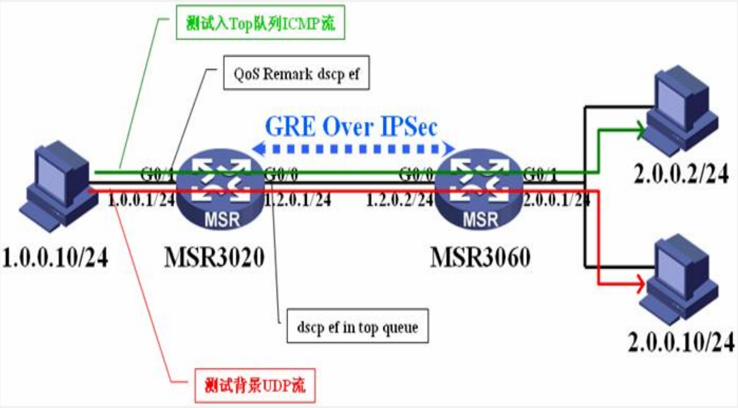
MSR系列路由器对IPSec内不同流量进行QoS保证的解决方案

丘子隽 2007-11-26 发表

MSR系列路由器

对IPSec内不同流量进行QoS保证的解决方案

一、组网:



MSR之间存在运营商的2M物理链路，为了使QoS有效果，在G0/0接口上使用了LR限速2M。

二、需求描述

所有内网之间的流量都要经过GRE Over IPSec的隧道，需要对内网的部分流量进行QoS保证，由于在出接口处内网流量已经被IPSec加密，所以使用源、目的的ACL无法准确识别流量，因此需要通过别的方法。在分析过程中发现不论是GRE封装还是IPSec封装，内层IP头的DSCP等ToS字段都会拷贝到外层IP头相应字段，因此可以通过在内网给数据包Remark DSCP方式对流量进行着色，在外网接口对DSCP着色的IPSec数据流进行QoS操作。

三、配置

MSR3020配置

```
#
 encrypt-card fast-switch
#
 //QoS部分配置，缺省进入Bottom队列，对于DSCP为EF的流进入Top队列
 qos pql 1 default-queue bottom
 qos pql 1 protocol ip acl 3002 queue top
#
ike peer 1.2.0.2
 pre-shared-key h3c
 remote-address 1.2.0.2
 local-address 1.2.0.1
#
ipsec proposal def
#
ipsec policy gos 1 isakmp
 security acl 3000
 ike-peer 1.2.0.2
 proposal def
#
//匹配目的地址2.0.0.2
traffic classifier 2.0.0.2 operator and
 if-match acl 3001
#
//Remark DSCP为EF
traffic behavior myef
 remark dscp ef
#
//定义QoS策略，使目的地址为2.0.0.2的数据流被Remark DSCP EF
qos policy 2002ef
 classifier 2.0.0.2 behavior myef
#
acl number 3000
 rule 0 permit gre source 1.2.0.1 0 destination 1.2.0.2 0
//匹配目的为2.0.0.2/32
acl number 3001
 rule 0 permit ip destination 2.0.0.2 0
//匹配DSCP为EF
acl number 3002 name ef
 rule 0 permit ip dscp ef
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.2.0.1 255.255.255.0
 ipsec policy gos
 //在接口上使能PQ
 qos pq pql 1
 //对接口进行2M限速，使QoS有效果
 qos lr outbound cir 2048 cbs 128000 ebs 0
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 1.0.0.1 255.255.255.0
 //在内网入接口使能MQC，进行DSCP着色
 qos apply policy 2002ef inbound
#
interface Encrypt11/0
 ipsec binding policy gos
#
interface Tunnel0
 ip address 10.0.0.1 255.255.255.252
 source 1.2.0.1
 destination 1.2.0.2
#
 ip route-static 2.0.0.0 255.255.255.0 Tunnel0
#
```

MSR3060配置

```
#
ike peer 1.2.0.1
 pre-shared-key h3c
 remote-address 1.2.0.1
 local-address 1.2.0.2
#
ipsec proposal def
#
ipsec policy gos 1 isakmp
 security acl 3000
 ike-peer 1.2.0.1
 proposal def
#
acl number 3000
 rule 0 permit gre source 1.2.0.2 0 destination 1.2.0.1 0
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.2.0.2 255.255.255.0
 ipsec policy gos
 qos lr outbound cir 2048 cbs 128000 ebs 0
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 2.0.0.1 255.255.255.0
#
interface Tunnel0
 ip address 10.0.0.2 255.255.255.252
 source 1.2.0.2
 destination 1.2.0.1
#
 ip route-static 1.0.0.0 255.255.255.0 Tunnel0
#
```

四、解决方案

1、在内网接口进行DSCP着色

2、在外网接口对DSCP为EF的流进行PQ保证