

403 Forbidden

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](#)

MSR系列路由器 IPSEC VPN配置 （野蛮模式 WEB版）

目录

[MSR系列路由器 IPSEC VPN配置（野蛮模式 WEB版）](#)

[1 配置需求或说明](#)

[1.1 适用产品系列](#)

[1.2 配置需求及实现的效果](#)

[2 组网图](#)

[3 配置步骤](#)

[3.1 基本上网配置](#)

[3.2 配置IPSEC VPN](#)

[3.2.1 配置Router A](#)

[3.2.2 配置Router B](#)

[3.3 保存配置](#)

[3.4 验证配置结果](#)

1 配置需求或说明

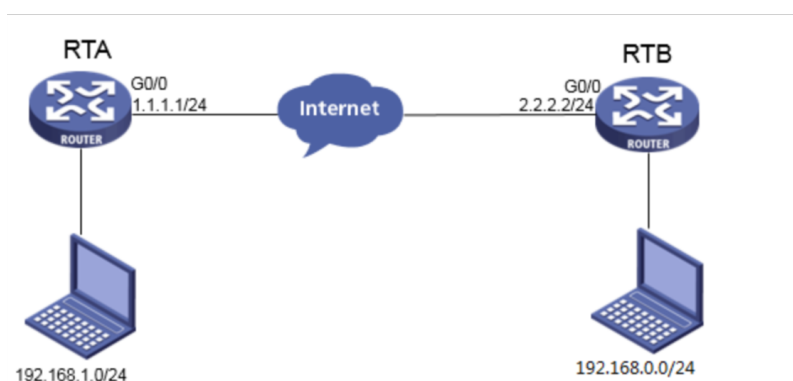
1.1 适用产品系列

本案例提到的MSR V7平台路由器是指Comware V7平台的MSR830-WiNet系列路由器，如MSR830-10BEI-WiNet、MSR830-6EI-WiNet、MSR830-5BEI-WiNet、MSR830-6BHI-WiNet、MSR830-10BHI-WiNet、MSR2630等

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



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。

添加IPsec 策略

添加IPsec 策略

名称 * tov7 (1-53字符)

接口 * WAN0(GE1/0/0)

组网方式
☒ 分支节点 ☐ 中心节点
对端网关地址 * 1.1.1.1 (例如: 1.1.1.1)

认证方式
预共享密钥

预共享密钥 * ... (1-128字符)

保护流配置 *

编号	受保护协议	本端受保护网段/掩码	本端受保护端口	对端受保护网段/掩码	对端受保护端口
	IP	192.168.0.0/24		192.168.1.0/24	

显示高级配置...

确定 取消

#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)

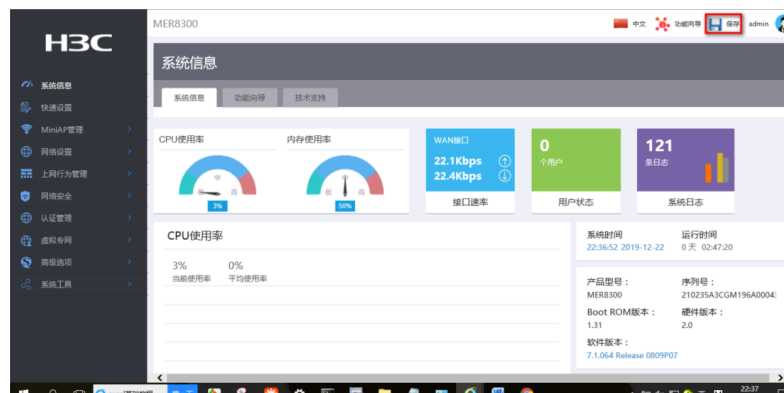
[返回基本配置](#)

[显示高级配置...](#)

确定 **取消**

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RTA下面的终端ping RTB对端内网电脑的地址

```
>ping 192.168.0.1

正在 Ping 192.168.0.1 具有 32 字节的数据:
请求超时。
来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=254
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=254
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=254

192.168.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

#查看总部IPSec VPN的监控信息

系统信息

快速设置

网络设置

上网行为管理

网络安全

认证管理

虚拟专用网

IPsec VPN

L2TP服务器端

L2TP客户端

高级选项

IPsec VPN

IPsec策略

监控信息

搜索

清除

刷新

ID	策略名称	状态
0	to7	Active

当前显示第1页，共1页。当前页共1条数据，已读

×

策略详情

刷新

对端地址	协商算法	流量特征	SPI	出/入报文数	出/入字节数
2.2.2.2	加密 ESP-AES-CBC-128 认证 ESP-SHA1 SA生存时间(KB/sec) 1843200/3600 SA删除时间(KB/sec) 1843199/3482	源IP 192.168.1.0/24 目的IP 192.168.0.0... Protocol ESP Src port 0 Des port 0	In 1961617292 [ESP] Out 1726183290 [ESP]	9/9	592/592