

组网及说明

1 配置需求或说明

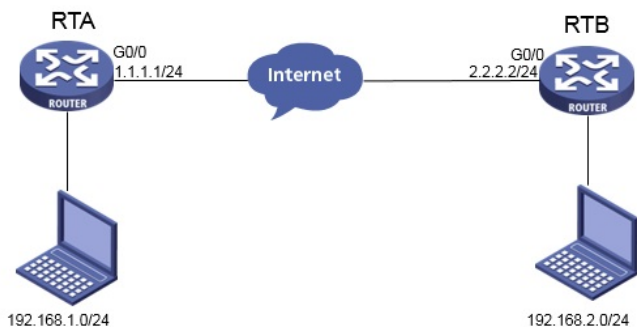
1.1 适用产品系列

本案例适用于MER3220、MER5200、MER8300路由器。

1.2 配置需求及实现的效果

Router A ERG2路由器和Router B 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



配置步骤

2 配置步骤

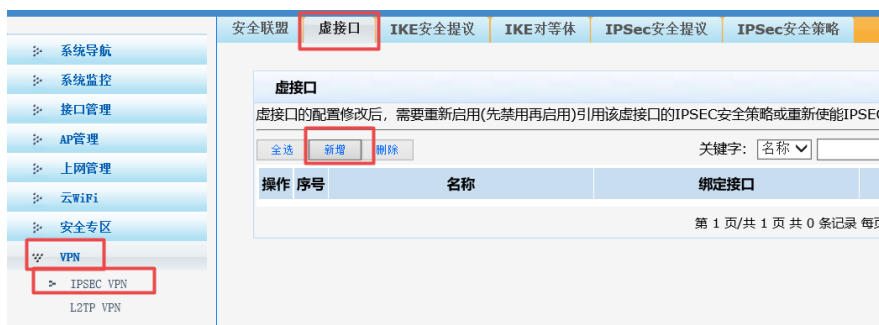
2.1 基本上网配置

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。和ERG2上网案例。

2.2 配置IPSEC VPN

2.2.1 配置ERG2 Router A

单击【VPN】--【IPsec VPN】--【虚接口】，点击【新增】



虚接口名称选择【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。

关键字: 名称

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

#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【DH1】，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，新的配置才能生效。

关键字: 名称

操作	序号	名称	认证算法	加密算法	DH组
	1	ERG2	MD5	3DES	DH1 modp768

第 1 页/共 1 页 共 1 条记录 每页 10 行

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: DH1 modp768

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，新的配置才能生效。

关键字: 名称

操作	序号	名称	认证算法	加密算法	DH组
	1	ERG2	MD5	3DES	DH1 modp768

第 1 页/共 1 页 共 1 条记录 每页 10 行

#配置IKE对等体 点击【新增】，虚接口选择【ipsec0】，对端地址填【2.2.2.2】，协商，模式选择【主模式】，安全提议一选择【ERG2】，预共享密钥填【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功能，新的配置才能生效。

关键字: 名称

操作	序号	名称	虚接口	对端地址	模式	ID类型	安全提议	DPD
	1	ERG2	ipsec0	2.2.2.2	主模式	----	ERG2	关闭

第 1 页/共 1 页 共 1 条记录 每页 10 行

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

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)

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功能，新的配置才能生效。

关键字: 名称

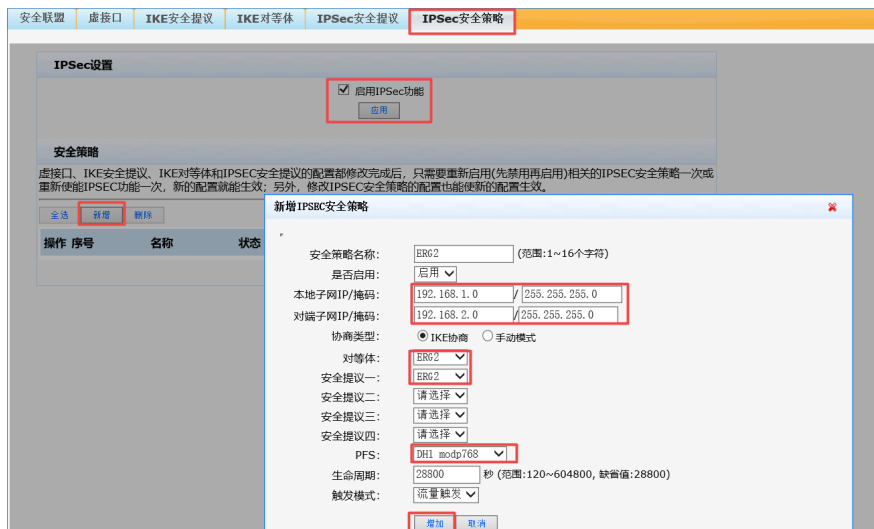
操作	序号	名称	虚接口	对端地址	模式	ID类型	安全提议	DPD
	1	ERG2	ipsec0	2.2.2.2	主模式	----	ERG2	关闭

