Configuración de la Autenticación Web para Invitados en AP Autónomos

Contenido

Introducción

Este documento describe cómo configurar el acceso de invitado en puntos de acceso (AP) autónomos con el uso de la página web interna que está incrustada en el AP mismo.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre estos temas antes de intentar esta configuración:

- Cómo configurar los AP autónomos para el funcionamiento básico
- Cómo configurar el servidor RADIUS local en AP autónomos
- Cómo funciona la autenticación web como medida de seguridad de capa 3

Componentes Utilizados

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

- AIR-CAP3502I-E-K9 que ejecuta la imagen Cisco IOS® 15.2(4)JA1
- Adaptador inalámbrico Intel Centrino Advanced-N 6200 AGN (controlador versión 13.4.0.9)
- utilidad del suplicante 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). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

La autenticación Web es una función de seguridad de capa 3 (L3) que permite que los AP autónomos bloqueen el tráfico IP (excepto los paquetes relacionados con DHCP y el servidor de nombres de dominio (DNS)) hasta que el invitado proporcione un nombre de usuario y una contraseña válidos en el portal web al que se redirige al cliente cuando se abre un navegador.

Con la autenticación web, se debe definir un nombre de usuario y una contraseña independientes para cada invitado. El invitado es autenticado con el nombre de usuario y la contraseña por el servidor RADIUS local o un servidor RADIUS externo.

Esta función se introdujo en Cisco IOS Release 15.2(4)JA1.

Configuración de AP

> Nota: Este documento asume que la Interfaz Virtual de Bridge (BVI) 1 en el AP tiene una dirección IP de 192.168.10.2 /24, y que el conjunto DHCP está definido internamente en el AP para las direcciones IP de 192.168.10.10 a 192.168.10.254 (direcciones IP de 192.168.10.1 a 192.168.10 10 están excluidos).

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

1. Agregue un nuevo Identificador de conjunto de servicios (SSID) , asígnele el nombre de Invitado y configúrelo para la autenticación Web:

```
<#root>

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 autenticación, donde debe especificar el protocolo de autenticación de proxy y denominarlo web_auth:

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

3. Aplique el SSID (Guest) y la regla de autenticación (web_auth) a la interfaz de radio. Este ejemplo utiliza radio 802.11b/g:

```
<#root>
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 dónde se autentican las credenciales del usuario. Vincule el nombre de la lista de métodos con la regla de autenticación web_auth y asígnele el nombre web_list:

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

5. Complete estos pasos para configurar la autenticación, la autorización y la contabilidad (AAA) en el AP y el servidor RADIUS local, y vincule la lista de métodos con el servidor RADIUS local en el AP:

   A. Activar AAA:

```
<#root>
ap(config)#
aaa new-model
```

   B. Configure el servidor RADIUS local:

```
<#root>
ap(config)#
radius-server local


ap(config-radsrv)#
nas 192.168.10.2 key cisco


ap(config-radsrv)#
exit
```

   C. Cree las cuentas de invitado y especifique su duración (en minutos). Cree una cuenta de usuario con el nombre de usuario y la contraseña user1, y establezca el valor de

duración en 60 minutos:

```
<#root>

ap(config)#

dot11 guest


ap(config-guest-mode)#

username  user1 lifetime 60 password user1


ap(config-guest-mode)#

exit


ap(config)#
```

Puede crear otros usuarios con el mismo proceso.

Nota: Debe habilitar radius-server local para crear cuentas de invitado.

D. Defina el AP como un servidor RADIUS:

```
<#root>

ap(config)#

radius-server host 192.168.10.2 auth-port 1812
 acct-port 1813 key cisco
```

E. Vincule la lista de autenticación Web con el servidor local:

```
<#root>

ap(config)#

aaa authentication login web_list group radius
```

