

## 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ERG2系列路由器 IPSEC VPN配置（野蛮模式）

## 目录

### [MER系列路由器和ERG2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 ERG2--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

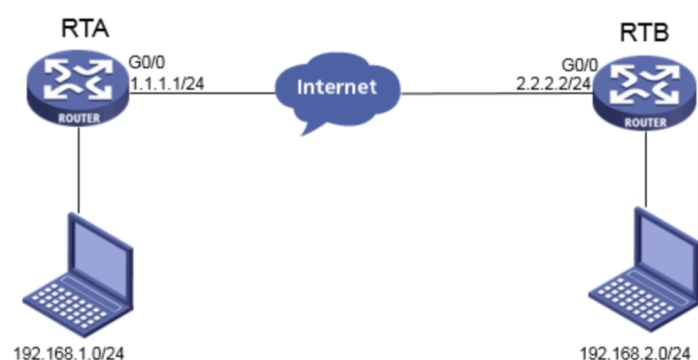
## 1.1 适用产品系列

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（192.168.2.0/24）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。并且ERG2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 ERG2--Router A

单击【VPN】--【IPsec VPN】--【虚接口】，点击【新增】，虚接口选择【ipsec0】，绑定接口选择【WAN1】，点击【增加】。

虚接口

虚接口的配置修改后，需要重新启用(先禁用再启用)引用该虚接口的IPSEC安全策略或重新使能IPSEC功能，新的配置才能生效。

全选 新增 删除 关键字: 名称 查询 显示全部

操作	序号	名称	绑定接口	描述
	1	ipsec0	WAN1	

第 1 页/共 1 页 共 1 条记录 每页 10 行 1 Go

新增虚接口列表

虚接口名称: ipsec0

绑定接口: WAN1

描述:

增加 取消

#配置IKE安全提议 点击【新增】，验证算法选择【MD5】，加密算法选择【3DES】，DH组选择【DH2】，点击【增加】。

安全联盟 虚接口 **IKE安全提议** IKE对等体 IPSec安全提议 IPSec安全策略

安全提议

安全提议的配置修改后，需要重新启用(先禁用再启用)引用该安全提议的IPSEC安全策略或重新使能IPSEC功能。

全选 **新增** 删除 关键字: 名称 查询 显示全部

新增IKE安全提议

安全提议名称: ERG2 (范围:1~16个字符)

IKE 验证算法: MD5

IKE 加密算法: 3DES

IKE DH组: DH2 modp1024

增加 取消

#配置IKE对等体，点击【新增】，虚接口选择【ipsec0】，对端地址选择【2.2.2.2】，协商模式选择【野蛮模式】，ID类型选择【NAME类型】，本端ID【ERG2】，对端ID【MER】，安全提议一选择【ERG2】，预共享密钥选择【123456】，点击【增加】。

安全联盟 | 虚接口 | IKE安全提议 | **IKE对等体** | IPSec安全提议 | IPSec安全策略

**对等体**

对等体的配置修改后，需要重新启用(先禁用再启用)引用该对等体的IPSEC安全策略或重新使能IPSEC功

全选 新增 删除 关键字: 名称

**新增IKE对等体**

对等体名称: ERG2 (范围:1~16个字符)

虚接口: ipsec0

对端地址: 2.2.2.2 (IP 或 域名)

协商模式: ☐ 主模式 ☒ 野蛮模式

ID类型: ☐ IP类型 ☒ NAME类型

本端ID: ERG2 (范围:1~32个字符)

对端ID: MER (范围:1~32个字符)

安全提议一: ERG2

安全提议二: 请选择

安全提议三: 请选择

安全提议四: 请选择

预共享密钥(PSK): 123456 (范围:1~128个字符)

生命周期: 28800 秒(范围:60~604800秒, 缺省值:28800)

DPD: ☐ 开启 ☒ 关闭

DPD周期: 10 秒(范围:1~60秒, 缺省值:10)

DPD超时时间: 30 秒(范围:1~300秒, 缺省值:30)

增加 取消

# 配置 IPsec 安全提议，安全协议选择【ESP】，验证算法选择【MD5】，加密算法选择【3DES-CBC】，点击【增加】。

The screenshot shows the 'IPSec安全提议' (IPSec Security Proposal) configuration page. The '新增IPSEC安全提议' (Add New IPsec Security Proposal) dialog box is open. The '安全提议名称' (Security Proposal Name) is set to 'ERG2'. The '安全协议类型' (Security Protocol Type) is set to 'ESP'. The 'ESP验证算法' (ESP Authentication Algorithm) is set to 'MD5'. The 'ESP加密算法' (ESP Encryption Algorithm) is set to '3DES'. The '增加' (Add) button is highlighted.

