مثال تكوين مرشح قائمة التحكم في الوصول لنقطة الوصول

المحتويات

المقدمة

يشرح هذا المستند كيفية تكوين عوامل التصفية المستندة إلى قائمة التحكم في الوصول (ACL) على نقاط الوصول (Cisco Aironet APs) باستخدام واجهة سطر الأوامر (CLI).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- تكوين توصيل لاسلكي باستخدام نقطة وصول Aironet ومهايئ عميل Aironet 802.11 a/b/g
- ACLs

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- نقطة الوصول من السلسلة Aironet 1200 Series التي تشغل الإصدار JA1(7)12.3 من برنامج Cisco IOS®
- مهايئ عميل Aironet 802.11a/b/g
- برنامج Aironet Desktop Utility (ADU)، الإصدار 2.5

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

أنت يستطيع استعملت مرشح على APs أن ينجز هذا مهمة:

- تقييد الوصول إلى شبكة LAN اللاسلكية (WLAN)
- توفير طبقة إضافية من الأمان اللاسلكي

يمكنك إستخدام أنواع مختلفة من عوامل التصفية لتصفية حركة المرور استنادا إلى:

- البروتوكولات المحددة
- عنوان MAC لجهاز العميل
- عنوان IP الخاص بجهاز العميل

يمكنك أيضا تمكين عوامل التصفية لتقييد حركة المرور من المستخدمين على شبكة LAN السلكية. تسمح عوامل تصفية عنوان IP وعنوان MAC بإعادة توجيه حزم البث الأحادي والبث المتعدد التي يتم إرسالها إلى أو من عناوين IP أو MAC معينة أو تمنعها.

توفر عوامل التصفية المستندة إلى البروتوكول طريقة أكثر دقة لتقييد الوصول إلى بروتوكولات معينة من خلال واجهات إيثرنت والراديو لنقطة الوصول. أنت يستطيع استعملت أحد هذا طريقة أن يشكل المرشح على ال APs:

- Web Gui
- CLI

يشرح هذا المستند كيفية إستخدام قوائم التحكم في الوصول (ACL) لتكوين عوامل التصفية من خلال واجهة سطر الأوامر. أحلت لمعلومة على كيف أن يشكل مرشح من خلال ال gui، بشكل مرشح.

يمكنك إستخدام واجهة سطر الأوامر (CLI) لتكوين هذه الأنواع من عوامل التصفية المستندة إلى قائمة التحكم في الوصول على نقطة الوصول:

- المرشحات التي تستخدم قوائم التحكم في الوصول القياسية
- المرشحات التي تستخدم قوائم التحكم في الوصول الموسعة
- المرشحات التي تستخدم قوائم التحكم في الوصول (ACL) إلى عنوان MAC

ملاحظة: يقتصر عدد الإدخالات المسموح بها على قائمة التحكم في الوصول (ACL) على وحدة المعالجة المركزية لنقطة الوصول. إذا كان هناك عدد كبير من الإدخالات لإضافتها إلى قائمة التحكم في الوصول (ACL)، على سبيل المثال، عند تصفية قائمة عناوين MAC للعملاء، أستخدم محول في الشبكة يمكنه تنفيذ المهمة.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

استعملت الأمر lookup أداة (يسجل زبون فقط) أن يجد كثير معلومة على الأمر يستعمل في هذا وثيقة.

تفترض جميع التكوينات الواردة في هذا المستند أنه قد تم بالفعل إنشاء اتصال لاسلكي. يركز هذا المستند فقط على كيفية إستخدام واجهة سطر الأوامر (CLI) لتكوين عوامل التصفية. إذا لم يكن لديك توصيل لاسلكي أساسي، ارجع إلى

مثال تكوين توصيل LAN اللاسلكي الأساسي.

عوامل التصفية التي تستخدم قوائم الوصول القياسية

يمكنك إستخدام قوائم التحكم في الوصول (ACL) القياسية للسماح بإدخال أجهزة العميل إلى شبكة WLAN أو عدم السماح بذلك استنادا إلى عنوان IP الخاص بالعميل. تقارن قوائم التحكم في الوصول (ACL) القياسية عنوان المصدر لحزم IP إلى العناوين التي تم تكوينها في قائمة التحكم في الوصول (ACL) من أجل التحكم في حركة المرور. يمكن الإشارة إلى هذا النوع من قائمة التحكم في الوصول (ACL) كمصدر قائمة تحكم في الوصول (ACL) المستندة إلى عنوان IP.

