

# MSR2600-XX/3600-51F系列路由器和MSR810/93X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

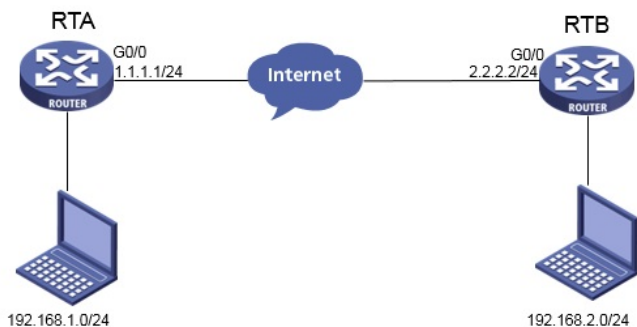
#### 1.1 适用产品系列

本案例适用于如MSR2600-10、MSR2600-17、MSR3600-51F等MSR2600-XX/3600-52F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

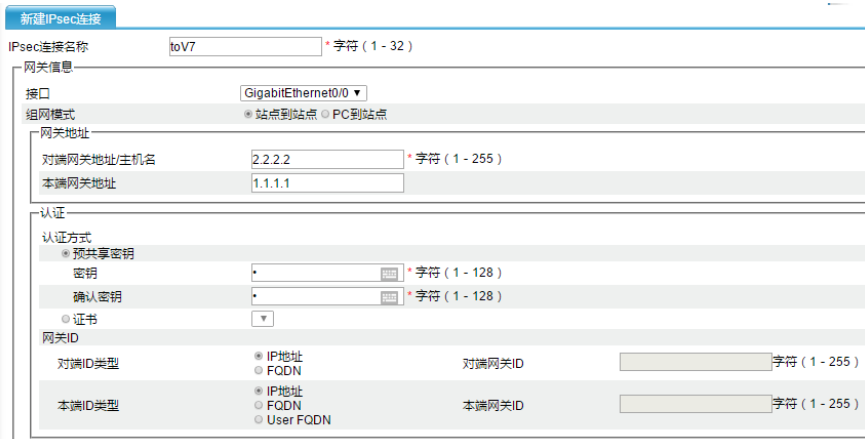
#### 3.2 配置IPSEC VPN

##### 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】，预共享密钥填写【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】，预共享密钥保证两端一致【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】

保护流配置

受保护协议: ip

本端受保护网段/反掩码: 192.168.2.0 / 0.0.0.255

对端受保护网段/反掩码: 192.168.1.0 / 0.0.0.255

高级查询 刷新 添加 删除

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

返回

保护流配置

受保护协议: ip

本端受保护网段/反掩码: 192.168.2.0 / 0.0.0.255

对端受保护网段/反掩码: 192.168.1.0 / 0.0.0.255

高级查询 刷新 添加 删除

编号	受保护协议	本端受保护网段/...	对端受保护网段/...
1	ip	192.168.2.0/0.0...	192.168.1.0/0.0...

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

返回

#点击【显示高级配置】

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【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。

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: 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, 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】

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 \* MD5

ESP加密算法 \* 3DES-CBC

封装模式 \*  传输模式  隧道模式

PFS

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**

#点击【确定】

[显示高级配置...](#)



#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 1000
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

策略名称	状态	接口	本端地址	对端地址	安全提议
TOV5	Active	GigabitEthernet0/0	2.2.2.2	1.1.1.1	ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5

#MSR V5看到的隧道情况

连接名	接口	对端地址	本端地址	连接状态
tov7	GigabitEthernet0/0	2.2.2.2	1.1.1.1	Connected

配置关键点