排除Catalyst 3850交换机上的安全ACL TCAM耗尽故障

目录

简介

本文档介绍Catalyst 3850交换机如何在硬件中实施安全访问控制列表(ACL)，以及如何在各种类型的ACL中使用安全三态内容可寻址存储器(TCAM)。

背景信息

此列表提供了各种类型ACL的定义：

- **VLAN访问控制列表(VACL)**- VACL是应用于VLAN的ACL。它只能应用于VLAN，而不能应用于其他类型的接口。安全边界是允许或拒绝在VLAN之间传输的流量，以及允许或拒绝VLAN内的流量。VLAN ACL在硬件中受支持，对性能没有影响。
- **端口访问控制列表(PACL)**- PACL是应用于第2层交换机端口接口的ACL。安全边界是允许或拒绝VLAN内的流量。PACL在硬件中受支持，对性能没有影响。
- **路由器ACL(RACL)**- RACL是应用于接口的ACL，该接口已分配第3层地址。它可应用于具有IP地址的任何端口，如路由接口、环回接口和VLAN接口。安全边界是允许或拒绝在子网或网络之间传输的流量。RACL在硬件中受支持，对性能没有影响。
- **基于组的ACL(GACL)** - GACL是在ACL的对象组中定义的基于组的ACL。

问题

在Catalyst 3850/3650交换机上，输入PACL和输出PACL访问控制实体(ACE)安装在两个独立的区域/组中。这些区域/银行称为ACL TCAM(TAQ)。VACL输入和输出ACE存储在单个区域(TAQ)中。 由于多普勒硬件限制，VACL不能同时使用两个TAQ。因此，VACL/vlmap的值掩码结果(VMR)空间只有可用于安全ACL的一半。当超过以下任何硬件限制时，会显示以下日志：

```
%ACL_ERRMSG-4-UNLOADED: 1 fed:  Output IPv4 L3 ACL on interface Vl215
for label 19 on asic255 could not be programmed in hardware and traffic will be dropped.

%ACL_ERRMSG-4-UNLOADED: 1 fed:  Output IPv4 L3 ACL on interface Vl216
```

```
for label 20 on asic255 could not be programmed in hardware and traffic will be dropped.

%ACL_ERRMSG-4-UNLOADED: 1 fed:  Output IPv4 L3 ACL on interface Vl218
for label 22 on asic255 could not be programmed in hardware and traffic will be dropped.
```
但是，当这些日志出现时，安全ACE TCAM可能不会显示为已满。

解决方案

假设一个ACE始终使用一个VMR是不正确的。给定ACE可以使用：

- 0个VMR（如果它与以前的ACE合并）。
- 1 VMR（如果VCU位可用于处理范围）。
- 3 VMR（如果由于没有可用的VCU位而扩展）。

Catalyst 3850产品手册建议支持3,000个安全ACL条目。但是，这些规则定义了如何配置这3,000个ACE:

- VACL/vlmap共支持1500个条目，因为它们只能使用两个TAQ中的一个。
- MAC VACL/vlmap需要三个VMR/ACE。这意味着每个方向必须支持460个ACE。
- IPv4 VACL/vlmap需要两个VMR/ACE。这意味着每个方向必须支持690个ACE。
- IPv4 PACL、RACL和GACL需要一个VMR/ACE。这意味着每个方向必须支持1,380个ACE。
- MAC PACL、RACL和GACL需要两个VMR/ACE。这意味着每个方向必须支持690个ACE。
- IPv6 PACL、RACL和GACL需要两个VMR/ACE。这意味着每个方向必须支持690个ACE。

排除Catalyst 3850交换机上的安全ACL TCAM故障

- 检查安全TCAM利用率：

  注意：尽管安装的安全ACE少于3,072个，但可能已达到前面提到的限制之一。例如，如果客户在输入方向应用了大多数RACL，则他们可以使用1,380个可用于入站RACL的条目。但是，TCAM耗尽日志可能会显示，然后才会使用所有3,072个条目。

```
3850#show platform tcam utilization asic all
CAM Utilization for ASIC# 0
 Table                                              Max Values        Used Values
 ------------------------------------------------------------------------------
 Unicast MAC addresses                              32768/512          85/22
 Directly or indirectly connected routes            32768/7680        125/127
 IGMP and Multicast groups                          8192/512           0/16
 QoS Access Control Entries                         3072                68
 Security Access Control Entries                    3072               1648
 Netflow ACEs                                       1024                15
 Input Microflow policer ACEs                        256                 7
 Output Microflow policer ACEs                       256                 7
 Flow SPAN ACEs                                      256                13
 Control Plane Entries                               512               195
 Policy Based Routing ACEs                          1024                 9
 Tunnels                                             256                12
 Input Security Associations                         256                 4
 Output Security Associations and Policies           256                 9
 SGT_DGT                                            4096/512           0/0
 CLIENT_LE                                          4096/64            0/0
 INPUT_GROUP_LE                                     6144                 0
 OUTPUT_GROUP_LE                                    6144                 0
```

