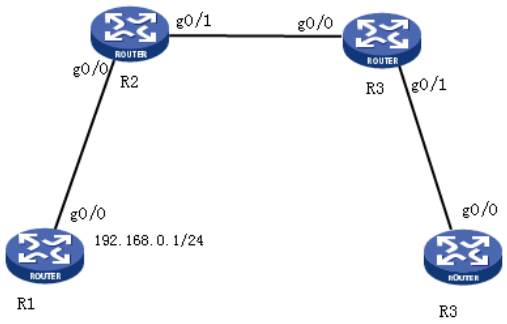
浙江某客户 GRE over IPSEC 配置QOS带宽保障问题经验案例

IPsec QoS 王鑫 2016-01-25 发表

浙江某集团客户，MSR（V7）设备配置GRE over IPSEC，最近一直反馈有5-8个站点的IPSEC生产业务时通时断，表现不太稳定。



图一：现场组网简化图

据现场代理商和客户沟通，了解到IPSEC不通的时候多集中在正常上班时间，下班后业务相对稳定，通过收集诊断信息发现，在正常上班时间，接口流量比较大，而下班以后，接口流量有所缓解，根据此现象，倾向于怀疑出口发生拥塞，导致生产业务的数据被丢弃，造成不通，因此想通过配置QOS的带宽保证，然后观察是否有所改善

R1配置：

```
sysname R1
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
#
 ip route-static 0.0.0.0 0 10.1.1.2
```

R2配置：

```
#
 version 7.1.059, Alpha 7159
#
 sysname R2
#
traffic classifier OA operator and
 if-match acl 3100
#
traffic classifier baozhang operator and
 if-match dscp af41
```

```
#
traffic classifier shengchan operator and
 if-match acl 3200
#
traffic behavior OA
 remark dscp af11
#
traffic behavior baozhang
 queue af bandwidth 7500
#
traffic behavior shengchan
 remark dscp af41
#
qos policy baozhang
 classifier baozhang behavior baozhang
#
qos policy h3c
 classifier OA behavior OA
 classifier shengchan behavior shengchan
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.1.2 255.255.255.0
 qos apply policy h3c inbound
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 speed 10
 ip address 20.1.1.1 255.255.255.0
 qos apply policy baozhang outbound
#
interface GigabitEthernet6/1
 port link-mode route
 combo enable copper
#
interface Tunnel0 mode gre
 ip address 100.1.1.1 255.255.255.0
 source LoopBack0
 destination 3.3.3.3
#
 ip route-static 1.1.1.0 24 10.1.1.1
 ip route-static 3.3.3.0 24 20.1.1.2
 ip route-static 4.4.4.0 24 Tunnel0
#
acl advanced 3000
 rule 0 permit ip source 2.2.2.2 0 destination 3.3.3.3 0
```

#

acl advanced 3100

description OA

rule 0 permit ip source 1.1.1.1 0 destination 4.4.4.1 0

#

acl advanced 3200

description shengchan

rule 0 permit ip source 1.1.1.2 0 destination 4.4.4.2 0

#

ipsec transform-set 1

esp encryption-algorithm 3des-cbc

esp authentication-algorithm md5

#

ipsec policy 1 1 isakmp

transform-set 1

security acl 3000

remote-address 20.1.1.2

qos pre-classify

ike-profile 1

#

ike profile 1

keychain 1

exchange-mode aggressive

match remote identity address 20.1.1.2 255.255.255.255

#

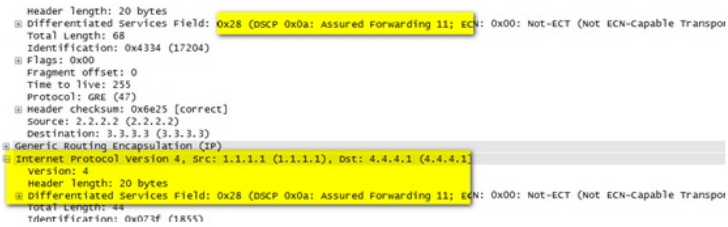
ike keychain 1

pre-shared-key address 20.1.1.2 255.255.255.255 key cipher c3$STYDRRG6K/HIL34vVlqQkBoU uXcOhg==

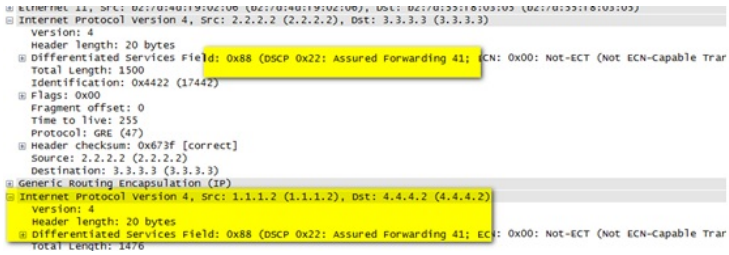
#

R1和R4为对称配置，略！

实验室通过验证，在R2的入接口对数据流标记正常：



图二：OA数据成功标记示例



图三：shengchan数据成功标记示例

现场按照如上方法配置后，问题得到解决，所以此问题是由于正常工作时间，接口拥塞，生成业务被丢弃导致。

1.当在接口上同时应用了IPsec安全策略与QoS策略时，缺省情况下，QoS使用封装后报文的外层IP头

信息来对报文进行分类。但如果希望QoS基于被封装报文的原始IP头信息对报文进行分类，则需要配置QoS预分类功能来实现

2.示例中对OA业务只做了标记，未进行拥塞管理配置，第一是为了验证标记效果；第二对此业务标记，留作后面进行业务改造使用，对当前业务不造成任何影响