مثال تكوين تسجيل قائمة التحكم في الوصول (ACL) المحسنة للمحولات من السلسلة Nexus 7000 و 7700

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين تسجيل قائمة التحكم في الوصول المحسن (OAL) (ACL) على محولات Cisco Nexus 7000 و 7700 Series Switches.

المتطلبات الأساسية

المتطلبات

توصيك Cisco بأن تكون لديك معرفة بتكوينات Nexus مع قوائم التحكم في الوصول (ACL) الأساسية قبل أن تحاول التكوين الموضح في هذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- سلسلة مبدلات Cisco Nexus 7000
- سلسلة مبدلات Cisco Nexus 7700

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

توفر قوائم التحكم في الوصول (ACL) التي تم تمكين التسجيل عليها رؤية لحركة المرور لأنها تجتاز الشبكة أو يتم إسقاطها بواسطة أجهزة الشبكة. لسوء الحظ، يمكن أن يكون تسجيل قائمة التحكم في الوصول (ACL) كثيف وحدة المعالجة المركزية (CPU) ويمكن أن يؤثر سلبا على الوظائف الأخرى لجهاز الشبكة. لتقليل دورات وحدة المعالجة المركزية (CPU)، يستخدم محول Cisco Nexus 7000 Series شبكات محلية ظاهرية (OAL).

يوفر إستخدام OALs دعم الأجهزة لتسجيل قائمة التحكم في الوصول. يسمح OAL بالحزم أو إسقاطها في الجهاز ويستخدم روتينا محسنا لإرسال المعلومات إلى المشرف بحيث يمكن إنشاء رسائل التسجيل. على سبيل المثال، عندما تضرب الحزمة قائمة تحكم في الوصول (ACL) مع تمكين التسجيل أثناء إعادة توجيهها في الجهاز، يتم إنشاء نسخة من الحزمة في الجهاز وتتم معاقبة الحزمة إلى المشرف للتسجيل وفقا للفاصل الزمني الذي تم تكوينه.

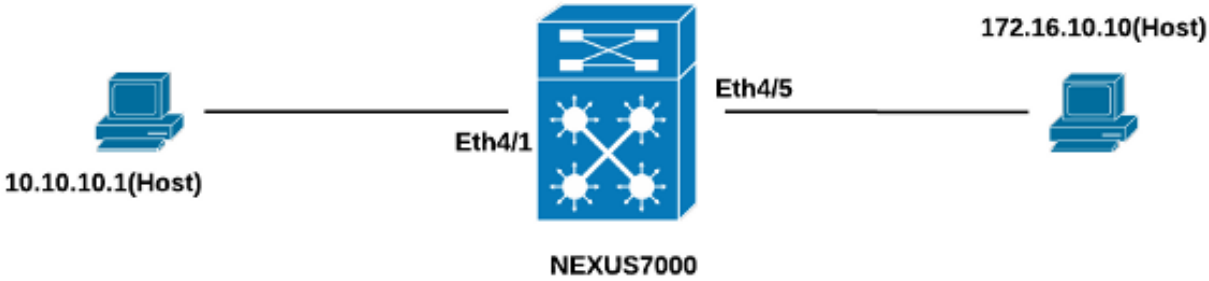
التكوين

يوفر هذا القسم معلومات يمكنك إستخدامها لتكوين محول Nexus لاستخدام قوائم التحكم في الوصول (OAL).

في المثال الموضح في هذا القسم، هناك مضيف في عنوان IP 10.10.10.1 يرسل حركة مرور البيانات إلى مضيف آخر في عنوان IP 172.16.10.10 من خلال واجهة Nexus 7000 Series، تحتوي على قائمة تحكم في الوصول (ACL) مع تسجيل تم تكوينه.

الرسم التخطيطي للشبكة

يقع الاتصال بين الأجهزة المضيفة ومحول Nexus 7000 Series وفقا لهذا المخطط:



التكوينات

أتمت هذا steps in order to شكلت المفتاح لاستخدام OALs:

1. شكلت هذا أمر شامل in order to مكنت OAL:

```
logging ip access-list cache entries 8000
logging ip access-list cache interval 300
 logging ip access-list cache threshold 0
```

فيما يلي مثال:

```
Nexus-7000# conf t
.Enter configuration commands, one per line.  End with CNTL/Z
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
 Nexus-7000(config)#logging ip access-list cache threshold 0
```

2. تطبيق هذا التكوين للتسجيل:

```
  <logging level acllog <number
<acllog match-log-level <number
<logging logfile [name] <number
```

فيما يلي مثال:

```
Nexus-7000(config)# logging level acllog 5
Nexus-7000(config)# acllog match-log-level  5
Nexus-7000(config)# logging logfile acllog 5
```

