تكوين مصادقة الويب للضيوف على نقاط الوصول (APs) المستقلة

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين الوصول الضيف على نقاط الوصول (APs) المستقلة باستخدام صفحة الويب الداخلية المضمنة في نقطة الوصول نفسها.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من هذا موضوع قبل أن يحاول أنت هذا تشكيل:

- كيفية تكوين نقاط الوصول المستقلة للتشغيل الأساسي
- كيفية تكوين خادم RADIUS المحلي على نقاط الوصول (AP) المستقلة
- كيفية عمل مصادقة الويب كمقياس أمان للطبقة 3

المكونات المستخدمة

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

- AIR-CAP3502I-E-K9 التي تشغل الصورة Cisco IOS® 15.2(4)JA1
- مهايئ لاسلكي طراز Intel Centrino Advanced-N 6200 AGN (برنامج تشغيل إصدار 13.4.0.9)

• الأداة المساعدة لنظام التشغيل Microsoft Windows 7

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

مصادقة الويب هي ميزة أمان الطبقة 3 (L3) التي تمكن نقاط الوصول (APs) الذاتية من حظر حركة مرور IP (باستثناء الحزم ذات الصلة ب DHCP و DNS) Domain Name Server) حتى يوفر الضيف اسم مستخدم وكلمة مرور صحيحين في بوابة الويب التي يتم إعادة توجيه العميل إليها عند فتح مستعرض.

باستخدام مصادقة الويب، يجب تعريف اسم مستخدم وكلمة مرور منفصلتين لكل ضيف. تتم مصادقة الضيف باستخدام اسم المستخدم وكلمة المرور إما بواسطة خادم RADIUS المحلي أو خادم RADIUS خارجي.

تم إدخال هذه الميزة في الإصدار 15.2(4)JA1 من Cisco IOS.

تكوين نقطة الوصول

ملاحظة: يفترض هذا المستند أن واجهة Bridge الظاهرية (1 (BVI على نقطة الوصول لها عنوان IP بقيمة 192.168.10.2 /24، وأن تجمع DHCP معرف داخليا على نقطة الوصول لعناوين 192.168.10.10 IP حتى 192.168.10.254 (يتم إستبعاد عناوين 192.168.10.1 IP حتى 192.168.10.10.10).

أتمت هذا steps in order to شكلت ال ap ل ضيف منفذ:

1. قم بإضافة معرف مجموعة خدمة (SSID) جديد، وتسمية **Guest**، وتكوينه لمصادقة الويب:

```
ap(config)#dot11 ssid Guest
ap(config-ssid)#authentication open
ap(config-ssid)#web-auth
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
```

2. قم بإنشاء قاعدة مصادقة، حيث يجب عليك تحديد بروتوكول مصادقة الوكيل، وتسميته **web_auth**:

```
ap(config)#ip admission name web_auth proxy http
```

3. تطبيق **Guest**) SSID) وقاعدة المصادقة (**web_auth**) على واجهة الراديو. يستخدم هذا المثال راديو 802.11b/g:

```
ap(config)#interface dot11radio 0

ap(config-if)#ssid Guest

ap(config-if)#ip admission web_auth

ap(confi-if)#no shut

ap(config-if)#exit
```

4. قم بتعريف قائمة الطرق التي تحدد مكان مصادقة مسوغات المستخدم. قم بربط اسم قائمة الطرق باستخدام قاعدة مصادقة **web_auth**، وقم بتسميته **web_list**:

```
ap(config)#ip admission name web_auth method-list authentication web_list
```

5. أكمل هذه الخطوات لتكوين المصادقة والتفويض والمحاسبة (AAA) على نقطة الوصول وخادم RADIUS المحلي، وربط قائمة الطرق بخادم RADIUS المحلي على نقطة الوصول:

تمكين المصادقة والتفويض والمحاسبة (AAA):

```
ap(config)#aaa new-model
```

قم بتكوين خادم RADIUS المحلي:

```
ap(config)#radius-server local

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

قم بإنشاء حسابات الضيوف، وحدد مدة حياتهم (بالدقائق). خلقت واحد مستعمل حساب مع username وكلمة من **مستعمل 1**، وعينت العمر قيمة إلى 60 دقيقة:

