Konfigurationsbeispiel für die interne Webauthentifizierung von Gastzugriff auf unabhängigen Access Points

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration des Gastzugriffs auf autonomen Access Points (APs) mithilfe der internen Webseite, die in den Access Point selbst eingebettet ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, vor dem Versuch dieser Konfiguration über Kenntnisse dieser Themen zu verfügen:

- Konfigurieren autonomer APs für den Basisbetrieb
- Konfigurieren des lokalen RADIUS-Servers auf autonomen APs
- Funktionsweise der Web-Authentifizierung als Sicherheitsmaßnahme für Layer 3

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AIR-CAP3502I-E-K9 zum Ausführen von Cisco IOS® Image 15.2(4)JA1
- Intel Centrino Advanced-N 6200 AGN Wireless-Adapter (Treiberversion 13.4.0.9)
- Microsoft Windows 7 Supplicant-Dienstprogramm

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Bei der Webauthentifizierung handelt es sich um eine Sicherheitsfunktion auf Layer 3 (L3), mit der die autonomen APs IP-Datenverkehr blockieren können (mit Ausnahme von DHCP und Paketen für Domain Name Server (DNS)), bis der Gast im Webportal, in das der Client beim Öffnen eines Browsers umgeleitet wird, einen gültigen Benutzernamen und ein gültiges Kennwort bereitstellt.

Bei der Webauthentifizierung müssen für jeden Gast ein separater Benutzername und ein separates Kennwort definiert werden. Der Gast wird entweder vom lokalen RADIUS-Server oder einem externen RADIUS-Server mit Benutzername und Kennwort authentifiziert.

Diese Funktion wurde in Cisco IOS Release 15.2(4)JA1 eingeführt.

AP-Konfiguration

> **Hinweis:** In diesem Dokument wird davon ausgegangen, dass Bridge Virtual Interface (BVI) 1 am AP die IP-Adresse 192.168.10.2/24 hat und dass der DHCP-Pool auf dem AP intern für die IP-Adressen 192.168.10.10 bis 192.168.10.254 IP (IP) definiert ist. Adressen 192.168.10.1 bis 192.168.10.10 sind ausgeschlossen).

Gehen Sie wie folgt vor, um den Access Point für den Gastzugriff zu konfigurieren:

1. Fügen Sie einen neuen Service Set Identifier (SSID) hinzu, nennen Sie ihn **Guest,** und konfigurieren Sie ihn für die Webauthentifizierung:

```
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. Erstellen Sie eine Authentifizierungsregel, in der Sie das Proxy-Authentifizierungsprotokoll

angeben und es **web_auth** nennen müssen:

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

3. Wenden Sie die SSID (**Guest**) und die Authentifizierungsregel (**web_auth**) auf die Funkschnittstelle an. In diesem Beispiel wird die 802.11b/g-Funkeinheit verwendet:

```
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. Definieren Sie die Methodenliste, die angibt, wo die Benutzeranmeldeinformationen authentifiziert werden. Verknüpfen Sie den Methodenlistennamen mit der **web_auth-**Authentifizierungsregel, und nennen Sie sie **web_list**:

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

5. Gehen Sie wie folgt vor, um die AAA-Konfiguration (Authentication, Authorization, Accounting) auf dem Access Point und dem lokalen RADIUS-Server zu konfigurieren und die Methodenliste mit dem lokalen RADIUS-Server auf dem Access Point zu verknüpfen:

   AAA aktivieren:

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

   Konfigurieren Sie den lokalen RADIUS-Server:

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

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Erstellen Sie die Gastkonten, und geben Sie deren Lebensdauer (in Minuten) an. Erstellen Sie ein Benutzerkonto mit einem Benutzernamen und einem Kennwort für **user1**, und legen Sie den Lebenszeitwert auf 60 Minuten fest:

```
ap(config)#dot11 guest

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

