某局点S10508 packet-filter调用报错的经验案例

VLAN 叶靖 2019-10-30 发表

组网及说明

某局点购买了一台V7版本的交换机S10508设备作为网关设备，现在现场通过在网关接口上调用packet-filter，以实现对流量的控制。

问题描述

某局点购买了一台S10508设备，设备版本为version 7.1.070, Release 7577P06，现在现场通过在网关接口interface vlan-interface1001上调用packet-filter，以实现对流量的限制，但是现在在interface vlan-interface1001接口上调用packet-filter时，设备提示报错，提示应用失败，具体提示报错如下：

```
[      Vlan-interface1001]packet-filter 3999 in
[      Vlan-interface1001]packet-filter 3999 inbound
Failed to apply IPv4 ACL 3999 to the inbound direction of interface Vlan-interface1001 on chassis 1 (slot 0
, 9), chassis 2 (slot 0).
[      Vlan-interface1001]quti
                          ^
```

过程分析

针对packet-fillter调用失败的情况，首先我们需要确认下设备的具体单板情况和配置情况，现场单板信息如下：

==========display device verbose==========

Chassis	Slot	Type	State	Subslot	Soft Ver	Patch Ver
1	0	LSUM2TGS48SG0	Normal	0	S10500-7577P06	None
1	1	NONE	Absent	0	NONE	None
1	2	NONE	Absent	0	NONE	None
1	3	NONE	Absent	0	NONE	None
1	4	LSUM1SUPC0	Master	0	S10500-7577P06	None
1	5	LSUM1SUPC0	Slave	0	S10500-7577P06	None
1	6	NONE	Absent	0	NONE	None
1	7	NONE	Absent	0	NONE	None
1	8	NONE	Absent	0	NONE	None
1	9	LSUM3FWCEA0	Normal	0	S10500-7577P06	None
1	10	NONE	Absent	0	NONE	None
1	11	LSUM1FAB08B0	Normal	0	S10500-7577P06	None
1	12	LSUM1FAB08B0	Normal	0	S10500-7577P06	None
2	0	LSUM2TGS48SG0	Normal	0	S10500-7577P06	None
2	1	NONE	Absent	0	NONE	None
2	2	NONE	Absent	0	NONE	None
2	3	NONE	Absent	0	NONE	None
2	4	LSUM1SUPC0	Master	0	S10500-7577P06	None
2	5	LSUM1SUPC0	Slave	0	S10500-7577P06	None
2	6	NONE	Absent	0	NONE	None
2	7	NONE	Absent	0	NONE	None
2	8	NONE	Absent	0	NONE	None
2	9	NONE	Absent	0	NONE	None
2	10	NONE	Absent	0	NONE	None
2	11	LSUM1FAB08B0	Normal	0	S10500-7577P06	None
2	12	LSUM1FAB08B0	Normal	0	S10500-7577P06	None

现场报错的板卡为LSUM2TGS48SG0和LSUM3FWCEA0板卡，并没有找到有相关限制。

然后查看现场配置如下：

```
#
interface Vlan-interface1001
 description uplink-to-FW-ME60
 ip address 192.168.138.18 255.255.255.240
#
#
acl advanced 3999
 description baoguolv
```

rule 0 permit tcp source object-group 管理地址 destination-port eq www
rule 1 permit tcp source object-group 管理地址 destination-port eq 443
rule 2 permit tcp source object-group 管理地址 destination-port eq 8080
rule 3 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 11201
rule 4 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 11202
rule 5 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 5678
rule 6 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 6379
rule 7 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 1433
rule 8 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 1521
rule 9 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 8099
rule 10 permit tcp destination 10.159.240.64 0.0.0.63 destination-port eq 8087

然后我们一般会怀疑是否为设备的acl资源占用达到上限，导致packet-filter调用失败，于是我们首先查看设备的ACL资源占用情况，
可以通过下面的命令查看ACL资源占用情况：
[SW]probe

[SW-probe]display qos-acl resource
现场通过上面的命令查看结果如下：

```
[SJZXHX-1-probe]display qos-acl resource
Interfaces: XGE1/0/0/1 to XGE1/0/0/48 (chassis 1 slot 0)
-------------------------------------------------------------------------
Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
VFP ACL          1024       512        0          512        50%
IFP ACL          16384      4096       1          12287      25%
IFP Meter        8192       2048       0          6144       25%
IFP Counter      8192       2048       0          6144       25%
EFP ACL          1024       0          0          1024       0%
EFP Meter        512        0          0          512        0%
EFP Counter      512        0          0          512        0%

Interfaces: XGE1/9/0/1 to XGE1/9/0/4 (chassis 1 slot 9)
-------------------------------------------------------------------------
Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
VFP ACL          2048       1536       0          512        75%
IFP ACL          8192       2048       0          6144       25%
IFP Meter        4096       1024       0          3072       25%
IFP Counter      4096       1024       0          3072       25%
EFP ACL          1024       0          0          1024       0%
EFP Meter        512        0          0          512        0%
EFP Counter      512        0          0          512        0%

Interfaces: XGE2/0/0/1 to XGE2/0/0/48 (chassis 2 slot 0)
-------------------------------------------------------------------------
Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
VFP ACL          1024       512        0          512        50%
IFP ACL          16384      4096       1          12287      25%
IFP Meter        8192       2048       0          6144       25%
IFP Counter      8192       2048       0          6144       25%
EFP ACL          1024       0          0          1024       0%
EFP Meter        512        0          0          512        0%
EFP Counter      512        0          0          512        0%
```

可以查看到现场交换机acl资源是足够的。
然后经现场测试，无论是在interface vlan-interface1001还是对应的物理接口上调用都会报错，且调用在outbound方向也是同样的报错。最后，经过大量测试发现，只要将acl 3999中的下面配置删除后就正常，只要ACL中调用object-group 就会出现失败现象。

rule 0 permit tcp source object-group 管理地址 destination-port eq www
rule 1 permit tcp source object-group 管理地址 destination-port eq 443
rule 2 permit tcp source object-group 管理地址 destination-port eq 8080

解决方法

避免在ACL中调用object-group，可以采用匹配网段的形式来进行配置