本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

MER系列路由器和ERG2系列路由器 IPSEC VPN配置（野蛮模式）

目录

1 配置需求或说明

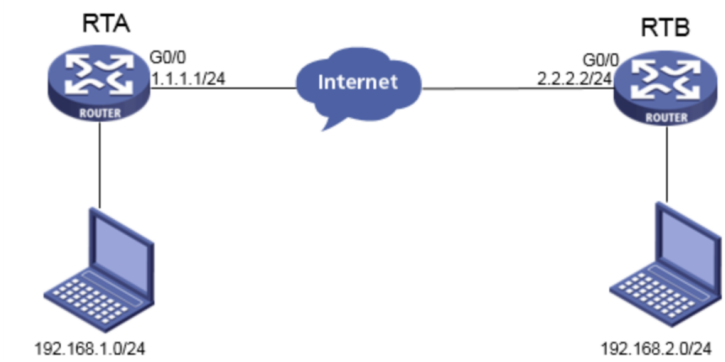
1.1 适用产品系列

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使用ERG2路由器，Router B均使用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。并且ERG2路由器是不固定的IP地址。

2 组网图



3 配置步骤

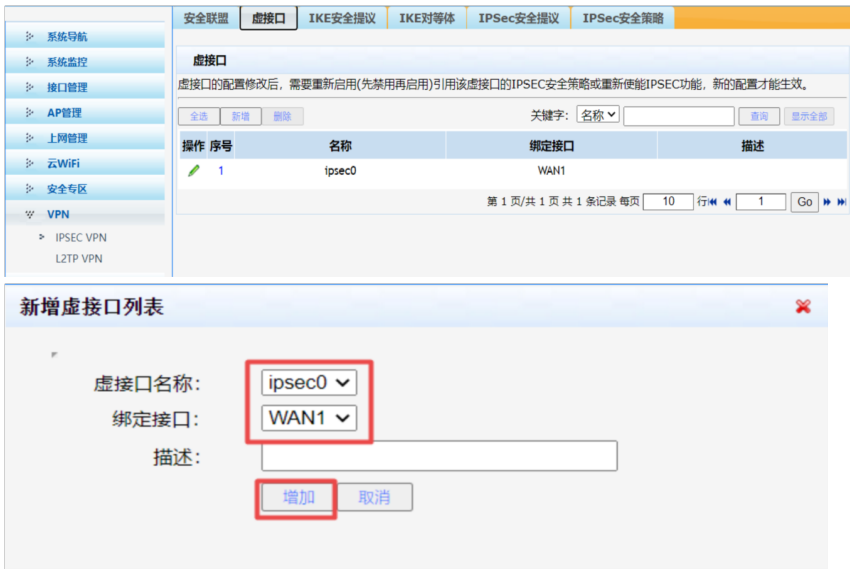
3.1 基本上网配置

路由器基本上网配置省略，可参考“路由器上网配置方法”案例。

3.2 配置IPSEC VPN