```
ap(config-guest-mode)#exit

ap(config)#
```

Sie können andere Benutzer mit demselben Prozess erstellen.

Hinweis: Sie müssen **Radius-Server Local** aktivieren, um Gastkonten zu erstellen. Definieren Sie den Access Point als RADIUS-Server:

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

Verknüpfen Sie die Webauthentifizierungsliste mit dem lokalen Server:

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

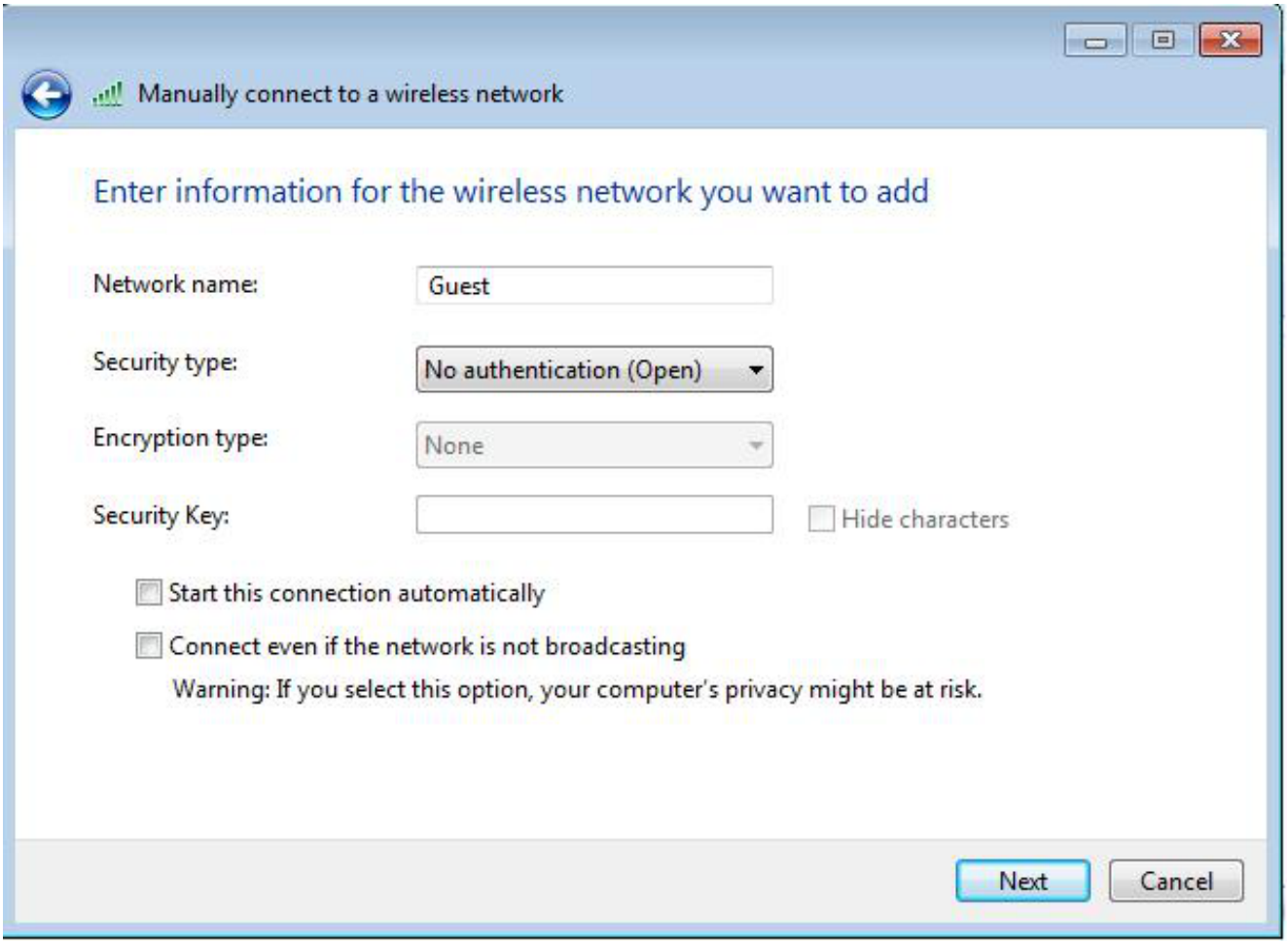
Hinweis: Sie können einen externen Radius-Server verwenden, um die Gastbenutzerkonten zu hosten. Hierzu konfigurieren Sie den Befehl **radius-server host** so, dass er auf den externen Server anstatt auf die AP-IP-Adresse zeigt.

Konfigurieren des Wireless-Clients

Gehen Sie wie folgt vor, um den Wireless-Client zu konfigurieren:

1. Um das Wireless-Netzwerk im Windows Supplicant-Dienstprogramm mit der SSID **Guest** zu konfigurieren, navigieren Sie zu **Netzwerk und Internet > Manage Wireless Networks (Wireless-Netzwerke verwalten)**, und klicken Sie auf **Add (Hinzufügen)**.

2. Wählen Sie **Manuell eine Verbindung mit einem Wireless-Netzwerk** aus, und geben Sie die erforderlichen Informationen ein, wie in diesem Bild gezeigt:



3. Klicken Sie auf **Weiter**.

Überprüfung

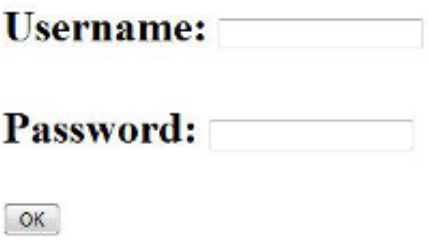
Nachdem die Konfiguration abgeschlossen ist, kann der Client normal eine Verbindung zum SSID herstellen. Dies wird auf der AP-Konsole angezeigt:

