MSR IPSEC QOS功能的配置

王继尧 2011-11-18 发表

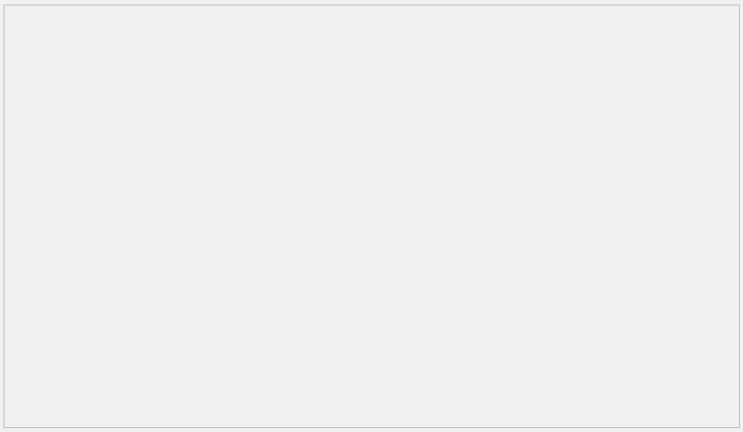
MSR 路由器IPSEC QOS功能的配置

一、 组网需求：

RTA和RTB之间通过2M 链路互相连接，RTA连接一个业务网段192.168.100.1/24，RTB连接一个业务网段192.168.200.1/24,要求2个网段之间的IP流在RTA和RTB之间用IPSec加密传送，在该业务网段有实时业务、生产业务及普通业务三种流量，实时业务为192.168.100.2 <--> 192.168.200.2, 生产业务为192.168.100.3 <--> 192.168.200.3，普通业务为192.168.100.4 <--> 192.168.200.4。在实际应用中，出于业务重要性考虑，要求实时业务保证带宽为0.5M，超过保证带宽报文链路拥塞时丢弃；生产业务保证带宽为1M,超过保证带宽报文链路拥塞时可以和普通业务竞争带宽。普通业务不做带宽保证。

设备清单：MSR系列路由器2台

二、 组网图：



三、 配置步骤：

RTA配置：

```
acl number 3000   //安全ACL
 rule 0 permit ip source 192.168.100.2 0 destination 192.168.200.2 0
 rule 5 permit ip source 192.168.100.3 0 destination 192.168.200.3 0
 rule 10 permit ip source 192.168.100.4 0 destination 192.168.200.4 0
acl number 3001  //实时业务分类ACL
 rule 5 permit ip source 192.168.100.2 0
acl number 3002  //生产业务分类ACL
 rule 0 permit ip source 192.168.100.3 0
#
ike peer r2               //定义IKE对等体
 pre-shared-key simple h3c
 remote-address 200.0.0.2
 local-address 200.0.0.1
#
ipsec proposal r2        //定义ipsec提议
#
ipsec policy r2 10 isakmp  //定义IPSec策略，协商方式为isakmp，即使用IKE协商
 security acl 3000   //定义需要加密传送的ACL
 ike-peer r2        //选择使用的IKE对等体
 proposal r2        //选择安全策略
 qos pre-classify   //配置报文信息预提取功能, 使QoS基于被封装报文的原始IP头信息对报文进行分类
#
traffic classifier 2 operator and  //生产业务流分类
 if-match acl 3002
traffic classifier 1 operator and   //实时业务流分类
 if-match acl 3001
#
```

```
traffic behavior 2        //生产业务流行为
 queue af bandwidth 1000
traffic behavior 1        //实时业务流行为
 queue ef bandwidth 500 cbs 12500
#
qos policy ipsec-qos    //配置QOS策略
 classifier 1 behavior 1
 classifier 2 behavior 2
#
interface GigabitEthernet0/0  //配置RTA连接RTB接口，应用QOS策略及IPSEC策略，配置LR模拟2M带宽
 port link-mode route
 ip address 200.0.0.1 255.255.255.0
 qos lr outbound cir 2000 cbs 125000 ebs 0
 qos apply policy ipsec-qos outbound
 ipsec policy r2
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.100.1 255.255.255.0
#
ip route-static 192.168.200.0 255.255.255.0 200.0.0.2 //配置静态路由，可以使用动态路由代替
RTB配置：
acl number 3000   //安全ACL
 rule 0 permit ip source 192.168.200.2 0 destination 192.168.100.2 0
 rule 5 permit ip source 192.168.200.3 0 destination 192.168.100.3 0
 rule 10 permit ip source 192.168.200.4 0 destination 192.168.100.4 0
acl number 3001  //实时业务分类ACL
 rule 5 permit ip source 192.168.200.2 0
acl number 3002  //生产业务分类ACL
 rule 0 permit ip source 192.168.200.3 0
#
ike peer r1               //定义IKE对等体
 pre-shared-key simple h3c
 remote-address 200.0.0.1
 local-address 200.0.0.2
#
ipsec proposal r1         //定义ipsec提议
#
ipsec policy r1 10 isakmp   //定义IPSec策略，协商方式为isakmp，即使用IKE协商
 security acl 3000   //定义需要加密传送的ACL
 ike-peer r1         //选择使用的IKE对等体
 proposal r1         //选择安全策略
 qos pre-classify   //配置报文信息预提取功能, 使QoS基于被封装报文的原始IP头信息对报文进行分类
#
traffic classifier 2 operator and  //生产业务流分类
 if-match acl 3002
traffic classifier 1 operator and   //实时业务流分类
 if-match acl 3001
#
traffic behavior 2        //生产业务流行为
 queue af bandwidth 1000
traffic behavior 1        //实时业务流行为
 queue ef bandwidth 500 cbs 12500
#
qos policy ipsec-qos    //配置QOS策略
 classifier 1 behavior 1
 classifier 2 behavior 2
#
interface GigabitEthernet0/0  //配置RTB连接RTA接口，应用QOS策略及IPSEC策略，配置LR模拟2M带宽
 port link-mode route
```

```
 ip address 200.0.0.2 255.255.255.0
 qos lr outbound cir 2000 cbs 125000 ebs 0
 qos apply policy ipsec-qos outbound
 ipsec policy r1
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.200.1 255.255.255.0
#
ip route-static 192.168.100.0 255.255.255.0 200.0.0.1 //配置静态路由，可以使用动态路由代替
```

四、 配置关键点：

1）需保证需要加密的数据IP可达；

2）在IPSEC策略视图中需要配置qos pre-classify使能报文信息预提取功能, 使QoS可基于被封装报文的原始IP头信息对报文进行分类；（如果是使用IP优先级进行分类，可以不用使能该命令，因为MSR上IPSEC会自动把原始IP头中的IP优先级复制到外层IP头）

3）在接口上同时使能IPsec和QoS，同一个IPsec安全联盟的数据流如果被QoS分类进入不同队列，会导致部分报文发送乱序。由于IPsec具有防重放功能，IPsec入方向上对于防重放窗口之外的报文会进行丢弃，从而导致丢包现象。因此当IPsec与QoS结合使用时，须保证IPsec分类与QoS分类规则配置保持一致。如果在测试过程中安全ACL必须配置为大的网段，可以在对端MSR系统视图下配置命令undo ipsec anti-replay check关闭防重放功能解决该问题。