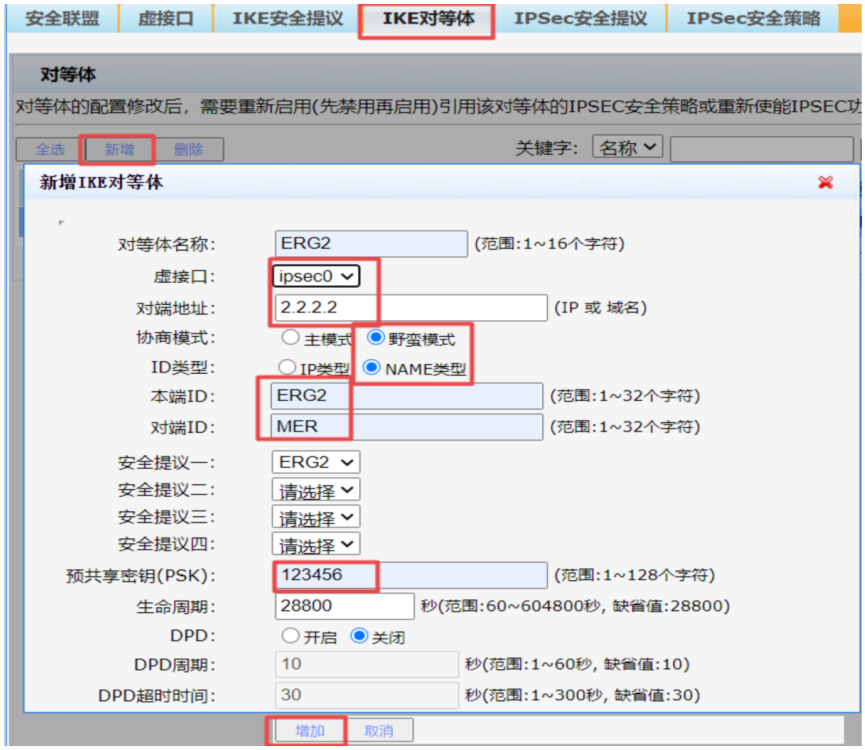
3.2.1 配置 ERG2--Router A

单击【VPN】--【IPsec VPN】--【虚接口】，点击【新增】，虚接口选择【ipsec0】，绑定接口选择【WAN1】，点击【增加】。

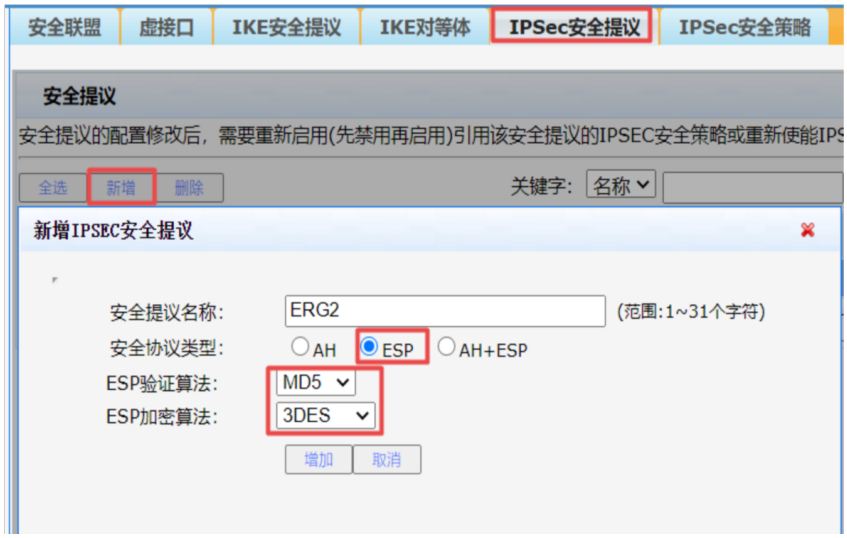


#配置IKE安全提议 点击【新增】，验证算法选择【MD5】，加密算法选择【3DES】，DH组选择【DH2】，点击【增加】。

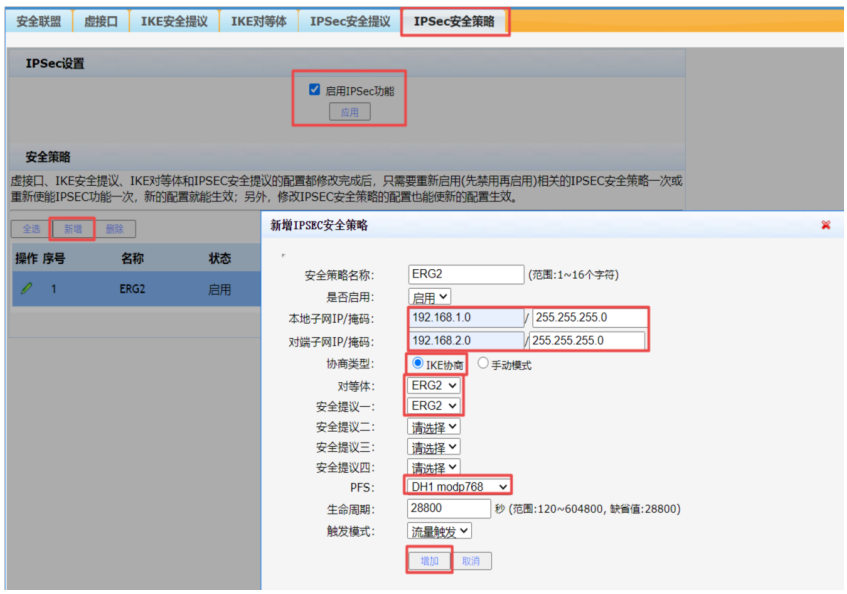
#配置IKE对等体，点击【新增】，虚接口选择【ipsec0】，对端地址选择【2.2.2.2】，协商模式选择【野蛮模式】，ID类型选择【NAME类型】，本段ID【ERG2】，对端ID【MER】，安全提议一选择【ERG2】，预共享密钥选择【123456】，点击【增加】。



