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

内容

概要

このドキュメントでは、Catalyst 3850 スイッチによるハードウェアでのセキュリティ アクセス コントロール リスト（ACL）の実装方法と、各種 ACL におけるセキュリティ TCAM（Ternary Content Addressable Memory）の使用方法について説明します。

背景説明

このリストでは、さまざまな種類の ACL を定義しています。

- **VLAN アクセス コントロール リスト（VACL）：VACLは VLAN に適用されている ACL です。**これは、VLAN にのみ適用可能で、他の種類のインターフェイスには適用できません。セキュリティ境界線により、VLAN 間を移動するトラフィックの許可または拒否と、VLAN 内のトラフィックの許可または拒否を行います。VLAN ACL はハードウェアでサポートされ、パフォーマンスには影響しません。
- **ポート アクセス コントロール リスト(PACL)：PACLはレイヤ 2 のスイッチポート インターフェイスに適用される ACL です。**セキュリティ境界線により、VLAN 内のトラフィックの許可または拒否を行います。PACL はハードウェアでサポートされ、パフォーマンスには影響しません。
- **ルータ ACL（RACL）：RACLは、レイヤ 3 アドレスが割り当てられたインターフェイスに適用される ACL です。**これはルーティングされたインターフェイス、ループバック インターフェイス、VLAN インターフェイスなど、IP アドレスを持つすべてのポートに適用できます。セキュリティ境界線により、サブネットまたはネットワーク間のトラフィックの許可または拒否を行います。RACL はハードウェアでサポートされ、パフォーマンスには影響しません。
- **グループ ベースの ACL（GACL）：GACL は** ACL のオブジェクト グループで定義されたグループ ベースの ACL です。

問題

Catalyst 3850/3650 スイッチでは、入力 PACL と出力 PACL のアクセス制御エンティティ (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（TAQ）と呼ばれます。VACL の入出力 ACE は、単一の領域（TAQ）に保存されます。ドップラー ハードウェアの制限により、VACL は両方の TAQ を使用できません。したがって、VACL/vlmap にはセキュリティ ACL に用意されている Value Mask Result (VMR) の半分のスペースしかありません。以下のログは、これらのハードウェア制限のいずれかを超過した場合に表示されます。

```
%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.
```

しかし、これらのログが表示されても、セキュリティ ACE TCAM が満杯になったように見えないことがあります。

解決方法

各 ACE が常に 1 VMR を消費すると仮定するのは誤りです。ACE は、以下の量の VMR を消費することがあります。

- 以前の ACE とマージした場合は、VMR を消費しません。
- VCU ビットを対応範囲内の処理に使用できる場合、ACE は 1 VMR を消費します。
- これが拡張された場合は、VCU ビットが使用できないため、3 VMR を消費します。

Catalyst 3850 データ シートによれば、3,000 のセキュリティ ACL エントリまでがサポートされています。しかし、この 3,000 の ACE は、以下の規則に従って設定する必要があります。

- 2 つの TAQ のうち片方のみを使用できるため、VACL/vlmaps は合計で 1.5K のエントリをサポートしています。
- MAC VACL/vlmap には 3 VMR/ACE が必要です。よって、各方向に 460 の ACE をサポートする必要があります。
- IPv4 VACL/vlmap には 2 VMR/ACE が必要です。よって、各方向に 690 の ACE をサポートする必要があります。
- IPv4 PACL、RACL、GACL には 1 VMR/ACE が必要です。よって、各方向に 1,380 の ACE をサポートする必要があります。
- MAC PACL、RACL、GACL には 2 VMR/ACE が必要です。よって、各方向に 690 の ACE をサポートする必要があります。
- IPv6 PACL、RACL、GACL には 2 VMR/ACE が必要です。よって、各方向に 690 の ACE をサポートする必要があります。

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 の使用率を確認します。

  注：インストールされているセキュリティの ACE が 3,072 未満であっても、これまでに説明した限界値のうちの 1 つに達していることがあります。たとえば、RACL の大部分が入力

方向に適用されている場合は、インバウンド RACL に 1,380 エントリまで使用できます。しかし、3,072 のエントリがすべて使用される前にも TCAM の枯渇が口グに報告されてしまうことがあります。

```
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ている ACL のハードウェアの状態を以下のように確認してください。

```
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 のインストールや削除の都度、acl-event ログを確認してください。

```
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 の Content-Addressable Memory (CAM) を印刷します。

```
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
```

- 項目別の ACL のヒット、ドロップカウンタを印刷します。

```
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
```