Autenticação do web interna para o acesso do convidado no exemplo de configuração autônomo AP

Índice

Introdução

Este documento descreve como configurar para o acesso do convidado nos Access point autônomos (AP) com o uso do página da web interno que é encaixado no AP próprio.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos antes que você tente esta configuração:

- Como configurar AP autônomos para a operação básica
- Como configurar o servidor Radius local em AP autônomos
- Como autenticação da Web como uma medida dos trabalhos da Segurança da camada 3

Componentes Utilizados

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

- AIR-CAP3502I-E-K9 que executa a imagem 15.2(4)JA1 do ® do Cisco IOS
- Adaptador Wireless avançado-n de Intel Centrino 6200 AGN (versão do driver 13.4.0.9)
- Utilidade do suplicante de 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 uns recursos de segurança da camada 3 (L3) que permitam os AP autônomos de obstruir o tráfego IP (exceto DHCP e Domain Name Server (DNS) - pacotes relacionados) até que o convidado forneça um nome de usuário válido e uma senha no portal da web a que o cliente está reorientado quando um navegador é aberto.

Com autenticação da Web, um nome de usuário e senha separado deve ser definido para cada convidado. O convidado é autenticado com o nome de usuário e senha pelo servidor Radius local ou por um servidor de raio externo.

Esta característica foi introduzida no Cisco IOS Release 15.2(4)JA1.

Configuração AP

> Nota: Este documento supõe que o Bridge Virtual Interface (BVI) 1 no AP tem um endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.10.2 /24, e que o conjunto de DHCP está definido internamente no AP para endereços IP 192.168.10.10 com 192.168.10.254 (os endereços IP 192.168.10.1 com 192.168.10.10 são excluídos).

Termine estas etapas a fim configurar o AP para o acesso do convidado:

1. Adicionar um Service Set Identifier (SSID) novo, nomeie-o **convidado,** e configurar-lo para a autenticação da 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. Crie uma regra da autenticação, onde você deva especificar o protocolo de autenticação de proxy, e nomeie-a **web_auth**:

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

3. Aplique o SSID (**convidado**) e a regra da autenticação (**web_auth**) à interface de rádio. Este exemplo usa o rádio 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 a lista de método que especifica onde as credenciais do usuário são autenticadas. Ligue o nome da lista de método com a regra da autenticação do **web_auth**, e nomeie-o **web_list**:

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

5. Termine estas etapas a fim configurar o Authentication, Authorization, and Accounting (AAA) no AP e no servidor Radius local, e ligue a lista de método com o servidor Radius local no AP:

   Permita o AAA:

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

   Configurar o servidor Radius local:

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

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Crie as contas do convidado, e especifique sua vida (nos minutos). Crie uma conta de usuário com um nome de usuário e senha do **usuário1**, e ajuste o valor da 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)#
```

   Você pode criar outros usuários com o mesmo processo.

   Nota: Você deve permitir o **local do raio-server** a fim criar contas do convidado.
   Defina o AP como um servidor Radius:

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

   Ligue a lista da autenticação da Web com o servidor local:

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

Nota: Você pode usar um servidor de raio externo a fim hospedar as contas de usuário

convidado. A fim fazer isto, configurar o **comando radius-server host** apontar ao servidor interno em vez do endereço IP de Um ou Mais Servidores Cisco ICM NT AP.

Configurar o cliente Wireless

Termine estas etapas a fim configurar o cliente Wireless:

1. A fim configurar a rede Wireless em seus indicadores a utilidade do suplicante que com o SSID nomeou **Convidado**, navegue à **rede e o Internet > controla redes Wireless**, e o clique **adiciona**.

2. Selecione **conectam manualmente a uma rede Wireless**, e incorporam a informação requerida, segundo as indicações desta imagem:

3. Clique em Next.

Verificar

Depois que a configuração está completa, o cliente pode conectar ao SSID normalmente, e você vê este no console 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
```

O cliente tem um endereço IP dinâmico de 192.168.10.11. Contudo, quando você tenta sibilar o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente, falha porque o cliente não é autenticado inteiramente:

```
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 abre um navegador, e tenta alcançar **http://1.2.3.4** por exemplo, o cliente está reorientado à página de login interna:

> Nota: Este teste é terminado com um endereço IP de Um ou Mais Servidores Cisco ICM NT aleatório incorporado diretamente (aqui a URL incorporada é **1.2.3.4**) sem a necessidade para a tradução de uma URL com o DNS, porque o DNS não foi usado no teste. Nos cenários normais, o usuário incorpora o Home Page URL, e o tráfego DNS é permitido até que o cliente envie a mensagem HTTP GET ao endereço resolved, que está interceptado pelo AP. As paródias AP o endereço de site, e reorientam o cliente à página de login armazenada internamente.

Uma vez que o cliente é reorientado à página de login, as credenciais do usuário estão incorporadas e verificadas contra o servidor Radius local, conforme a configuração AP. Após a autenticação bem sucedida, o tráfego que vem de e vai ao cliente é permitido inteiramente.

Está aqui a mensagem que é enviada ao usuário após a autenticação bem sucedida:

Após a autenticação bem sucedida, você pode ver a informação do IP de cliente:

```
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 sibilos ao cliente depois que a autenticação bem sucedida está completa devem trabalhar corretamente:

```
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.

> Nota: Vaguear entre AP durante a autenticação da Web não fornece uma experiência lisa, porque os clientes devem entrar a cada AP novo a que conectam.

Personalização

Similar aos IO no Roteadores ou no Switches, você pode personalizar sua página com um arquivo feito sob encomenda; contudo, não é possível reorientar a um página da web externo.

Use estes comandos a fim personalizar os arquivos portais:

- arquivo de página de login HTTP do proxy da admissão IP
- o HTTP do proxy da admissão IP expirou arquivo de página
- arquivo de página do sucesso HTTP do proxy da admissão IP
- arquivo de página da falha HTTP do proxy da admissão IP