7606-X设备下发包过滤失败

ACL 李先福 2019-12-16 发表

组网及说明

无

问题描述

现场反馈在vlan接口下下发包过滤不生效，设备报日志提示包过滤下发失败。

过程分析

看logbuffer，有报acl资源不足。资源不足打印有很多原因，像slice资源不足，acl资源不足，range资源不足，都有可能，要具体情况具体分析。

%Dec 6 15:01:18:203 2019 S7606-X PFILTER/3/PFILTER_IF_NO_RES: -Chassis=1-Slot=2; Failed to apply or refresh IPv4 ACL shi_lian_she rule 546 to the inbound direction of interface Vlan-interface3019. The resources are insufficient.

%Dec 6 15:01:20:351 2019 S7606-X PFILTER/3/PFILTER_IF_NO_RES: -Chassis=1-Slot=0; Failed to apply or refresh IPv4 ACL shi_lian_she rule 546 to the inbound direction of interface Vlan-interface3017. The resources are insufficient.

查看acl资源，发现资源还有剩余。

==== display qos-acl resource ====

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

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%
IFP ACL	4096	1024	1720	1352	66%
IFP Meter	2048	512	0	1536	25%
IFP Counter	2048	512	0	1536	25%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Interfaces: XGE1/2/0/1 to XGE1/2/0/48 (chassis 1 slot 2)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	512	0	512	50%
IFP ACL	4096	1536	1720	840	79%
IFP Meter	2048	768	0	1280	37%
IFP Counter	2048	768	0	1280	37%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

查看客户配置的acl，发现使用了大量的range配置，导致Range资源不足，类似如下匹配端口号范围的的rule下发时，匹配范围不一样，底层会单独占用range资源。

rule 3 permit tcp source 52.48.96.9 0 destination 67.48.0.49 0 destination-port range ftp-data ftp
rule 13 permit udp destination-port range snmp snmptrap
rule 19 permit tcp source 50.0.0.0 0.255.255.255 destination 67.0.0.0 0.255.255.255 destination-port gt 1024
rule 50 permit tcp source 55.67.33.66 0 destination 67.64.1.33 0 destination-port range ftp-data 22
rule 18 deny tcp destination 67.0.0.86 0 source-port range 22 telnet
rule 50 permit tcp source 67.33.0.0 0.0.3.255 destination 55.94.8.0 0.0.0.15 destination-port range 30000 30006
rule 53 permit tcp source 67.33.0.0 0.0.3.255 destination 55.94.8.32 0.0.0.31 destination-port range 9080 9082
rule 69 permit tcp source 67.33.0.0 0.0.3.255 destination 55.66.0.14 0 destination-port range 9080 9081