安全联盟 虚接口 IKE安全提议 IKE对等体 **IPSec安全提议** IPSec安全策略

安全提议

安全提议的配置修改后，需要重新启用(先禁用再启用)引用该安全提议的IPSEC安全策略或重新使能IPSec安全策略。

全选 新增 删除 关键字: 名称

新增IPSEC安全提议

安全提议名称: ERG2 (范围:1~31个字符)

安全协议类型: ☐ AH ☒ ESP ☐ AH+ESP

ESP验证算法: MD5

ESP加密算法: 3DES

增加 取消

#配置IPSec安全策略，勾选“启用IPSec功能”，点击“启用”，本地子网配置【192.168.1.0/255.255.255.0】，对端子网配置【192.168.2.0/255.255.255.0】，协商类型选择【IKE协商】，对等体选择【ERG2】，安全提议一选择【ERG2】，PFS配置【DH1】，点击【增加】。

**IPSec安全策略**

**IPSec设置**

☒ 启用IPSec功能

**安全策略**

虚接口、IKE安全提议、IKE对等体和IPSec安全提议的配置都修改完成后，只需要重新启用(先禁用再启用)相关的IPSec安全策略一次或重新启用IPSec功能一次，新的配置就能生效；另外，修改IPSec安全策略的配置也能使新的配置生效。

**新增IPSec安全策略**

安全策略名称: ERG2 (范围:1~16个字符)

是否启用: 启用

本地子网IP/掩码: 192.168.1.0 / 255.255.255.0

对端子网IP/掩码: 192.168.2.0 / 255.255.255.0

协商类型: ☒ IKE协商 ☐ 手动模式

对等体: ERG2

安全提议一: ERG2

安全提议二: 请选择

安全提议三: 请选择

安全提议四: 请选择

PFS: DH1 modp768

生命周期: 28800 秒 (范围:120~604800, 缺省值:28800)

触发模式: 流量触发

增加 取消

#添加静态路由 单击【高级设置】--【路由设置】---【静态路由】 点击【新增】，目的地址填【192.168.2.0】，子网掩码【255.255.255.0】，出接口选择【IPSec0】，点击【增加】。

**静态路由**

**静态路由表**

操作 序号 目的地址 子网掩码 下一跳地址

**新增静态路由列表**

目的地址: 192.168.2.0

子网掩码: 255.255.255.0

下一跳地址:

出接口: ipsec0

描述: (可选, 范围:1~15个字符)

增加 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【123456】，点击【显示高级配置】

修改IPsec 策略

修改IPsec 策略

名称 \* MER (1-63字符)

接口 \* WAN0(GEO)

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【FQDN】配置【MER】，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】

注意：除了上面的配置外还需要在命令行配置 **match remote identity fqdn ERG2** 否则无法建立。



修改IPsec 策略

高级配置

IKE配置

IPsec配置

协商模式

野蛮模式

本端身份类型

FQDN

MER

(1-255字符)

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

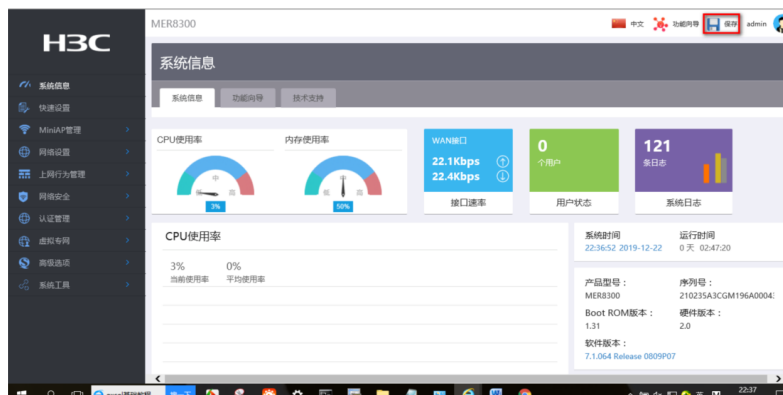
秒 (60-604800, 缺省值为86400)

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。然后点击【返回基本配置】，再点击【确定】

### 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ERG2下面的终端ping对端MER的内网电脑的地址触发隧道

```
C:\Users\<redacted>>ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
请求超时。
来自 192.168.2.1 的回复: 字节=32 时间=2ms TTL=254
来自 192.168.2.1 的回复: 字节=32 时间=2ms TTL=254
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=254

192.168.2.1 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 = 1ms, 最长 = 2ms, 平均 = 1ms
```

#在ERG2上面看到的安全联盟

安全联盟SA

通过安全联盟SA，IPSec能够对不同的数据流提供不同级别的安全保护。在这里可以查询到相应隧道当前状态，了解隧道建立的各个参数。

刷新

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
ERG2	in	2.2.2.2 =>1.1.1.1	....	....	0x6611ed51	3DES_MD5	192.168.2.0/24 =>192.168.1.0/24
ERG2	out	1.1.1.1 =>2.2.2.2	....	....	0xa1f59e4a	3DES_MD5	192.168.1.0/24 =>192.168.2.0/24

第 1 页/共 1 页 共 2 条记录 每页 10

#在MER上查看隧道信息

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"/>	MER	Active	WAN0(GE0)	2.2.2.2	1.1.1.1	ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5	