第 1 页/共 1 页 共 1 条记录 每页 10 行

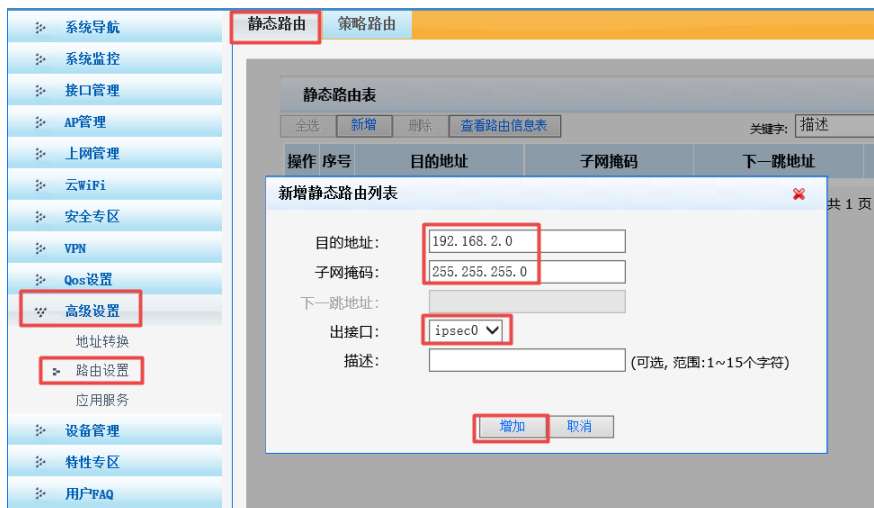
#配置IPSEC安全提议 点击【新增】，安全协议类型选择【ESP】，验证算法选择【MD5】，加密算法选择【3DES】，点击【增加】



#配置IPSEC安全策略本地子网IP填写【192.168.1.0/255.255.255.0】，对端子网IP填写【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选择【DH1】，点击【增加】

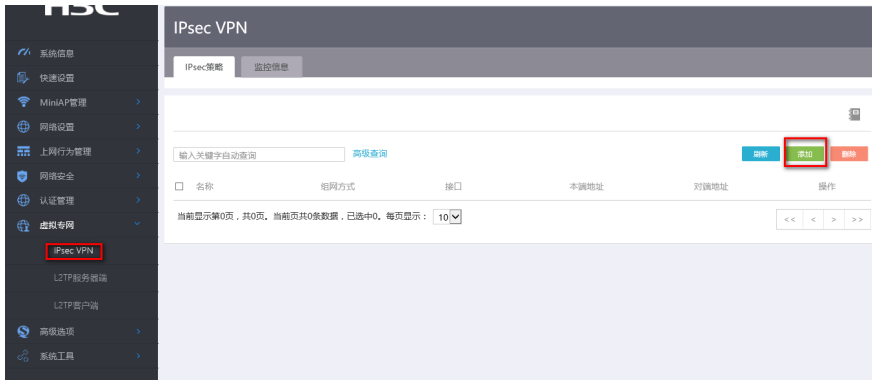


#配置静态路由 选择【高级设置】，选择【路由设置】，静态路由点击【新增】，目的地址填【192.168.2.0】，子网掩码填【255.255.255.0】，出接口选择【ipsec0】

