目次

概要

Catalyst 3850 スイッチはハードウェアのセキュリティ アクセス コントロール リスト（ACL）がどのように実装されている、そしてどのようにセキュリティ Ternary Content Addressable Memory（TCAM）が ACL のさまざまな型間で利用されるかこの資料に説明されています。

背景説明

このリストは ACL のさまざまな型に定義を提供します:

- **VLAN Access Control List（VACL）** - VACL は VLAN に適用される ACL です。 それはインターフェイスの VLAN および他の型にしか適用することができません。 セキュリティ境界は VLAN 内の VLAN と割り当てまたは拒否トラフィック間の移動割り当てまたは拒否トラフィックにあります。 VLAN ACL はハードウェアでサポートされ、パフォーマンスに効果をもたらしません。
- **ポート アクセス制御リスト（PACL）** - PACL はレイヤ2 スイッチポート インターフェイスに適用される ACL です。 セキュリティ境界は VLAN 内の割り当てまたは拒否トラフィックにあります。 PACL はハードウェアでサポートされ、パフォーマンスに効果をもたらしません。
- **ルータ ACL（RACL）** - RACL はそれに割り当てられるレイヤ3 アドレスがあるインターフェイスに適用される ACL です。 それはルーテッドインターフェイス、ループバックインターフェイスおよび VLANインターフェイスのような IP アドレスがあるあらゆるポートに適用することができます。 セキュリティ境界はサブネットかネットワークの間で移動する拒否トラフィックにまたは割り当てあります。 RACL はハードウェアでサポートされ、パフォーマンスに効果をもたらしません。
- **グループ ベース ACL（GACL）** - GACL は ACL のためのオブジェクト グループで定義されるグループ ベース ACL です。

問題

Catalyst 3850/3650 スイッチで、入力された PACL および出力 PACL アクセスコントロール エンティティ（ACE）は 2 つの別々の領域/バンクにインストールされています。 これらの領域/バンクは ACL TCAM（TAQs）と問い合わせられます。 VACL 入出力 ACE は単一領域（TAQ）で保存されます。 ドップラー ハードウェアの制約が原因で、VACL は両方 TAQs を使用できません。 従って、VACL/vlmap に値マスク結果（VMR）領域半分がセキュリティ ACL に利用可能 なあり

ますただ。 これらの口グはこれらのハードウェア制限のうちのどれかが超過するとき現われます:

ただしこれらの口グが現われるとき、セキュリティ ACE TCAM は完全ようではないかもしれません。

解決策

不正確 1 ACE が 1 VMR を常に消費すると仮定するためにです。 ある特定の ACE は消費する場合があります:

- 前の ACE とマージされて得る場合 0 VMRs。
- VCU ビットが範囲を処理して利用できる場合 1 VMR。
- VCU ビットが利用できないのでそれが拡張されて得る場合 3 VMRs。

Catalyst 3850 データシートは 3,000 のセキュリティ ACL エントリがサポートされることを提案します。 ただし、これらのルールはこの 3,000 ACE がどのように設定することができるか定義します:

- それらが 2 TAQs の 1 つだけを使用できるように VACL/vlmaps サポート 1.5K エントリの合計。
- MAC VACL/vlmap は 3 VMR/ACEs を必要とします。 これは 460 ACE が各方向でサポートする必要があることを意味します。
- IPv4 VACL/vlmap は 2 VMR/ACEs を必要とします。 これは 690 ACE が各方向でサポートする必要があることを意味します。
- IPv4 PACL、RACL および GACL 必要 1 VMR/ACE。 これは 1,380 ACE が各方向でサポートする必要があることを意味します。
- MAC PACL、RACL および GACL 必要 2 VMR/ACEs。 これは 690 ACE が各方向でサポートする必要があることを意味します。
- IPv6 PACL、RACL および GACL 必要 2 VMR/ACEs。 これは 690 ACE が各方向でサポートする必要があることを意味します。

Catalyst 3850 スイッチのセキュリティ ACL TCAM のトラブルシューティング

- セキュリティ TCAM 利用をチェックして下さい:

  注 インストール済みセキュリティ ACE が 3,072 より小さいのに、以前に述べられる制限の 1 つは達するかもしれません。 たとえば、顧客は入力方向で適用される RACL のほとんどがあれば、受信 RACL のために利用可能 な 1,380 のエントリを使い果すことができます。 ただし、TCAM 枯渇口グは 3,072 のエントリがすべて使用される前に出て来ることができます。

```
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
```

- TCAM にインストールされる ACL のハードウェア状態をチェックして下さい:

```
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>
```

- ACL がインストールされていたり/取除かれる時はいつでも ACL イベント ログをチェックして下さい:

```
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 連想記憶メモリ（CAM）を印刷して下さい:

```
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
```

- 項目別にされた ACL ヒットおよびドロップ カウンタを印刷して下さい:

```
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
```