Pesquise defeitos a exaustão de TCAM da segurança ACL em Catalyst 3850 Switch

Índice

[Introdução](#)
[Informações de Apoio](#)
[Problema](#)
[Solução](#)
[Pesquisando defeitos a segurança ACL TCAM em Catalyst 3850 Switch](#)

Introdução

Este documento explica como os Catalyst 3850 Switch executam o Access Control Lists (ACLs) da Segurança no hardware e como o Ternary Content Addressable Memory da Segurança (TCAM) é utilizado entre vários tipos de ACL.

Informações de Apoio

Esta lista fornece definições para vários tipos de ACL:

- **VLAN Access Control List (VACL)** - Um VACL é um ACL que seja aplicado a um VLAN. Pode somente ser aplicado a um VLAN e a nenhum outro tipo de relação. O limite da Segurança é ao tráfego do permit or deny que se move entre VLAN e tráfego do permit or deny dentro de um VLAN. O VLAN ACL é apoiado no hardware, e não tem nenhum efeito no desempenho.
- **Access Control List da porta (PACL)** - Um PACL é um ACL aplicado a uma relação do switchport da camada 2. O limite da Segurança é ao tráfego do permit or deny dentro de um VLAN. O PACL é apoiado no hardware e não tem nenhum efeito no desempenho.
- **Roteador ACL (RACL)** - Um RACL é um ACL que seja aplicado a uma relação que tenha um endereço da camada 3 atribuído a ele. Pode ser aplicado a toda a porta que tiver um endereço IP de Um ou Mais Servidores Cisco ICM NT tal como interfaces roteada, interfaces de loopback, e interfaces de VLAN. O limite da Segurança é ao tráfego do permit or deny que se move entre sub-redes ou redes. O RACL é apoiado no hardware, e não tem nenhum efeito no desempenho.
- **ACL Grupo-baseado (GACL)** - GACL é ACL grupo-baseado definido nos [grupos de objetos para o ACL](#).

Problema

No Switches do catalizador 3850/3650, as entidades entradas do controle de acesso PACL e de saída PACL (ACE) são instaladas em dois regiões/bancos separados. Estes regiões/bancos são

chamados ACL TCAM (TAQs). A entrada e saída ACE VACL é armazenada em uma única região (TAQ). Devido a uma limitação do hardware de Doppler, o VACL não pode usar ambo TAQs. Consequentemente, VACL/vlmap têm somente a metade do espaço do resultado da máscara do valor (VMR) disponível às seguranças ACL. Estes logs aparecem quando qualquens um limites do hardware são excedidos:

```
%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.
```

Contudo, a Segurança ACE TCAM não pôde parecer estar completa quando estes logs aparecem.

Solução

Está incorreta supor que um ACE consome sempre um VMR. Um ACE dado pode consumir:

- 0 VMRs se obtém fundido com um ACE precedente.
- 1 VMR se os bit VCU estão disponíveis para segurar a escala.
- 3 VMRs se obtém expandida porque nenhum bit VCU está disponível.

A folha de dados do catalizador 3850 sugere que 3,000 entradas de segurança ACL estejam apoiadas. Contudo, estas regras definem como estes 3,000 ACE podem ser configurados:

- Apoio VACL/vlmaps um o total das entradas 1.5K como podem usar somente um dos dois TAQs.
- O MAC VACL/vlmap precisa três VMR/ACEs. Isto significa que 460 ACE devem ser apoiados em cada sentido.
- O IPv4 VACL/vlmap precisa dois VMR/ACEs. Isto significa que 690 ACE devem ser apoiados em cada sentido.
- Necessidade uma VMR/ACE do IPv4 PACL, RACL, e GACL. Isto significa que 1,380 ACE devem ser apoiados em cada sentido.
- Necessidade dois VMR/ACEs MAC PACL, RACL, e GACL. Isto significa que 690 ACE devem ser apoiados em cada sentido.
- Necessidade dois VMR/ACEs do IPv6 PACL, RACL, e GACL. Isto significa que 690 ACE devem ser apoiados em cada sentido.

Pesquisando defeitos a segurança ACL TCAM em Catalyst 3850 Switch

- Verifique a utilização de TCAM da Segurança:

  Note: Mesmo que a Segurança instalada ACE fosse menos de 3,072, um dos limites mencionados previamente pôde ter sido alcançado. Por exemplo, se um cliente tem a maioria do rACLs aplicado no sentido da entrada, podem usar-se acima de 1,380 entradas disponíveis para o RACL de entrada. Contudo, os logs da exaustão de TCAM podem aparecer antes que todas as 3,072 entradas estejam usadas.

```
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
```

- Verifique o estado de hardware dos ACL instalado no TCAM:

```
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>
```

- Verifique logs do ACL-evento sempre que os ACL são instalados/removidos:

```
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>
```

- Imprima para fora o Content Addressable Memory ACL (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
```

- Imprima a batida para fora especificada e os contadores de queda ACL:

```
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
```