Autenticación del Web interna para el acceso de invitado en el ejemplo de configuración autónomo AP

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configuración AP](#)
[Configure al cliente de red inalámbrica](#)
[Verificación](#)
[Troubleshooting](#)
[Arreglo para requisitos particulares](#)

Introducción

Este documento describe cómo configurar para el acceso de invitado en el (APS) autónomo de los Puntos de acceso con el uso de la página web interna que se integra en el AP sí mismo.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente esta configuración:

- Cómo configurar los AP autónomos para la operación básica
- Cómo configurar al servidor de RADIUS local en los AP autónomos
- Cómo autenticación Web como trabajos de la capa 3 de una medida de Seguridad

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AIR-CAP3502I-E-K9 que funciona con la imagen 15.2(4)JA1 del ® del Cisco IOS
- Adaptador de red inalámbrica avanzado-n de Intel Centrino 6200 AGN (versión del driver 13.4.0.9)
- Utilidad del supplicant de Microsoft Windows 7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La autenticación Web es una función de seguridad de la capa 3 (L3) que permite a los AP autónomos para bloquear el tráfico IP (excepto el DHCP y el Domain Name Server (DNS) - los paquetes relacionados) hasta que el invitado proporcione un nombre de usuario válido y una contraseña en el portal web al cual reorientan al cliente cuando abren a un navegador.

Con la autenticación Web, un nombre de usuario y contraseña separado se debe definir para cada invitado. A un servidor RADIUS externo autentica al invitado con el nombre de usuario y contraseña el servidor de RADIUS local o.

Esta característica fue introducida en el Cisco IOS Release 15.2(4)JA1.

Configuración AP

> **Note**: Este documento asume que el (BVI) 1 del Interfaz Virtual de Bridge en el AP tiene una dirección IP de 192.168.10.2 /24, y que definen al agrupamiento DHCP internamente en el AP para los IP Addresses 192.168.10.10 con 192.168.10.254 (IP Addresses 192.168.10.1 con 192.168.10.10 se excluyen).

Complete estos pasos para configurar el AP para el acceso de invitado:

1. Agregue un nuevo Service Set Identifier (SSID), nómbrelo **invitado,** y configurelo para la autenticación Web:

```
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. Cree una regla de la autenticación, donde usted debe especificar el protocolo de autenticación de representación, y nómbrela **web_auth**:

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

3. Aplique el SSID (**invitado**) y la regla de la autenticación (**web_auth**) a la interfaz radio. Este ejemplo utiliza la radio 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. Defina la lista de métodos que especifica donde se autentican los credenciales de usuario. Conecte el nombre de la lista de métodos a la regla de la autenticación del **web_auth**, y nómbrelo **web_list**:

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

5. Complete estos pasos para configurar el Authentication, Authorization, and Accounting (AAA) en el AP y el servidor de RADIUS local, y enlace la lista de métodos al servidor de RADIUS local en el AP:

   Permiso AAA:

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

   Configure al servidor de RADIUS local:

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

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Cree las cuentas de invitado, y especifique su curso de la vida (en los minutos). Cree una cuenta de usuario con un nombre de usuario y contraseña del **user1**, y fije el valor del curso de la vida a 60 minutos:

```
ap(config)#dot11 guest

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

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

ap(config)#
```

Usted puede crear a otros usuarios con el mismo proceso.

Note: Usted debe permitir al **local del radio-servidor** para crear las cuentas de invitado. Defina el AP como servidor de RADIUS:

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

Enlace la lista de la autenticación Web al servidor local:

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

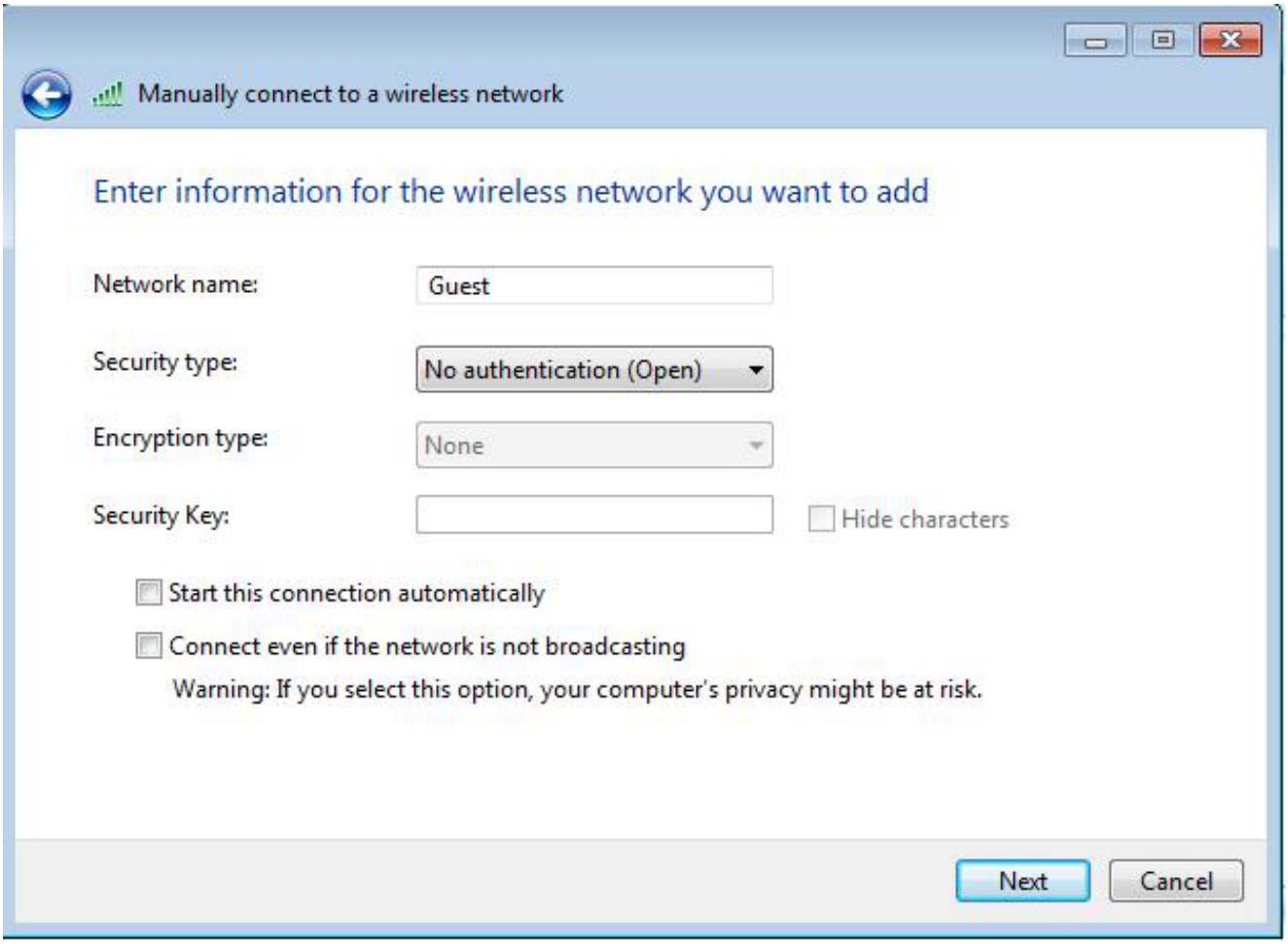
Note: Usted puede utilizar a un servidor RADIUS externo para recibir las cuentas de Usuario invitado. Para hacer esto, configure el **comando radius-server host** de señalar al servidor externo en vez de la dirección IP AP.

Configure al cliente de red inalámbrica

Complete estos pasos para configurar al cliente de red inalámbrica:

1. Para configurar la red inalámbrica en sus ventanas que la utilidad del supplicant con el SSID nombró a **Guest**, navegue a la **red y Internet > maneja las redes inalámbricas**, y el haga click en Add

2. Seleccione **conectan manualmente con una red inalámbrica**, y ingresan la Información requerida, tal y como se muestra en de esta imagen:



3. Haga clic en Next (Siguiente).

Verificación

Después de que la configuración sea completa, el cliente puede conectar con el SSID normalmente, y usted ve esto en la consola AP:

```
%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
```

El cliente tiene un IP Address dinámico de 192.168.10.11. Sin embargo, cuando usted intenta hacer ping la dirección IP del cliente, falla porque no autentican al cliente completamente:

```
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)
```

Si el cliente abre a un navegador, e intenta alcanzar **http://1.2.3.4** por ejemplo, reorientan al cliente a la página de registro interna:

Username:

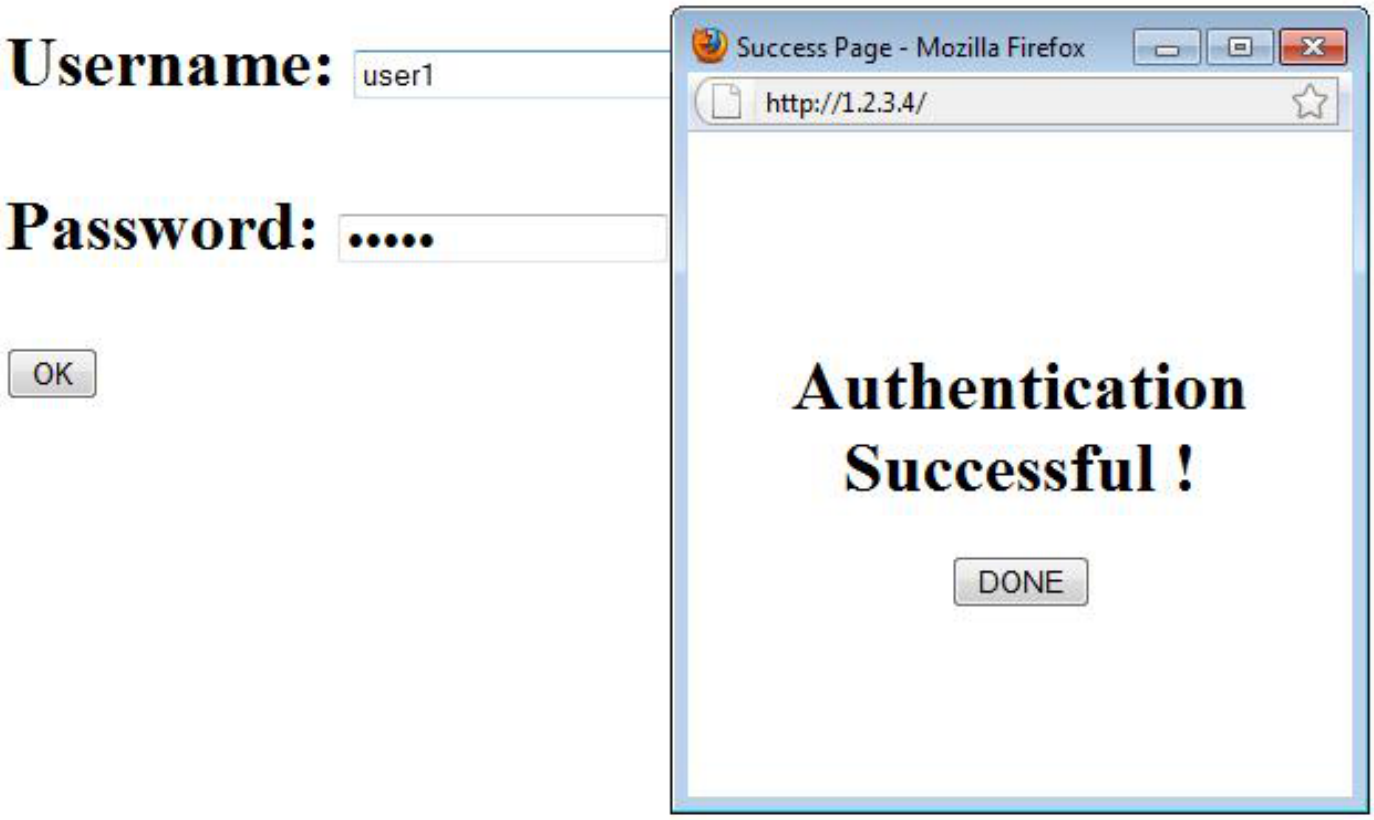
Password:

OK

> **Note**: Esta prueba se completa con un IP Address al azar ingresado directamente (aquí el URL ingresado es **1.2.3.4**) sin la necesidad de la traducción de un URL con el DNS, porque el DNS no fue utilizado en la prueba. En las circunstancias normales, el usuario ingresa el Home Page URL, y se permite el tráfico DNS hasta que el cliente envíe el mensaje HTTP GET al direccionamiento resolved, que es interceptado por el AP. Las parodias AP el direccionamiento de sitio web, y reorientan al cliente a la página de registro salvada internamente.

Una vez que reorientan al cliente a la página de registro, los credenciales de usuario se ingresan y se verifican contra el servidor de RADIUS local, según la configuración AP. Después de la autenticación satisfactoria, el tráfico que viene de y va al cliente se permite completamente.

Aquí está el mensaje que se envía al usuario después de la autenticación satisfactoria:



Después de la autenticación satisfactoria, usted puede ver IP del cliente la información:

```
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
```

Los ping al cliente después de que la autenticación satisfactoria sea completa deben trabajar correctamente:

```
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
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

> **Note**: La itinerancia entre los AP durante la autenticación Web no proporciona una experiencia lisa, porque los clientes deben iniciar sesión a cada nuevo AP con el cual conecten.

Arreglo para requisitos particulares

Similar al IOS en el Routers o el Switches, usted puede personalizar su página con un archivo de encargo; sin embargo, no es posible reorientar a una página web externa.

Utilice estos comandos para personalizar los archivos porta:

- archivo de página de registro HTTP del proxy de la admisión del IP
- el HTTP del proxy de la admisión del IP expiró archivo de paginación
- archivo de paginación del éxito HTTP del proxy de la admisión del IP
- archivo de paginación del error HTTP del proxy de la admisión del IP