```
ap(config)#dot11 guest

ap(config-guest-mode)#username  user1 lifetime 60 password user1

ap(config-guest-mode)#exit

#(ap(config
```

يمكنك إنشاء مستخدمين آخرين بنفس العملية.

ملاحظة: يجب تمكين **خادم RADIUS المحلي** لإنشاء حسابات الضيوف.
تعريف نقطة الوصول كخادم RADIUS:

```
ap(config)#radius-server host 192.168.10.2 auth-port 1812
acct-port 1813 key cisco
```

ربط قائمة مصادقة الويب مع الخادم المحلي:

```
ap(config)#aaa authentication login web_list group radius
```

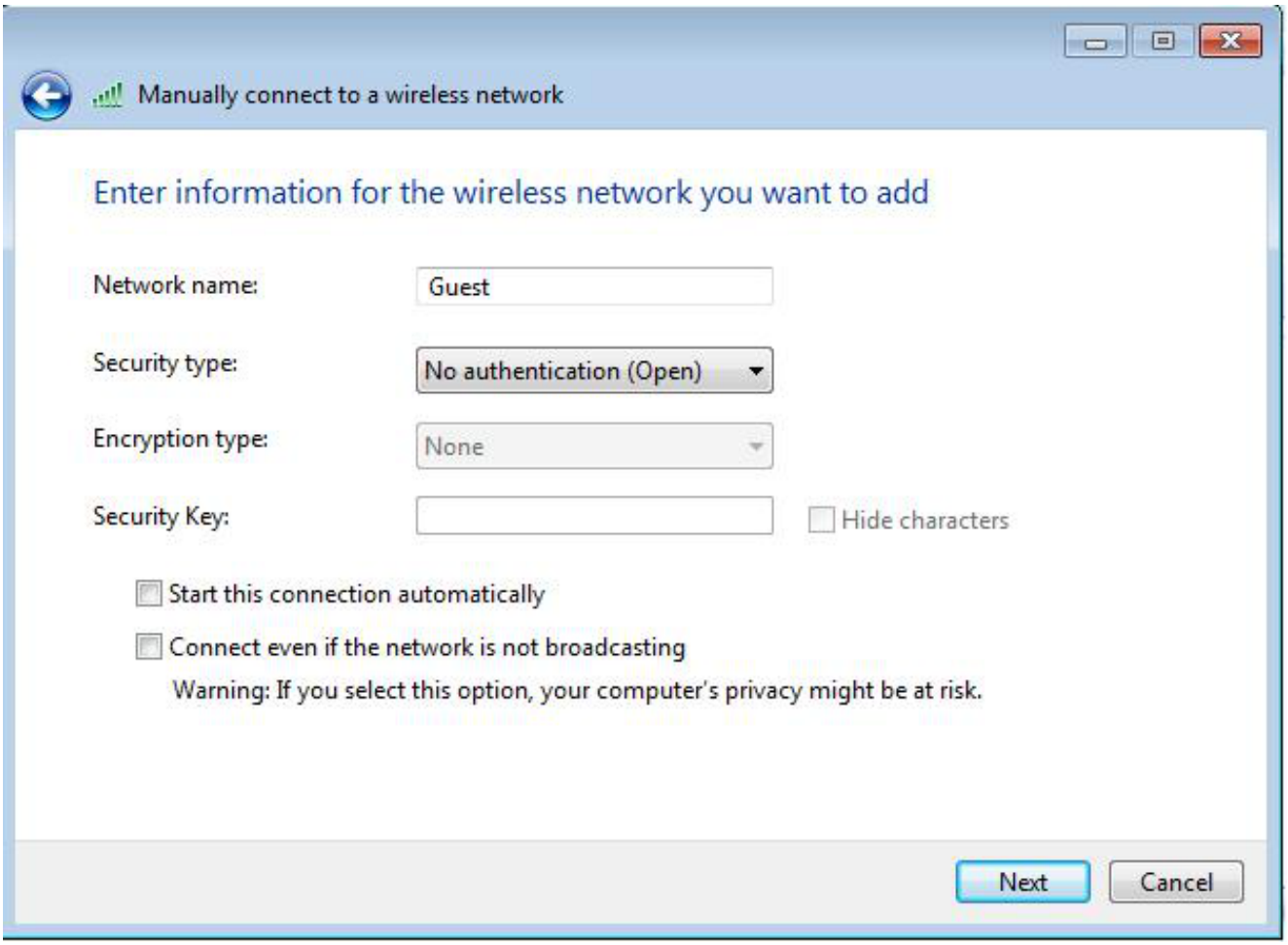
ملاحظة: يمكنك إستخدام خادم RADIUS خارجي لاستضافة حسابات المستخدمين الضيوف. للقيام بهذا الإجراء، قم بتكوين الأمر **radius-server host** للإشارة إلى الخادم الخارجي بدلا من عنوان IP لنقطة الوصول.

تكوين العميل اللاسلكي

أتمت هذا steps in order to شكلت الزبون لاسلكي:

من أجل تكوين الشبكة اللاسلكية على الأداة المساعدة الخاصة بمحول Windows باستخدام اسم **ضيف** SSID، انتقل إلى **الشبكة والإنترنت > إدارة الشبكات اللاسلكية**، ثم انقر على **إضافة**.

2. حدد **التوصيل يدويا بشبكة لاسلكية**، وأدخل المعلومات المطلوبة، كما هو موضح في هذه الصورة:



3. انقر فوق **Next (التالي)**.

التحقق من الصحة

بعد اكتمال التكوين، يمكن للعميل الاتصال ب SSID بشكل طبيعي، ويمكنك ملاحظة ذلك على وحدة تحكم نقطة الوصول:

