Resolución de problemas de agotamiento de TCAM ACL de seguridad en switches Catalyst 3850

Contenido

Introducción

Este documento explica cómo los switches Catalyst 3850 implementan listas de control de acceso (ACL) de seguridad en hardware y cómo se utiliza la memoria direccionable de contenido ternario (TCAM) de seguridad entre varios tipos de ACL.

Antecedentes

Esta lista proporciona definiciones para varios tipos de ACL:

- **Lista de control de acceso de VLAN (VACL)**: una VACL es una ACL que se aplica a una VLAN. Sólo se puede aplicar a una VLAN y a ningún otro tipo de interfaz. El límite de seguridad es permitir o denegar el tráfico que se mueve entre VLAN y permitir o denegar el tráfico dentro de una VLAN. La ACL VLAN se soporta en el hardware y no tiene ningún efecto en el rendimiento.
- **Lista de control de acceso a puertos (PACL)**: una PACL es una ACL aplicada a una interfaz de puerto de switch de capa 2. El límite de seguridad es permitir o denegar el tráfico dentro de una VLAN. El PACL es compatible con el hardware y no tiene ningún efecto en el rendimiento.
- **Router ACL (RACL)**: una RACL es una ACL que se aplica a una interfaz que tiene asignada una dirección de Capa 3. Se puede aplicar a cualquier puerto que tenga una dirección IP como interfaces ruteadas, interfaces de loopback e interfaces VLAN. El límite de seguridad es permitir o denegar el tráfico que se mueve entre subredes o redes. La RACL se soporta en el hardware y no tiene efecto en el rendimiento.
- **ACL basada en grupo (GACL)**: GACL es una ACL basada en grupo definida en [grupos de objetos para ACL](#).

Problema

En los switches Catalyst 3850/3650, las entidades de control de acceso (ACE) PACL de entrada y PACL de salida se instalan en dos regiones/bancos independientes. Estas regiones/bancos se denominan ACL TCAM (TAQ). Las ACE de entrada y salida de VACL se almacenan en una sola región (TAQ). Debido a una limitación de hardware Doppler, VACL no puede utilizar ambas TAQ. Por lo tanto, VACL/vlmap solo tienen la mitad del espacio de resultado de la máscara de valor (VMR) disponible para las ACL de seguridad. Estos registros aparecen cuando se supera cualquiera de estos límites de hardware:

```
%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.
```

Sin embargo, es posible que el TCAM ACE de seguridad no parezca estar lleno cuando aparecen estos registros.

Solución

Es incorrecto suponer que una ACE siempre consume un VMR. Un ACE determinado puede consumir:

- 0 VMRs si se fusiona con una ACE anterior.
- 1 VMR si los bits VCU están disponibles para manejar el rango.
- 3 VMRs si se expande porque no hay bits VCU disponibles.

La hoja de datos de Catalyst 3850 sugiere que se soportan 3000 entradas de ACL de seguridad. Sin embargo, estas reglas definen cómo se pueden configurar estas 3000 ACE:

- Las VACL/VLAN admiten un total de 1,500 entradas, ya que sólo pueden utilizar una de las dos TAQ.
- MAC VACL/vlmap necesita tres VMR/ACE. Esto significa que se deben admitir 460 ACE en cada dirección.
- VACL/vlmap IPv4 necesita dos VMR/ACE. Esto significa que se deben admitir 690 ACE en cada dirección.
- IPv4 PACL, RACL y GACL necesitan un VMR/ACE. Esto significa que se deben admitir 1380 ACE en cada dirección.
- MAC PACL, RACL y GACL necesitan dos VMR/ACE. Esto significa que se deben admitir 690 ACE en cada dirección.
- IPv6 PACL, RACL y GACL necesitan dos VMR/ACE. Esto significa que se deben admitir 690 ACE en cada dirección.

Resolución de problemas de Security ACL TCAM en switches Catalyst 3850

- Verifique el uso de TCAM de seguridad:

  Nota: Aunque las ACE de seguridad instaladas son inferiores a 3072, es posible que se haya alcanzado uno de los límites antes mencionados. Por ejemplo, si un cliente tiene la

mayoría de las RACL aplicadas en la dirección de entrada, puede utilizar hasta 1380 entradas disponibles para la RACL entrante. Sin embargo, los registros de agotamiento de TCAM pueden aparecer antes de que se utilicen las 3072 entradas.

```
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 el estado de hardware de las ACL instaladas en el 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 los registros de acl-event cada vez que se instalan/eliminan las ACL:

```
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 la memoria de contenido direccionable (CAM) de 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 los contadores de caídas y de visitas de ACL desglosados:

```
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
```