تنسيق صياغة الأمر لقائمة تحكم في الوصول (ACL) قياسية هو **access-list** *access-list-number* **{allowed | رفض} {*عنوان IP* للمضيف | *حرف بدل مصدر IP* | أي}**.

في البرنامج Cisco IOS® Software، الإصدار 12.3(7)JA، يمكن أن يكون رقم قائمة التحكم في الوصول (ACL) أي رقم من 1 إلى 99. يمكن لقوائم التحكم في الوصول (ACL) القياسية أيضا إستخدام النطاق الممتد من 1300 إلى 1999. هذه الأرقام الإضافية هي قوائم التحكم في الوصول (ACL) إلى IP الموسعة.

عندما يتم تكوين قائمة تحكم في الوصول (ACL) قياسية لرفض الوصول إلى عميل، يظل العميل مرتبطا بنقطة الوصول (AP). ومع ذلك، لا يوجد اتصال بيانات بين نقطة الوصول والعميل.

يوضح هذا المثال قائمة تحكم في الوصول (ACL) قياسية تم تكوينها لتصفية عنوان IP للعميل 10.0.0.2 من الواجهة اللاسلكية (واجهة Radio0). عنوان IP لنقطة الوصول هو 10.0.0.1.

بعد القيام بذلك، لا يمكن للعميل الذي يحمل عنوان IP 10.0.0.2 إرسال البيانات أو تلقيها من خلال شبكة WLAN حتى وإن كان العميل مقترنا بنقطة الوصول.

أكمل الخطوات التالية لإنشاء قائمة تحكم في الوصول (ACL) قياسية من خلال واجهة سطر الأوامر:

1. سجل الدخول إلى نقطة الوصول من خلال CLI (واجهة سطر الأوامر).أستخدم منفذ وحدة التحكم أو أستخدم برنامج Telnet للوصول إلى قائمة التحكم في الوصول (ACL) من خلال واجهة إيثرنت أو الواجهة اللاسلكية.
2. دخلت شامل تشكيل أسلوب على ال ap:

```
AP#configure terminal
```

3. قم بإصدار هذه الأوامر لإنشاء قائمة التحكم في الوصول (ACL) القياسية:

```
AP<config>#access-list 25 deny host 10.0.0.2
Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2. ---!
AP<config>#access-list 25 permit any
.Allow all other hosts to access the network ---!
```

4. أصدرت هذا أمر in order to طبقت هذا ACL إلى الإذاعة قارن:

```
AP<config>#interface Dot11Radio 0
AP<config-if>#ip access-group 25 in
.Apply the standard ACL to the radio interface 0 ---!
```

يمكنك أيضا إنشاء قائمة تحكم في الوصول (ACL) قياسية مسماة (NACL). يستخدم ACL اسما بدلا من رقم لتحديد قائمة التحكم في الوصول (ACL).

```
AP#configure terminal
AP<config>#ip access-list standard name
AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

أصدرت هذا أمر in order to استعملت ACLs قياسي أن ينكر المضيف 10.0.0.2 منفذ إلى ال WLAN شبكة:

```
AP#configure terminal
AP<config>#ip access-list standard TEST
.Create a standard NACL TEST ---!

