H3C S75E交换机portal用户带acl上线时无需下发deny any规则的说明

ACL Portal 张磊 2013-10-31 发表

H3C S75E交换机portal用户带acl上线时无需下发deny any规则的说明

一、 组网:

H3C S75E 交换机作为用户pc的网关，在三层虚接口下开启portal 认证，且用户在认证成功后下发安全acl 3100。

关键配置如下

portal server imc ip 10.8.8.8 port 8080 key simple h3c url http://10.8.8.8/portal

#

interface Vlan-interface10

ip address 10.6.6.6 255.255.255.0

portal server imc method direct

#

acl number 3100

description TO_OA_User

rule 0 permit ip destination 10.1.1.0 0.0.0.255

rule 1 permit ip destination 172.16.1.1 0

rule 2 permit ip destination 10.1.1.5 0

rule 3 permit ip destination 10.1.1.6 0

rule 5 permit ip destination 10.1.20.0 0.0.0.255

rule 10 permit ip destination 36.0.0.11 0

rule 15 permit ip destination 10.30.0.0 0.0.255.255

rule 20 permit ip destination 10.1.13.0 0.0.0.255

rule 25 permit ip destination 10.1.3.30 0

rule 100 deny ip

二、 问题描述:

大量用户上线后，随机出现个别pc可以认证成功但是无法访问acl 3100中允许的个别目标网段。

三、 过程分析:

设备上开启portal认证后未经认证的用户是无法上网的，原因是potral 下发了deny ip的acl 。用户上线成功后下发3100 ，此时只需下发permit 的网段就好了，最后的rule 100是不需要下发的（因为开启portal时早已下发）。此处下发acl 3100时，由于用户较多，acl下发较多，导致某些用户上线时acl 3100 下发在不同的slice中，导致rule 0 和rule 100同时生效，因此部分用户的报文因匹配rule 100而被deny 了。

四、 解决方法:

修改acl 3100的内容，删除rule 100 deny ip即可，这样一来不仅可以避免由于下发安全或隔离acl导致正常报文被deny 的问题，而且也可以很大程度上节约设备上硬件acl的消耗。

说明:

1、本文以安全acl 为例，实际当中隔离acl的实现原理也是如此。

2、本文档同样适用于H3C S10500、低端H3C S5500EI H3C S5800等BCM芯片的交换机下发安全或隔离acl的情况。