```
DOT11-6-ASSOC: Interface Dot11Radio0, Station ap 0027.10e1.9880%
[Associated KEY_MGMT[NONE

ap#show dot11 ass

:Client Stations on Dot11Radio0 802.11

: [SSID [Guest

MAC Address    IP address   IPV6 address  Device    Name  Parent  State

0027.10e1.9880  0.0.0.0     ::           ccx-client  ap   self    Assoc
```

يكون للعميل عنوان IP ديناميكي 192.168.10.11. ومع ذلك، عند محاولة إختبار اتصال عنوان IP الخاص بالعميل، فإنه يفشل لأن العميل لم تتم مصادقته بالكامل:

```
ap#PING 192.168.10.11

.Type escape sequence to abort

:Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds

.....

(Success rate is 0 percent (0/5
```

إذا قام العميل بفتح مستعرض وحاول الوصول إلى http://1.2.3.4 على سبيل المثال، تتم إعادة توجيه العميل إلى صفحة تسجيل الدخول الداخلية:

Username:

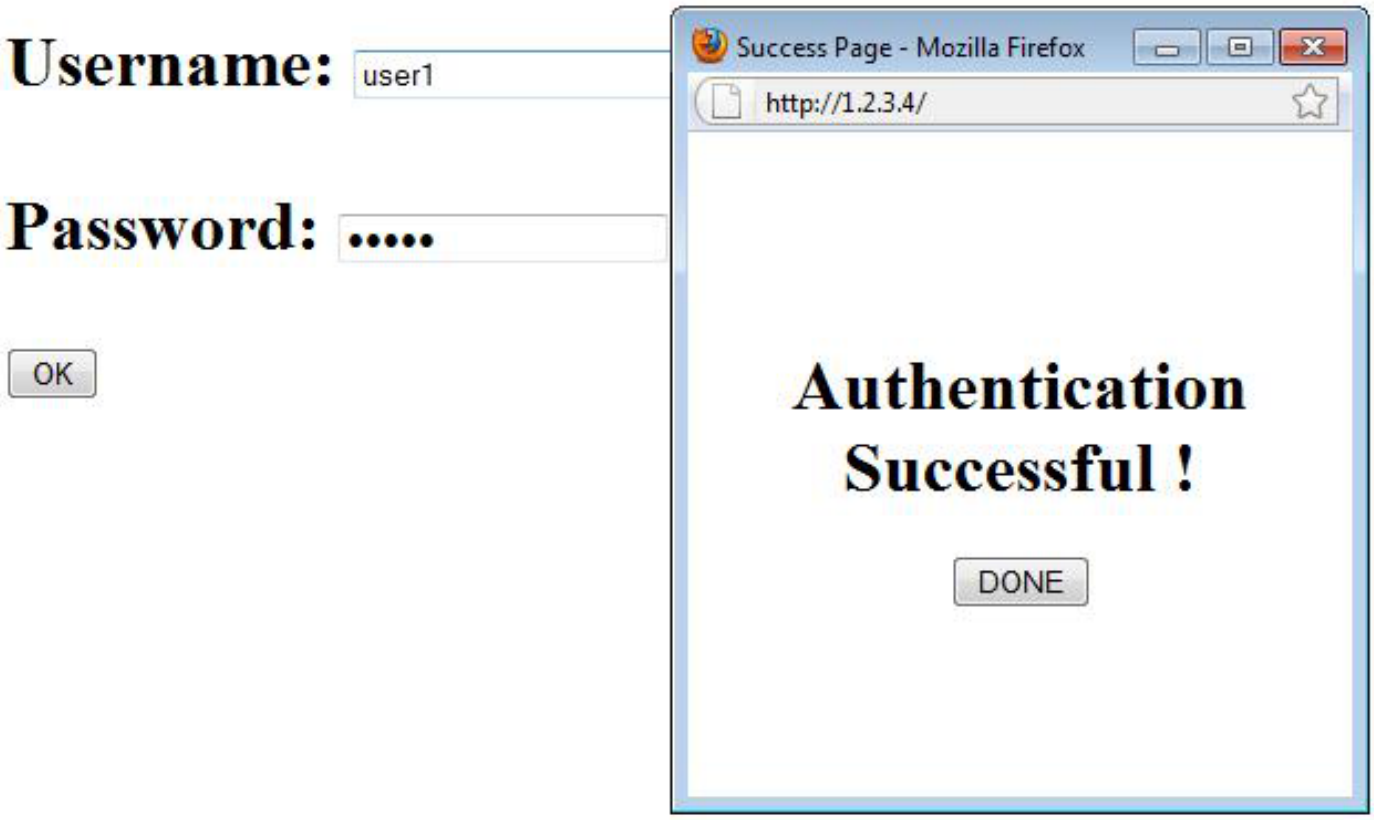
Password:

OK

ملاحظة: يتم إكمال هذا الاختبار بإدخال عنوان IP عشوائي مباشرة (هنا يكون عنوان URL الذي تم إدخاله هو **1.2.3.4**) دون الحاجة إلى ترجمة عنوان URL عبر DNS، نظرا لعدم إستخدام DNS في الاختبار. في السيناريوهات العادية، يدخل المستخدم عنوان URL للصفحة الرئيسية، ويتم السماح بحركة مرور DNS حتى يرسل العميل رسالة HTTP GET إلى العنوان الذي تم حله، والذي يتم اعتراضه بواسطة نقطة الوصول. تقوم نقطة الوصول بتزوير عنوان موقع الويب، وتعيد توجيه العميل إلى صفحة تسجيل الدخول المخزنة داخليا.

