排除故障安全ACL在Catalyst 3850交换机的TCAM耗尽

目录

简介

本文解释Catalyst 3850交换机如何在硬件方面实现安全访问控制列表(ACL)，并且安全三重内容可编址存储器如何在ACL中的多种类型使用。

背景信息

此列表为ACL的多种类型提供定义：

- **VLAN访问控制列表(VACL)** - VACL是应用对VLAN的ACL。它可能只应用到VLAN和没有其他种接口。安全边界是允许或否决移动在VLAN和permit之间的流量或者否决在VLAN内的流量。硬件方面支持VLAN ACL，并且没有效果在性能。
- **访问控制表波尔特(PACL)** - PACL是ACL应用对Layer2 switchport接口。安全边界是允许或否决在VLAN内的流量。硬件方面支持PACL并且没有效果在性能。
- **路由器ACL (RACL)** - RACL是应用对接口有一第3层地址分配到它的ACL。它可以应用到有一个IP地址例如路由接口、回环接口和VLAN接口的所有端口。安全边界是允许或否决移动在子网或网络之间的流量。硬件方面支持RACL，并且没有效果在性能。
- **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，被输入的PACL和输出PACL访问控制实体(ACE)在两个独立的地区/内存段中安装。这些区域/内存段呼叫ACL TCAMs (TAQs)。VACL输入和输出ACE在单区域(塔格山)存储。由于多谱勒仪硬件限制， VACL不能使用两TAQs。所以， VACL/vlmap只有半值掩码结果(VMR)空间联机对安全ACL。当这些硬件限额中的任一个超过时，这些日志出现：

```
%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.
```
然而，当这些日志出现时，安全ACE TCAM也许不看来全双工。

解决方案

它是不正确假设，一个ACE总是消耗一VMR。给的ACE能消耗：

- 0 VMRs，如果获得合并与上一个ACE。
- 1 VMR，如果VCU位是可用处理范围。
- 3 VMRs，如果它获得展开，因为VCU位不是可用的。

Catalyst 3850数据表或宣传单页建议支持3,000个安全ACL条目。然而，这些规则定义了这3,000 ACE如何可以配置：

- VACL/vlmaps支持总共1.5K条目，他们只能使用一两个TAQs。
- MAC VACL/vlmap需要三个VMR/ACEs。这意味着在每个方向必须支持460 ACE。
- IPv4 VACL/vlmap需要两个VMR/ACEs。这意味着在每个方向必须支持690 ACE。
- IPv4 PACL、RACL和GACL需要一VMR/ACE。这意味着在每个方向必须支持1,380 ACE。
- MAC PACL、RACL和GACL需要两VMR/ACEs。这意味着在每个方向必须支持690 ACE。
- IPv6 PACL、RACL和GACL需要两VMR/ACEs。这意味着在每个方向必须支持690 ACE。

排除故障在Catalyst 3850交换机的安全ACL TCAM

- 检查安全TCAM利用率：

  Note:即使已安装安全ACE少于3,072是，以前被提及的其中一个限额也许已经达到了。例如，如果客户有应用的大多RACL在输入方向，他们能用完1,380个条目可用为入站RACL。然而，在使用前， TCAM耗尽日志能出现全部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
```

- 检查在TCAM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>
```

- 检查ACL事件日志，每当ACL安装/已经删除：

```
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>
```

- 打印出来ACL内容可寻址内存(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
```

- 打印被分条列述的ACL命中数和丢弃计数器：

```
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
```