Identificar e Solucionar Problemas de Esgotamento de TCAM da ACL de Segurança em Switches Catalyst 3850

Contents

Introduction

Este documento explica como os switches Catalyst 3850 implementam as Listas de Controle de Acesso (ACLs - Access Control Lists) de segurança no hardware e como a TCAM (Ternary Content Addressable Memory) de segurança é utilizada entre vários tipos de ACLs.

Informações de Apoio

Esta lista fornece definições para vários tipos de ACLs:

- **VLAN Access Control List (VACL)** - Uma VACL é uma ACL aplicada a uma VLAN. Ele só pode ser aplicado a uma VLAN e nenhum outro tipo de interface. O limite de segurança é permitir ou negar o tráfego que se move entre VLANs e permitir ou negar o tráfego dentro de uma VLAN. A ACL da VLAN é suportada no hardware e não tem efeito no desempenho.
- **Port Access Control List (PACL)** - Uma PACL é uma ACL aplicada a uma interface de porta de switch da Camada 2. O limite de segurança é permitir ou negar o tráfego dentro de uma VLAN. O PACL é suportado no hardware e não tem efeito no desempenho.
- **RACL (Router ACL)** - Uma RACL é uma ACL aplicada a uma interface que tem um endereço de Camada 3 atribuído a ela. Ele pode ser aplicado a qualquer porta que tenha um endereço IP como interfaces roteadas, interfaces de loopback e interfaces VLAN. O limite de segurança é permitir ou negar o tráfego que se move entre sub-redes ou redes. O RACL é suportado no hardware e não tem efeito no desempenho.
- **ACL baseada em grupo (GACL)** - A GACL é uma ACL baseada em grupo definida em [Grupos de objetos para ACL](#).

Problema

Nos switches Catalyst 3850/3650, o PACL de entrada e as ACEs (PACL Access Control Entities,

Entidades de Controle de Acesso) de PACL de saída são instalados em duas regiões/bancos separados. Essas regiões/bancos são chamados de ACL TCAMs (TAQs). As ACEs de entrada e saída da VACL são armazenadas em uma única região (TAQ). Devido a uma limitação de hardware Doppler, a VACL não pode usar ambos os TAQs. Portanto, o VACL/vlmap tem apenas metade do espaço do Resultado da Máscara de Valor (VMR) disponível para ACLs de segurança. Estes registros aparecem quando qualquer um destes limites de hardware é excedido:

```
%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.
```

No entanto, o TCAM de ACE de segurança pode não parecer estar cheio quando esses logs são exibidos.

Solução

Éincorreto supor que uma ECA sempre consome uma VMR. Uma determinada ACE pode consumir:

- 0 VMRs se forem mesclados com uma ACE anterior.
- 1 VMR se os bits da VCU estiverem disponíveis para tratar do intervalo.
- 3 VMRs se ele for expandido porque nenhum bit de VCU está disponível.

A Folha de Dados do Catalyst 3850 sugere que 3.000 entradas de ACL de segurança são suportadas. No entanto, essas regras definem como essas 3.000 ACEs podem ser configuradas:

- VACL/vlmaps suportam um total de 1,5 K entradas, pois podem usar apenas um dos dois TAQs.
- O MAC VACL/vlmap precisa de três VMR/ACEs. Isso significa que 460 ACEs devem ser suportadas em cada direção.
- A VACL/vlmap IPv4 precisa de duas VMR/ACEs. Isso significa que 690 ACEs devem ser suportadas em cada direção.
- A PACL IPv4, a RACL e a GACL precisam de uma VMR/ACE. Isso significa que 1.380 ACEs devem ser suportadas em cada direção.
- O MAC PACL, o RACL e o GACL precisam de duas VMR/ACEs. Isso significa que 690 ACEs devem ser suportadas em cada direção.
- A PACL IPv6, a RACL e a GACL precisam de duas VMR/ACEs. Isso significa que 690 ACEs devem ser suportadas em cada direção.

Troubleshooting de TCAM de ACL de Segurança em Catalyst 3850 Switches

- Verificar a utilização do TCAM de segurança:

  Note: Embora as ACEs de segurança instaladas sejam menores que 3.072, um dos limites mencionados anteriormente pode ter sido atingido. Por exemplo, se um cliente tiver a maioria dos RACLs aplicados na direção de entrada, ele poderá usar até 1.380 entradas

disponíveis para o RACL de entrada. No entanto, os registros de exaustão do TCAM podem aparecer antes que todas as 3.072 entradas sejam 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 do hardware das ACLs instaladas 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 os registros de acl-event sempre que as ACLs forem instaladas/removidas:

```
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 a CAM (Content Addressable Memory, Memória endereçável de conteúdo) da ACL:

```
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 os contadores de queda e acerto de ACL detalhado:

```
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
```