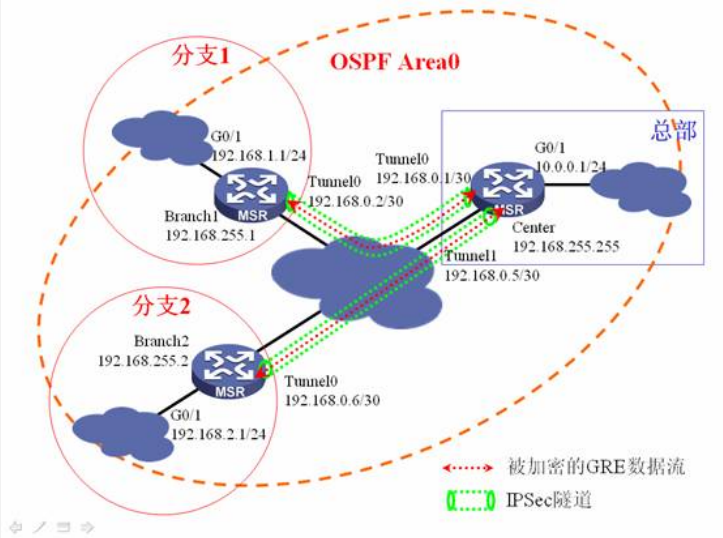
MSR路由器GRE Over IPSec + OSPF功能的配置

丘子隽 2006-12-13 发表

MSR路由器
GRE Over IPSec + OSPF功能的配置

关键词：MSR;GRE;IPSec;IKE;OSPF;VPN;多分支;传输模式

一、**组网需求**:
其中一台MSR作为总部网络的出口路由器，对2个分支提供GRE Over IPSec的接入，另外两台MSR分别是2个企业分支网络的出口路由器，通过GRE Over IPSec方式接入到总部。总部与各个分支在GRE隧道上启动OSPF路由协议，传送总部和分支的各个路由，该配置实际使用较多，即可以运行OSPF等IGP，又能对所有总部与分支之间的流量进行加密，该应用的弊端在于分支之间的流量需要经过总部转发
设备清单：MSR路由器3台
二、组网图:



三、配置步骤:
设备和版本：MSR、Version 5.20, Beta 1202。

Center的配置

```
#
 //OSPF的Router ID
 router id 192.168.255.254
#
//创建与分支1的IKE Peer，可根据实际需要可以采用野蛮模式和NAT穿越
ike peer branch1
 //预共享密钥
 pre-shared-key h3c-msr
 //分支1路由器的地址
 remote-address 1.0.0.1
 //指定本端地址
 local-address 1.0.0.254
#
//建立与分支2的IKE Peer
ike peer branch2
 //预共享密钥
 pre-shared-key h3c-msr

 //分支2路由器的地址
 remote-address 1.0.0.2
 //指定本端地址
 local-address 1.0.0.254
#
//建立IPSec提议
ipsec proposal default
 //这里采用传输模式，也可以使用隧道模式
 encapsulation-mode transport
#
//建立IPSec策略branch，序号10，用于与分支1的GRE连接，使用ISAKMP方式
ipsec policy branch 10 isakmp
 //对匹配ACL 3000的流量使用该策略
 security acl 3000
 //指定所使用的IKE Peer
 ike-peer branch1
 //指定使用的IPSec提议
```

```
 proposal default
#
//建立IPSec策略branch，序号20，用于与分支2的GRE连接，使用ISAKMP方式
ipsec policy branch 20 isakmp
 //对匹配ACL 3001的流量使用该策略
 security acl 3001
 //指定所使用的IKE Peer
 ike-peer branch2
 //指定使用的IPSec提议
 proposal default
#
//ACL 3000，精确匹配总部路由器和分支1路由器的出口地址
acl number 3000
 rule 0 permit ip source 1.0.0.254 0 destination 1.0.0.1 0
//ACL 3001，精确匹配总部路由器和分支2路由器的出口地址
acl number 3001
 rule 0 permit ip source 1.0.0.254 0 destination 1.0.0.2 0
#
//用于Router ID的环回地址
interface LoopBack0
 ip address 192.168.255.254 255.255.255.255
#
//总部外网出口G0/0
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 //总部路由器的出口地址
 ip address 1.0.0.254 255.255.255.0
 //绑定IPSec策略branch
 ipsec policy branch
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 //公司总部内网接口地址
 ip address 10.0.0.1 255.255.255.0
#
//用于与分支1建立GRE连接的隧道接口
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 //指定源地址，注意与ACL 3000吻合
 source GigabitEthernet0/0
 //指定目的地址，注意与ACL 3000吻合
 destination 1.0.0.1
#
//用于与分支2建立GRE连接的隧道接口
interface Tunnel1
 ip address 192.168.0.5 255.255.255.252
 //指定源地址，注意与ACL 3001吻合
 source GigabitEthernet0/0
 //指定目的地址，注意与ACL 3001吻合
 destination 1.0.0.2
#
//OSPF进程1，在AREA 0中使能所有配置公司内网地址的接口，不使能G0/0（总部出口）
ospf 1

 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 192.168.255.254 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.0.4 0.0.0.3
#
```

