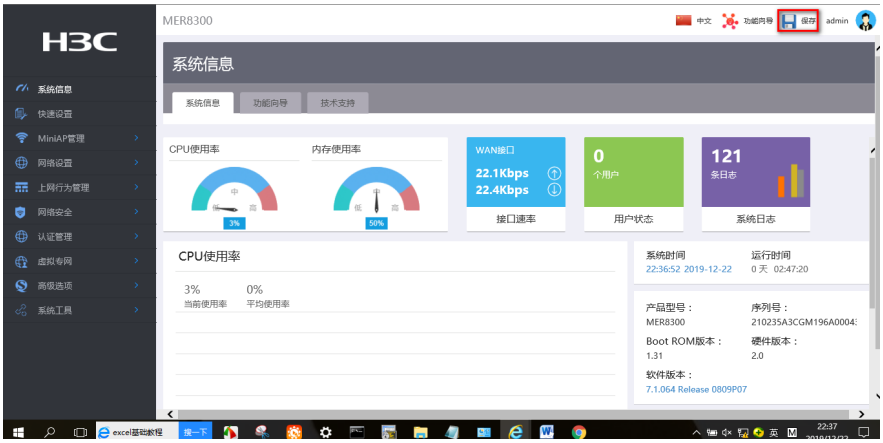


#配置IKE，协商模式选择主模式，本端地址为2.2.2.2，对端地址为1.1.1.1，认证算法，加密算法，PFS分别选择MD5，3DES-CBC，DH1，保证两端的算法一致。

#配置IPsec，安全协议选择ESP，认证算法选择MD5，加密算法选择3DES-CBC，PFS选择Group1，并保证两端算法一致。

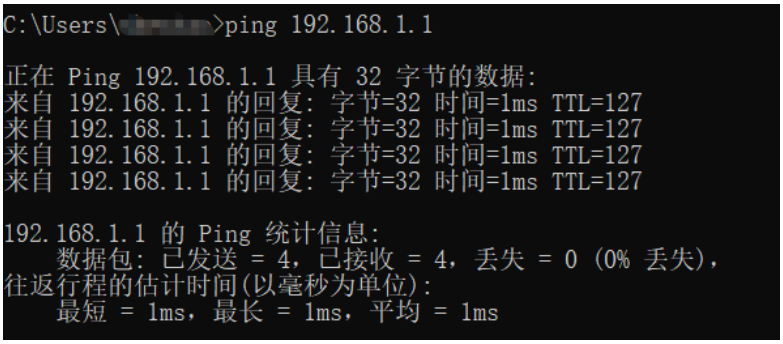
3.3 保存配置

#点击页面右上角保存按钮，ERG2默认保存配置



3.4 验证配置结果

#在MER下面的终端ping对端ERG2内网电脑的地址



#MER可以看到隧道情况

#ERG2看到的隧道情况


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
ERG2 out 1.1.1.1 =>2.2.2.2 ---- ---- 0xd0b620e5 3DES_MD5 192.168.1.0/24 =>192.168.2.0/24
ERG2 in 2.2.2.2 =>1.1.1.1 ---- ---- 0x9317b1d0 3DES_MD5 192.168.2.0/24 =>192.168.1.0/24
第 1 页/共 1 页 共 2 条记录 每页 10 行
1
Go

配置关键点