AP<config-std-nacl>#deny host 10.0.0.2
Disallow the client with IP address 10.0.0.2 !--- access to the network. AP<config-std- ---!
nacl>#permit any
Allow all other hosts to access the network. AP<config-std-nacl>#exit ---!
Exit to global configuration mode. AP<config>#interface Dot11Radio 0 ---!
Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in ---!
.Apply the standard NACL to the radio interface ---!
```

عوامل التصفية التي تستخدم قوائم الوصول الموسعة

تقارن قوائم التحكم في الوصول (ACL) الموسعة عناوين المصدر والوجهة لحزم IP إلى العناوين التي تم تكوينها في قائمة التحكم في الوصول من أجل التحكم في حركة المرور. توفر قوائم التحكم في الوصول (ACL) الموسعة أيضا وسيلة لتصفية حركة المرور استنادا إلى بروتوكولات معينة. يوفر ذلك تحكم أكثر دقة لتنفيذ عوامل التصفية على شبكة WLAN.

تسمح قوائم التحكم في الوصول (ACL) الموسعة للعميل بالوصول إلى بعض الموارد على الشبكة بينما لا يمكن للعميل الوصول إلى الموارد الأخرى. على سبيل المثال، يمكنك تنفيذ عامل تصفية يسمح لحركة مرور DHCP و Telnet إلى العميل أثناء تقييده لجميع حركة مرور البيانات الأخرى.

هذه هي صياغة الأمر لقائمة التحكم في الوصول (ACL) الموسعة:

ملاحظة: يتم تضمين هذا الأمر بأربعة سطور بسبب الاعتبارات المكانية.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
[log-input] [time-range time-range-name
```

في البرنامج Cisco IOS Software، الإصدار 12.3(7)JA، يمكن لقوائم التحكم في الوصول (ACL) الموسعة إستخدام أرقام في النطاق من 100 إلى 199. يمكن أن تستخدم قوائم التحكم في الوصول (ACL) الموسعة أيضا أرقاما في النطاق من 2000 إلى 2699. هذا هو النطاق الموسع لقوائم ACL الموسعة.

ملاحظة: تظهر الكلمة الأساسية **السجل** في نهاية إدخالات قائمة التحكم في الوصول (ACL) الفردية:

- رقم قائمة التحكم في الوصول (ACL) واسمها
- ما إذا كان قد تم السماح للحزمة أو رفضها
- المعلومات الخاصة بالمنفذ

يمكن لقوائم التحكم في الوصول (ACL) الموسعة أيضا إستخدام أسماء بدلا من أرقام. هذه هي الصياغة لإنشاء قوائم التحكم في الوصول (ACL) الموسعة:

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-
[name
```

يستخدم مثال التكوين هذا قوائم التحكم في الوصول (ACL) الموسعة. المتطلب هو أن ACL موسع ينبغي أن يسمح Telnet منفذ إلى الزبون. يجب عليك تقييد جميع البروتوكولات الأخرى على شبكة WLAN. أيضا، يستعمل العملاء DHCP in order to حصلت العنوان. يجب إنشاء قائمة تحكم في الوصول (ACL) موسعة:

- يسمح ب DHCP و telnet حركة مرور

• ينفي كل انواع المرور الاخري

بمجرد تطبيق قائمة التحكم في الوصول (ACL) الموسعة هذه على واجهة الراديو، يتصل العملاء بنقطة الوصول ويحصلون على عنوان IP من خادم DHCP. كما يستطيع العملاء إستخدام برنامج Telnet. يتم رفض جميع أنواع حركة المرور الأخرى.

أتمت هذا steps in order to خلقت ACL موسع على ال AP:

1. سجل الدخول إلى نقطة الوصول من خلال CLI (واجهة سطر الأوامر).أستخدم منفذ وحدة التحكم أو برنامج Telnet للوصول إلى قائمة التحكم في الوصول (ACL) من خلال واجهة إيثرنت أو الواجهة اللاسلكية.
2. دخلت شامل تشكيل أسلوب على ال ap:

```
AP#configure terminal
```

3. أصدرت هذا أمر in order to خلقت ال موسع ACL:

```
AP<config>#ip access-list extended Allow_DHCP_Telnet
.Create an extended ACL Allow_DHCP_Telnet ---!

