Dépannage de l'épuisement de la TCAM des listes de contrôle d'accès de sécurité sur les commutateurs Catalyst 3850

Contenu

Introduction

Ce document explique comment les commutateurs Catalyst 3850 mettent en oeuvre des listes de contrôle d'accès (ACL) de sécurité dans le matériel et comment la mémoire TCAM (Ternary Content Addressable Memory) de sécurité est utilisée parmi différents types de listes de contrôle d'accès.

Informations générales

Cette liste fournit des définitions pour différents types de listes de contrôle d’accès :

- **VLAN Access Control List (VACL)** : une VACL est une liste de contrôle d'accès appliquée à un VLAN. Il ne peut être appliqué qu’à un VLAN et à aucun autre type d’interface. La limite de sécurité est d'autoriser ou de refuser le trafic qui se déplace entre des VLAN et d'autoriser ou de refuser le trafic au sein d'un VLAN. La liste de contrôle d’accès VLAN est prise en charge dans le matériel et n’a aucun effet sur les performances.
- **Liste de contrôle d'accès de port (PACL)** : une liste de contrôle d'accès de port est une liste de contrôle d'accès appliquée à une interface de port de commutateur de couche 2. La limite de sécurité est d'autoriser ou de refuser le trafic au sein d'un VLAN. La liste de contrôle d'accès est prise en charge dans le matériel et n'a aucun effet sur les performances.
- **Router ACL (RACL)** : une RACL est une liste de contrôle d'accès appliquée à une interface à laquelle une adresse de couche 3 lui est affectée. Il peut être appliqué à n'importe quel port qui possède une adresse IP telle que les interfaces routées, les interfaces de bouclage et les interfaces VLAN. La limite de sécurité est d'autoriser ou de refuser le trafic qui se déplace entre des sous-réseaux ou des réseaux. Le RACL est pris en charge dans le matériel et n'a aucun effet sur les performances.
- **Liste de contrôle d'accès basée sur le groupe (GACL)** - La liste de contrôle d'accès basée sur

le groupe est définie dans Groupes d'objets pour ACL.

Problème

Sur les commutateurs Catalyst 3850/3650, les entités de contrôle d'accès (ACE) PACL d'entrée et de sortie sont installées dans deux régions/banques distinctes. Ces régions/banques sont appelées TCAM ACL (TAQs). Les entrées et sorties des listes de contrôle d'accès VACL sont stockées dans une seule région (TAQ). En raison d'une limitation matérielle Doppler, VACL ne peut pas utiliser les deux TAQ. Par conséquent, la VACL/vlmap ne dispose que de la moitié de l'espace VMR (Value Mask Result) disponible pour les ACL de sécurité. Ces journaux apparaissent lorsque l'une de ces limites matérielles est dépassée :

```
%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.
```

Cependant, il se peut que la TCAM ACE de sécurité ne soit pas pleine lorsque ces journaux apparaissent.

Solution

Il est incorrect de supposer qu'une ACE consomme toujours une VMR. Une ACE donnée peut consommer :

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

La fiche technique du Catalyst 3850 indique que 3 000 entrées de liste de contrôle d'accès de sécurité sont prises en charge. Cependant, ces règles définissent comment ces 3 000 ACE peuvent être configurées :

- VACL/vlmaps prennent en charge un total de 1,5 000 entrées car ils ne peuvent utiliser qu'une seule des deux TAQ.
- MAC VACL/vlmap nécessite trois VMR/ACE. Cela signifie que 460 ACE doivent être pris en charge dans chaque direction.
- IPv4 VACL/vlmap nécessite deux VMR/ACE. Cela signifie que 690 ACE doivent être pris en charge dans chaque direction.
- PACL, RACL et GACL IPv4 nécessitent un VMR/ACE. Cela signifie que 1 380 ACE doivent être pris en charge dans chaque direction.
- MAC PACL, RACL et GACL ont besoin de deux VMR/ACE. Cela signifie que 690 ACE doivent être pris en charge dans chaque direction.
- PACL IPv6, RACL et GACL ont besoin de deux VMR/ACE. Cela signifie que 690 ACE doivent être pris en charge dans chaque direction.

Dépannage de la TCAM des listes de contrôle d'accès de sécurité sur les commutateurs Catalyst 3850

- Vérifier l'utilisation TCAM de sécurité :

  Note: Même si les ACE de sécurité installées sont inférieures à 3 072, l'une des limites précédemment mentionnées peut avoir été atteinte. Par exemple, si un client a appliqué la plupart des RACL dans la direction d'entrée, il peut utiliser jusqu'à 1 380 entrées disponibles pour le RACL entrant. Cependant, les journaux d'épuisement TCAM peuvent s'afficher avant l'utilisation des 3 072 entrées.

```
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 matériel des listes de contrôle d'accès installées 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>
```

- Vérifier les journaux des événements d'appels chaque fois que des listes de contrôle d'accès sont installées/supprimées :

```
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>
```

- Imprimer la mémoire CAM (Content Addressable Memory) de la liste de contrôle d'accès :

```
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
```

- Imprimer les compteurs de succès et de rejet des listes de contrôle d’accès détaillées :

```
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
```