MSR系列路由器 IPSEC VPN配置（主模式 WEB版）

目录

1 配置需求或说明

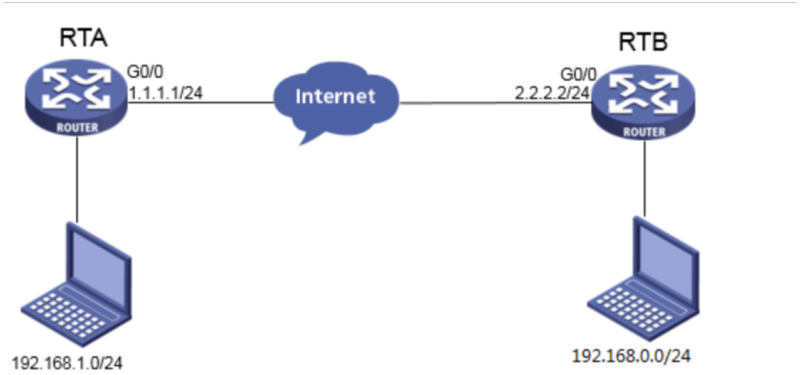
1.1 适用产品系列

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。

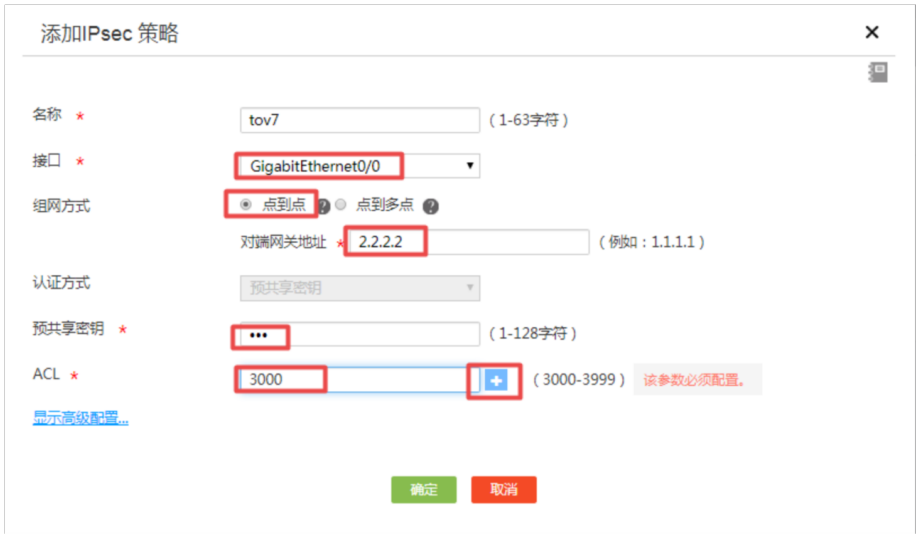
3.2 配置IPSEC VPN

3.2.1 配置Router A

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


H3C
系统信息
快速设置
网络设置
上网行为管理
网络安全
认证管理
虚拟专网
IPsec VPN
L2TP服务器端
L2TP客户端
IPsec VPN
IPsec策略
监控信息
查询
高级查询
刷新
添加
名称
接口
本端地址
对端地址
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
<<
<

#选择点到点，对端网关地址填写对端公网地址，预共享秘钥保证两端一致，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。



