6520X adcampus下发acl包过滤无法禁用止ssh登录

ADCampus方案 packet-filter SSH 许鹏鹏 2020-03-19 发表

组网及说明

标准adcampus组网，终端--access--leaf--spine

问题描述

leaf设备上有vlan 4094地址是172.16.20.1 和vlan1地址是172.16.11.1，客户希望用户上线后不能ssh这两个地址登录设备。于是在相应的vsi接口下发包过滤，正确下发包过滤后发现还是能ssh上去，怀疑包过滤不生效。

过程分析

包过滤配置是正确的

#

acl number 3011 match-order auto

rule 60 deny ip destination 172.16.20.0 0.0.0.255

rule 70 deny ip destination 172.16.11.0 0.0.0.255

#

#

interface Vsi-interface3501

ip binding vpn-instance lan

ip address 10.12.13.1 255.255.255.0

mac-address 0000-0000-0003

local-proxy-arp enable

packet-filter 3011 inbound

dhcp select relay proxy

dhcp relay information circuit-id vxlan-port

dhcp relay information enable

dhcp relay source-address interface Vsi-interface4094

dhcp relay request-from-tunnel discard

distributed-gateway local

远程现网发现其实包过滤是生效的，vsi下面新上线的用户无法ping通172.16.20.1和172.16.11.1这两个地址，但是为什么新上线的用户还是能ssh这两个地址登录到设备上呢？这是正常现象，因为在overlay网络中，ssh报文的优先级比包过滤的优先级要高，所以这时候即使ADcampus里面用户组间策略默认是禁用了所有端口，也是没有用的。

解决方法

用户可以通过软件acl来禁止相应的用户ssh登录

设置一条acl匹配登录的源ip

Acl number 3001

Rule 0 deny ip source 10.12.13.0 0.0.0.255

Rule 5 permit ip

然后通过ssh server acl 3001全局下调用即可