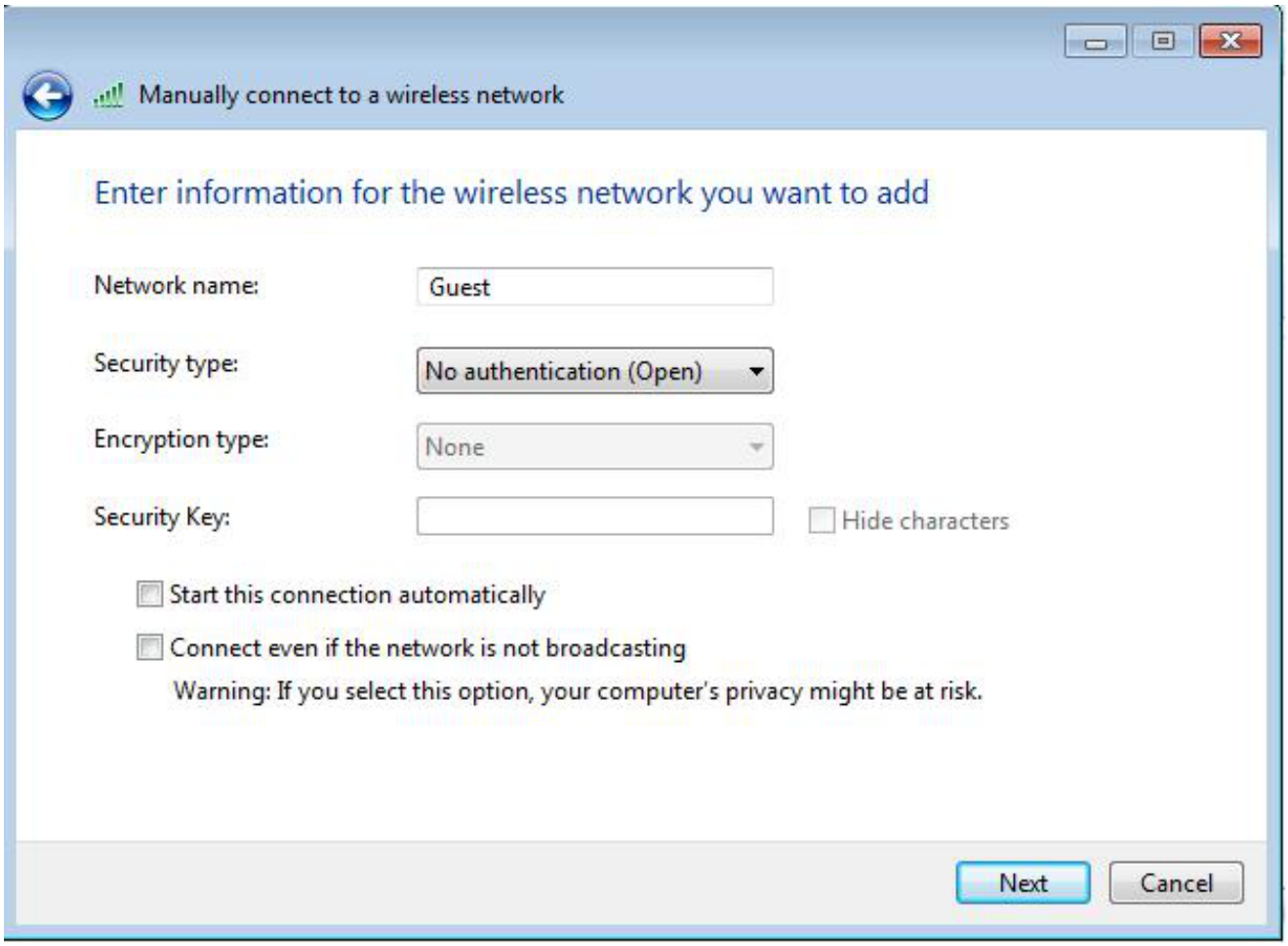
Nota: Puede utilizar un servidor RADIUS externo para alojar las cuentas de usuario invitado. Para hacer esto, configure el comando radius-server host para que apunte al servidor externo en lugar de a la dirección IP del AP.

Configuración del cliente inalámbrico

Complete estos pasos para configurar el cliente inalámbrico:

1. Para configurar la red inalámbrica en su utilidad del suplicante de Windows con el SSID llamado Invitado, navegue hasta Red e Internet > Manejar redes inalámbricas, y haga clic en Agregar.

2. Seleccione Manually connect to a wireless network, e ingrese la información requerida, como se muestra en esta imagen:



3. Haga clic en Next (Siguiente).

Verificación

Una vez que se completa la configuración, el cliente puede conectarse al SSID normalmente, y esto se ve en la consola AP:

```
<#root>

%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 una dirección IP dinámica de 192.168.10.11. Sin embargo, cuando intenta hacer ping en la dirección IP del cliente, se produce un error porque el cliente no está totalmente autenticado:

```
<#root>

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 un navegador e intenta alcanzar http://1.2.3.4, por ejemplo, el cliente se redirige a la página de inicio de sesión interno:

Username:

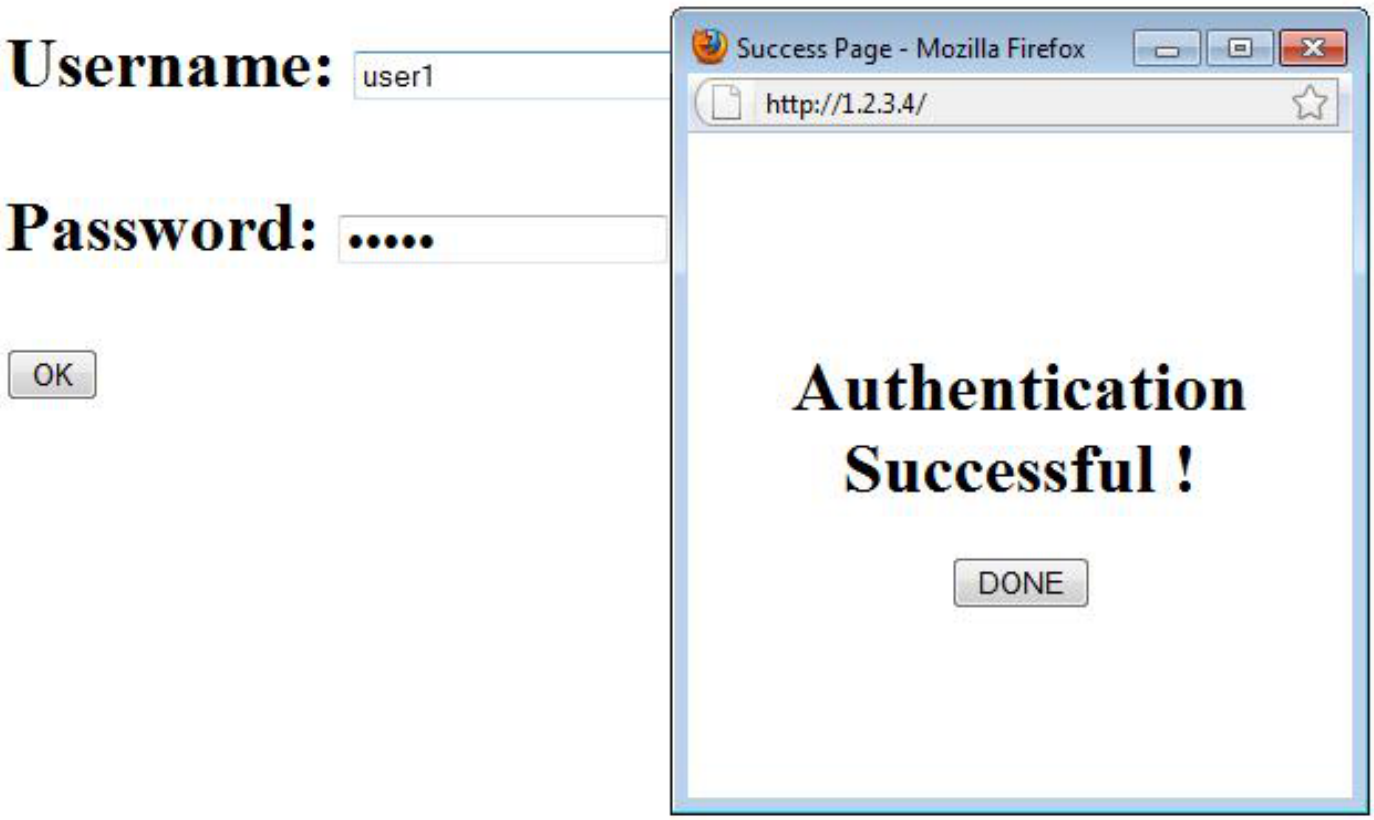
Password:

OK

Nota: Esta prueba se completa con una dirección IP aleatoria introducida directamente (donde la URL introducida es 1.2.3.4) sin necesidad de traducción de una URL a través del DNS, ya que el DNS no se utilizó en la prueba. En escenarios normales, el usuario ingresa la URL de la página de inicio y se permite el tráfico DNS hasta que el cliente envía el mensaje HTTP GET a la dirección resuelta, que es interceptada por el AP. El AP falsifica la dirección del sitio web y redirige al cliente a la página de inicio de sesión almacenada internamente.

Una vez que el cliente se redirige a la página de login, las credenciales del usuario se ingresan y verifican contra el servidor RADIUS local, según la configuración AP. Después de una autenticación exitosa, el tráfico que viene y va al cliente está totalmente permitido.

Este es el mensaje que se envía al usuario después de una autenticación exitosa:



Después de una autenticación exitosa, puede ver la información de IP del cliente:

<#root>

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 completar la autenticación exitosa deberían funcionar correctamente:

<#root>

```
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
```

Troubleshoot

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

> Nota: Roaming entre APs durante la autenticación web no proporciona una experiencia sin problemas, porque los clientes deben iniciar sesión en cada nuevo AP al que se conectan.

Personalización

De forma similar al IOS de los routers o switches, puede personalizar la página con un archivo personalizado; sin embargo, no es posible redirigir a una página web externa.

Utilice estos comandos para personalizar los archivos del portal:

- 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).