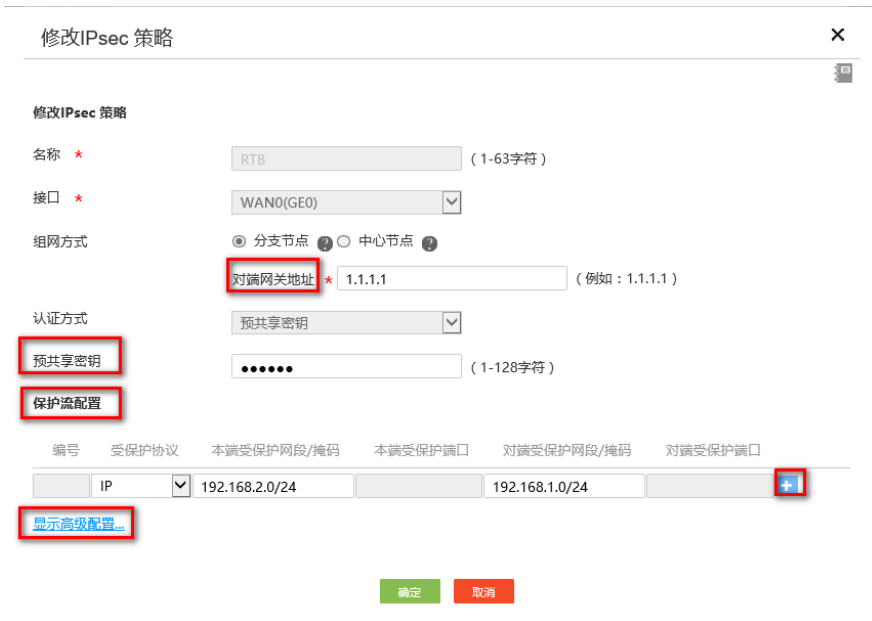


3.2.2 配置MER Router B

#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123456，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。



#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。



#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

安全协议 *

ESP认证算法 *

ESP加密算法 *

封装模式 * 传输模式 隧道模式

PFS

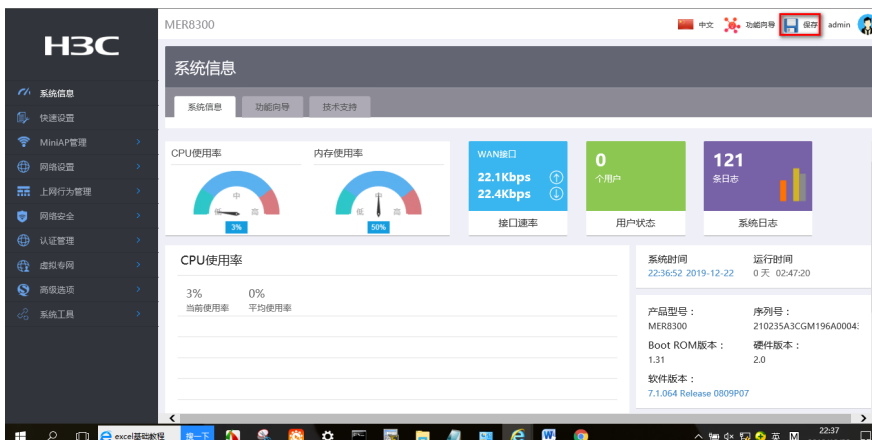
基于时间的SA生存时间 秒 (180-604800, 缺省值为3600)

基于流量的生存时间 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，ERG2默认保存配置



3.4 验证配置结果

#在MER下面的终端ping对端ERG2内网电脑的地址

```
C:\Users\>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=127

192.168.1.1 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
```

#MER可以看到隧道情况

IPsec策略 监控信息

输入关键字自动查询 [高级查询](#) [确定](#) [删除](#)

策略名称	状态	接口	本端地址	对端地址	安全提议	操作
1	Active	WAN0(GE0)	2.2.2.2	1.1.1.1	ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5	删除

#ERG2看到的隧道情况

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	out	1.1.1.1 =>2.2.2.2	----	----	0xd0b620e5	3DES_MD5	192.168.1.0/24 =>192.168.2.0/24
ERG2	in	2.2.2.2 =>1.1.1.1	----	----	0x9317b1d0	3DES_MD5	192.168.2.0/24 =>192.168.1.0/24

配置关键点