Autonomous AP でのゲスト アクセス用の内部 Web 認証の設定例

目次

概要

このドキュメントでは、Autonomous アクセス ポイント（AP）自体に組み込まれている内部 Web ページを使用して、その AP にゲスト アクセス用の設定を行う方法について説明します。

前提条件

要件

この設定を開始する前に、次の項目に関する知識を得ておくことを推奨します。

- 基本操作用に Autonomous AP を設定する方法
- Autonomous AP での ローカル RADIUS サーバの設定方法
- レイヤ 3 のセキュリティ対策として Web 認証が機能する方法

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® イメージ 15.2(4)JA1 を実行する AIR-CAP3502I-E-K9
- Intel Centrino Advanced-N 6200 AGN ワイヤレス アダプタ（ドライバ バージョン 13.4.0.9）

- Microsoft Windows 7 のサプリカント ユーティリティ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

Web 認証は、ブラウザが開いたときにクライアントがリダイレクトされる Web ポータルで、有効なユーザ名とパスワードをゲストが入力するまで、Autonomous AP が IP トラフィック（DHCP およびドメイン ネーム サーバ（DNS）関連のパケットを除く）をブロックできるようにする、レイヤ 3（L3）のセキュリティ機能です。

Web 認証では、各ゲスト用に異なるユーザ名とパスワードを定義する必要があります。 ゲストはローカル RADIUS サーバまたは外部 RADIUS サーバでユーザ名とパスワードを使用して認証されます。

この機能は、Cisco IOS リリース 15.2(4)JA1 で導入されました。

AP の設定

> **注:** このドキュメントでは、AP のブリッジ仮想インターフェイス（BVI）1 の IP アドレスが 192.168.10.2 /24 であり、AP の内部的に定義されている DHCP プールの IP アドレスが 192.168.10.10 から 192.168.10.254（IP アドレス 192.168.10.1 から 192.168.10.10 は除外）であると仮定します。

ゲスト アクセス用に AP を設定するには、次の手順を実行します。

1. 新しい Service Set Identifier（SSID）を追加し、これを **Guest** と指定して、Web 認証用に設定します。

```
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. 認証規則を作成します。プロキシ認証プロトコルを指定して、**web_auth** と名前を付けます。

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

3. 無線インターフェイスに SSID（Guest）および認証規則（web_auth）を適用します。 この例では、 802.11b/g radio を使用しています。

```
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. ユーザのクレデンシャルの認証方法を指定する方式リストを定義します。 方式リストの名前を web_auth 認証ルールとリンクさせ、これに web_list という名前を付けます。

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

5. AP とローカル RADIUS サーバで認証、許可、アカウンティング（AAA）を設定し、AP で方式リストをローカル RADIUS サーバにリンクするには、次の手順を実行します。

   AAA を有効にします。

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

   ローカル RADIUS サーバを設定します。

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

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   ゲスト アカウントを作成し、ライフタイムを指定します（分単位）。 user1 というユーザ名とパスワードを持つユーザ アカウントを 1 つ作成し、ライフタイムを 60 分に設定します。

```
ap(config)#dot11 guest

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

ap(config-guest-mode)#exit

ap(config)#
```

   同じプロセスで他のユーザを作成できます。

注: ゲスト アカウントを作成するには **radius-server local** を有効にする必要があります。 AP を RADIUS サーバとして定義します。

