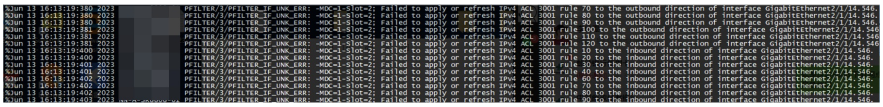
某局点 SR8808HX 子接口包过滤配置下发失败

packet-filter ACL **曾招维** 2023-06-28 发表

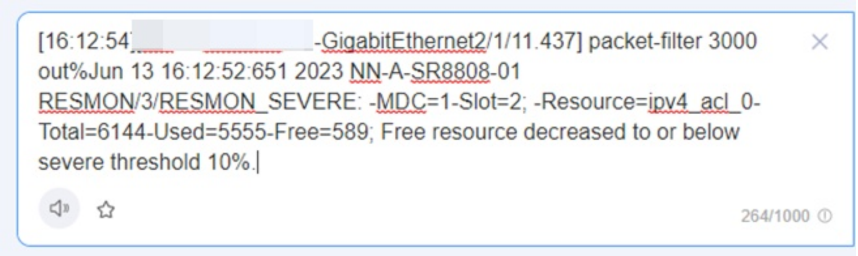
告警信息

子接口包过滤配置下发失败或配置刷新失败：



```
%Jun 13 16:13:19:380 2023 [redacted] PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 70 to the outbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:380 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 80 to the outbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:380 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 90 to the outbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:381 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 100 to the outbound direction of interface GigabitEthernet2/1/14.546
%Jun 13 16:13:19:381 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 110 to the outbound direction of interface GigabitEthernet2/1/14.546
%Jun 13 16:13:19:381 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 120 to the outbound direction of interface GigabitEthernet2/1/14.546
%Jun 13 16:13:19:400 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 10 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:400 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 20 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:401 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 30 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:401 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 40 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:402 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 60 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:402 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 70 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:402 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 80 to the inbound direction of interface GigabitEthernet2/1/14.546.
%Jun 13 16:13:19:403 2023            PFILTER/3/PFILTER_IF_UNK_ERR: -MDC=1-Slot=2; Failed to apply or refresh IPv4 ACL 3001 rule 90 to the inbound direction of interface GigabitEthernet2/1/14.546.
```

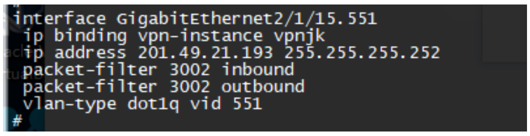
提示资源低于阈值：



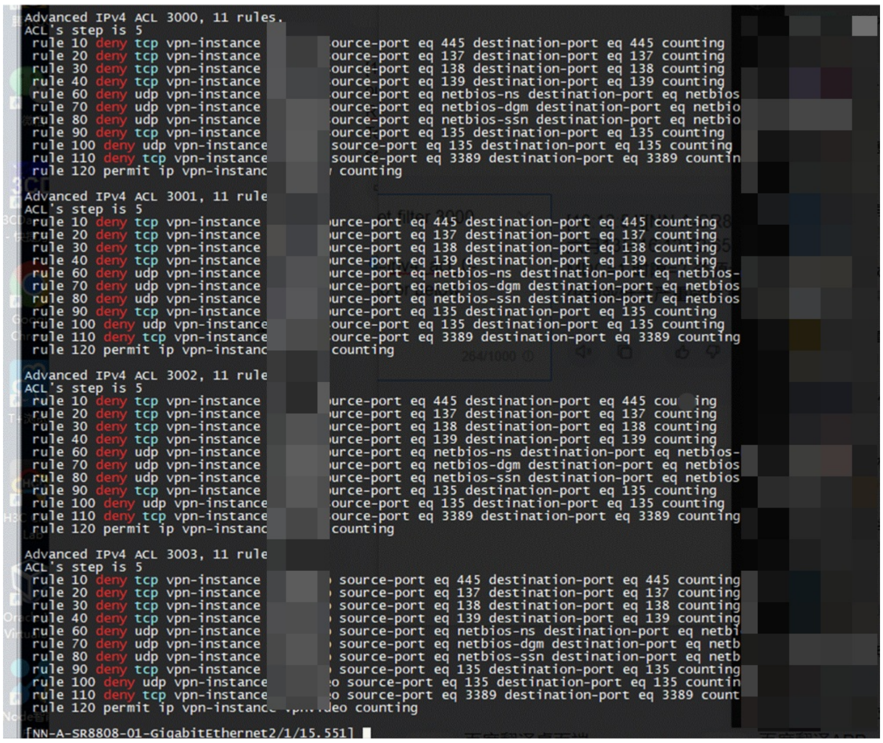
```
[16:12:54[redacted]-GigabitEthernet2/1/11.437] packet-filter 3000
out%Jun 13 16:12:52:651 2023 NN-A-SR8808-01
RESMON/3/RESMON_SEVERE: -MDC=1-Slot=2; -Resource=ipv4_acl_0-
Total=6144-Used=5555-Free=589; Free resource decreased to or below
severe threshold 10%.
```

