

# 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](#)

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 IPSEC VPN配置（主模式）

## 目录

### [MER系列路由器 IPSEC VPN配置（主模式）](#)

#### [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

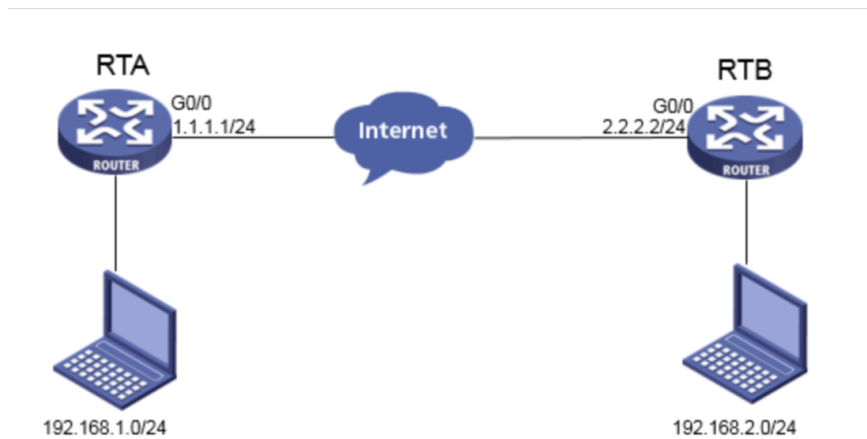
## 1.1 适用产品系列

本案例适用于MER3220、MER5200、MER8300路由器。

## 1.2 配置需求及实现的效果

Router A和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（192.168.2.0/24）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“MER系列路由器基本上网（静态IP）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】，单击【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192.168.1.0/24，对端受保护网段192.168.2.0/24。

修改IPsec 策略

修改IPsec 策略

名称 \*  
RTA (1-63字符)

接口 \*  
WAN0(GE0)

组网方式  
☒ 分支节点 ☐ 中心节点

对端网关地址 \*  
2.2.2.2 (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
1	IP	192.168.1.0/255.255.255.0		192.168.2.0/255.255.255.0	

IP

显示高级配置...

确定 取消

#配置IKE，协商模式选择主模式，本端地址为1.1.1.1，对端地址为2.2.2.2，认证算法，加密算法，PFS分别选择MD5，3DES-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

主模式

本端身份类型

IP地址

1.1.1.1

(例如: 1.1.1.1)

对端身份类型 \*

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，PFS选择Group1，并保证两端算法一致。



高级配置

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 Group\_1

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

### 3.2.2 配置Router B

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



IPsec VPN

IPsec策略 监控信息

输入关键字自动查询 高级查询

新增 添加 删除

名称	组网方式	接口	本端地址	对端地址	操作
当前显示第0页，共0页。当前页共0条数据，已选中0。每页显示：10					

虚拟专网

IPsec VPN

L2TP服务端

L2TP客户端

高级选项

系统工具

#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192.168.2.0/24，对端受保护网段192.168.1.0/24。

修改IPsec 策略

修改IPsec 策略

名称 \*  
RTB (1-63字符)

接口 \*  
WAN0(GE0)

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	192.168.2.0/24		192.168.1.0/24	

显示高级配置...

确定 取消

#配置IKE，协商模式选择主模式，本端地址为2.2.2.2，对端地址为1.1.1.1，认证算法，加密算法，PFS分别选择MD5，3DES-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

主模式

本端身份类型

IP地址

2.2.2.2

( 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 \*

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，PFS选择Group1，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 \*    MD5

ESP加密算法 \*    3DES-CBC

封装模式 \*    ☐ 传输模式 ☒ 隧道模式

PFS    Group\_1

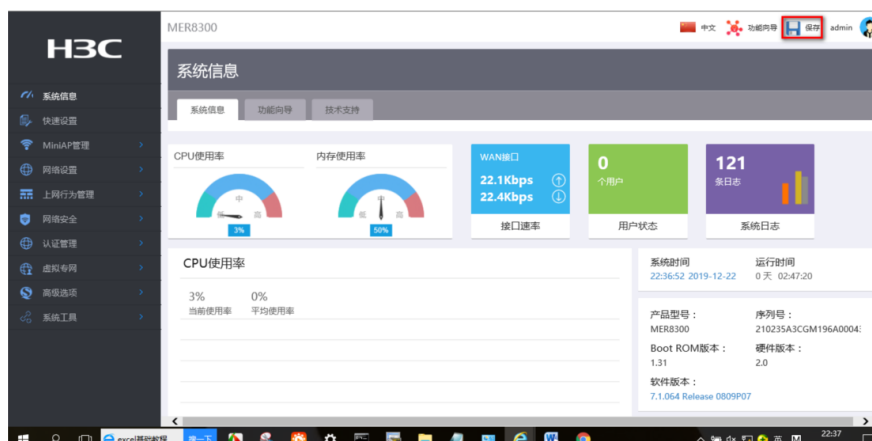
基于时间的SA生存时间    3600    秒 (180-604800, 缺省值为3600)

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](#)

### 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MER下面的终端ping对端内网电脑的地址

```
C:\Users\Administrator>ping 192.168.2.3

正在 Ping 192.168.2.3 具有 32 字节的数据:
请求超时。
来自 192.168.2.3 的回复: 字节=32 时间=2ms TTL=62
来自 192.168.2.3 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.2.3 的回复: 字节=32 时间=1ms TTL=62

192.168.2.3 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 = 1ms, 最长 = 2ms, 平均 = 1ms

C:\Users\Administrator>
```

