Contenido

Introducción

Este documento explica cómo los Catalyst 3850 Switch implementan el Listas de control de acceso (ACL) de la Seguridad en hardware y cómo el Ternary Content Addressable Memory de la Seguridad (TCAM) se utiliza entre los diversos tipos de ACL.

Antecedentes

Esta lista proporciona las definiciones para los diversos tipos de ACL:

- **VLAN Access Control List (VACL)** - Un VACL es un ACL que se aplica a un VLA N. Puede ser aplicado solamente a un VLA N y a ningún otro tipo de interfaz. El límite de la Seguridad está al tráfico del permit or deny que se mueve entre los VLA N y el tráfico del permit or deny dentro de un VLA N. El VLA N ACL se soporta en hardware, y no tiene ningún efecto sobre el funcionamiento.
- **Lista de control de acceso del puerto (PACL)** - Un PACL es un ACL aplicado a una interfaz del switchport de la capa 2. El límite de la Seguridad está al tráfico del permit or deny dentro de un VLA N. El PACL se soporta en hardware y no tiene ningún efecto sobre el funcionamiento.
- **Router ACL (RACL)** - Un RACL es un ACL que se aplica a una interfaz que tenga un direccionamiento de la capa 3 asignado a él. Puede ser aplicado a cualquier puerto que tenga una dirección IP tal como interfaces ruteadas, interfaces del loopback, y interfaces VLAN. El límite de la Seguridad está al tráfico del permit or deny que se mueve entre las subredes o las redes. El RACL se soporta en hardware, y no tiene ningún efecto sobre el funcionamiento.
- **ACL basado en el grupo (GACL)** - GACL es ACL basado en el grupo definido en los [grupos de objetos para el ACL](#).

Problema

En el Switches del Catalyst 3850/3650, las entidades entradas del control de acceso PACL y de la salida PACL (ACE) están instaladas en dos regiones/bancos separados. Estas regiones/bancos se llaman ACL TCAM (TAQs). La entrada y salida ACE VACL se salva en una sola región (TAQ). Debido a una limitación del hardware de Doppler, el VACL no puede utilizar ambo TAQs. Por lo tanto, VACL/vlmap tienen solamente mitad del valor de la máscara del espacio del resultado (VMR) disponible para los ACL de seguridades. Estos registros aparecen cuando se exceden

ninguno de estos límites del hardware:

Sin embargo, la Seguridad ACE TCAM no pudo aparecer ser llena cuando aparecen estos registros.

Solución

Es incorrecta asumir que un ACE consume siempre un VMR. ACE dado puede consumir:

- 0 VMRs si consigue combinado con ACE anterior.
- 1 VMR si los bits VCU están disponibles manejar el rango.
- 3 VMRs si consigue ampliado porque no hay bits VCU disponibles.

La hoja de datos del Catalyst 3850 sugiere que 3,000 entradas de ACL de seguridad estén soportadas. Sin embargo, estas reglas definen cómo estos 3,000 ACE pueden ser configurados:

- Soporte VACL/vlmaps un total de entradas 1.5K como pueden utilizar solamente uno de los dos TAQs.
- El MAC VACL/vlmap necesita tres VMR/ACEs. Esto significa que 460 ACE se deben soportar en cada dirección.
- El IPv4 VACL/vlmap necesita dos VMR/ACEs. Esto significa que 690 ACE se deben soportar en cada dirección.
- Necesidad una VMR/ACE del IPv4 PACL, RACL, y GACL. Esto significa que 1,380 ACE se deben soportar en cada dirección.
- Necesidad dos VMR/ACEs MAC PACL, RACL, y GACL. Esto significa que 690 ACE se deben soportar en cada dirección.
- Necesidad dos VMR/ACEs del IPv6 PACL, RACL, y GACL. Esto significa que 690 ACE se deben soportar en cada dirección.

Resolver problemas el ACL de seguridad TCAM en los Catalyst 3850 Switch

- Utilización de TCAM de la Seguridad del control:

  Nota: Aunque la Seguridad instalada ACE es menos de 3,072, uno de los límites mencionados previamente pudo haber sido alcanzado. Por ejemplo, si un cliente hace la mayor parte de los RACL aplicar en la dirección de la entrada, pueden utilizar encima de 1,380 entradas disponibles para el RACL entrante. Sin embargo, los registros del agotamiento de TCAM pueden aparecer antes de que se utilicen las 3,072 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
```

- Marque al estado del hardware de ACL instalados 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>
```

- Marque los registros del ACL-evento siempre que los ACL estén instalados/quitados:

```
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 el 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 el golpe hacia fuera detallado y a los contadores de caídas 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
```