问题描述

现场开局，使用SR8808HX（Version 7.1.075, Release 8261P29）替换之前的交换机，在大量子接口配置包过滤，提示资源不足、配置下发失败，相关ACL是关闭部分vpn实例相关端口的服务，如下：



```
interface GigabitEthernet2/1/15.551
 ip binding vpn-instance vpnjk
 ip address 201.49.21.193 255.255.255.252
 packet-filter 3002 inbound
 packet-filter 3002 outbound
 vlan-type dot1q vid 551
#
```



```
Advanced IPv4 ACL 3000, 11 rules,
ACL's step is 5
 rule 10 deny tcp vpn-instance [redacted]ource-port eq 445 destination-port eq 445 counting
 rule 20 deny tcp vpn-instance [redacted]ource-port eq 137 destination-port eq 137 counting
 rule 30 deny tcp vpn-instance [redacted]ource-port eq 138 destination-port eq 138 counting
 rule 40 deny tcp vpn-instance [redacted]ource-port eq 139 destination-port eq 139 counting
 rule 60 deny udp vpn-instance [redacted]ource-port eq netbios-ns destination-port eq netbios
 rule 70 deny udp vpn-instance [redacted]ource-port eq netbios-dgm destination-port eq netbio
 rule 80 deny udp vpn-instance [redacted]ource-port eq netbios-ssn destination-port eq netbio
 rule 90 deny tcp vpn-instance [redacted]ource-port eq 135 destination-port eq 135 counting
 rule 100 deny udp vpn-instance [redacted] source-port eq 135 destination-port eq 135 counting
 rule 110 deny tcp vpn-instance [redacted] source-port eq 3389 destination-port eq 3389 countin
 rule 120 permit ip vpn-instanc[redacted] counting

Advanced IPv4 ACL 3001, 11 rule[redacted]
ACL's step is 5
 rule 10 deny tcp vpn-instance [redacted]urce-port eq 445 destination-port eq 445 counting
 rule 20 deny tcp vpn-instance [redacted]urce-port eq 137 destination-port eq 137 counting
 rule 30 deny tcp vpn-instance [redacted]urce-port eq 138 destination-port eq 138 counting
 rule 40 deny tcp vpn-instance [redacted]urce-port eq 139 destination-port eq 139 counting
 rule 60 deny udp vpn-instance [redacted]urce-port eq netbios-ns destination-port eq netbios-
 rule 70 deny udp vpn-instance [redacted]urce-port eq netbios-dgm destination-port eq netbios
 rule 80 deny udp vpn-instance [redacted]urce-port eq netbios-ssn destination-port eq netbios
 rule 90 deny tcp vpn-instance [redacted]urce-port eq 135 destination-port eq 135 counting
 rule 100 deny udp vpn-instance [redacted]ource-port eq 135 destination-port eq 135 counting
 rule 110 deny tcp vpn-instance [redacted]ource-port eq 3389 destination-port eq 3389 counting
 rule 120 permit ip vpn-instanc[redacted] counting

Advanced IPv4 ACL 3002, 11 rule[redacted]
ACL's step is 5
