Probleemoplossing security ACL (uitgebreid) via Catalyst 3850 switches

Inhoud

Inleiding

Dit document legt uit hoe Catalyst 3850-switches security toegangscontrolelijsten (ACL's) implementeren in hardware en hoe security Ternary Content Adresseerbare Geheugen (TCAM) wordt gebruikt onder verschillende typen ACL's.

Achtergrondinformatie

Deze lijst bevat definities voor verschillende typen ACL's:

- **VLAN Access Control List (VACL)** - Een VACL is een ACL die op een VLAN wordt toegepast. Het kan alleen op een VLAN en geen ander type interface worden toegepast. De veiligheidsgrens is om verkeer toe te staan of te ontkennen dat zich tussen VLAN's beweegt en verkeer binnen een VLAN toe te staan of te ontkennen. VLAN ACL wordt ondersteund in hardware en heeft geen effect op de prestaties.
- **Port Access Control List (PACL)** - Een PACL is een ACL die is toegepast op een Layer 2-switchpoortinterface. De veiligheidsgrens is om verkeer binnen een VLAN toe te staan of te ontkennen. De PACL wordt ondersteund in hardware en heeft geen effect op de prestaties.
- **Router ACL (RACL)** - Een RACL is een ACL die wordt toegepast op een interface met een Layer 3-adres dat aan deze ACL is toegewezen. Het kan op elke poort worden toegepast die een IP-adres heeft, zoals routed interfaces, loopback interfaces en VLAN-interfaces. De veiligheidsgrens is om verkeer toe te staan of te ontkennen dat zich tussen subnetten of netwerken beweegt. De RACL wordt ondersteund door hardware en heeft geen effect op de prestaties.
- **Op groep gebaseerde ACL (GACL)** - GACL is op groep gebaseerd ACL gedefinieerd in Objectgroepen voor ACL.

Probleem

Op Catalyst 3850/3650 switches worden input-PACL en uitvoer PACL-toegangscontrole-entiteiten

(ACE's) geïnstalleerd in twee afzonderlijke regio's/banken. Deze regio's/banken worden ACL's (TAQ's) genoemd. VACL-invoer en -uitvoer ACE's worden opgeslagen in één gebied (TAQ). Vanwege een Doppler hardwarebeperking kan VACL niet beide TAQ's gebruiken. Daarom heeft VACL/vlmap alleen de helft van de VMR (Value Mask Result)-ruimte beschikbaar voor security ACL's. Deze logbestanden verschijnen wanneer een van deze hardwaregrenzen wordt overschreden:

```
%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.
```

Security ACE TCAM zal echter waarschijnlijk niet vol blijken te zijn wanneer deze logbestanden verschijnen.

Oplossing

Het is onjuist om aan te nemen dat één ACE altijd één VMR consumeert. Een bepaalde ACE kan consumeren:

- 0 VMRs als deze wordt samengevoegd met een vorige ACE.
- 1 VMR. als VCU-bits beschikbaar zijn om het bereik aan te kunnen.
- 3 VMR's als deze wordt uitgebreid omdat er geen VCU-bits beschikbaar zijn.

Het gegevensblad Catalyst 3850 suggereert dat 3.000 security ACL-items worden ondersteund. Deze regels definiëren echter hoe deze 3.000 ACE's kunnen worden geconfigureerd:

- VACL/Vlmaps ondersteunen een totaal van 1.5K ingangen aangezien zij slechts één van de twee TAQ's kunnen gebruiken.
- MAC VACL/Vlmap heeft drie VMR/ACE's nodig. Dit betekent dat 460 ACE's in elke richting moeten worden ondersteund.
- IPv4 VACL/VLAN's heeft twee VMR./ACE's nodig. Dit betekent dat 690 ACE's in elke richting moeten worden ondersteund.
- IPv4 PACL, RACL en GACL hebben één VMR./ACE nodig. Dit betekent dat 1.380 ACE's in elke richting moeten worden ondersteund.
- MAC PACL, RACL en GACL hebben twee VMR./ACE's nodig. Dit betekent dat 690 ACE's in elke richting moeten worden ondersteund.
- IPv6 PACL, RACL en GACL's hebben twee VMR/ACE's nodig. Dit betekent dat 690 ACE's in elke richting moeten worden ondersteund.

Security ACL-camera voor probleemoplossing op Catalyst 3850 switches

- Controleer het gebruik van veiligheidssoftware:

  Opmerking: Hoewel de geïnstalleerde veiligheidsACE's minder dan 3.072 zijn, zou een van de eerder genoemde limieten bereikt kunnen zijn. Bijvoorbeeld, als een klant de meeste RACL's heeft toegepast in de invoerrichting, kunnen zij 1.380 ingangen gebruiken die

beschikbaar zijn voor de inkomende RACL. De TCAM-uitputtingslogboeken kunnen echter verschijnen voordat alle 3.072 items gebruikt worden.

```
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
```

- Controleer de hardwarestatus van ACL's die in TCAM is geïnstalleerd:

```
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>
```

- Controleer de logbestanden van gebeurtenis van ACL's wanneer deze zijn geïnstalleerd/verwijderd:

```
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>
```

- Print het ACL-contentadresseerbare geheugen (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
```

- Standaard ACL-hit en -valtellers afdrukken

```
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
```