

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 （主模式 WEB版）

目录

[MSR系列路由器 IPSEC VPN配置（主模式 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

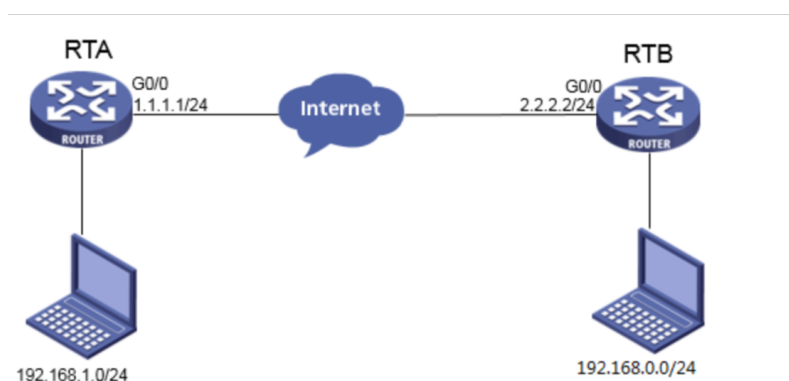
1.1 适用产品系列

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192.168.0.0/24。

添加IPsec 策略

名称 *

tov7

(1-63字符)

接口 *

GigabitEthernet0/0

组网方式

点到点

点到多点

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)

ACL *

3000

+

(3000-3999)

该参数必须配置。

[显示高级配置...](#)

确定

取消

保护流配置

受保护协议

ip

本端受保护网段/反掩码

192.168.1.0

/

0.0.0.255

本端受保护端口

对端受保护网段/反掩码

192.168.0.0

/

0.0.0.255

对端受保护端口

查询

高级查询

刷新

添加

删除

■	编号	受保护协议	本端受保护网段/反...	本端受保护端口	对端受保护网段/反...	对端受保护端口
■	1	ip	192.168.1.0/0.0.0...		192.168.0.0/0.0.0...	

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：

10 ▼

<< < 1 > >>

返回

ACL *

3000

+

(3000-3999)

[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 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 * 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 是

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



#在命令行配置拒绝感兴趣流ACL 3001和出接口调用ACL 3001

注意：如果设备默认有ipsec no-nat-process enable的命令可以不配置，如果没有，需要配置如下拒绝感兴趣流否则数据不通或者单通。

```
#
acl advanced 3001
 rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
 rule 5 permit ip
#
#
interface GigabitEthernet0/0
 port link-mode route
 description Multiple_Line
 ip address 1.1.1.1 255.255.255.0
 tcp mss 1280
 nat outbound 3001
 ipsec apply policy tov7
#
```

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-A
(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	保护协议	本端受保护网络/掩码	本端保护端口	对端受保护网络/掩码	对端受保护端口
1	IP	192.168.0.0/255.255.255		192.168.1.0/255.255.255	

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

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 *

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。

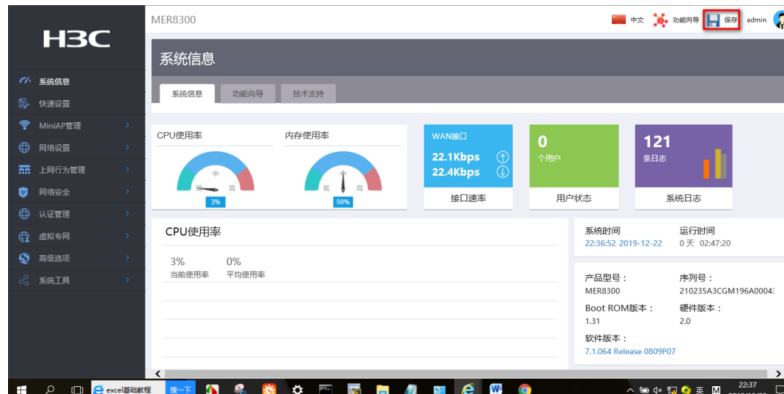
#在命令行配置拒绝感兴趣流ACL 3001和出接口调用ACL 3001

注意：如果设备默认有ipsec no-nat-process enable的命令可以不配置，如果没有，需要配置如下拒绝感兴趣流否则数据不通或者单通。

```
#
acl advanced 3001
 rule 0 deny ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 5 permit ip
#
#
interface GigabitEthernet1/0/0
 port link-mode route
 description single_line1
 combo enable copper
 ip address 2.2.2.2 255.255.255.0
 nat outbound 3001
 ipsec apply policy WAN0
 ipsec no-nat-process enable
#
```

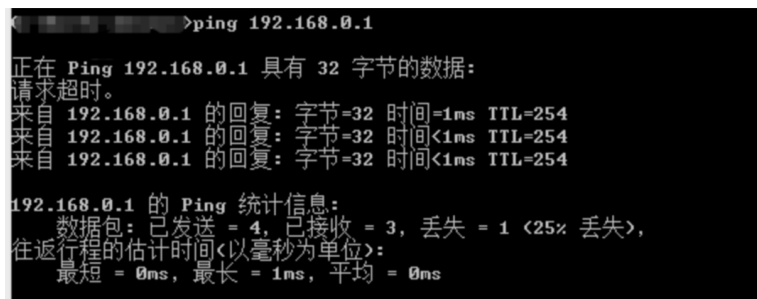
3.3 保存配置

#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



#查看总部IPSec VPN的监控信息

