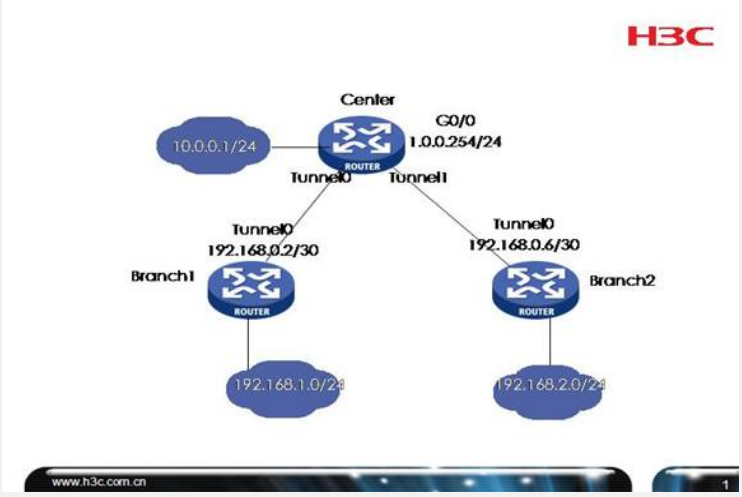
SR6600路由器IPSec over GRE配合OPSF功能的配置

管祥杰 2008-12-11 发表

SR6600路由器
IPSec Over GRE配合OSPF功能的配置

关键词：SR66;GRE;IPSec;IKE;OSPF;VPN;多分支

一、组网需求:
其中一台SR66作为总部网络的出口路由器，对2个分支提供GRE的接入，另外两台SR66分别是2个企业分支网络的出口路由器，通过GRE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，总部和分支在GRE隧道上使用IPSec策略，对特定的流量进行加密，该应相比于GRE Over IPSec + OSPF配置上的不同体现在IPSec配置上；在转发流量上的不同，只对部分流量加密，而不是所有
设备清单：SR6600路由器3台
二、组网图:



三、配置步骤:

Center的配置
//OSPF的Router ID **router id 192.168.255.255** # //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-sr66** //分支1路由器的地址，注意是对端GRE隧道接口的地址 **remote-address 192.168.0.2** //指定本端地址，是本端GRE隧道接口的地址 **local-address 192.168.0.1** # //传建与分支2的IKE Peer **ike peer branch2** //预共享密钥 **pre-shared-key h3c-sr66** //分支2路由器的地址，注意是对端GRE隧道接口的地址 **remote-address 192.168.0.6** //指定本端地址，是本端GRE隧道接口的地址 **local-address 192.168.0.5** # //建立IPSec提议，只能使用隧道模式 **ipsec proposal default** # //建立IPSec策略branch1，序号1，用于与分支1的GRE连接，使用ISAKMP方式 **ipsec policy branch1 1 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branch2，序号1，用于与分支2的GRE连接，使用ISAKMP方式
ipsec policy branch2 1 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，匹配总部内网与分支1内网的流量
acl number 3000
 rule 0 permit ip source 10.0.0.0 0.255.255.255 destination 192.168.1.0 0.0.0.255
//ACL 3001，匹配总部内网与分支2内网的流量
acl number 3001
 rule 0 permit ip source 10.0.0.0 0.255.255.255 destination 192.168.2.0 0.0.0.255
#
//用于Router ID的环回地址
interface LoopBack0
 ip address 192.168.255.255 255.255.255.255
#
//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
#
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
 source GigabitEthernet0/0
 //指定目的地址
 destination 1.0.0.1
//绑定IPSec策略branch1
 ipsec policy branch1
#
//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
 source GigabitEthernet0/0

 //指定目的地址
 destination 1.0.0.2
//绑定IPSec策略branch2
 ipsec policy branch2
#
//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 192.168.255.255 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-sr66
 remote-address 192.168.0.1
 local-address 192.168.0.2
#
//IPSec提议，也需要与总部配置一致
ipsec proposal default
#
//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 192.168.1.0 0.0.0.255 destination 10.0.0.0 0.0.0.255
#
//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
#
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
 source GigabitEthernet0/0
 //指定隧道目的地址
 destination 1.0.0.254
//绑定IPSec策略center
 ipsec policy center
#
//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-sr66
 remote-address 192.168.0.5
 local-address 192.168.0.6
#
//IPSec提议，也需要与总部配置一致
ipsec proposal default
#
//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 192.168.2.0 0.0.0.255 destination 10.0.0.0 0.255.255.255
#
//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
#
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
 source GigabitEthernet0/0
 //指定隧道目的地址
 destination 1.0.0.254
//绑定IPSec策略center
 ipsec policy center
#
//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配置是对特殊的内网流量；

2) 分支的ACL需要与总部ACl互为镜像；

3) IPSce Over GRE的专门配置可以参考典型配置；

4) 总部的IPSec策略要创建多个，且安全提议必须使用隧道模式；

5) 所有的IPSec策略都绑定在对应的GRE接口上；

6) 所有的出接口G0/0都不使能OSPF，且必须保证总部和分支出接口能互通。