ICG2000/3000/5000系列路由器和ICG2000D/ICG3000F系列路由器对接 IPSEC VPN主模式（WEB）

IPSec VPN　史晓虎　2020-11-07 发表

组网及说明

1 配置需求或说明

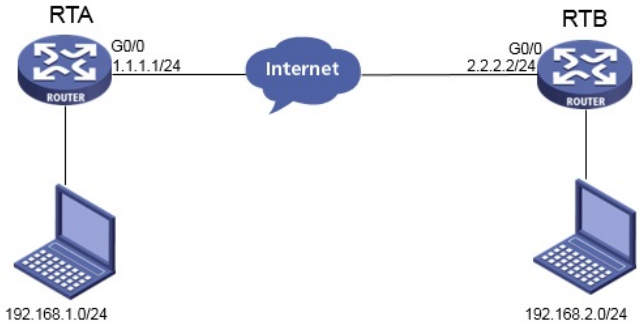
1.1 适用产品系列

本案例适用于如ICG2000、ICG2000B、ICG2000C、ICG2200、ICG3000、ICG3000B、ICG3000D、ICG3000E、ICG5000、ICG5000B等ICG2000、ICG3000、ICG5000系列的路由器。

1.2 配置需求及实现的效果

Router A MSR V5路由器和Router B MSR V7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

3 配置步骤

3.1 基本上网配置

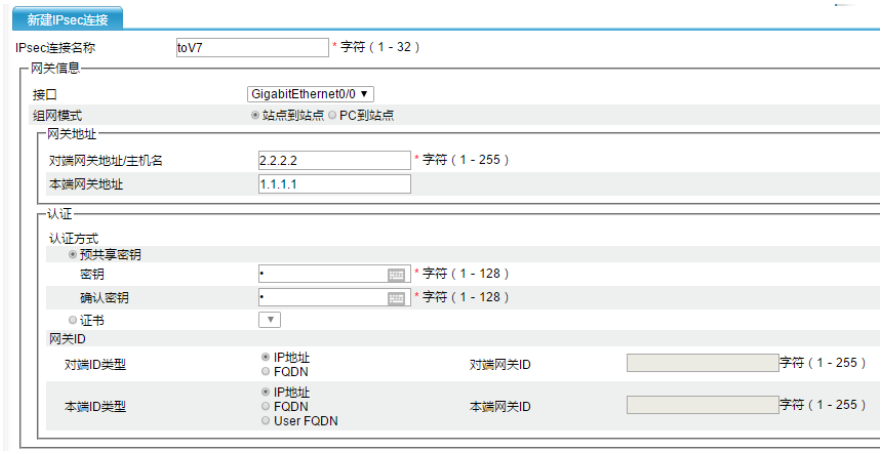
路由器基本上网配置省略，MSR V5路由器的上网具体设置步骤请参考“2.1.2 路由器外网使用固定IP地址上网配置方法”章节中“MSR830[930][2600]系列路由器基本上网（静态IP）命令行配置（V5）”案例，MSR V7路由器的上网具体设置步骤请参考“2.1.2 路由器外网使用固定IP地址上网配置方法”章节中“MSR830-WiNet系列路由器基本上网（静态IP）命令行配置（V7）”案例