AP<config-extd-nacl>#permit tcp any any eq telnet
Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc ---!
Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps ---!
Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any ---!
Deny all other traffic types. AP<config-extd-nacl>#exit ---!
.Return to global configuration mode ---!
```

4. أصدرت هذا أمر in order to طبقت ال ACL إلى الإذاعة قارن:

```
AP<config>#interface Dot11Radio 0
AP<config-if>#ip access-group Allow_DHCP_Telnet in
.Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface ---!
```

المرشحات باستخدام قوائم التحكم في الوصول (ACL) المستندة إلى MAC

يمكنك إستخدام المرشحات المستندة إلى عنوان MAC لتصفية أجهزة العميل بناء على عنوان MAC المرمز بشكل ثابت. عندما يتم رفض وصول عميل من خلال عامل تصفية مستند إلى MAC، لا يمكن للعميل الاقتران بنقطة الوصول. تسمح عوامل تصفية عنوان MAC بإعادة توجيه حزم البث الأحادي والبث المتعدد التي يتم إرسالها من عناوين MAC المحددة أو توجيهها إليها.

هذه هي صياغة الأمر لإنشاء قائمة تحكم في الوصول (ACL) مستندة إلى عنوان MAC على نقطة الوصول:

ملاحظة: تم تضمين هذا الأمر في سطرين بسبب الاعتبارات المكانية.

```
access-list access-list-number {permit | deny} 48-bit-hardware-address 48-bit-hardware-address-mask
```

في البرنامج Cisco IOS Software، الإصدار 12.3(7)JA، يمكن لقوائم التحكم في الوصول (ACL) لعنوان MAC إستخدام أرقام في النطاق من 700 إلى 799 كرقم قائمة التحكم في الوصول (ACL). يمكنهم أيضا إستخدام الأرقام في النطاق الموسع من 1100 إلى 1199.

يوضح هذا المثال كيفية تكوين عامل تصفية مستند إلى MAC من خلال CLI، لتصفية العميل باستخدام عنوان MAC 0040.96a5.b5d4:

1. سجل الدخول إلى نقطة الوصول من خلال CLI (واجهة سطر الأوامر).أستخدم منفذ وحدة التحكم أو برنامج Telnet للوصول إلى قائمة التحكم في الوصول (ACL) من خلال واجهة إيثرنت أو الواجهة اللاسلكية.

2. دخلت شامل تشكيل أسلوب على ال AP CLI:

```
AP#configure terminal
```

3. إنشاء قائمة التحكم في الوصول (ACL) لعنوان MAC 700.لا تسمح قائمة التحكم في الوصول (ACL) هذه للعميل 0040.96a5.b5d4 بالاقتران بنقطة الوصول.

```
access-list 700 deny 0040.96a5.b5d4 0000.0000.0000
This ACL denies all traffic to and from !--- the client with MAC address ---!
.0040.96a5.b5d4
```

4. أصدرت هذا أمر in order to طبقت هذا baser ACL على القارن لاسلكي:

```
dot11 association mac-list 700

.Apply the MAC-based ACL ---!
```

عقب يشكل أنت هذا مرشح على ال ap، الزبون مع هذا {upper}mac address، أي كان سابقا يقترن إلى ال ap، يتبدد. ترسل وحدة تحكم AP هذه الرسالة:

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

عوامل التصفية باستخدام قوائم التحكم في الوصول (ACL) المستندة إلى الوقت

قوائم التحكم في الوصول (ACL) المستندة إلى الوقت هي قوائم تحكم في الوصول (ACL) يمكن تمكينها أو تعطيلها لفترة زمنية محددة. توفر هذه الإمكانية القوة والمرونة لتحديد سياسات السيطرة على الوصول التي تسمح بأنواع معينة من حركة المرور أو تحرمها.

يوضح هذا المثال كيفية تكوين قائمة التحكم في الوصول (ACL) المستندة إلى الوقت من خلال CLI، حيث يتم السماح باتصال Telnet من الداخل إلى الشبكة الخارجية في أيام الأسبوع أثناء ساعات العمل:

ملاحظة: يمكن تحديد قائمة تحكم في الوصول (ACL) المستندة إلى الوقت إما على منفذ Fast Ethernet أو على منفذ الراديو لنقطة الوصول Aironet AP، استنادا إلى متطلباتك. ولا يتم تطبيقها مطلقا على الواجهة الظاهرية لمجموعة الجسر (BVI).

1. سجل الدخول إلى نقطة الوصول من خلال CLI (واجهة سطر الأوامر).أستخدم منفذ وحدة التحكم أو برنامج Telnet للوصول إلى قائمة التحكم في الوصول (ACL) من خلال واجهة إيثرنت أو الواجهة اللاسلكية.
2. دخلت شامل تشكيل أسلوب على ال AP CLI:

