

组网及说明

1 配置需求或说明

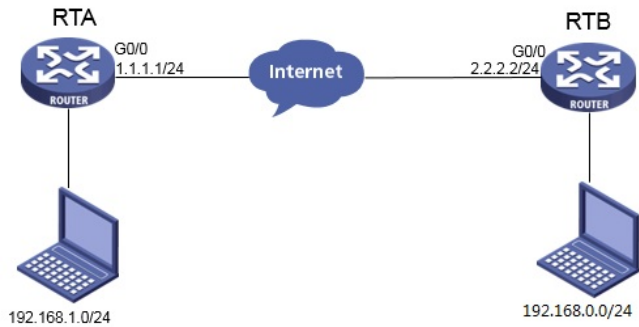
1.1 适用产品系列

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192.168.1.0/24，对端受保护网段192.168.0.0/24。

添加IPsec策略

名称 * (1-63字符)

接口 *

组网方式 点到点 点到多点

对端网关地址 * (例如: 1.1.1.1)

认证方式

预共享密钥 * (1-128字符)

ACL * (3000-3999) 该参数必须配置。

[显示高级配置...](#)

确定

取消

保护流配置

受保护协议

本端受保护网段/反掩码 / 本端受保护端口

对端受保护网段/反掩码 / 对端受保护端口

编号	受保护协议	本端受保护网段/反...	本端受保护端口	对端受保护网段/反...	对端受保护端口
1	ip	192.168.1.0/0.0.0...		192.168.0.0/0.0.0...	

当前显示第1页，共1页。当前页共1条数据，已选中0。每页显示：

受保护协议

ip

本端受保护网段/反掩码 192.168.1.0 / 0.0.0.255 本端受保护端口

对端受保护网段/反掩码 192.168.0.0 / 0.0.0.255 对端受保护端口