Branch1配置

```
#
 //OSPF的Router ID
 router id 192.168.255.1
#
//连接总部的IKE Peer，须与总部配置保持一致
ike peer center
 pre-shared-key h3c-msr
 remote-address 1.0.0.254
 local-address 1.0.0.1
#
//IPSec提议，也需要与总部配置一致
ipsec proposal default
 encapsulation-mode transport
#
//IPSec策略center，需要1，使用ISAKMP方式
ipsec policy center 1 isakmp
 //对于匹配ACL 3000的流量使用该策略
 security acl 3000
 //指定IKE Peer
 ike-peer center
 //指定使用的安全提议
 proposal default
#
//ACL 3000，需要与总部路由器的ACL 3000互为镜像
acl number 3000
 rule 0 permit ip source 1.0.0.1 0 destination 1.0.0.254 0
#
//用于Router ID的环回口
interface LoopBack0
 ip address 192.168.255.1 255.255.255.255
#
//分支1外网出接口G0/0
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 //分支1出接口IP地址
 ip address 1.0.0.1 255.255.255.0
 //绑定IPSec策略center
 ipsec policy center
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 //分支1内网地址
 ip address 192.168.1.1 255.255.255.0
#
//用于连接总部的GRE隧道接口
interface Tunnel0
 ip address 192.168.0.2 255.255.255.252
 //指定隧道源地址，注意与ACl 3000吻合
 source GigabitEthernet0/0
 //指定隧道目的地址，注意与ACL 3000吻合
 destination 1.0.0.254
#
//OSPF进程1，在AREA 0使能各个配置私网地址的接口，不使能G0/0（外网出口）
ospf 1
 area 0.0.0.0
  network 192.168.255.1 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.1.0 0.0.0.255
#
```

Branch2配置

```
#
 //OSPF的Router ID
 router id 192.168.255.2
#
//连接总部的IKE Peer，须与总部配置保持一致
ike peer center
 pre-shared-key h3c-msr
 remote-address 1.0.0.254
 local-address 1.0.0.2
#
//IPSec提议，也需要与总部配置一致
ipsec proposal default
 encapsulation-mode transport
#
//IPSec策略center，需要1，使用ISAKMP方式
ipsec policy center 1 isakmp
 //对于匹配ACL 3000的流量使用该策略
 security acl 3000
 //指定IKE Peer
 ike-peer center
 //指定使用的安全提议
 proposal default
#
//ACL 3000，需要与总部路由器的ACL 3001互为镜像
acl number 3000
 rule 0 permit ip source 1.0.0.2 0 destination 1.0.0.254 0
#
//用于Router ID的环回口
interface LoopBack0
 ip address 192.168.255.2 255.255.255.255
#
//分支1外网出接口G0/0
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 //分支1出接口IP地址
 ip address 1.0.0.2 255.255.255.0
 //绑定IPSec策略center
 ipsec policy center
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 //分支1内网地址
 ip address 192.168.2.1 255.255.255.0
#
//用于连接总部的GRE隧道接口
interface Tunnel0
 ip address 192.168.0.6 255.255.255.252
 //指定隧道源地址，注意与ACl 3000吻合
 source GigabitEthernet0/0
 //指定隧道目的地址，注意与ACL 3000吻合
 destination 1.0.0.254
#
//OSPF进程1，在AREA 0使能各个配置私网地址的接口，不使能G0/0（外网出口）
ospf 1
 area 0.0.0.0
  network 192.168.255.2 0.0.0.0
  network 192.168.0.4 0.0.0.3
  network 192.168.2.0 0.0.0.255
#
```

四、**配置关键点**：

1) 总部ACL配置需要注意**不能配置Deny的规则**，否则部分分支可能不能连通；

2) 分支的ACL需要与总部ACl互为镜像；

3) GRE Over IPSec的专门配置可以参考典型配置；

4) 总部的IPSec策略只能创建一个，在不同的序号中指定不同IKE Peer；

5) 所有的IPSec策略都绑定在出接口G0/0，且该接口不能使能OSPF；

6) 保证总部和各分支之间的外网地址可以互通；

7) ACL一定不要最后添加一条deny ip的规则，该配置会导致不需要加密的流量被丢弃。