portal与包过滤同时配置时客户端未认证但可以跨三层访问

Portal packet-filter **李欣** 2019-11-28 发表

问题描述

核心交接SVI口起portl配置，下联接入层接口配置packet-filter，发现终端192.168.117.0/24未认证可以跨三层访问其他IP 192.168.3.200，但是无法ping通网关
型号：S7506E-V
版本： version 7.1.045, Release 7184
1、下联接入层接口配置及包过滤引用
interface Ten-GigabitEthernet1/0/0/48
 packet-filter 3000 inbound

acl number 3000
rule 1 permit ip source 192.168.116.2xx 0
rule 2 permit ip source 192.168.116.2xx 0
rule 3 permit ip source 192.168.116.3x 0
rule 4 permit ip source 192.168.116.2x 0
rule 5 permit ip source 192.168.116.3x0
rule 7 permit ip source 192.xx.0 0.0.0.255
rule 8 permit ip source 192.168.116.x 0
rule 9 permit ip destination 192.168.117.x 0 //网关
rule 10 deny ip destination 10.10.x.0 0.0.0.255
rule 20 permit ip
3、客户端网关SVI配置
interface Vlan-interface117
 ip address 192.168.117.x 255.255.255.0
 portal enable method direct
 portal apply web-server xxx

解决方法

包过滤rule20放通所有，优先于portal禁止所有客户端报文通过生效，故未认证可以ping通192.168.3.200;
但访问网关的流量rule9通过后，还需上送cpu处理会被起portal认证默认下发的rule4拒绝，导致ping不通网关

如下1,3,4是起portal后自动下发的规则，rule2是认证通过后下发给设备的
rule1（free-rule）：用户所在的子网、用户所在的VLAN、用户接入的接口表示
rule 2：认证通过后放通客户端源IP的报文
rule3（重定向）：直接认证方式下所有网段的HTTP报文上报CPU处理；二次地址认证方式下用户所在私网网段的HTTP报文上报CPU处理；三层认证方式下配置的认证网段的HTTP报文上报CPU处理。

rule4（丢弃）：Portal认证接口下的所有用户报文不允许通过。

解决方法：
若需要做流量限制，统一下发portal free-rule规则