Configurar a autenticação da Web para convidados em APs autônomos

Contents

Introdução

Este documento descreve como configurar o acesso de convidado em access points (APs) autônomos com o uso da página da Web interna que está incorporada no próprio AP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos antes de tentar esta configuração:

- Como configurar APs autônomos para operação básica
- Como configurar o servidor RADIUS local em APs autônomos
- Como funciona a autenticação da Web como uma medida de segurança de Camada 3

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AIR-CAP3502I-E-K9 que executa a imagem Cisco IOS® 15.2(4)JA1
- Adaptador sem fio Intel Centrino Advanced-N 6200 AGN (Versão do driver 13.4.0.9)
- utilitário suplicante do Microsoft Windows 7

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

A autenticação da Web é um recurso de segurança de Camada 3 (L3) que permite que os APs autônomos bloqueiem o tráfego IP (exceto pacotes relacionados ao DHCP e ao Servidor de Nome de Domínio (DNS)) até que o convidado forneça um nome de usuário e uma senha válidos no portal da Web para os quais o cliente é redirecionado quando um navegador é aberto.

Com a autenticação da Web, um nome de usuário e uma senha separados devem ser definidos para cada convidado. O convidado é autenticado com o nome de usuário e a senha pelo servidor RADIUS local ou por um servidor RADIUS externo.

Esse recurso foi introduzido no Cisco IOS versão 15.2(4)JA1.

Configuração de AP

> Observação: este documento supõe que a BVI (Bridge Virtual Interface) 1 no AP tenha um endereço IP de 192.168.10.2 /24 e que o pool de DHCP seja definido internamente no AP para endereços IP de 192.168.10.10 a 192.168.10.254 (endereços IP de 192.168.10.1 a 192.168.1) 0,10).

Conclua estas etapas para configurar o AP para acesso de convidado:

1. Adicione um novo Service Set Identifier (SSID) , nomeie-o como Guest e configure-o para autenticação da 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. Crie uma regra de autenticação, onde você deve especificar o protocolo de autenticação de proxy e nomeá-lo web_auth:

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

3. Aplique o SSID (Guest) e a regra de autenticação (web_auth) à interface de rádio. Este exemplo usa rádio 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 a lista de métodos que especifica onde as credenciais do usuário são autenticadas. Vincule o nome da lista de métodos à regra de autenticação web_auth e nomeie-a como web_list:

```
<#root>

ap(config)#

ip admission name web_auth method-list authentication web_list
```

5. Conclua estas etapas para configurar a Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization, and Accounting) no AP e no servidor RADIUS local, e vincule a lista de métodos com o servidor RADIUS local no AP:

   A. Ativar AAA:

```
<#root>

ap(config)#

aaa new-model
```

   B. Configure o servidor RADIUS local:

```
<#root>

ap(config)#

radius-server local


ap(config-radsrv)#

nas 192.168.10.2 key cisco


ap(config-radsrv)#

exit
```

   C. Crie as contas de convidado e especifique seu tempo de vida (em minutos). Crie uma conta de usuário com um nome de usuário e uma senha de user1 e defina o valor do

tempo de vida como 60 minutos:

```
<#root>

ap(config)#

dot11 guest


ap(config-guest-mode)#

username  user1 lifetime 60 password user1


ap(config-guest-mode)#

exit


ap(config)#
```

Você pode criar outros usuários com o mesmo processo.

Observação: você deve habilitar radius-server local para criar contas de convidado.

D. Defina o AP como um servidor RADIUS:

```
<#root>

ap(config)#

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

E. Vincule a lista de autenticação da Web ao servidor local:

