Risoluzione dei problemi di sicurezza relativi all'esaurimento del TCAM ACL sugli switch Catalyst 3850

Sommario

Introduzione

In questo documento viene spiegato come gli switch Catalyst 3850 implementano gli Access Control Lists (ACL) di sicurezza nell'hardware e come la sicurezza TCAM (Ternary Content Addressable Memory) viene utilizzata tra i vari tipi di ACL.

Premesse

Di seguito vengono fornite le definizioni per i vari tipi di ACL:

- **VACL (VLAN Access Control List)**: un VACL è un ACL applicato a una VLAN. Può essere applicata solo a una VLAN e a nessun altro tipo di interfaccia. Il limite di sicurezza è quello di autorizzare o bloccare il traffico che si sposta tra le VLAN e autorizzare o bloccare il traffico all'interno di una VLAN. L'ACL VLAN è supportato nell'hardware e non influisce sulle prestazioni.
- **Port Access Control List (PACL)**: un PACL è un ACL applicato a un'interfaccia di porta switch di layer 2. Il limite di sicurezza è quello di autorizzare o bloccare il traffico all'interno di una VLAN. Il PACL è supportato nell'hardware e non influisce sulle prestazioni.
- **ACL del router (RACL)**: un ACL è un ACL applicato a un'interfaccia alla quale è assegnato un indirizzo di layer 3. Può essere applicata a qualsiasi porta con un indirizzo IP, ad esempio interfacce indirizzate, interfacce di loopback e interfacce VLAN. Il limite di sicurezza è quello di autorizzare o negare il traffico che si sposta tra subnet o reti. Il racl è supportato nell'hardware e non ha alcun effetto sulle prestazioni.
- **ACL basato su gruppi (GACL)** - GACL è un ACL basato su gruppi definito in [Object Group for ACL](#).

Problema

Sugli switch Catalyst 3850/3650, le entità di controllo dell'accesso (ACE) PACL di input e output vengono installate in due aree/banche separate. Queste regioni/banche sono chiamate ACL TCAM (TAQ). Le ACE di input e output VACL vengono memorizzate in un'area singola (TAQ). A causa di una limitazione hardware Doppler, VACL non può utilizzare entrambi i TAQ. Pertanto, i VACL/vlmap hanno solo metà dello spazio VMR (Value Mask Result) disponibile per gli ACL di sicurezza. Questi registri vengono visualizzati quando viene superato uno dei seguenti limiti 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.
```

Tuttavia, Security ACE TCAM potrebbe non apparire pieno quando questi registri vengono visualizzati.

Soluzione

Non è corretto supporre che un ACE consumi sempre un VMR. Una voce ACE specifica può utilizzare:

- 0 VMR se viene unita a un ACE precedente.
- 1 VMR se sono disponibili bit VCU per gestire l'intervallo.
- 3 VMR se viene espanso perché non sono disponibili bit VCU.

Il data sheet dello switch Catalyst 3850 suggerisce che sono supportate 3.000 voci ACL di sicurezza. Tuttavia, queste regole definiscono la modalità di configurazione di queste 3.000 ACE:

- VACL/vlmap supportano un totale di 1.5K voci in quanto possono utilizzare solo uno dei due TAQ.
- MAC VACL/vlmap richiede tre VMR/ACE. Questo significa che 460 ACE devono essere supportati in ciascuna direzione.
- Per IPv4 VACL/vlmap sono necessari due VMR/ACE. Ciò significa che devono essere supportate 690 ACE in ciascuna direzione.
- IPv4 PACL, RACL e GACL necessitano di un VMR/ACE. Questo significa che 1.380 ACE devono essere supportati in ciascuna direzione.
- MAC PACL, RACL e GACL necessitano di due VMR/ACE. Ciò significa che devono essere supportate 690 ACE in ciascuna direzione.
- Per IPv6 PACL, RACL e GACL sono necessari due VMR/ACE. Ciò significa che devono essere supportate 690 ACE in ciascuna direzione.

Risoluzione dei problemi relativi agli ACL TCAM di sicurezza sugli switch Catalyst 3850

- Verifica dell'utilizzo di TCAM per la sicurezza:

  Nota: Anche se le ACE di protezione installate sono inferiori a 3.072, uno dei limiti

precedentemente menzionati potrebbe essere stato raggiunto. Ad esempio, se un cliente ha applicato la maggior parte degli ACL nella direzione di input, può utilizzare fino a 1.380 voci disponibili per gli ACL in entrata. Tuttavia, i log di esaurimento TCAM possono essere visualizzati prima che vengano utilizzate tutte le 3.072 voci.

```
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
```

- Controllare lo stato dell'hardware degli ACL installati nel 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>
```

- Controllare i registri eventi degli ACL ogni volta che gli ACL vengono installati o rimossi:

```
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>
```

- Stampare il file ACL Content Addressable Memory (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
```

- Stampa i contatori dettagliati delle visite agli 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
```