某局点SR6608路由器Portal ACL规格问题处理经验案例

ACL Portal 张玺 2014-04-21发表

一、问题现象
某局点客户在SR6608上进行Portal认证配置时，出现以下log提示：
%Feb 13 18:35:13:306 2014 SR6608-1 SHELL/6/SHELL_CMD: -Task=vt0-IPAddr=18.1.251.14-User=h3c; Command is portal free-rule 320 source any destination ip 18.106.62.77 mask 255.255.255.255
%Feb 13 18:35:13:309 2014 SR6608-1 PORTAL/4/PORTAL_ACL_FAILURE: -Slot=2; The number of ACLs on the device has reached the maximum.
%Feb 13 18:35:13:512 2014 SR6608-1 SHELL/6/SHELL_CMD: -Task=vt0-IPAddr=18.1.251.14-User=h3c; Command is portal free-rule 321 source any destination ip 18.106.63.77 mask 255.255.255.255
%Feb 13 18:35:13:515 2014 SR6608-1 PORTAL/4/PORTAL_ACL_FAILURE: -Slot=2; The number of ACLs on the device has reached the maximum.

二、问题分析
从以上故障信息可以初步判断，这是一个与Portal ACL规格相关的问题。
根据客户收集的诊断信息，我们首先查看其中的配置信息，观察客户都做了哪些配置。可见：

1、类似下面的Portal free-rule命令，共配置了200条左右。
portal free-rule 323 source any destination ip 18.106.65.77 mask 255.255.255.255
客户SR6608路由器使用的主控板为RPE-X1，可以支持1024条Portal free-rule，显然该规格可以满足客户需求。
2、客户SR6608路由器下联分支网点较多，所以使用了450个子接口与网点连接。目前已经有近100个子接口启用了Portal。
客户SR6608路由器使用的业务板卡为FIP-210，上面每个物理接口支持1024个子接口，显然该规格可以满足客户需求。
3、客户SR6608路由器配置了6个ACL，每个ACL下面有100个左右的rule。显然SR66的ACL规格也完全可以满足客户需求。

既然以上规格都满足要求，我们把目光投向另一个规格：Portal ACL条数。该规格包括静态rule和动态rule。这个不是指系统视图下配置的ACL num和ACL rule的规格。
Portal ACL条数的规格对RPE+FIP210而言，是20000。
通过客户的配置可以看到，Portal free-rule都是全局的，这些全局的free-rule会下发到启用Portal的每个接口。按照用户的需求（900条Portal free-rule和450个子接口），单单free-rule的Portal ACL（不包含启用Portal后默认生成的ACL以及认证用户动态生成的ACL）就要达到900*450，显然超出了20000的规格。
这样，问题终于得到定位。

三、问题处理方法
这个问题可以通过更改配置解决，方法如下：

客户配置的这些free-rule是针对每个网点的BFD和ATM，每个网点对应两条，450个网点一共900条。只需要在配置Portal free-rule的时候指定接口即可，就可以使Portal ACL的条数从900*450下降到2*450=900。
portal free-rule 0 source int g 0/0.1 ip any destination ip 18.1.90.2 mask 255.255.255.255