```
<#root>

ap(config)#

aaa authentication login web_list group radius
```

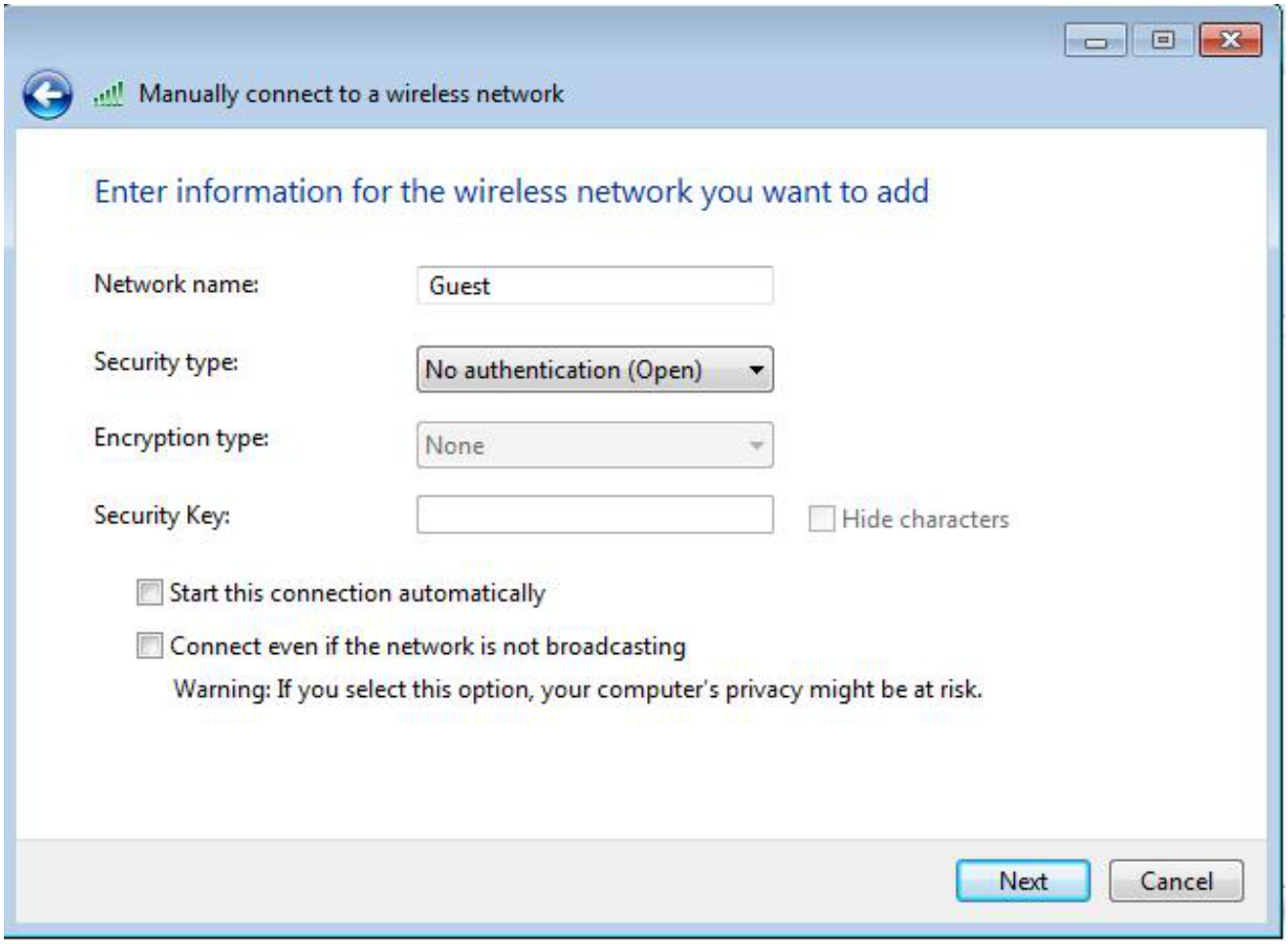
Observação: você pode usar um servidor radius externo para hospedar as contas de usuário convidado. Para fazer isso, configure o comando radius-server host para apontar para o servidor externo em vez do endereço IP do AP.

Configurar o cliente sem fio

Conclua estas etapas para configurar o cliente sem fio:

