Catalyst 3850 스위치에서 보안 ACL TCAM 소모 문제 해결

목차

소개

이 문서에서는 Catalyst 3850 스위치가 하드웨어에 보안 ACL(Access Control List)을 구현하는 방법과 다양한 유형의 ACL에서 보안 TCAM(Ternary Content Addressable Memory)을 어떻게 활용하는지 설명합니다.

배경 정보

이 목록은 다양한 유형의 ACL에 대한 정의를 제공합니다.

- **VACL(VLAN Access Control List)** - VACL은 VLAN에 적용되는 ACL입니다.VLAN에만 적용할 수 있으며 다른 유형의 인터페이스도 적용할 수 없습니다.보안 경계는 VLAN 간에 이동하는 트래픽을 허용하거나 거부하며 VLAN 내에서 트래픽을 허용하거나 거부하는 것입니다.VLAN ACL은 하드웨어에서 지원되며 성능에 영향을 미치지 않습니다.
- **PACL(Port Access Control List)** - PACL은 레이어 2 스위치 포트 인터페이스에 적용되는 ACL입니다.보안 경계는 VLAN 내의 트래픽을 허용하거나 거부하는 것입니다.PACL은 하드웨어에서 지원되며 성능에 영향을 미치지 않습니다.
- **RACL(Router ACL)** - RACL은 레이어 3 주소가 할당된 인터페이스에 적용되는 ACL입니다.라우티드 인터페이스, 루프백 인터페이스, VLAN 인터페이스 등의 IP 주소가 있는 모든 포트에 적용할 수 있습니다.보안 경계는 서브넷 또는 네트워크 간에 이동하는 트래픽을 허용하거나 거부하는 것입니다.RACL은 하드웨어에서 지원되며 성능에 영향을 미치지 않습니다.
- **GACL(Group-based ACL)** - GACL은 ACL에 대한 개체 그룹에 정의된 그룹 기반 ACL입니다.

문제

Catalyst 3850/3650 스위치에서는 입력 PACL 및 출력 PACL ACE(Access Control Entities)가 두 개의 개별 지역/은행에 설치됩니다.이러한 지역/은행을 ACL TCAM(TAQ)이라고 합니다.VACL 입력 및 출력 ACE는 단일 영역(TAQ)에 저장됩니다. 도플러 하드웨어 제한 때문에 VACL은 두 TAQ를 모두 사용할 수 없습니다.따라서 VACL/vlmap은 보안 ACL에 사용할 수 있는 VMR(Value Mask Result) 공간의 절반만 가집니다.이러한 로그는 다음 하드웨어 제한 중 하나를 초과할 때 나타납니

다.

```
%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.
```

그러나 이러한 로그가 표시될 때 보안 ACE TCAM이 꽉 차지 않은 것 같습니다.

솔루션

하나의 ACE가 항상 하나의 VMR을 사용한다고 가정하는 것은 잘못된 것입니다.지정된 ACE는 다음을 사용할 수 있습니다.

- 0VMR을 이전 ACE와 병합하는 경우
- 1 VCU 비트를 사용하여 범위를 처리할 수 있는 경우 VMR
- 3 VCU 비트를 사용할 수 없으므로 확장되는 경우 VMR

Catalyst 3850 Data Sheet에서는 3,000개의 보안 ACL 항목이 지원됨을 제안합니다.그러나 이러한 규칙은 이러한 3,000개의 ACE를 구성하는 방법을 정의합니다.

- VACL/vlmaps는 두 TAQ 중 하나만 사용할 수 있으므로 총 1.5K 항목을 지원합니다.
- MAC VACL/vlmap에는 3개의 VMR/ACE가 필요합니다.즉, 각 방향에서 460개의 ACE를 지원해야 합니다.
- IPv4 VACL/vlmap에는 VMR/ACE가 2개 필요합니다.즉, 각 방향에서 690개의 ACE를 지원해야 합니다.
- IPv4 PACL, RACL 및 GACL에는 VMR/ACE가 1개 필요합니다.즉, 각 방향에서 1,380개의 ACE를 지원해야 합니다.
- MAC PACL, RACL 및 GACL에는 VMR/ACE 2개가 필요합니다.즉, 각 방향에서 690개의 ACE를 지원해야 합니다.
- IPv6 PACL, RACL 및 GACL에는 VMR/ACE가 2개 필요합니다.즉, 각 방향에서 690개의 ACE를 지원해야 합니다.

Catalyst 3850 스위치의 보안 ACL TCAM 문제 해결

- 보안 TCAM 사용률 확인:

  참고:설치된 보안 ACE가 3,072개 미만이지만 이전에 언급한 제한 중 하나에 도달했을 수 있습니다.예를 들어, 고객이 대부분의 RACL을 입력 방향으로 적용한 경우 인바운드 RACL에 사용할 수 있는 항목을 1,380개까지 사용할 수 있습니다.그러나 3,072개의 항목이 모두 사용되기 전에 TCAM 소모 로그가 표시될 수 있습니다.

```
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
```

- TCAM에 설치된 ACL의 하드웨어 상태를 확인합니다.

```
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>
```

- ACL이 설치/제거될 때마다 acl-event 로그를 확인합니다.

```
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>
```

- ACL CAM(Content Addressable Memory) 인쇄:

```
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
```

- 항목별 ACL 적중 및 삭제 카운터를 출력합니다.

```
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
```