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

Web 認証リストをローカル サーバとリンクします。

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

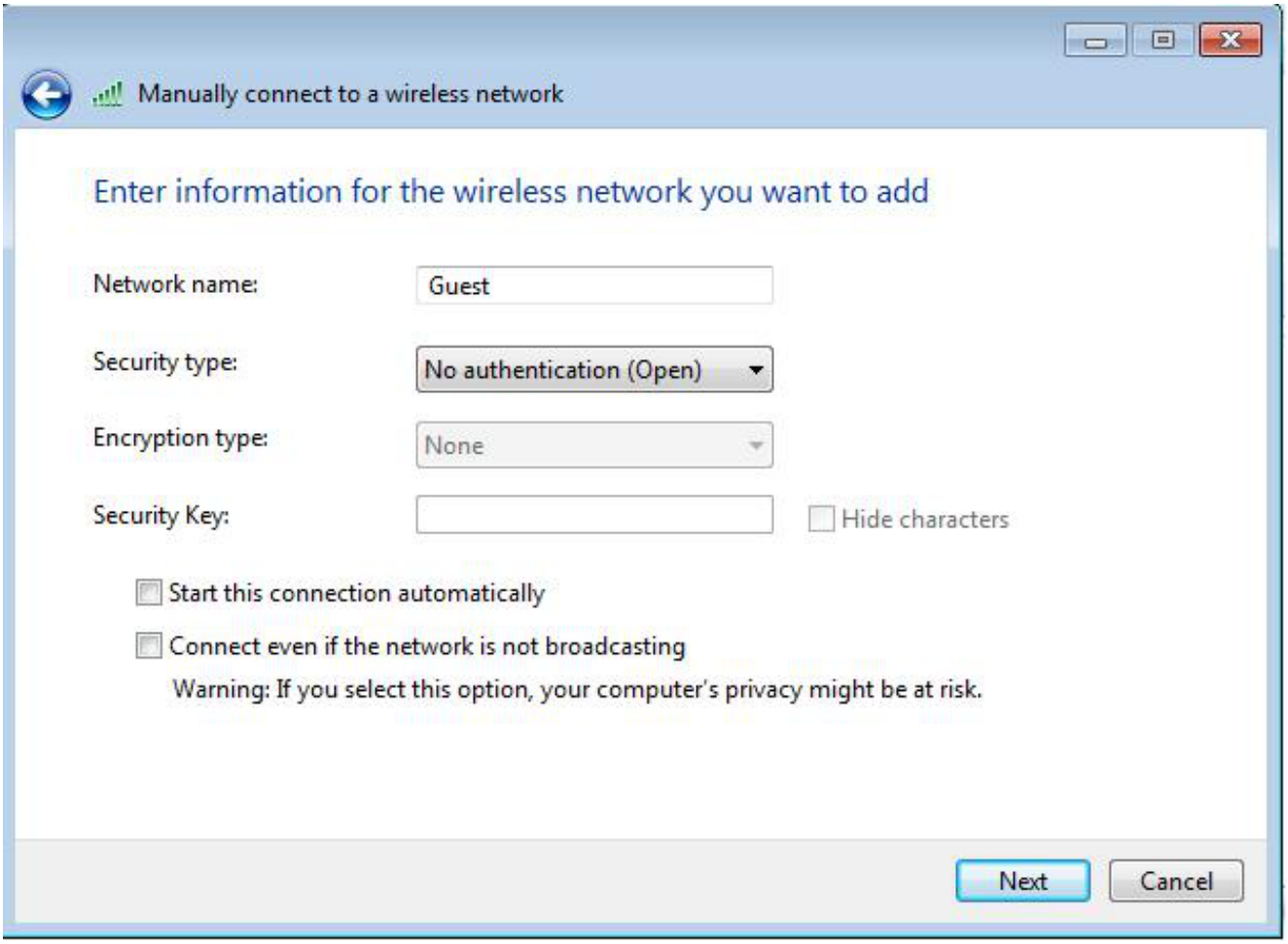
注: ゲスト ユーザ アカウントをホストするために外部 RADIUS サーバを使用できます。 これを行うには、**radius-server host コマンド**を、AP の IP アドレスではなく外部サーバを指すように設定します。

無線クライアントの設定

次の手順を実行して、無線クライアントを設定します。

1. 名前が **Guest** の SSID を使用して、Windows のサプリカント ユーティリティでワイヤレス ネットワークを設定するには、[Network and Internet] > [Manage Wireless networks] と移動して [Add] をクリックします。

2. [Manually connect to a wireless network] を選択して、次に示すように必要な情報を入力します。



3. [Next] をクリックします。

確認

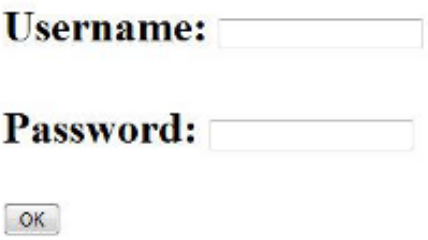
設定が完了したら、クライアントは SSID に正常に接続でき、AP コンソールに次のように表示されます。

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

ap#show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address    IP address   IPV6 address  Device    Name  Parent  State

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

クライアントには 192.168.10.11 のダイナミック IP アドレスがあります。 ただし、クライアントの IP アドレスへ ping を実行しようとすると、クライアントは完全に認証されないため失敗します:

```
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)
```