بمجرد إعادة توجيه العميل إلى صفحة تسجيل الدخول، يتم إدخال بيانات اعتماد المستخدم والتحقق منها مقابل خادم RADIUS المحلي، وفقا لتكوين نقطة الوصول. بعد المصادقة الناجحة، يتم السماح بالكامل لحركة مرور البيانات التي تأتي من العميل وتذهب إليه.

فيما يلي الرسالة التي يتم إرسالها إلى المستخدم بعد المصادقة الناجحة:



بعد المصادقة الناجحة، يمكنك عرض معلومات IP الخاصة بالعميل:

```
ap#show dot11 ass

:Client Stations on Dot11Radio0 802.11

: [SSID [Guest

MAC Address    IP address    IPV6 address  Device   Name  Parent  State

0027.10e1.9880  192.168.10.11 ::       ccx-client  ap    self   Assoc
```

يجب أن تعمل إختبارات الاتصال بالعميل بعد اكتمال المصادقة الناجحة بشكل صحيح:

```
ap#ping 192.168.10.11

.Type escape sequence to abort

:Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ملاحظة: لا يوفر التجوال بين نقاط الوصول أثناء مصادقة الويب تجربة سلسة، لأنه يجب على العملاء تسجيل الدخول إلى كل نقطة وصول جديدة يتصلون بها.

التخصيص

على غرار برنامج IOS على الموجهات أو المحولات، يمكنك تخصيص صفحتك باستخدام ملف مخصص، ومع ذلك، لا يمكن إعادة التوجيه إلى صفحة ويب خارجية.

أستخدم هذه الأوامر لتخصيص ملفات المدخل:

- **ملف صفحة تسجيل الدخول إلى HTTP لوكيل إدخال ip**
- **ملف صفحة http منتهية الصلاحية لوكيل الدخول إلى ip**
- **ملف صفحة نجاح HTTP لوكيل الدخول إلى IP**
- **ملف صفحة فشل HTTP لوكيل إدخال IP**

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).