1. Para configurar a rede sem fio no utilitário suplicante do Windows com o SSID chamado Guest, navegue para Network and Internet > Manage Wireless Networks e clique em Add.

2. Selecione Conectar manualmente a uma rede sem fio e insira as informações necessárias, como mostrado na imagem:



3. Clique em Next.

Verificar

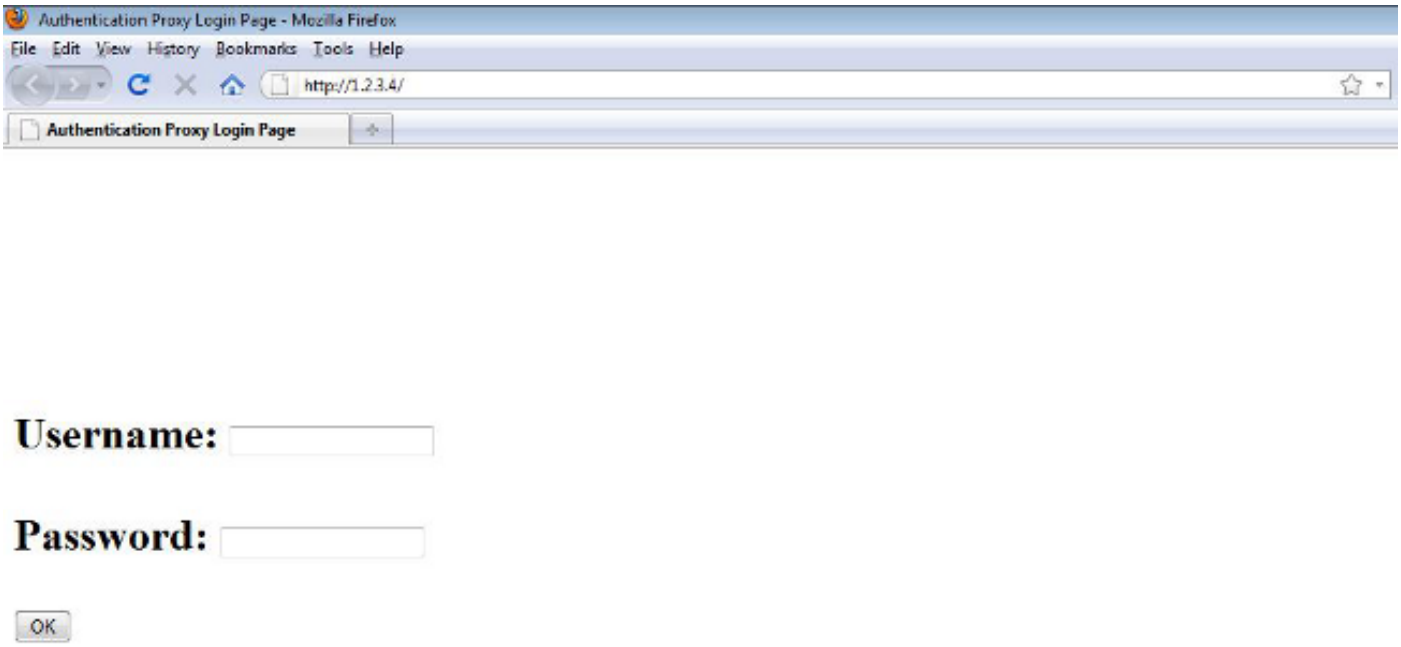
Após a conclusão da configuração, o cliente pode se conectar ao SSID normalmente, e você vê isso no console do AP:

```
<#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
```

O cliente tem um endereço IP dinâmico de 192.168.10.11. No entanto, quando você tenta fazer ping do endereço IP do cliente, ele falha porque o cliente não 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)
```

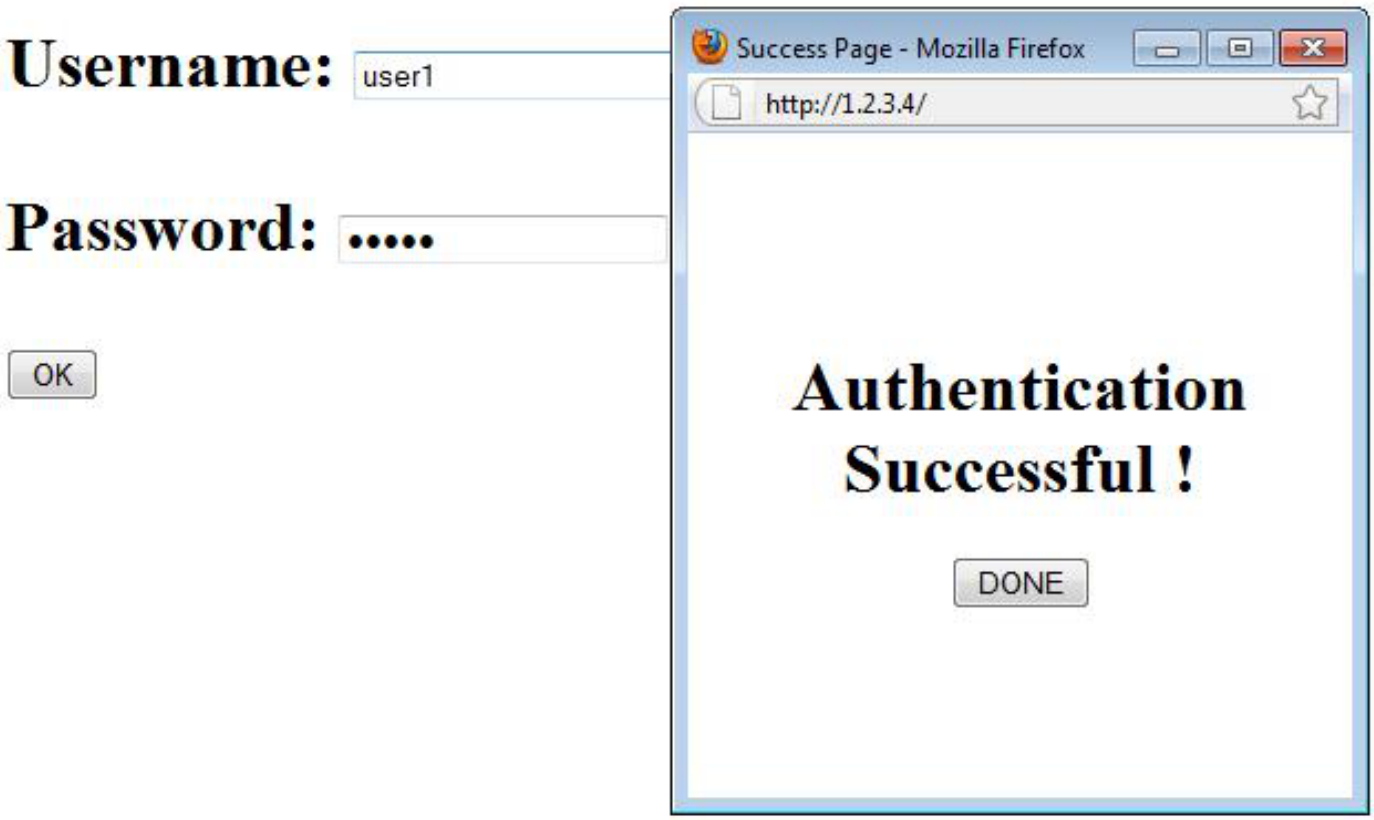
Se o cliente abrir um navegador e tentar acessar http://1.2.3.4, por exemplo, o cliente será redirecionado para a página de login interno:



> Observação: este teste é concluído com um endereço IP aleatório inserido diretamente (onde o URL inserido é 1.2.3.4) sem a necessidade de tradução de um URL através do DNS, porque o DNS não foi usado no teste. Em situações normais, o usuário digita o URL da home page e o tráfego DNS é permitido até que o cliente envie a mensagem HTTP GET para o endereço resolvido, que é interceptado pelo AP. O AP falsifica o endereço do site e redireciona o cliente para a página de login armazenada internamente.

Quando o cliente é redirecionado para a página de login, as credenciais do usuário são inseridas e verificadas no servidor RADIUS local, de acordo com a configuração do AP. Após a autenticação bem-sucedida, o tráfego que vem e vai para o cliente é totalmente permitido.

Esta é a mensagem que é enviada ao usuário após a autenticação bem-sucedida:



Após a autenticação bem-sucedida, você pode exibir as informações de IP do 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

Os pings para o cliente após a conclusão da autenticação bem-sucedida devem funcionar corretamente:

<#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
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

> Observação: o roaming entre APs durante a autenticação da Web não proporciona uma experiência tranquila, pois os clientes devem fazer login em cada novo AP ao qual se conectam.

Personalização

Semelhante ao IOS em roteadores ou switches, você pode personalizar sua página com um arquivo personalizado; no entanto, não é possível redirecionar para uma página da Web externa.

Use estes comandos para personalizar os arquivos do portal:

- arquivo de página de login http de proxy de admissão de IP
- arquivo de paginação expirada http do ip admission proxy
- arquivo de página de êxito de http de proxy de admissão de IP
- arquivo de paginação de falha de http de proxy de admissão de IP

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.