3. قم بتكوين قائمة التحكم في الوصول (ACL) لتمكين التسجيل. يجب تكوين الإدخالات باستخدام الكلمة الأساسية **log** الممكنة، كما هو موضح في هذا المثال:

```
Nexus-7000(config)# ip access-list test1
Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
Nexus-7000(config-acl)# 20 deny ip any any log
#(Nexus-7000(config-acl
Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
permit ip 10.10.10.1/32 172.16.10.10/32 log 10
deny ip any any log 20
#(Nexus-7000(config-acl
```

4. تطبيق قائمة التحكم في الوصول (ACL) التي قمت بتكوينها في الخطوة السابقة على الواجهة المطلوبة:

```
Nexus-7000# conf t
.Enter configuration commands, one per line. End with CNTL/Z
Nexus-7000(config)# int ethernet 4/1
Nexus-7000(config-if)# ip access-group test1 in
Nexus-7000(config-if)# ip access-group test1 out
#(Nexus-7000(config-if
Nexus-7000(config-if)# show run int ethernet 4/1
Command: show running-config interface Ethernet4/1!
Time: Mon Jun 30 16:30:38 2014!
(version 6.2(6
interface Ethernet4/1
ip access-group test1 in
ip access-group test1 out
ip address 10.10.10.2/24
no shutdown
#(Nexus-7000(config-if
```

التحقق من الصحة

أستخدم المعلومات المقدمة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

في المثال الذي يتم إستخدامه في هذا المستند، يتم بدء إختبار الاتصال من المضيف في عنوان IP 10.10.10.1 إلى

المضيف في عنوان IP 172.16.10.1. أدخل الأمر **show ip access-list cache** في واجهة سطر الأوامر للتحقق من تدفق حركة المرور:

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
------------------------------------------------------------
Ethernet4/1 (1)ICMP 368 0 0 172.16.10.10 10.10.10.1
Number of cache entries: 1
------------------------------------------------------------
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

أنت يستطيع رأيت ال logging كل 300 ثاني، بما أن هذا هو التقصير وقت فاصل:

```
Nexus-7000# show logging logfile
(Jun 29 19:19:01 Nexus-7000 %SYSLOG-1-SYSTEM_MSG : Logging logfile (acllog 2014
cleared by user
Jun 29 19:20:57 Nexus-7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by 2014
admin on console0
,Jun 29 19:21:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1 2014
:Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol
ICMP"(1), Hit-count = 2589"
,Jun 29 19:26:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1 2014
:Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol
ICMP"(1), Hit-count = 4561"
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ملاحظات التكوين

يوفر هذا القسم معلومات إضافية حول التكوين الموضح في هذا المستند.

التسجيل التفصيلي لقائمة التحكم في الوصول (ACL)

في إصدارات نظام التشغيل Nexus (NX-OS) 6.2(6) والإصدارات الأحدث، يتوفر تسجيل *مفصل* لقائمة التحكم في الوصول (ACL). تسجل الميزة هذه المعلومات:

- عناوين IP للمصدر والوجهة
- منافذ المصدر والوجهة
- واجهة المصدر
- البروتوكول
- اسم قائمة التحكم في الوصول (ACL)
- إجراء قائمة التحكم في الوصول (ACL) (السماح أو الرفض)
- الواجهة المطبقة
- عدد الحزم

أدخل الأمر **logging ip access-list detail** في واجهة سطر الأوامر (CLI) لتمكين التسجيل التفصيلي. فيما يلي مثال:

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
.be reset to zero and will contain Hit Count per ACL type Flow
#(Nexus-7000(config
```

هنا مثال على إخراج التسجيل بعد تمكين التسجيل التفصيلي:

```
,Jul 18 02:20:38 Nexus7k-1-oal %ACLLOG-6-ACLLOG_FLOW_INTERVAL: Src IP: 10.10.10.1 2014
:Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/5, Protocol
ICMP"(1), ACL Name: test1, ACE Action: Permit, Appl Intf: Ethernet4/5, Hit-count: 69"
```

أوصاف أوامر OAL العامة

يصف هذا القسم أوامر OAL العامة التي يتم إستخدامها لتكوين محول Nexus 7000 Series لاستخدام OALs.

	الوصف
switch(config)# logging ip access-list cache {{entries number_of_entries} | {interval seconds} | {rate-limit number_of_packet} | {threshold number_of_packet}} المحول(config)# لا يوجد ذاكرة تخزين مؤقت لقائمة الوصول إلى IP للتسجيل {entries | الفاصل الزمني | معدل الحد | العتبة}	يقوم هذا الأمر بتعيين معلمات OAL العم
إدخالات num_entries	يقوم هذا الأمر بتحويل معلمات OAL العم إلى الإعدادات الافتراضية. تحدد هذه المعلمات الحد الأقصى لعدد إد السجل التي يتم تخزينها مؤقتا في البرنامج المدى هو 0 إلى 1،048،576. القيمة الافت هي 8000 مدخل.
فاصل ثانية	تحدد هذه المعلمات الحد الأقصى للفاصل الزمني قبل إرسال إدخال إلى syslog. الم هو من 5 إلى 86،400. القيمة الافتراضية 300 ثانية.
عتبة num_packet	تحدد هذه المعلمات عدد تطابقات الحزم (عمليات الوصول) قبل إرسال إدخال إلى syslog. المدى هو من 0 إلى 000،000، القيمة الافتراضية هي 0 حزم (تحديد المع الإيقاف)، مما يعني أن سجل النظام لا يتم تشغيله بواسطة عدد تطابقات الحزم.