 rule 10 deny tcp vpn-instance [redacted]urce-port eq 445 destination-port eq 445 cou ing
 rule 20 deny tcp vpn-instance [redacted]urce-port eq 137 destination-port eq 137 counting
 rule 30 deny tcp vpn-instance [redacted]urce-port eq 138 destination-port eq 138 counting
 rule 40 deny tcp vpn-instance [redacted]urce-port eq 139 destination-port eq 139 counting
 rule 60 deny udp vpn-instance [redacted]urce-port eq netbios-ns destination-port eq netbios-
 rule 70 deny udp vpn-instance [redacted]urce-port eq netbios-dgm destination-port eq netbios
 rule 80 deny udp vpn-instance [redacted]urce-port eq netbios-ssn destination-port eq netbios
 rule 90 deny tcp vpn-instance [redacted]urce-port eq 135 destination-port eq 135 counting
 rule 100 deny udp vpn-instance [redacted]ource-port eq 135 destination-port eq 135 counting
 rule 110 deny tcp vpn-instance [redacted]ource-port eq 3389 destination-port eq 3389 counting
 rule 120 permit ip vpn-instanc[redacted] counting

Advanced IPv4 ACL 3003, 11 rule[redacted]
ACL's step is 5
 rule 10 deny tcp vpn-instance [redacted] source-port eq 445 destination-port eq 445 counting
 rule 20 deny tcp vpn-instance [redacted] source-port eq 137 destination-port eq 137 counting
 rule 30 deny tcp vpn-instance [redacted] source-port eq 138 destination-port eq 138 counting
 rule 40 deny tcp vpn-instance [redacted] source-port eq 139 destination-port eq 139 counting
 rule 60 deny udp vpn-instance [redacted] source-port eq netbios-ns destination-port eq netbi
 rule 70 deny udp vpn-instance [redacted] source-port eq netbios-dgm destination-port eq netb
 rule 80 deny udp vpn-instance [redacted] source-port eq netbios-ssn destination-port eq netb
 rule 90 deny tcp vpn-instance [redacted] source-port eq 135 destination-port eq 135 counting
 rule 100 deny udp vpn-instance [redacted]o source-port eq 135 destination-port eq 135 countin
 rule 110 deny tcp vpn-instance [redacted]o source-port eq 3389 destination-port eq 3389 count
 rule 120 permit ip vpn-instance [redacted]deo counting

[NN-A-SR8808-01-GigabitEthernet2/1/15.551]
```

过程分析

一般此类问题的解决方向有两个：1、优化ACL配置；2、用高规格板卡。

针对现场现象可从下面几个思路进行ACL配置优化：

1、现场acl的rule规则定义了明细的源端口和目的端口，子接口双向做包过滤，acl相关规格是rule写的越长占用资源越多，所以只定义源端口或者目的端口规则进行包过滤；

2、acl 3000、3001、3003除了vpn实例不同之外，其他信息都一致，若将acl 3000、3001、3003合并直接在主接口上调用包过滤，也可以减少资源占用。

(这里的话其实大家会存在一个疑问，在接口做的包过滤是否会在子接口生效，而且咱们的SR88对于QOS是有限制必须配置在子接口。

SR88的Qos下发在哪?

如果是子接口，不管聚合还是非聚合，均需要下发在子接口。 VLAN虚接口均需要下发在成员端口。)

3、设备支持全局包过滤，设备只对部分端口流量做限制，可大大减少资源占用。

解决方法

现场采用全局包过滤方式实现需求，包过滤配置在子接口正常生效。