

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](#)

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MSRV5系列 路由器 IPSEC VPN配置（野蛮 模式）

目录

[MER系列路由器和MSRV5系列路由器 IPSEC VPN配置（野蛮模式）](#)

[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 MSRV5--Router A](#)

[3.2.2 配置MER--Router B](#)

[3.3 保存配置](#)

[3.4 验证配置结果](#)

1 配置需求或说明

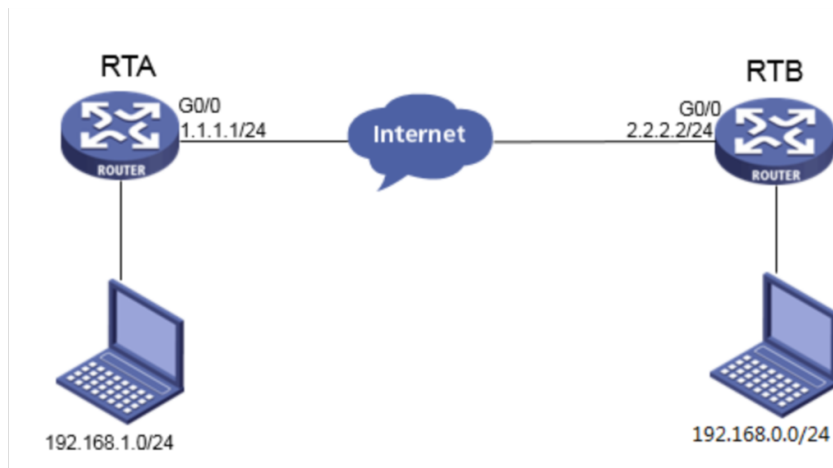
1.1 适用产品系列

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（192.168.0.0/24）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。并且MSRV5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 MSRV5--Router A

#单击【VPN】--【IPsec VPN】--【新建】



#接口名称选择【G0/0】，组网模式选择【站点到站点】，

对端网关地址填【2.2.2.2】，预共享密钥填写【1】，网关ID对端ID类型和本端ID类型选择【IP地址】

新建IPsec连接

IPsec连接名称: tomer * 字符 (1 - 32)

网关信息

接口: GigabitEthernet0/0

组网模式: ☒ 站点到站点 ☐ PC到站点

网关地址

对端网关地址/主机名: 2.2.2.2 * 字符 (1 - 255)

本端网关地址:

认证

认证方式: ☒ 预共享密钥 ☐ 证书

密钥: * 字符 (1 - 128)

确认密钥: * 字符 (1 - 128)

网关ID

对端ID类型: ☒ IP地址 ☐ FQDN 对端网关ID: * 字符 (1 - 255)

本端ID类型: ☒ IP地址 ☐ FQDN ☐ User FQDN 本端网关ID: * 字符 (1 - 255)

筛选方式选择【流量特征】，源地址填写【192.168.1.0/0.0.0.255】，目的地地址填写【192.168.0.0/0.0.0.255】，点击【高级】，第一阶段交换模式选择【野蛮模式】，认证算法选择【MD5】，加密算法选择【3DES】，第二阶段协议选择【ESP】，ESP认证算法选择【MD5】，ESP加密算法选择【3DES】，点击【确定】

筛选器

筛选方式: 流量特征

源地址/通配符: 192.168.1.0 / 0.0.0.255 *

目的地址/通配符: 192.168.0.0 / 0.0.0.255 *

反向路由注入: ☐ 开启 ☒ 关闭

高级

第一阶段

交换模式: ☐ 主模式 ☒ 野蛮模式

认证算法: MD5

加密算法: 3DES

DH: Diffie-Hellman Group1

SA的生存周期: 86400 秒 (60 - 604800, 缺省值 = 86400)

第二阶段

协议: ESP

ESP认证算法: MD5

ESP加密算法: 3DES

封装模式: ☒ 隧道模式 ☐ 传输模式

PFS: None

SA的生存周期

基于时间的生存周期: 3600 秒 (180 - 604800, 缺省值 = 3600)

基于流量的生存周期: 1843200 千字节 (2560 - 4294967295, 缺省值 = 1843200)

DPD: ☐ 开启 ☒ 关闭

星号 (*) 为必填写项

确定 取消

3.2.2 配置MER--Router B

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



#选择【中心节点】，选择公网接口【WAN0】，填写预共享

密钥【1】，点击【显示高级配置】

添加IPsec 策略

添加IPsec 策略

名称 *
tomsr (1-63字符)

接口 *
WAN0(GE0)

组网方式
☐ 分支节点 ☒ 中心节点

认证方式
预共享密钥

预共享密钥 *
 (1-128字符)

显示高级配置...

确定 取消

#配置IKE，协商模式选择【野蛮模式】，本端身份类型选择【IP地址】配置【2.2.2.2】，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】

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 2.2.2.2 (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 *
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】，并保证两端算法一致。然后点击【返回基本配置】，再点击【确定】

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 * MD5

ESP加密算法 * 3DES-CBC

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)

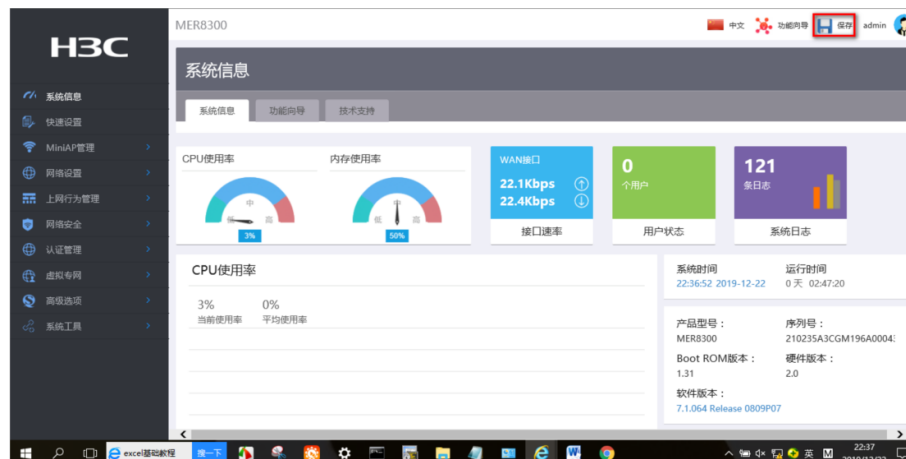
[返回基本配置](#)

[显示高级配置...](#)

确定 取消

3.3 保存配置

#MER和MSRV5点击页面右上角保存按钮



3.4 验证配置结果

#在MSRV5下面的终端ping对端MER的内网的地址触发隧道

```
C:\Users\██████████\ping 192.168.0.1

正在 Ping 192.168.0.1 具有 32 字节的数据:
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
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 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

#在MSRV5上查看隧道情况

IPsec连接		监控信息			
	连接名	接口	对端地址	本端地址	连接状态
<input type="checkbox"/>	tomor	GigabitEthernet0/0	2.2.2.2		Connected

#在MER上查看隧道信息

IPsec策略

监控信息

输入关键字自动查询

高级查询

刷新

删除

<input type="checkbox"/>	策略名称	状态	接口	本端地址	对端地址	安全提议	操作
<input type="checkbox"/>	tomsr	Active	WAN0(GE0)	2.2.2.2	1.1.1.2	ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5	

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:

1