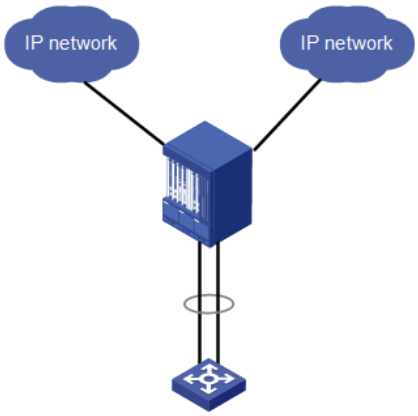
某局点SR8808-X IPoE认证通过后终端无法访问认证服务器的处理经验案例

ipoe 认证 策略路由 **孙轶宁** 2019-07-28 发表

组网及说明

客户用SR8808-X做IPoE认证，共两个出口，不同用户组的用户从不同出口出去。



问题描述

客户反馈在认证通过前能够正常打开认证web页面，且能够正常ping通认证服务器地址，但是认证通过之后，公网能够正常访问，但是发现认证web无法弹出认证通过的页面，并且不能ping通认证服务器地址。

过程分析

1、检查认证通过用户的会话，查看是否下发了什么限制。可以看到下发了user-group以及限速配置，没有下发user-profile

[BRAS]dis ip subscriber session username test1 verbose

Basic:

Description : -
Username : test1
Domain : dm2
VPN instance : N/A
IP address : 172.16.0.2
User address type : N/A
MAC address : 1111-1111-1111
Service-VLAN/Customer-VLAN : -/-
Access interface : GE1/1/4/1
User ID : 0x30000044
VPI/VCI(for ATM) : -/-
VSI Index : -
VSI link ID : -
VXLAN ID : -
DNS servers : 223.5.5.5
114.114.114.114
IPv6 DNS servers : N/A
DHCP lease : 86400 sec
DHCP remain lease : 85127 sec
Access time : Jul 18 15:57:37 2019
Online time(hh:mm:ss) : 00:17:54
Service node : Chassis 1 Slot 1 CPU 0
Authentication type : Web
IPv4 access type : DHCP
IPv4 detect state : Detecting
State : Online

AAA:

ITA policy name : N/A
IP pool : test
IPv6 pool : N/A
Primary DNS server : N/A
Secondary DNS server : N/A

Primary IPv6 DNS server : N/A
Secondary IPv6 DNS server : N/A
Session idle cut : 1800 sec, 1024 bytes, direction:Both
Session duration : 172800000 sec, remaining: 172798925 sec
Traffic quota : Unlimited
Traffic remained : Unlimited
Acct start-fail action : Online
Acct update-fail action : Online
Acct quota-out action : Offline
Dual-stack accounting mode : Merge
Max IPv4 multicast addresses: 4
IPv4 multicast address list : N/A
Max IPv6 multicast addresses: 4
IPv6 multicast address list : N/A
Accounting start time : Jul 18 16:00:55 2019
Redirect URL : N/A

QoS:
User profile : N/A
Session group profile : N/A
User group ACL : a (active)
Inbound CAR : CIR 3145kbps PIR 3145kbps CBS N/A (active)
Outbound CAR : CIR 3145kbps PIR 3145kbps CBS N/A (active)
Inbound user priority : N/A
Outbound user priority : N/A

Flow statistic:
Uplink packets/bytes : 5514/798161
Downlink packets/bytes : 7403/5458022
IPv6 uplink packets/bytes : 0/0
IPv6 downlink packets/bytes : 0/0

2、检查与user-group有关的配置，发现接口下调用了PBR，里面匹配了user-group。

```
policy-based-route policy1 permit node 3
 if-match acl 3000
 apply next-hop 1.1.1.1
#
policy-based-route policy1 permit node 4
 if-match acl 3001
 apply next-hop 2.2.2.2
#
acl advanced 3000
 rule 5 permit ip user-group a
#
acl advanced 3001
 rule 5 permit ip user-group b
```

3、找客户确认了一下，这个PBR就是实现不同用户组的用户从不同出口出去的需求，且终端访问认证服务器的流量会经过88，因此判断是该PBR造成终端无法访问认证服务器：认证前终端不属于这几个user-group，匹配不到PBR，认证通过后终端属于这些user-group，流量匹配到了PBR并转发到公网，导致无法访问认证服务器。

解决方法

原因是接口下调用了PBR，PBR下的ACL匹配user-group，认证前不属于这几个user-group，匹配不到PBR，认证通过后PBR匹配到了流量并转发到公网，导致无法访问认证服务器，因此在PBR写条deny动作的节点拒绝这些内网流量即可解决这个问题。