3.2 配置IPSEC VPN

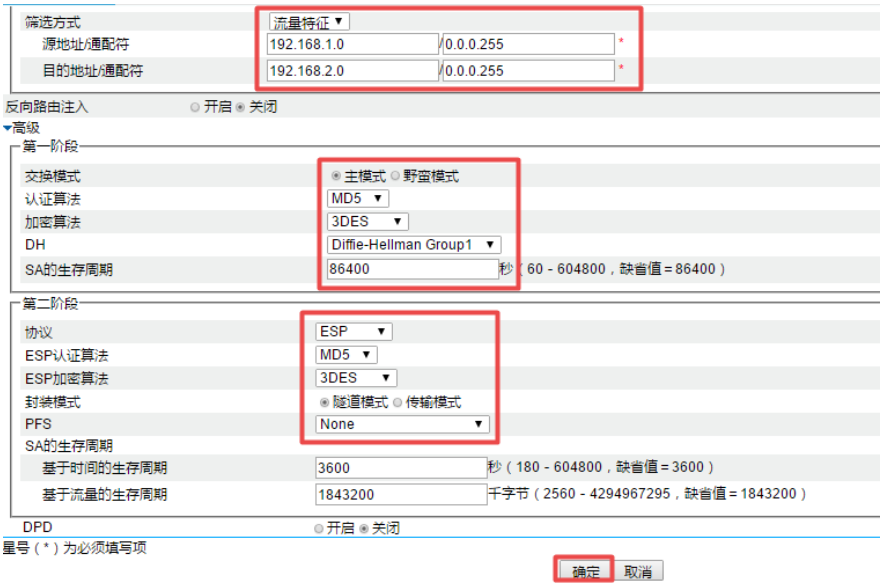
3.2.1 配置MSR V5 Router A

单击【VPN】--【IPsec VPN】，点击【新建】

#接口选择【G0/0】，组网模式选择【站点到站点】，对端网关地址填写【2.2.2.2】，本端网关地址填写【1.1.1.1】，预共享秘钥填写【1】



#筛选方式选择【流量特征】，源地址/通配符填写【192.168.1.0/0.0.0.255】，目的地址/通配符填写【192.168.2.0/0.0.0.255】，第一阶段交换模式选择【主模式】，认证加密算法选择【MD5/3DES】，第二阶段协议选择【ESP】，认证加密算法选择【MD5/3DES】，点击【确定】

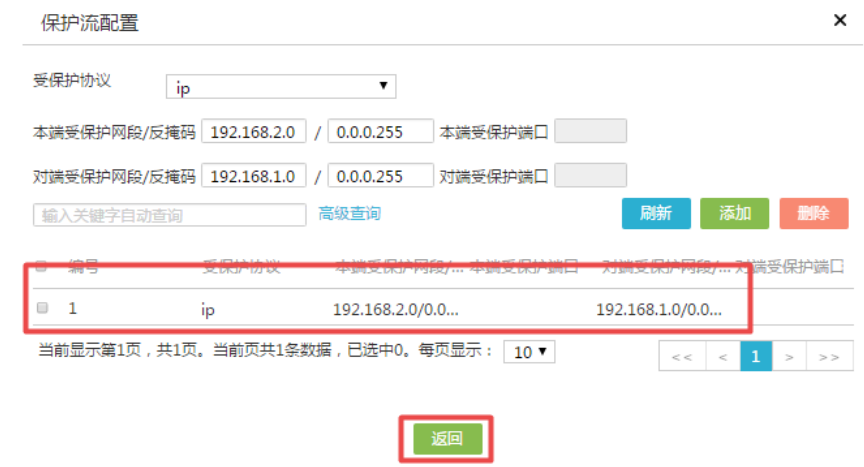


3.2.2. 配置MSR V7 Router B

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

#选择【G0/0】接口，组网方式选择【点到点】对端网关地址填写【1.1.1.1】，预共享秘钥保证两端一致【1】，添加ACL【3000】点击【+】

#添加两端的保护流，协议选择【ip】本端受保护网段【192.168.2.0/0.0.0.255】，对端受保护网段【192.168.1.0/0.0.0.255】，点击【添加】，完成后点击【返回】



#点击【显示高级配置】

#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】，算法组合选择【自定义】，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，算法组合选择【自定义】，安全协议选择【ESP】，认证算法选择【MD5】，加密算法选择【3DES-CBC】，并保证两端算法一致，点击【返回基本配置】

#点击【确定】

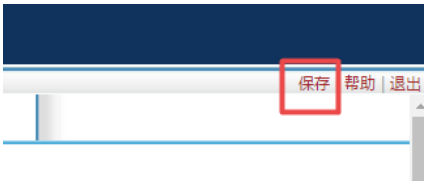
#在设备的命令行添加感兴趣流不做NAT转换的命令，在公网口G0/0调用

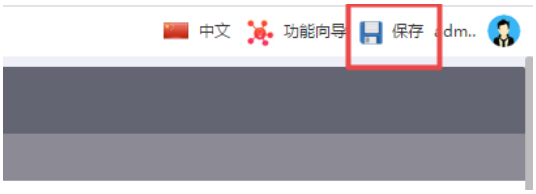
```
#
acl advanced 3001
 rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 5 permit ip
#
#
interface GigabitEthernet0/0
 port link-mode route
 description Multiple_Line
 ip address 2.2.2.2 255.255.255.0
 tcp mss 1280
 nat outbound 3001
 ipsec apply policy TOV5
#
```

注：如果不调用deny数据流的操作会出现单通的情况，V5设备下的终端可以ping通V7下的终端，V7下的终端 ping不通V5下的终端。

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

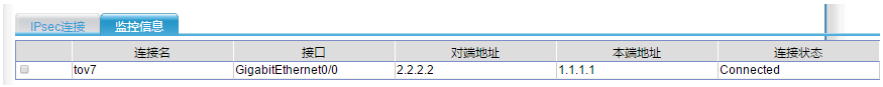
#在MSRV7下面的终端ping对端MSRV5内网电脑的地址

```
C:\Users\lenovo>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
请求超时。
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=254
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=254
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=254
```

#MSR V7可以看到隧道情况

#MSR V5看到的隧道情况



配置关键点