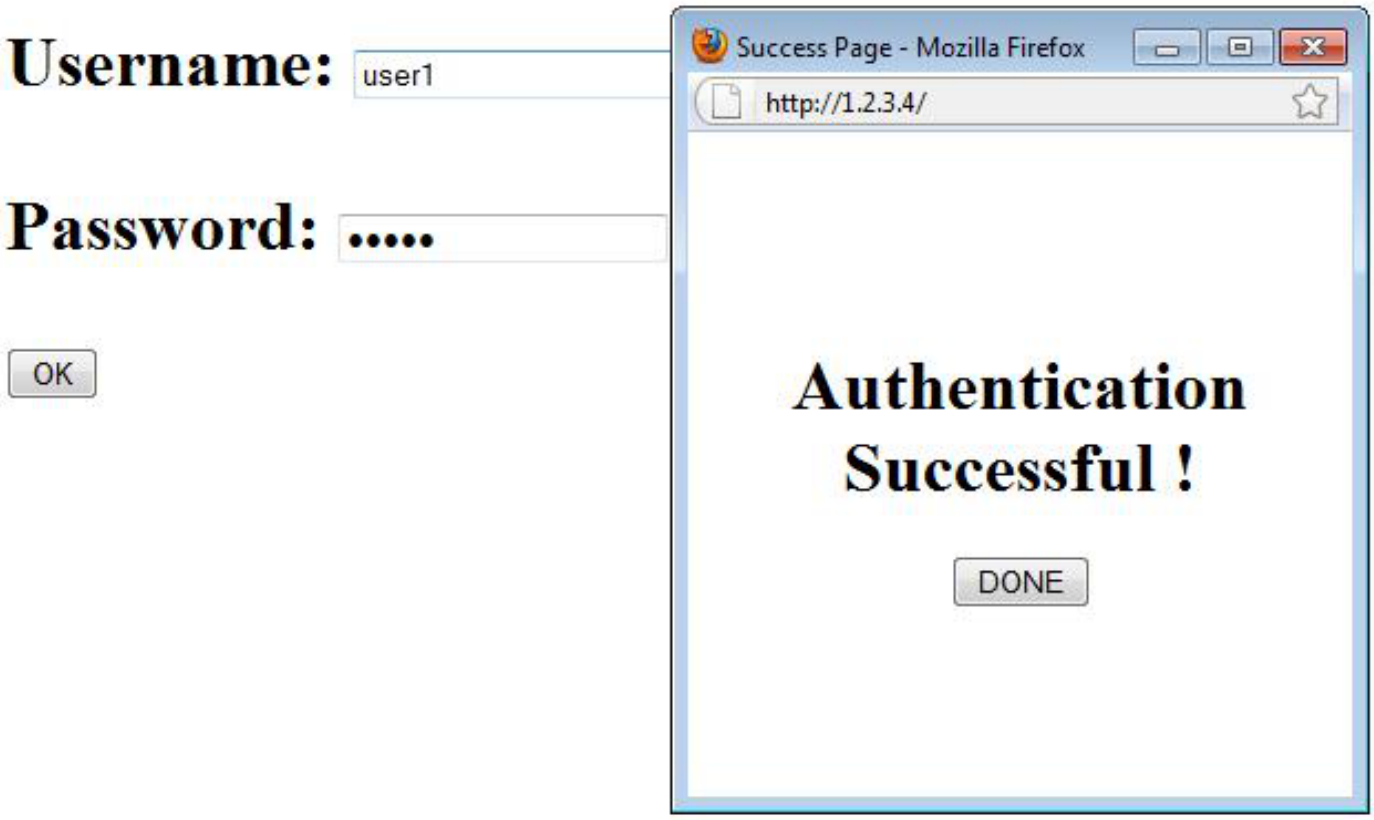
クライアントがブラウザを開き、たとえば **http://1.2.3.4** に到達しようとすると、クライアントは内部ログイン ページにリダイレクトされます。



> **注:** このテストは、DNS による URL 変換を必要とせずに（テストでは DNS を使用しなかったため）、直接入力された任意の IP アドレス（この例で入力された URL は **1.2.3.4**）で実行されます。 通常のシナリオでは、ユーザがホームページの URL を入力すると、解決するアドレス（これが AP によって代行受信される）に HTTP GET メッセージをクライアントが送信するまで DNS のトラフィックが許可されます。 AP は、Web サイトのアドレスをスプーフィングして、内部に保存されているログイン ページにクライアントをリダイレクトします。

クライアントがログイン ページにリダイレクトされると、ユーザ クレデンシャルが入力され、AP 設定に従ってローカル RADIUS サーバに対して検証されます。 認証が成功すると、クライアントで送受信されるトラフィックが完全に許可されます。

認証に成功した後にユーザに送信されるメッセージ例を次に示します。



認証が成功すると、クライアントの IP 情報を表示できます。

```
ap#show dot11 ass
802.11 Client Stations on Dot11Radio0:
SSID [Guest] :
MAC Address    IP address    IPV6 address  Device   Name  Parent  State
0027.10e1.9880  192.168.10.11 ::       ccx-client  ap    self   Assoc
```

正常な認証が完了した後、クライアントへの ping は正しく動作します。

```
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
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

> **注:** Web 認証中は、クライアントが接続するたびに新しい AP にログインする必要があるため、AP 間のローミングは円滑に行われません。

Customization

ルータやスイッチでの IOS と同様、ユーザはカスタム ファイルを使ってページをカスタマイズできます。 ただし、外部 Web ページへリダイレクトすることはできません。

ポータル ファイルをカスタマイズするには、次のコマンドを使用します。

- ip admission proxy http login page file
- ip admission proxy http expired page file
- ip admission proxy http success page file
- ip admission proxy http failure page file