某局点S7506X包过滤不生效的经验案例

packet-filter 丁佳欣 2022-07-25 发表

组网及说明

null

问题描述

现场在S7506X交换机vlan interface接口上调用packet-filter阻断某网段互访的流量未生效。

过程分析

现场测试终端连接交换机自动获取到ip地址10.10.10.7

dhcp server ip-pool vlan4000

gateway-list 10.10.10.1

network 10.10.10.0 mask 255.255.255.0

调用acl 3999 在int vlan 4000（终端网关）deny 10.10.xx.0到192.168.xx.0的流量。

dis acl 3999

Advanced IPv4 ACL 3999, 4 rules,

ACL's step is 5, start ID is 0

rule 9 deny ip source 192.168.xx.0 0.0.255.255 destination 10.10.xx.0 0.0.0.255

rule 10 deny ip source 10.10.xx.0 0.0.0.255 destination 192.168.xx.0 0.0.255.255

rule 100 permit ip

#

[7506X-Vlan-interface4000]dis this

#

interface Vlan-interface4000

description test

ip address 10.10.10.1 255.255.255.0

packet-filter 3999 inbound

packet-filter 3999 outbound

结果现场测试，终端仍能够ping通目的网段192.168.xx.0的地址，packet-filter阻断的配置并未生效。

查看现场设备acl资源充足：

Interfaces: GE1/0/0/1 to GE1/0/0/24, XGE1/0/0/25 to XGE1/0/0/28 (chassis 1 slot 0)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%
IFP ACL	4096	1024	4	3068	25%
IFP Meter	2048	512	0	1536	25%
IFP Counter	2048	512	0	1536	25%
EFP ACL	1024	0	58	966	5%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Interfaces: GE1/1/0/1 to GE1/1/0/48 (chassis 1 slot 1)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%
IFP ACL	4096	1024	4	3068	25%
IFP Meter	2048	512	0	1536	25%
IFP Counter	2048	512	0	1536	25%
EFP ACL	1024	0	58	966	5%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Interfaces: GE2/0/0/1 to GE2/0/0/24, XGE2/0/0/25 to XGE2/0/0/28 (chassis 2 slot 0)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%
IFP ACL	4096	1024	4	3068	25%
IFP Meter	2048	512	0	1536	25%
IFP Counter	2048	512	0	1536	25%
EFP ACL	1024	0	58	966	5%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Interfaces: GE2/1/0/1 to GE2/1/0/48 (chassis 2 slot 1)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%
IFP ACL	4096	1024	4	3068	25%
IFP Meter	2048	512	0	1536	25%
IFP Counter	2048	512	0	1536	25%
EFP ACL	1024	0	58	966	5%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

-- display transceiver diagnosis interface --

解决方法

ping交换机本地地址无法过滤，是由于设备底层上cpu的ACL规则中下发了permit动作，规则的优先级高，不会再受用户deny规则的影响，所以是正常的现象。

如果一定要过滤到交换机本地的流量，可以考虑配置本地PBR，将cpu发送的报文丢弃，ACL中需要匹配明细的规则，防止对正常的报文产生影响。

对本地报文应用策略

通过本配置，可以将已经配置的策略应用到本地，指导设备本身产生报文的发送。应用策略时，该策略必须已经存在，否则配置将失败。

对本地报文只能应用一个策略。应用新的策略前必须删除本地原来已经应用的策略。

若无特殊需求，建议用户不要对本地报文应用策略。否则，有可能会对本地报文的发送造成不必要的影响（如ping、telnet服务的失效）。

现场再次确认发现终端ping交换机本地目的网段192.168.xx.0的地址能够ping通，如果ping交换机本地其他目的网段192.168.xx.0的终端地址则无法pig通，接口包过滤生效。

表1 对本地报文应用策略

操作	命令	说明
进入系统视图	**system-view**	-
对本地报文应用策略	**ip local policy-based-route** *policy-name*	缺省情况下，对本地报文没有应用策略

```
interface Vlan-interface50
ip address 50.xx.xx.1 255.255.0.0
#
acl number 3999
rule 0 permit icmp source 50.xx.xx.1 0 destination 50.xx.xx.5 0
#
policy-based-route cc permit node 10
if-match acl 3999
apply output-interface NULL0
#
ip local policy-based-route cc
#
```