rule 92 permit tcp destination 67.0.1.50 0 destination-port range 88 288
rule 115 permit tcp source 67.33.0.0 0.0.3.255 destination 55.66.0.32 0 destination-port range 7002 7003
rule 116 permit tcp source 67.33.0.0 0.0.3.255 destination 55.65.8.50 0 destination-port range 7001 7003
rule 138 permit tcp source 67.17.1.0 0.0.0.255 destination 52.48.42.17 0 destination-port range 8083 8084
rule 143 permit tcp source 67.33.2.80 0 destination 67.0.1.71 0 destination-port range 8080 8081
rule 260 permit tcp destination 67.0.1.33 0 destination-port range 51716 51718
rule 285 permit tcp source 67.32.0.0 0.15.255.255 destination 67.64.0.0 0.0.255.255 destination-port range 137 139
rule 328 permit tcp source 67.33.0.0 0.0.255.255 destination 55.66.16.24 0 destination-port range 7011 7027
rule 340 permit tcp source 67.17.1.0 0.0.0.255 destination 55.66.16.29 0 destination-port range 8886 8887
rule 352 permit tcp source 67.33.0.0 0.0.255.255 destination 55.66.8.11 0 destination-port range 8228 8229
rule 418 permit tcp source 67.17.1.0 0.0.0.255 destination 55.64.9.128 0.0.0.63 destination-port range 50001 50002
rule 430 permit tcp source 67.17.1.0 0.0.0.255 destination 55.64.9.128 0.0.0.63 destination-port range 10091 10092
rule 474 permit tcp source 67.17.1.0 0.0.0.255 destination 55.64.0.10 0 destination-port range 5501 5503
rule 499 permit tcp source 67.32.0.0 0.15.255.255 destination 67.64.0.75 0 destination-port range 8081 8082
rule 503 permit tcp source 67.32.0.0 0.15.255.255 destination 67.64.0.72 0.0.0.3 destination-port range 8080 8150
rule 526 permit tcp source 67.32.0.0 0.15.255.255 destination 67.64.6.27 0 destination-port range 11443 11444
rule 532 permit tcp source 67.33.0.0 0.0.255.255 destination 55.66.16.66 0 destination-port range 7001 7027
rule 534 permit tcp source 67.33.0.0 0.0.255.255 destination 55.66.0.88 0 destination-port range 5000 5100
rule 536 permit tcp source 67.33.0.0 0.0.255.255 destination 55.66.0.88 0 destination-port range 7777 9999
rule 546 permit tcp source 67.32.0.0 0.15.255.255 destination 67.64.1.89 0 destination-port range 7070 8888
rule 550 permit tcp source 67.32.0.0 0.15.255.255 destination 55.67.0.8 0 destination-port range 8025 8026
rule 585 permit tcp source 67.64.6.33 0 destination 67.64.1.120 0.0.0.7 destination-port range 2121 60030
rule 8 permit tcp destination 67.0.0.80 0.0.0.3 source-port range 22 telnet

本地设备查看芯片的range资源：
[2074-S7506E-probe]bcm c 1 slot 2 ch 0 dump/FP_RANGE_CHECK
FP_RANGE_CHECK.ipipe0[0]: <UPPER_BOUNDS=0xffff,LOWER_BOUNDS=0x578,FIELD_SELECT=3,ENABLE=1>

FP_RANGE_CHECK.ipipe0[1]:
<UPPER_BOUNDS=0x578,LOWER_BOUNDS=0,FIELD_SELECT=3,ENABLE=1>

FP_RANGE_CHECK.ipipe0[2]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[3]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[4]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[5]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[6]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,EN

ABLE=0>

FP_RANGE_CHECK.ipipe0[7]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,EN
ABLE=0>

FP_RANGE_CHECK.ipipe0[8]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,EN
ABLE=0>

FP_RANGE_CHECK.ipipe0[9]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,EN
ABLE=0>

FP_RANGE_CHECK.ipipe0[10]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[11]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[12]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[13]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[14]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[15]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[16]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[17]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[18]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[19]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[20]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[21]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[22]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[23]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[24]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[25]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[26]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[27]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,E
NABLE=0>

FP_RANGE_CHECK.ipipe0[28]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[29]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[30]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

FP_RANGE_CHECK.ipipe0[31]: <UPPER_BOUNDS=0,LOWER_BOUNDS=0,FIELD_SELECT=0,ENABLE=0>

UPPER_BOUNDS 范围上限值
LOWER_BOUNDS 范围下限值
ENABLE 表项是否使能，ENABLE=1表示已经使用，ENABLE=0表示空闲。
默认使用的两个为IPV4_UCOSPF_TTL占用，将0 - 1400、1400 - 65535的TTL为1的ospf报文以不同的限速速率上送cpu。
FIELD_SELECT 检查的字段选择, 0:L4 Source Port, 1:L4 Destination Port, 2:VLAN_ID, 3:L3_PACKET_LENGTH
L4 Source Port源端口范围相同的占用同一条资源；L4 Destination Port目的端口号范围相同的占用同一条资源。

解决方法

现网acl资源是够的，很多匹配的端口范围很小，建议通过eq方式写成多条rule，减少range资源的占用，效果是一样的。