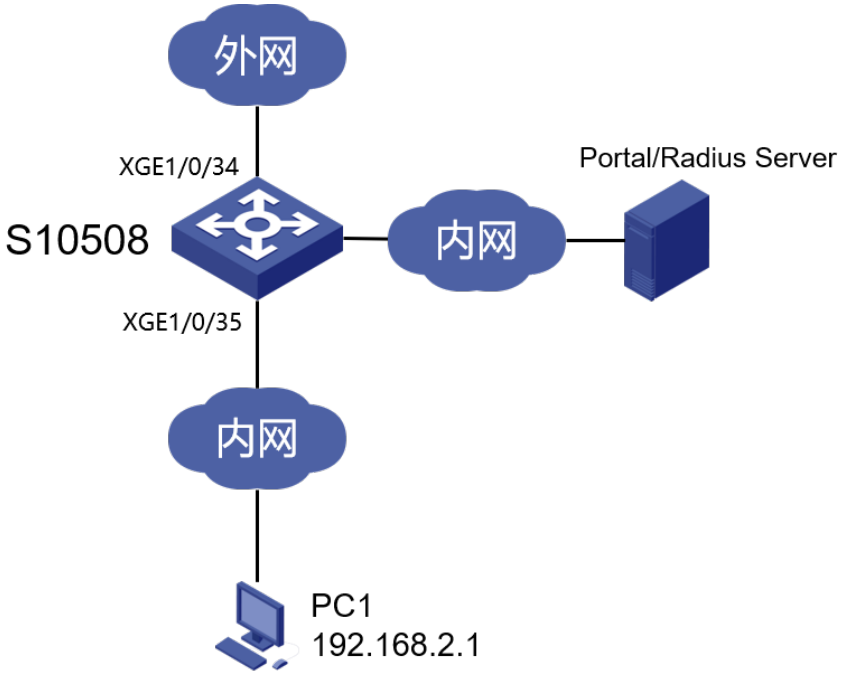
H3C S10508交换机由于Packet-filter策略导致Portal认证不成功问题

丁犁 2018-03-26 发表

S10508交换机作为PC1的网关设备，在该交换机上部署Portal策略，实现内网PC1访问外网时进行Portal准入。
当部署完Portal认证策略后，发现PC1无法重定向认证界面，Portal认证不成功。



观察S10508网关interface vlan 100接口的配置如下：

```
#
interface Vlan-interface100
 ip address 192.168.2.254 255.255.255.0
 packet-filter 3333 inbound
 portal enable method direct
 portal apply web-server newpt
#
acl advanced 3333
 rule 1 permit ip source 192.168.1.1 0
 rule 3 deny ip
#
```

发现，在部署Portal的用户网关接口上，部署了包过滤策略，该策略仅允许源地址为192.168.1.1的流量通过其他流量全部deny。那么是否由于Packet-filter导致PC1用户Portal重定向认证不成功呢？下面就需要检查S10508交换机Packet-filter与Portal策略哪个优先匹配流量了。
在S10508交换机诊断模式下，观察1/0/35 对应的Slot1槽位芯片下发的策略规则：

```
[S10508]probe [S10508-probe]debug qacl show acl-resc slot 1 chip 0 ..... ----------
---------- Pri 10, Group 8,usedEntries 3 ,mode Single, physlice 8/ ==========
========== acl type usedEntries[3] ==========
========== [37 ]Portal Redirect 2 //Portal重定向策略 [39 ]Portal Deny
1 ========== ---------- Pri
11, Group 7,usedEntries 2 ,mode Single, physlice 7/ ==========
====== acl type usedEntries[2] ==========
[100]PktFilter IP on VRF 2//inbound方向的Packet-filter策略 ==========
========== ---------- .....
```

其中Portal Redirect重定向的acl type为[37]；PktFilter IP on VRF包过滤规则的acl type为[100]。
Portal Redirect重定向策略下发到编号为8的physlice中，其优先级Pri为10；
Packet-filter策略下发到编号为7的physlice中，其优先级Pri为11。

对于下发到不同physlice中的策略，设备优先选择Pri优先级高的策略执行（及Pri数值越大越优先）。说明Packet-filter优先与Portal策略。

到此为止，即可确认导致PC Portal重定向认证失败的原因就是Packet-filter导致的。

由于Packet-filter优先与Portal策略，因此需要在ACL 3333中允许认证PC的流量通过，这样才能匹配到Portal策略，问题解决。

```
#
interface Vlan-interface100
 ip address 192.168.2.254 255.255.255.0
 packet-filter 3333 inbound
 portal enable method direct
 portal apply web-server newpt
#
acl advanced 3333
 rule 1 permit ip source 192.168.1.1 0
 rule 2 permit ip source 192.168.2.1 0 //增加
 rule 3 deny ip
#
```

交换机不同physlice之间，若Action动作冲突，则可通过Slice Pri优先级进行判断，Pri优先级数值，越大越优先。