#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。

#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

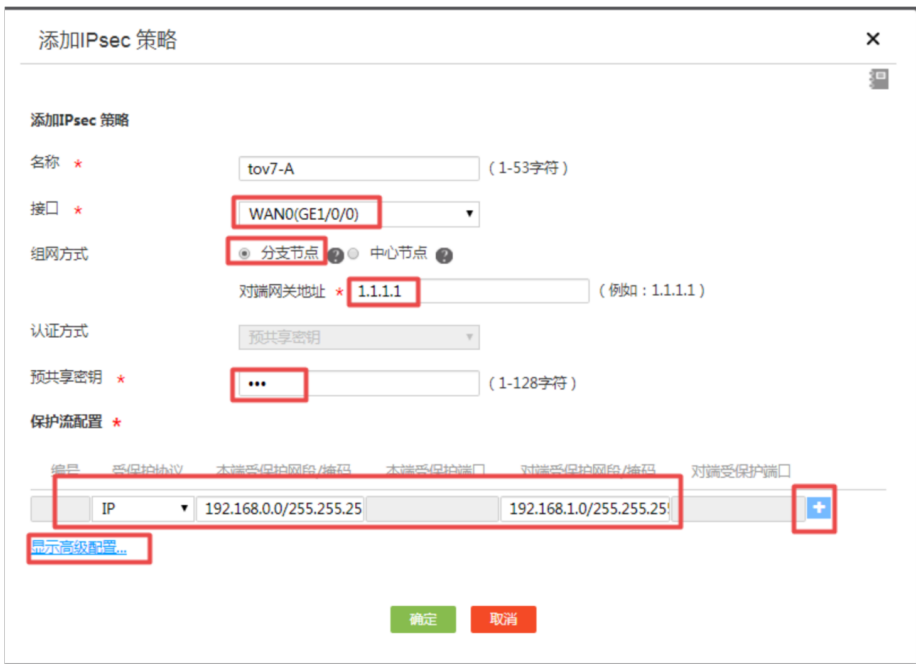
注意：如果设备默认有ipsec no-nat-process enable的命令可以不配置，如果没有，需要配置如下拒绝感兴趣流否则数据不通或者单通。

```
#
acl advanced 3001
 rule 0 deny ip source 192.168.1.0 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，预共享秘钥保证两端一致，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。



#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。

#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

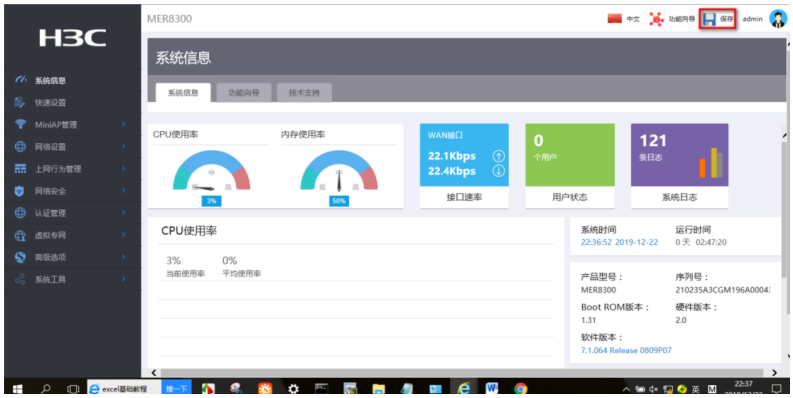
注意：如果设备默认有ipsec no-nat-process enable的命令可以不配置，如果没有，需要配置如下拒绝感兴趣流否则数据不通或者单通。

```
#
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
#
```

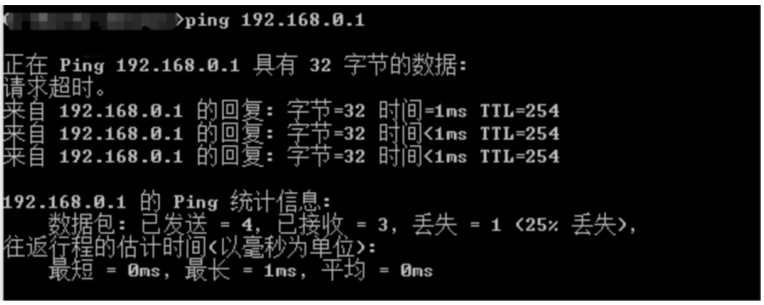
3.3 保存配置

#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