```
AP#configure terminal
```

3. إنشاء نطاق زمني. للقيام بذلك، قم بإصدار هذا الأمر في وضع التكوين العام:

```
AP<config>#time-range Test
Create a time-range with name Test. AP(config-time-range)# periodic weekdays 7:00 to ---!
19:00
.Allows access to users during weekdays from 7:00 to 19:00 hrs ---!
```

4. إنشاء قائمة تحكم في الوصول (ACL) رقم 101:

```
AP<config># ip access-list extended 101
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
Test
This ACL permits Telnet traffic to and from !--- the network for the specified time- ---!
.range Test
```

تسمح قائمة التحكم في الوصول (ACL) هذه بجلسة عمل Telnet إلى نقطة الوصول في أيام الأسبوع.

5. قم بإصدار هذا الأمر لتطبيق قائمة التحكم في الوصول (ACL) هذه المستندة إلى الوقت على واجهة الإيثرنت:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
```

```
.Apply the time-based ACL ---!
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

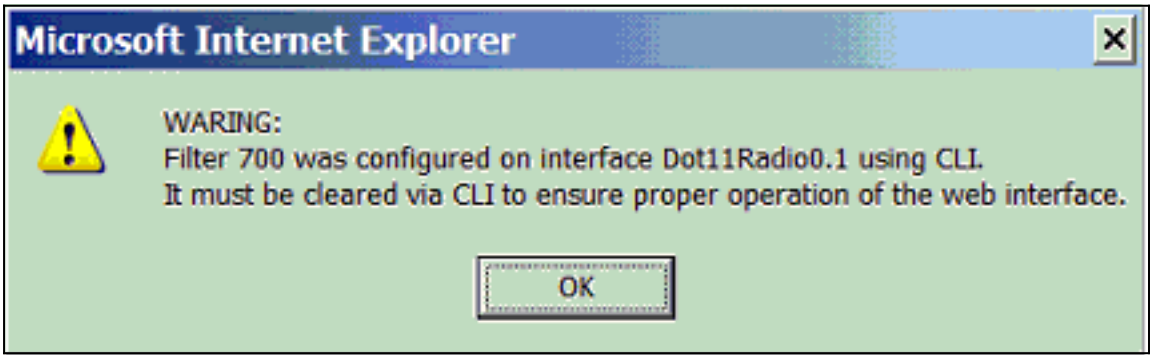
أكمل الخطوات التالية لإزالة قائمة التحكم في الوصول (ACL) من واجهة:

1. انتقل إلى وضع تكوين الواجهة.
2. أدخل **no** in front of the **ip access-group** أمر، كما يوضح هذا المثال:

```
interface interface
{no ip access-group {access-list-name | access-list-number} {in | out
```

يمكنك أيضا إستخدام اسم *number* **show access-list | أمر show ip in order to تحريت تشكيلك.** يوفر الأمر **access-list** تعدادا للحزم يوضح إدخال قائمة التحكم في الوصول (ACL) الذي يتم الوصول إليه.

تجنب إستخدام كل من واجهة سطر الأوامر (CLI) وواجهات مستعرض الويب لتكوين الجهاز اللاسلكي. إذا قمت بتكوين الجهاز اللاسلكي باستخدام CLI، فيمكن لواجهة مستعرض الويب عرض تفسير غير دقيق للتكوين. ومع ذلك، فإن عدم الدقة لا يعني بالضرورة أن الجهاز اللاسلكي مكون بشكل غير صحيح. على سبيل المثال، إذا قمت بتكوين قوائم التحكم في الوصول باستخدام CLI، يمكن لواجهة مستعرض الويب عرض هذه الرسالة:



إذا رأيت هذه الرسالة، فاستخدم واجهة سطر الأوامر (CLI) لحذف قوائم التحكم في الوصول واستخدام واجهة مستعرض الويب لإعادة تكوينها.

معلومات ذات صلة

- تكوين عوامل التصفية
- صفحة الدعم اللاسلكي
- الدعم التقني والمستندات - Cisco Systems

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).