Contenu

Introduction

Ce document explique comment les Commutateurs du Catalyst 3850 implémentent le Listes de contrôle d'accès (ACL) de Sécurité dans le matériel et comment la mémoire associative ternaire de Sécurité (TCAM) est utilisée parmi de divers types d'ACLs.

Informations générales

Cette liste fournit des définitions pour différents types d'ACLs :

- **Liste de contrôle d'accès VLAN (VACL)** - Un VACL est un ACL qui est appliqué à un VLAN. Il peut seulement être appliqué à un VLAN et à aucun autre type d'interface. La borne de Sécurité est de permettre ou refuser le trafic que les mouvements entre les VLAN et l'autorisation ou refusent au trafic dans un VLAN. L'ACL VLAN est pris en charge dans le matériel, et n'exerce aucun effet sur la représentation.
- **Liste de contrôle d'accès de port (PACL)** - Un PACL est un ACL appliqué à une interface de switchport de la couche 2. La borne de Sécurité est de permettre ou refuser le trafic dans un VLAN. Le PACL est pris en charge dans le matériel et n'exerce aucun effet sur la représentation.
- **ACL de routeur (RACL)** - Un RACL est un ACL qui est appliqué à une interface qui a une adresse attribuée de la couche 3 à lui. Il peut être appliqué à n'importe quel port qui a une adresse IP telle que les interfaces conduites, les interfaces de bouclage, et les interfaces VLAN. La borne de Sécurité est de permettre ou refuser le trafic qui se déplace entre les sous-réseaux ou les réseaux. Le RACL est pris en charge dans le matériel, et n'exerce aucun effet sur la représentation.
- **ACL basé sur groupe (GACL)** - GACL est ACL basé sur groupe défini aux [groupes d'objets pour l'ACL](#).

Problème

Sur des Commutateurs du Catalyst 3850/3650, des entités entrées de contrôle d'accès PACL et de sortie PACL (as) sont installées à deux régions/banques distinctes. Ces régions/banques s'appellent ACL TCAMs (TAQs). Des as d'entrée et sortie VACL sont enregistrés dans une région simple (TAQ). En raison d'une limitation matérielle de Doppler, VACL ne peut pas utiliser les deux TAQs. Par conséquent, VACL/vlmap ont seulement la moitié de valeur de masque de l'espace du

résultat (VMR) disponible à la Sécurité ACLs. Ces logs apparaissent quand l'un de ces limites de matériel sont dépassées :

Cependant, la Sécurité ACE TCAM ne pourrait pas sembler être pleine quand ces logs apparaissent.

Solution

Il est incorrect pour supposer qu'un ACE consomme toujours un VMR. ACE donné peut consommer :

- 0 VMRs s'il obtient fusionné avec ACE précédent.
- 1 VMR si les bits VCU sont disponibles pour manipuler la plage.
- 3 VMRs s'il obtient développé parce qu'aucun bit VCU n'est disponible.

La fiche technique du Catalyst 3850 suggère que 3,000 rubriques de liste ACL de Sécurité soient pris en charge. Cependant, ces règles définissent comment ces 3,000 as peuvent être configurés :

- Support VACL/vlmaps un total d'entrées 1.5K comme ils peuvent utiliser seulement un des deux TAQs.
- Le MAC VACL/vlmap a besoin de trois VMR/ACEs. Ceci signifie que 460 as doivent être pris en charge dans chaque direction.
- L'ipv4 VACL/vlmap a besoin de deux VMR/ACEs. Ceci signifie que 690 as doivent être pris en charge dans chaque direction.
- Le besoin un VMR/ACE de l'ipv4 PACL, RACL, et GACL. Ceci signifie que 1,380 as doivent être pris en charge dans chaque direction.
- Le besoin deux VMR/ACEs du MAC PACL, RACL, et GACL. Ceci signifie que 690 as doivent être pris en charge dans chaque direction.
- Le besoin deux VMR/ACEs de l'IPv6 PACL, RACL, et GACL. Ceci signifie que 690 as doivent être pris en charge dans chaque direction.

Dépannage de l'ACL TCAM de Sécurité sur des Commutateurs du Catalyst 3850

- Utilisation de la Sécurité TCAM de contrôle :

  Remarque: Quoique les as installés de Sécurité soient moins de 3,072, une des limites précédemment mentionnées pourrait avoir été atteinte. Par exemple, si un client a la majeure partie du RACLs appliqué dans la direction d'entrée, elles peuvent épuiser 1,380 entrées disponibles pour le RACL d'arrivée. Cependant, les logs d'épuisement TCAM peuvent apparaître avant que chacune des 3,072 entrées soit utilisé.

```
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
```

- Vérifiez l'état du matériel d'ACLs a installé dans le 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>
```

- L'acl-événement de contrôle se connecte toutes les fois qu'ACLs sont installés/retirés :

```
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>
```

- Copie la mémoire associative d'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
```

- Imprimez les compteurs spécifiés de hit et de baisse d'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
```