أستكشاف أخطاء قائمة التحكم في الوصول (ACL) الأمنية وإصلاحها باستخدام TCAM على محولات Catalyst 3850 switches

المحتويات

المقدمة
معلومات أساسية
المشكلة
الحل
أداة التحكم في الوصول للأمان وإصلاحها على محولات Catalyst 3850 Switches

المقدمة

يشرح هذا المستند كيفية تنفيذ محولات Catalyst 3850 switches لقوائم التحكم في الوصول إلى الأمان (ACLs) في الأجهزة وكيفية إستخدام الذاكرة القابلة للتوجيه (TCAM) الخاصة بالأمان في الأنواع المختلفة من قوائم التحكم في الوصول.

معلومات أساسية

توفر هذه القائمة تعريفات للأنواع المختلفة من قوائم التحكم في الوصول:

- **قائمة التحكم في الوصول إلى شبكة VLAN (VACL)** - VACL هي قائمة تحكم في الوصول إلى شبكة VLAN يتم تطبيقها على شبكة VLAN. هو يستطيع فقط كنت طبقت إلى VLAN ولا آخر نوع من قارن. حدود الأمان هي للسماح بحركة المرور التي تنتقل بين شبكات VLAN والسماح بحركة المرور أو رفضها داخل شبكة VLAN. يتم دعم قائمة التحكم في الوصول (ACL) لشبكة VLAN في الأجهزة، ولا تؤثر على الأداء.
- **قائمة التحكم في الوصول إلى المنفذ (PACL)** - قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) هي قائمة تحكم في الوصول الخاصة بالمنفذ (ACL) يتم تطبيقها على واجهة SwitchPort من الطبقة 2. حدود الأمان هي للسماح بحركة المرور أو رفضها داخل شبكة VLAN. يتم دعم قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) في الأجهزة ولا تؤثر على الأداء.
- **قائمة التحكم في الوصول للموجه (RACL)** - تعد قائمة التحكم في الوصول (RACL) قائمة تحكم في الوصول (ACL) يتم تطبيقها على واجهة تحتوي على عنوان الطبقة 3 الذي تم تعيينه لها. هو يستطيع كنت طبقت إلى أي ميناء أن يتلقى عنوان مثل يوجه قارن، loopback قارن، و VLAN قارن. تتمثل حدود الأمان في السماح بحركة المرور التي تنتقل بين الشبكات أو الشبكات الفرعية أو رفضها. يتم دعم قائمة التحكم في الوصول للاستقبال (RACL) في الأجهزة، ولا تؤثر على الأداء.
- **قائمة التحكم في الوصول (GACL) المستندة إلى المجموعة** - قوائم التحكم في الوصول (GACL) هي قائمة تحكم في الوصول (ACL) قائمة على مجموعة محددة في مجموعات الكائنات لقائمة التحكم في الوصول (ACL).

المشكلة

في محولات Catalyst 3850/3650، يتم تثبيت وحدات التحكم في الوصول إلى قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) للمدخلات ووحدات التحكم في الوصول إلى قائمة التحكم في الوصول الخاصة بالمنفذ (ACEs) للمخرجات في منطقتين/بنكين منفصلين. وتسمى هذه المناطق/البنوك بالوحدات النمطية (TAQs) ACL TCAM). يتم تخزين قوائم التحكم في الوصول إلى شبكة VACL الإدخال والإخراج في منطقة واحدة (TAQ). نظرا لقيود أجهزة Doppler، يتعذر على VACL إستخدام كل من TAQs. لذلك، تحتوي VACL/VLMAP فقط على نصف مساحة "نتيجة قناع القيمة" (VMR) المتوفرة لقوائم التحكم في الوصول (ACL) الأمنية. تظهر هذه السجلات عند تجاوز أي من حدود الأجهزة هذه:

```
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
```

ومع ذلك، قد لا يظهر ACE للأمان بشكل كامل عند ظهور هذه السجلات.

الحل

من غير الصحيح أن نفترض أن إدخال التحكم في الوصول (ACE) يستهلك دائما معرف فئة مورد (VMR) واحدا. يمكن أن يستهلك إدخال التحكم في الوصول (ACE) المحدد:

- 0 VMRs إذا تم دمجه مع ACE السابق.
- 1 VMR إذا كانت وحدات بت VCU متوفرة لمعالجة النطاق.
- 3 VMRs إذا تم توسيعها بسبب عدم توفر وحدات بت VCU.