```
%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
```

Der Client hat die dynamische IP-Adresse 192.168.10.11. Wenn Sie jedoch versuchen, die IP-Adresse des Clients zu pingen, schlägt sie fehl, weil der Client nicht vollständig authentifiziert ist:

```
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)
```

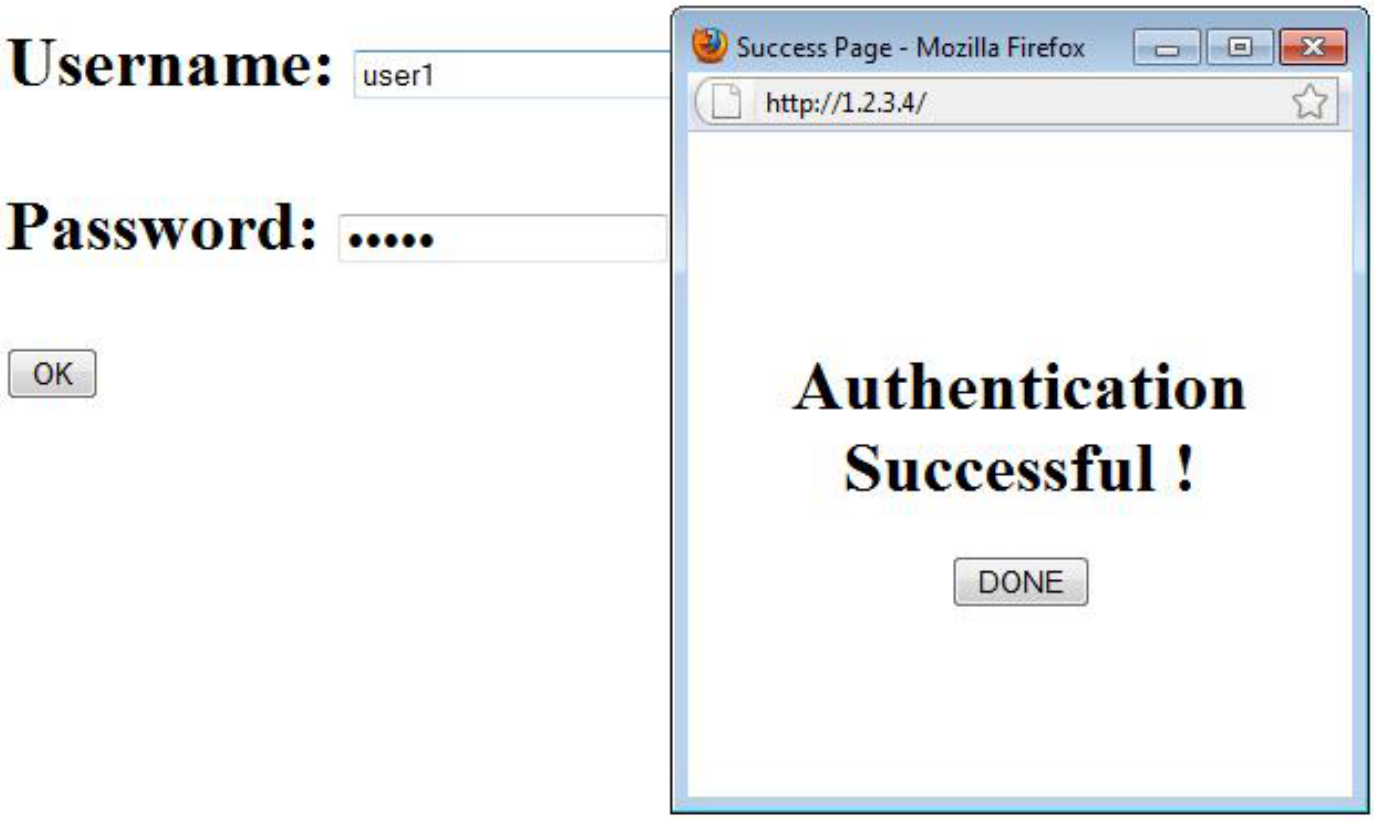
Wenn der Client beispielsweise einen Browser öffnet und versucht, **http://1.2.3.4** zu erreichen, wird der Client zur internen Anmeldeseite umgeleitet:



> **Hinweis:** Dieser Test wird mit einer zufälligen IP-Adresse abgeschlossen, die direkt eingegeben wird (hier ist die eingegebene URL **1.2.3.4**), ohne dass eine URL über den DNS übersetzt werden muss, da der DNS nicht im Test verwendet wurde. In normalen Szenarien gibt der Benutzer die URL der Startseite ein, und der DNS-Datenverkehr ist zulässig, bis der Client die HTTP GET-Nachricht an die aufgelöste Adresse sendet, die vom Access Point abgefangen wird. Der WAP kopiert die Website-Adresse und leitet den Client an die intern gespeicherte Anmeldeseite weiter.

