Fehlerbehebung: ACL-TCAM-Erschöpfung für Sicherheitsfunktionen auf Catalyst Switches der Serie 3850

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Catalyst Switches der Serie 3850 Zugriffskontrolllisten (ACLs) für die Sicherheit in der Hardware implementieren und wie TCAM (Security Ternary Content Addressable Memory) für die verschiedenen Arten von ACLs verwendet wird.

Hintergrundinformationen

Diese Liste enthält Definitionen für verschiedene Arten von ACLs:

- **VLAN Access Control List (VACL)** - Eine VACL ist eine ACL, die auf ein VLAN angewendet wird. Sie kann nur auf ein VLAN und keine andere Art von Schnittstelle angewendet werden. Die Sicherheitsgrenze besteht darin, Datenverkehr zwischen VLANs zuzulassen oder zu verweigern und den Datenverkehr innerhalb eines VLAN zuzulassen oder zu verweigern. Die VLAN-ACL wird von der Hardware unterstützt und hat keine Auswirkungen auf die Leistung.
- **Port Access Control List (PACL) (Port Access Control List**, PACL) - Eine PACL ist eine ACL, die auf eine Layer-2-Switch-Port-Schnittstelle angewendet wird. Die Sicherheitsgrenze besteht darin, Datenverkehr innerhalb eines VLAN zuzulassen oder zu verweigern. Die PACL wird von der Hardware unterstützt und hat keine Auswirkungen auf die Leistung.
- **Router ACL (RACL)** - Ein RACL ist eine ACL, die auf eine Schnittstelle angewendet wird, der eine Layer-3-Adresse zugewiesen ist. Sie kann auf jeden Port angewendet werden, der über eine IP-Adresse verfügt, z. B. geroutete Schnittstellen, Loopback-Schnittstellen und VLAN-Schnittstellen. Die Sicherheitsgrenze besteht darin, Datenverkehr zwischen Subnetzen oder Netzwerken zuzulassen oder zu verweigern. RACL wird von der Hardware unterstützt und hat keine Auswirkungen auf die Leistung.
- **Gruppenbasierte ACL (GACL)** - GACL ist eine in [Objektgruppen für](#) die [ACL](#) definierte gruppenbasierte ACL.

Problem

Auf Catalyst Switches der Serien 3850/3650 werden Eingabe-PACL und Ausgabe-ACEs (PACL Access Control Entities) in zwei separaten Regionen/Banken installiert. Diese Regionen/Banken werden als ACL TCAMs (TAQs) bezeichnet. Eingabe- und Ausgabe-ACEs für VACLs werden in einer Region (TAQ) gespeichert. Aufgrund einer Doppler-Hardware-Einschränkung kann VACL nicht beide TAQs verwenden. Aus diesem Grund verfügt VACL/vlmap nur über die Hälfte des VMR-Speichers (Value Mask Result), der den Sicherheits-ACLs zur Verfügung steht. Diese Protokolle werden angezeigt, wenn eine dieser Hardwarebeschränkungen überschritten wird:

```
%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.
```

Wenn diese Protokolle angezeigt werden, scheint der Sicherheits-ACE TCAM jedoch nicht vollständig zu sein.

Lösung

Es ist falsch anzunehmen, dass ein ACE immer einen VMR verwendet. Ein ACE kann Folgendes konsumieren:

- 0 VMRs, wenn sie mit einem vorherigen ACE zusammengeführt werden.
- 1 VMR, wenn VCU-Bits verfügbar sind, um den Bereich zu verarbeiten.
- 3 VMRs, wenn sie erweitert werden, weil keine VCU-Bits verfügbar sind.

Das Datenblatt zu Catalyst 3850 legt nahe, dass 3.000 Einträge für Sicherheitszugriffskontrolllisten unterstützt werden. Diese Regeln legen jedoch fest, wie diese 3.000 ACEs konfiguriert werden können:

- VACL/VLANs unterstützen insgesamt 1,5 K Einträge, da nur eine der beiden TAQs verwendet werden kann.
- MAC VACL/Vlmap benötigt drei VMR/ACEs. Das bedeutet, dass 460 ACEs in jede Richtung unterstützt werden müssen.
- IPv4 VACL/Vlmap benötigt zwei VMR/ACEs. Das bedeutet, dass 690 ACEs in jede Richtung unterstützt werden müssen.
- IPv4-PACL, RACL und GACL benötigen einen VMR/ACE. Das bedeutet, dass in jeder Richtung 1.380 ACEs unterstützt werden müssen.
- MAC PACL, RACL und GACL benötigen zwei VMR/ACEs. Das bedeutet, dass 690 ACEs in jede Richtung unterstützt werden müssen.
- IPv6 PACL, RACL und GACL benötigen zwei VMR/ACEs. Das bedeutet, dass 690 ACEs in jede Richtung unterstützt werden müssen.

Fehlerbehebung: Security ACL TCAM auf Catalyst 3850-Switches

- TCAM-Nutzung der Sicherheit überprüfen:

  Hinweis: Obwohl die installierten Sicherheits-ACEs weniger als 3.072 sind, ist eine der oben genannten Grenzen möglicherweise erreicht. Wenn beispielsweise ein Kunde die meisten RACLs in der Eingangsrichtung angewendet hat, kann er bis zu 1.380 Einträge für das eingehende RACL verwenden. Es können jedoch TCAM-Erschöpfungsprotokolle angezeigt werden, bevor alle 3.072 Einträge verwendet werden.

```
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
```

- Überprüfen Sie den Hardwarestatus der im TCAM installierten ACLs:

```
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>
```

- Überprüfen Sie die Ereignisprotokolle bei jeder Installation/Entfernung von ACLs:

```
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>
```

- Drucken Sie den ACL Content Addressable Memory (CAM) aus:

```
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
```

- Drucken Sie die Zähler für Treffer und Abbrüche von Zugriffskontrolllisten aus:

```
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
```