S5016PV5-EI做portal结合radius认证成功后无法上网

Radius Portal **苏亚东** 2022-02-28 发表

组网及说明

PC-(G1/0/7)S5016PV5-EI，设备上int vlan 16配置了portal，对该vlan内接入的终端进行portal认证。

问题描述

交换机结合radius做portal认证，能认证成功，交换机也有portal user信息，但是终端无法上网。
现场部署流统时发现该终端可以正常上网。

过程分析

交换机上display portal user能够看到认证的用户，并且也有下发成功的arp。

```
 ===============display arp all===============
 Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface              Aging Type
10.52.16.68     5405-db14-5f06 16           GE1/0/7                --    R
```

当设备开启portal时，设备默认会下发一条deny的acl，匹配所有该 vlan内的报文；而当终端portal认证通过时，设备上会下发一条portal user用于放通该终端的流量。从收集的信息来看，设备上acl资源充足，并且portal相关的acl、portal user都已经成功下发。

```
-------------------------------------------------------
 Pri  4, usedEntries   10, mode Double
 ----------------------------------------
  acl type                usedEntries[10]
 ----------------------------------------
  [39 ]Portal Free              6
  [40 ]Portal User              1      //终端认证成功后，用于放通流量的acl
  [41 ]Portal Redirect          2
  [42 ]Portal Deny              1   //终端认证前，默认deny所有流量
 ------------------------------------
```

```
========
Acl-Type Portal User, Stage IPCL 0, SinglePort, Installed, Active
Prio Mjr/Sub 0x204/0x5, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 1/24,
Rule Match --------
      Port: 6
      Source mac: 5405-DB14-5F06, FFFF-FFFF-FFFF
      Outer Vlan: 0x10, 0xfff
      Source IP: 10.52.16.68, 255.255.255.255
      IP Type: Any IPv4 packet
Actions --------
      Permit
      Red Permit
      Yel Permit
========
```

经确认，该交换机设备并不是终端的网关，而是作为二层转发设备。当部署流统后，访问对应的地址就可以通信，通过测试，发现实际不通是因为回程的流量被设备deny掉了。内部和研发分析讨论，确认这种二层设备启用portal认证，当访问的回程报文从网关返回时，携带的vlan tag也是vlan 16，能够命中那条默认的portal deny 的底层acl。正常portal认证都是针对内网流量使用的，而针对现场这种二层组网，建议将上行连接网关的端口设置为portal free-rule source interface，不对外网回复的报文进行portal处理。现场配置后终端可以正常访问外网。

```
========
Acl-Type Portal Deny, Stage IPCL 0, Global, Installed, Active
Prio Mjr/Sub 0x204/0x3, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 1/31,
Rule Match --------
      Global range
      Outer Vlan: 0x10, 0xfff    //匹配的外层vlan tag 0x10，换成十进制就是vlan 16
      IP Type: Any IPv4 packet
Actions --------
      Deny
      Account mode  packets,  green and non-green
Accounting: Hi 0, Lo 6377
========
```

解决方法

因此，综合以上排查，可以采用如下方式解决：

1、调整进行portal认证的设备，网关设备对终端进行portal认证；

2、保持当前组网不变的情况下，将该二层交换机和网关设备互连接口设置为portal free-ti source interface，不对网关侧回复的报文进行认证。