Wenn der Client zur Anmeldeseite umgeleitet wird, werden die Benutzeranmeldeinformationen gemäß der AP-Konfiguration für den lokalen RADIUS-Server eingegeben und überprüft. Nach erfolgreicher Authentifizierung ist der Datenverkehr vom und zum Client vollständig zulässig.

Die folgende Nachricht wird nach erfolgreicher Authentifizierung an den Benutzer gesendet:



Nach erfolgreicher Authentifizierung können Sie die Client-IP-Informationen anzeigen:

```
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
```

Pings an den Client nach erfolgreicher Authentifizierung sollten ordnungsgemäß funktionieren:

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

> **Hinweis:** Das Roaming zwischen APs während der Webauthentifizierung bietet kein reibungsloses Benutzererlebnis, da sich die Clients bei jedem neuen AP anmelden müssen, mit dem sie eine Verbindung herstellen.

Anpassung

Ähnlich wie IOS auf Routern oder Switches können Sie Ihre Seite mit einer benutzerdefinierten Datei anpassen. Es ist jedoch nicht möglich, auf eine externe Webseite umzuleiten.

Verwenden Sie diese Befehle, um die Portaldateien anzupassen:

- IP-Zugangsproxy http-Anmeldeseitendatei
- IP-Zugangsproxy http Abgelaufene Seitendatei
- ip administrator proxy http-Erfolgsseite Datei
- ip administrator proxy http Failure-page-Datei