排除Catalyst 3850交換機上的安全ACL TCAM耗盡故障

目錄

[簡介](#)
[背景資訊](#)
[問題](#)
[解決方案](#)
[Catalyst 3850交換器上的安全ACL TCAM疑難排解](#)

簡介

本檔案將說明Catalyst 3850交換器如何在硬體中實作安全存取控制清單(ACL)，以及在各種型別的ACL中如何使用安全三元內容可定址記憶體(TCAM)。

背景資訊

以下清單提供不同型別ACL的定義：

- **VLAN存取控制清單(VACL)**- VACL是應用於VLAN的ACL。它只能應用於VLAN，不能應用於其他型別的介面。安全邊界是允許或拒絕在VLAN之間移動的流量，以及允許或拒絕VLAN中的流量。硬體支援VLAN ACL，對效能沒有影響。
- **連線埠存取控制清單(PACL)**- PACL是套用到第2層交換器連線埠介面的ACL。安全邊界是允許或拒絕VLAN中的流量。硬體支援PACL，對效能沒有影響。
- **路由器ACL(RACL)**- RACL是應用於介面的ACL，該介面分配有第3層地址。它可以應用於具有IP地址的任何埠，例如路由介面、環回介面和VLAN介面。安全邊界是允許或拒絕在子網或網路之間移動的流量。硬體支援RACL，對效能沒有影響。
- **組型ACL(GACL)-** GACL是在用於ACL的對象組中定[義的組型ACL](#)。

問題

在Catalyst 3850/3650交換器上，輸入PACL和輸出PACL存取控制實體(ACE)安裝在兩個不同的區域/庫中。這些區域/銀行稱為ACL TCAM(TAQ)。VACL輸入和輸出ACE儲存在單個區域(TAQ)中。 由於Doppler硬體限制，VACL不能同時使用兩個TAQ。因此，VACL/vlmap只有值掩碼結果(VMR)空間的一半可用於安全ACL。超出以下任何硬體限制時，系統會顯示以下日誌：

```
%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，當這些日誌出現時，安全ACE TCAM可能未顯示為已滿。

解決方案

假設一個ACE始終消耗一個VMR是不正確的。給定的ACE可以消耗：

- 0個VMR（如果與以前的ACE合併）。
- 1 VMR（如果VCU位可用於處理該範圍）。
- 3個VMR（如果由於沒有VCU位可用而擴展）。

Catalyst 3850產品手冊建議支援3,000個安全ACL專案。但是，以下規則定義了如何配置這3,000個ACE:

- VACL/VLMAP共支援1.5K條目，因為它們只能使用兩個TAQ中的一個。
- MAC VACL/VLMAP需要三個VMR/ACE。這意味著每個方向必須支援460個ACE。
- IPv4 VACL/VLMAP需要兩個VMR/ACE。這意味著每個方向必須支援690個ACE。
- IPv4 PACL、RACL和GACL需要一個VMR/ACE。這意味著每個方向必須支援1,380個ACE。
- MAC PACL、RACL和GACL需要兩個VMR/ACE。這意味著每個方向必須支援690個ACE。
- IPv6 PACL、RACL和GACL需要兩個VMR/ACE。這意味著每個方向必須支援690個ACE。

Catalyst 3850交換器上的安全ACL TCAM疑難排解

- 檢查安全TCAM利用率：

  附註：即使安裝的安全ACE少於3,072個，也可能已經達到前面提到的一個限制。例如，如果客戶在輸入方向應用了大部分RACL，則他們最多可以使用入站RACL的1,380個條目。但是，TCAM耗盡日誌可以在所有3,072個條目被使用之前顯示。

```
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
```

- 檢查TCAM中安裝的ACL的硬體狀態：

```
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>
```

- 每當安裝/刪除ACL時都檢查acl事件日誌：

```
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>
```

- 列印ACL內容可定址儲存器(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
```

- 列印出逐項列出的ACL命中數和丟棄數計數器：

```
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
```