

组网及说明

1 配置需求或说明

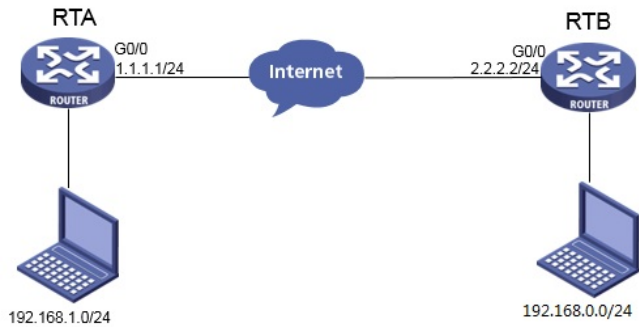
1.1 适用产品系列

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，预共享密钥保证两端一致。



#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，预共享密钥保证两端一致，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。

高级配置 **IKE配置** IPsec配置

协商模式 **野蛮模式**

本端身份类型 IP地址 (例如: 1.1.1.1)

对端身份类型 * IP地址 1.1.1.1 (例如: 1.1.1.1)

对等体存活检测 (DPD) 开启 关闭

算法组合 **自定义**

认证算法 * SHA1

加密算法 * DES-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SHA1, 加密算法选择AES-CBC-128, 并保证两端算法一致。

高级配置 **IKE配置** IPsec配置

算法组合 **自定义**

安全协议 * ESP

ESP认证算法 * SHA1

ESP加密算法 * AES-CBC-128

封装模式 * 传输模式 隧道模式

PFS

基于时间的SA生存时间 3600 秒 (180-604800, 缺省值为3600)

基于流量的生存时间 1843200 千字节 (2560-4294967295, 缺省值为1843200)

[返回基本配置](#)

[显示高级配置...](#)



3.3 保存配置

#点击页面右上角保存按钮

MER8300 中文 功能向导 保存 admin

系统信息

系统信息 功能向导 技术支持

CPU使用率 内存使用率

WAN接口 22.1Kbps 22.4Kbps 接口速率

0 个用户 用户状态

121 条日志 系统日志

CPU使用率 3% 0% 当前使用率 平均使用率

系统时间 22:36:52 2019-12-22 运行时间 0天 02:47:20

产品型号: MER8300 序列号: 210235A3CGM196A0004

Boot ROM版本: 1.31 硬件版本: 2.0

软件版本: 7.1.064 Release 0809P07

3.4 验证配置结果