- 检查TCAM中安装的ACL的硬件状态：

```
3850#show platform acl info acltype ?
  all   Acl type
 ipv4  Acl type
 ipv6  Acl type
 mac   Acl type

3850#show platform acl info acltype all
############################################################
#########                                ##################
#########                                ##################
########      Printing ACL Infos        ##################
#########                                ##################
############################################################
==================================
IPv4 ACL: Guest-ACL
     aclinfo: 0x52c41030
     ASIC255 Input L3 labels:  4
ipv4 Acl: Guest-ACL Version 16 Use Count 0  Clients 0x0
       10 permit udp any 8 host 224.0.0.2 eq 1985
       20 permit udp any 8 any eq bootps
       30 permit ip 10.100.176.0 255.255.255.0 any
<snip>

3850#show platform acl info switch 1
############################################################
#########                                ##################
#########                                ##################
########      Printing ACL Infos        ##################
#########                                ##################
############################################################
==================================
IPv4 ACL: Guest-ACL
     aclinfo: 0x52c41030
     ASIC255 Input L3 labels:  4
ipv4 Acl: Guest-ACL Version 16 Use Count 0  Clients 0x0
       10 permit udp any 8 host 224.0.0.2 eq 1985
       20 permit udp any 8 any eq bootps
       30 permit ip 10.100.176.0 255.255.255.0 any
 <snip>
```

- 在安装/删除ACL时检查acl-event logs:

```
3850#show mgmt-infra trace messages acl-events switch 1
[04/22/15 21:35:34.877 UTC 3a8 5692] START Input IPv4 L3 label_id 22
asic3 num_les 1 old_unload 0x0, cur_unloaded 0x0, trid 236 num_vmrs 11


[04/22/15 21:35:34.877 UTC 3a9 5692] Trying L3 iif_id 0x104608000000100
input base FID 14

[04/22/15 21:35:34.878 UTC 3aa 5692] Input IPv4 L3 label_id 22 hwlabel
22 asic3 status 0x0 old_unloaded 0x0 cur_unloaded 0x0 trid 236

[04/22/15 21:35:35.939 UTC 3ab 5692] MAC: 0000.0000.0000
Adding Input IPv4 L3 acl [Postage-Printer] BO 0x1 to leinfo le_id 29on asic 255

[04/22/15 21:35:35.939 UTC 3ac 5692] MAC: 0000.0000.0000 Rsvd
label 0 --> New label 23, asic255
```

```
[04/22/15 21:35:35.939 UTC 3ad 5692] START Input IPv4 L3 label_id 23
asic3 num_les 1 old_unload 0x0, cur_unloaded 0x0, trid 237 num_vmrs 5
<snip>
```

- 打印ACL内容可寻址存储器(CAM):

```
C3850-1#show platform acl cam
======== ACL TCAM (asic 0) =========
Printing entries for region ACL_CONTROL (135)
=============================================================
TAQ-4 Index-0 Valid StartF-1 StartA-1 SkipF-0 SkipA-0:
Entry allocated in invalidated state
Mask1 00f00000:00000000:00000000:00000000:00000000:00000000:00000000:00000000
Key1  00400000:00000000:00000000:00000000:00000000:00000000:00000000:00000000
AD    90220000:2f000000

TAQ-4 Index-1 Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 00f00000:0f000000:00000000:00000000:00000000:00000000:00000000:00000000
Key1  00400000:01000000:00000000:00000000:00000000:00000000:00000000:00000000
AD    00a00000:00000000
```

- 打印逐项列出的ACL命中和丢弃计数器：

```
C3850-1#show platform acl counters hardware switch 1
=============================================================
Ingress IPv4 Forward             (280):  397555328725 frames
Ingress IPv4 PACL Drop           (281):         147 frames
Ingress IPv4 VACL Drop           (282):           0 frames
Ingress IPv4 RACL Drop           (283):           0 frames
Ingress IPv4 GACL Drop           (284):           0 frames
Ingress IPv4 RACL Drop and Log   (292):        3567 frames
Ingress IPv4 PACL CPU            (285):           0 frames
Ingress IPv4 VACL CPU            (286):           0 frames
Ingress IPv4 RACL CPU            (287):           0 frames
Ingress IPv4 GACL CPU            (288):           0 frames
```