ملاحظة: يؤدي *الصيغة no* من أوامر CLI هذه فقط إلى إرجاع المعلمات إلى الإعدادات الافتراضية إذا تم تغييرها؛ وهو لا يزيل التكوين، نظرا لأن المحول من السلسلة Nexus 7000 Series لديه الخيار OAL فقط.

أوصاف أوامر التسجيل

يصف هذا القسم أوامر التسجيل التي يتم إستخدامها لتكوين محول Nexus 7000 Series لاستخدام قوائم التحكم في الوصول (OAL).

	الوصف
switch(config)# acllog match-log- level number مثال: switch(config)# acllog match-log- level 3	يحدد هذا الأمر مستوى التسجيل يجب مطابقته قبل تسجيل الإدخ في سجل قائمة التحكم في ال (ACLLOG). المدى هو من 0

switch(config)# no acllog match-log- level number مثال: switch(config)# no acllog match-log- level 6	7. القيمة الافتراضية هي 6. يرجع هذا الأمر مستوى التسجي الإعداد الافتراضي (6). يمكن هذا الأمر رسائل التسجيل المرفق المحدد الذي يحتوي عل مستوى الخطورة المحدد أو أع في المثال المستخدم في هذا
المحول(config)# مستوى خطورة المرفق للتسجيل مثال: switch(config)# مستوى التسجيل 3	المستند، يتم تعيين مستوى *log* على 3، بينما يكون الإعداد الاف هو 2.
المحول(config)# لا يوجد مستوى تسجيل [مستوى خطورة المرفق] مثال: switch(config)# no logging level 3	يقوم هذا الأمر بإعادة تعيين م خطورة التسجيل للمرفق المح مستواه الافتراضي. إذا لم تقم أي مرفق وأي خطورة فيقوم الجهاز بإعادة ضبط جمي المنشآت إلى مستوياتها الافتراض
switch(config)# تسجيل الدخول إلى ملف السجل-size bytes] [name rate-size] مثال: switch(config)# تسجيل الدخول إلى ملف acllog 3	في المثال المستخدم في هذا المستند، يتم إرجاع قائمة التحك الوصول إلى الوضع الافتراضي يقوم هذا الأمر بتكوين اسم مل السجل الذي يتم إستخدامه لتخ رسائل النظام والحد الأدنى لمس الخطورة قبل حدوث التسجيل. تحديد الحد الأقصى لحجم الملف إختياريا. مستوى الخطورة الافت هو 5، وحجم الملف الافتراضي 10،485،760.
switch(config)# no logging log file [logfile-name severity-level [size bytes]] مثال: switch(config)# no logging log file acllog 3	يقوم هذا الأمر بتعطيل التسجي ملف السجل.

ملاحظة: من أجل إدخال رسائل السجل في السجلات، يجب أن يكون مستوى التسجيل لمرفق سجل قائمة التحكم في الوصول (acllog) ومستوى خطورة التسجيل لملف السجل أكبر من أو يساوي إعداد مستوى *مطابقة سجل* قائمة التحكم في الوصول.

المبادئ التوجيهية والقيود

فيما يلي بعض الإرشادات والقيود المهمة التي يجب مراعاتها قبل تطبيق التكوين الموضح في هذا المستند:

- تدعم المحولات من السلسلة Nexus 7000 و 7700 تقنية OAL فقط.
- لا يعمل تسجيل قائمة التحكم في الوصول مع ميزة التقاط قائمة التحكم في الوصول (ACL).
- *السجل* لا يساند خيار في مخرج ACLs لحزم البث المتعدد.
- لا يتوفر دعم التسجيل التفصيلي لحزم IPv6.
- يجب تكوين مستوى التسجيل لمنشأة *acllog* وشدة *ملف تسجيل الدخول* بحيث تكون أكبر من أو تساوي إعداد *acllog match-log*.
- لا تستخدم الأمر **hardware access-list capture** أثناء إستخدام OAL. عند إستخدام هذا الأمر بجانب OAL،

وتمكين التقاط قائمة التحكم في الوصول (ACL)، تظهر رسالة تحذير لإعلامك بأنه يتم تعطيل تسجيل قائمة التحكم في الوصول لجميع سياقات الأجهزة الظاهرية (VDCs). عند تعطيل التقاط قائمة التحكم في الوصول (ACL)، يتم تمكين تسجيل قائمة التحكم في الوصول. لكي تعمل هذه العملية بشكل صحيح، قم بالتعطيل باستخدام الأمر **no hardware access-list capture**.

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).