

知 SR88 IPoe web认证匹配用户组user-group引流到不同公网出口

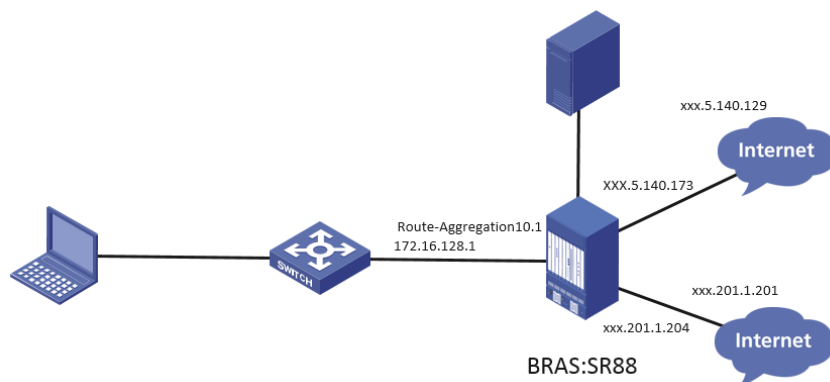
Portal

QoS

郭尧

2021-09-28 发表

组网及说明



SR88在出口做bras，两个公网出口，需要使用内网用户IPOE WEB认证通过后，通过服务器下发不同的用户组，不同用户组的用户走不同的公网口出去

问题描述

现场内网终端IPOE认证通过后，服务器用户组user-group下发成功，通过PBR策略匹配用户组后，引流到不同公网出口，但是无法访问外网，取消PBR后能够访问外网

过程分析

首先查看设备配置及用户组下发情况

IPOE认证部分配置如下：

```
#
traffic classifier 1 operator and
if-match acl 2001
#
traffic classifier 2 operator and
if-match acl 2001
#
traffic classifier permit operator and
if-match acl name permit
#
traffic classifier web_deny operator and
if-match acl name ip
#
traffic classifier web_http operator and
if-match acl name web_http
#
traffic classifier web_https operator and
if-match acl name web_https
#
traffic classifier web_out operator and
if-match acl name web_out
#
traffic classifier web_permit operator and
if-match acl name web_permit
#
traffic behavior 1
redirect slot 2
#
traffic behavior 2
filter permit
free account
#
traffic behavior permit
filter deny
#
traffic behavior web_deny
filter deny
free account
#
traffic behavior web_http
redirect http-to-cpu
#
traffic behavior web_https
redirect https-to-cpu
#
traffic behavior web_out
filter permit
free account
#
traffic behavior web_permit
filter permit
free account
#
qos policy 1
classifier 1 behavior 1
#
qos policy 2
classifier 2 behavior 2
```

```

#
qos policy out
解决方法
classifier web_out behavior web_out
取消调用web_out的CB动作，使流量只匹配PBR策略进行重定向
#
# 如需实现IPOE认证下发不同用户组，不同用户组流量走不同公网口出去，在正常配置完IPOE认证
及用户组相关配置后，建议使用QOS策略匹配对应用户组流量实现重定向
关键配置如下：_http behavior web_http
#classifier web_https behavior web_https
#access-group deny behavior web_deny
#classifier 1 behavior 1
#user-group group2
#interface Route-Aggregation10.1
#ip address 172.20.128.1 255.255.128.0
#rule 5 permit ip source 0.0.0.0 0.0.0.0
#lan-termination broadcast enable
#acl advanced 3000 ip-pool pool_sf
#policy-based user-map group2
#p subscriber l2-connected enable
#classifier 3040 operation and retry 2 interval 30
#p subscriber user-domain dm1
#p subscriber authentication-method web
#p subscriber pre-auth domain dm1
#p subscriber web-auth domain dm2
#classifier 3030
#accounting packet
#drop policy web-global inbound 全局调用QOS放通需要放通的网流量
#qos apply policy out global outbound
#affic behavior 3040
#accounting packet
#drop policy web-global inbound
#rule 5 permit ip source 172.21.255.0 0.0.0.255
#rule 10 permit source 172.16.0.0 0.0.255.255
#qos policy pcy
acl-basic 2001
classifier 2000 behavior 3030
#classifier 2000 behavior 3030
#classifier 3040 behavior 3040
#acl advanced 3000
interface GigabitEthernet2/1/16
#qos apply policy pcy inbound
#acl advanced 3001
rule 5 permit ip source 172.16.129.0 0.0.0.255
#
acl advanced 3003
rule 5 permit ip
#
acl advanced name deny
rule 0 permit ip destination 172.21.255.3 0
rule 1 permit ip destination 172.21.255.4 0
rule 2 permit ip destination 172.21.255.2 0
rule 5 permit ip destination 172.16.128.1 0
#
acl advanced name dns
rule 5 permit ip destination 172.21.255.4 0
#
acl advanced name dns-cmcc
rule 0 permit ip destination xxx.201.4.3 0 user-group cmcc
rule 5 permit ip destination xxx.201.17.2 0 user-group cmcc
#
acl advanced name dns-unicom
rule 0 permit ip destination xxx.7.92.98 0 user-group unicom
rule 5 permit ip destination xxx.5.203.98 0 user-group unicom
#
acl advanced name ip
rule 0 permit ip user-group web
#
acl advanced name permit

```

rule 5 permit ip destination 172.16.0.0 0.0.128.255 user-group cmcc
rule 10 permit ip destination 172.16.0.0 0.0.128.255 user-group unicom