تقترح ورقة بيانات Catalyst 3850 أن يتم دعم 3000 إدخال قائمة تحكم في الوصول (ACL) للأمان. ومع ذلك، تحدد هذه القواعد الكيفية التي يمكن بها تكوين وحدات التحكم في الوصول للبنية الأساسية (ACE) هذه التي يبلغ عددها 3000:

- تدعم خرائط VACL/VLAN إجمالي 1.5 ألف مدخل حيث أنها يمكن أن تستخدم فقط واحد من إثنين TAQ.
- يحتاج MAC VACL/VLMAP إلى ثلاثة أنظمة VMR/ACE. وهذا يعني أنه يجب دعم إدخالات التحكم في الوصول (ACE) بسرعة 460 في كل إتجاه.
- يحتاج IPv4 VACL/VLMAP إلى إثنين من VMR/ACEs. وهذا يعني أنه يجب دعم إدخالات التحكم في الوصول (ACE) إلى 690 في كل إتجاه.
- تحتاج قوائم التحكم في الوصول الخاصة بالمنفذ (PACL) و RACL و GACL للإصدار الرابع من بروتوكول الإنترنت إلى منفذ VMR/ACE واحد. وهذا يعني أنه يجب دعم 1380 من إدخالات التحكم في الوصول (ACE) في كل إتجاه.
- تحتاج قوائم التحكم في الوصول الخاصة بالمنفذ (MAC) و RACL و GACL إلى فتحتي VMR/ACE. وهذا يعني أنه يجب دعم إدخالات التحكم في الوصول (ACE) إلى 690 في كل إتجاه.
- تحتاج قوائم التحكم في الوصول الخاصة بالمنفذ (PACL) و RACL و GACL إلى فتحتي VMR/ACE. وهذا يعني أنه يجب دعم إدخالات التحكم في الوصول (ACE) إلى 690 في كل إتجاه.

أداة التحكم في الوصول للأمان وإصلاحها على محولات Catalyst 3850 Switches

- التحقق من إستخدام TCAM للأمان:

ملاحظة: على الرغم من أن إدخالات الأمان المثبتة أقل من 3072، قد يكون تم الوصول إلى أحد الحدود المذكورة سابقا. على سبيل المثال، إذا قام العميل بتطبيق معظم قوائم التحكم في الوصول للاستقبال

(RACL) في إتجاه الإدخال، فيمكنه إستخدام ما يصل إلى 1380 إدخالا متاحا لقوائم التحكم في الوصول للاستقبال (RACL) الواردة. ومع ذلك، يمكن أن تظهر سجلات إستهلاك TCAM قبل إستخدام جميع الإدخالات 3072.

```
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
```

- تحقق من حالة أجهزة قوائم التحكم في الوصول (ACL) المثبتة في TCAM:

```
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
       permit udp any 8 host 224.0.0.2 eq 1985 10
                 permit udp any 8 any eq bootps 20
      permit ip 10.100.176.0 255.255.255.0 any 30
                                                  <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
                              permit udp any 8 host 224.0.0.2 eq 1985 10
                                        permit udp any 8 any eq bootps 20
                                    permit ip 10.100.176.0 255.255.255.0 any 30
                                                                        <snip>
```

• التحقق من سجلات أحداث قائمة التحكم بالوصول (ACL) كلما تم تثبيت/إزالة قوائم التحكم بالوصول (ACL):

```
                                    3850#show mgmt-infra trace messages acl-events switch 1
                      UTC 3a8 5692] START Input IPv4 L3 label_id 22 21:35:34.877 04/22/15]
                     asic3 num_les 1 old_unload 0x0, cur_unloaded 0x0, trid 236 num_vmrs 11


                    UTC 3a9 5692] Trying L3 iif_id 0x104608000000100 21:35:34.877 04/22/15]
                                                                        input base FID 14

                     UTC 3aa 5692] Input IPv4 L3 label_id 22 hwlabel 21:35:34.878 04/22/15]
                             asic3 status 0x0 old_unloaded 0x0 cur_unloaded 0x0 trid 236 22

                                        UTC 3ab 5692] MAC: 0000.0000.0000 21:35:35.939 04/22/15]
    Adding Input IPv4 L3 acl [Postage-Printer] BO 0x1 to leinfo le_id 29on asic 255

                                    UTC 3ac 5692] MAC: 0000.0000.0000 Rsvd 21:35:35.939 04/22/15]
                                                    label 0 --> New label 23, asic255

                      UTC 3ad 5692] START Input IPv4 L3 label_id 23 21:35:35.939 04/22/15]
                     asic3 num_les 1 old_unload 0x0, cur_unloaded 0x0, trid 237 num_vmrs 5
                                                                        <snip>
```

• طباعة الذاكرة القابلة للتوجيه (CAM) الخاصة بمحتوى قائمة التحكم في الوصول:

```
                                                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
```

• طباعة عدادات الوصول والإفلات المفصلة لقائمة التحكم بالوصول (ACL):

```
                                        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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).