ICG2000D/ICG3000F系列路由器 IPSEC VPN配置（野蛮模式WEB版）

IPSec VPN　史晓虎　2021-01-04 发表

组网及说明

1 配置需求或说明

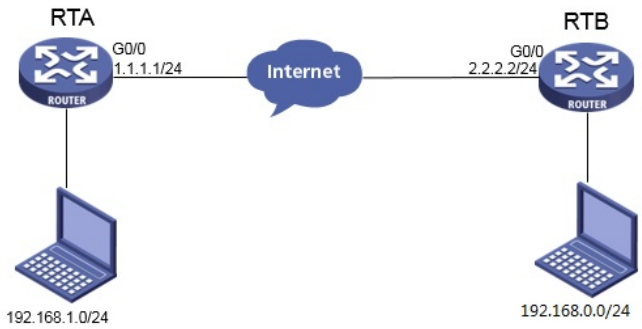
1.1 适用产品系列

本案例适用于如ICG2000D、ICG3000F系列的路由器

1.2 配置需求及实现的效果

Router A和Router B均使用MSR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（192.168.0.0/24）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

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 “MSR830-WiNet系列路由器基本上网基本上网（静态IP）WEB配置（V7）”案例。

3.2 配置IPSEC VPN

3.2.1 配置Router A

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

#选择点到多点，预共享秘钥保证两端一致。

#配置IKE，协商模式选择野蛮模式，本端地址为1.1.1.1，认证算法，加密算法，PFS分别选择SHA1，DES-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SHA1，加密算法选择AES-CBC-128，并保证两端算法一致。

3.2.2 配置Router B

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

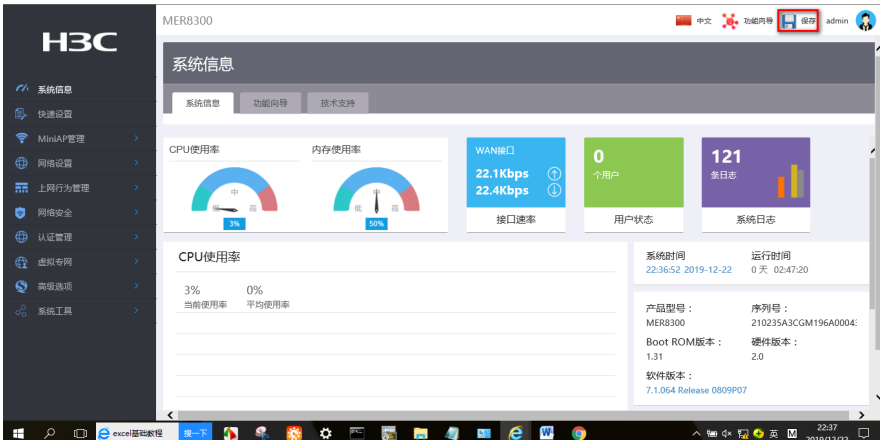
#选择分支节点，对端网关地址填写对端公网地址，预共享秘钥保证两端一致，添加两端的保护流，本端受保护网段192.168.0.0/24，对端受保护网段192.168.1.0/24。

#配置IKE，协商模式选择野蛮模式，对端地址为1.1.1.1，认证算法，加密算法，PFS分别选择SHA1，DES-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SHA1，加密算法选择AES-CBC-128，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



3.4 验证配置结果