#配置IPsec安全提议，安全协议选择【ESP】，验证算法选择【MD5】，加密算法选择【3DES-CBC】，点击【增加】。



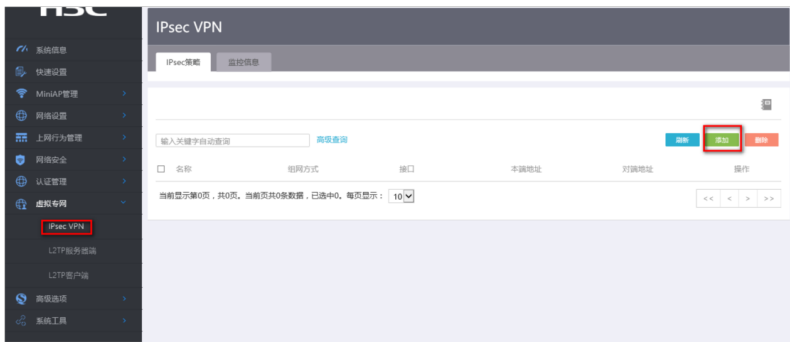
#配置IPSec安全策略，勾选“启用IPSec功能”，点击“启用”，本地子网配置【192.168.1.0/255.255.255.0】，对端子网配置【192.168.2.0/255.255.255.0】，协商类型选择【IKE协商】，对等体选择【ERG2】，安全提议一选择【ERG2】，PFS配置【DH1】，点击【增加】。



#添加静态路由 单击【高级设置】--【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【255.255.255.0】，出接口选择【IPSec0】，点击【增加】。

3.2.2 配置MER--Router B

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


IPsec VPN
IPsec策略
监控信息
系统信息
快速设置
MiniAP管理
网络设置
上网行为管理
网络安全
认证管理
虚拟专网
IPsec VPN
L2TP服务器端
L2TP客户端
高级选项
系统工具
输入关键字自动查询
高级查询
刷新
添加
删除
名称
组网方式
接口
本端地址
对端地址
操作
当前显示第0页，共0页。当前页共0条数据，已选中0。每页显示：
10

#选择【中心节点】，选择公网接口【WAN0】，填写预共享密钥【123456】，点击【显示高级配置】

#配置IKE，协商模式选择【野蛮模式】，本端身份类型选择【FQDN】配置【MER】，算法组合选择【自定义】，认证算法选择【MD5】，加密算法选择【3DES】，PFS选择【DH1】

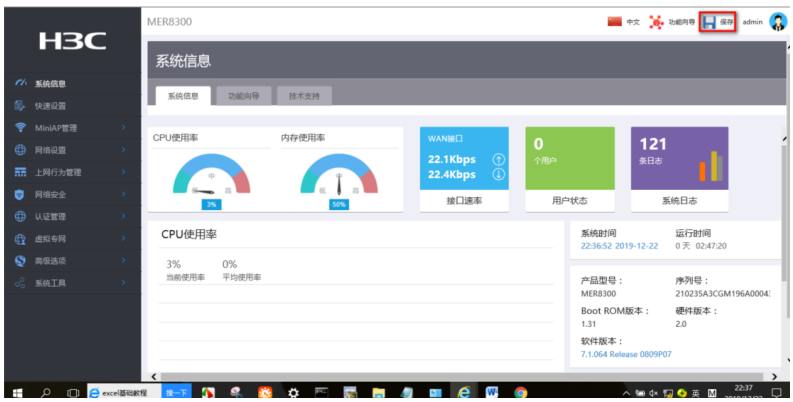
注意：除了上面的配置外还需要在命令行配置match remote identity fqdn ERG2 否则无法建立。


修改IPsec 策略
高级配置
IKE配置
IPsec配置
协商模式
野蛮模式
本端身份类型
FQDN
MER
(1-255字符)
对等体存活检测（DPD）
开启
关闭
算法组合
自定义
认证算法 *
MD5
加密算法 *
3DES-CBC
PFS *
DH group 1
SA生存时间
86400
秒 (60-604800, 缺省值为86400)
返回基本配置

#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。然后点击【返回基本配置】，再点击【确定】

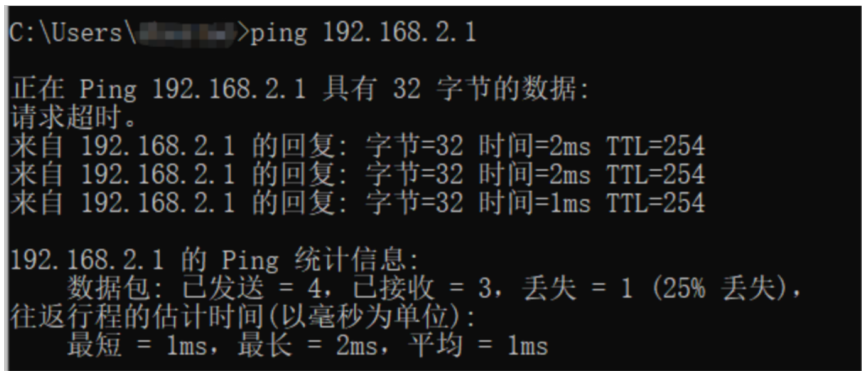
3.3 保存配置

#点击页面右上角保存按钮



3.4 验证配置结果

#在ERG2下面的终端ping对端MER的内网电脑的地址触发隧道



#在ERG2上面看到的安全联盟

#在MER上查看隧道信息