访客访问的内部Web验证在自治AP配置示例

目录

简介

本文描述如何为在自治接入点(AP)的访客访问配置有在AP被嵌入的使用的内部网页。

先决条件

要求

Cisco 建议您在尝试进行此配置之前了解下列主题：

- 如何配置基本操作的自治AP
- 如何配置在自治AP的本地RADIUS服务器
- Web验证作为第3层安全措施如何工作

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS镜像15.2(4)JA1的AIR-CAP3502I-E-K9
- Intel Centrino先进的N 6200个AGN无线适配器(驱动版本13.4.0.9)
- Microsoft Windows 7请求方工具

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

Web验证是使自治AP阻塞IP数据流的第3层(L3)安全功能(除了DHCP和域名服务器(DNS)有关的数据包)，直到访客在客户端重定向的Web门户提供一个有效用户名和密码，当打开时浏览器。

使用Web验证，必须为每访客定义一个分开的用户名和密码。访客验证与用户名和密码由本地RADIUS服务器或外部RADIUS服务器。

此功能在Cisco IOS版本15.2(4)JA1介绍。

AP配置

> **注意**：本文假设，网桥虚拟接口(BVI) 1在AP有192.168.10.2 /24的IP地址和DHCP池在IP地址的192.168.10.10 AP定义内部地通过192.168.10.254 (IP地址192.168.10.1通过192.168.10.10被排除)。

完成这些步骤为了配置访客访问的AP ：

1. 添加一新的服务集标识(SSID)，命名它**访客，**并且为Web验证配置它：

```
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. 创建验证规则，您必须指定代理验证协议，并且命名它**web_auth** ：

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

3. 运用SSID (**访客**)和验证规则(**web_auth**)对无线接口。此示例使用802.11b/g无线电：

```
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. 定义指定的方法列表用户凭证验证的地方。与**web_auth**验证规则连接方法列表名称，并且命名它**web_list** ：

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

5. 完成这些步骤为了配置在AP和本地RADIUS服务器的验证、授权和统计(AAA)，并且与在AP的本地RADIUS服务器连接方法列表：

   Enable (event) AAA ：

   ```
   ap(config)#aaa new-model
   ```
   配置本地RADIUS服务器：

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

   ap(config-radsrv)#nas 192.168.10.2 key cisco

   ap(config-radsrv)#exit
   ```
   创建访客帐户，并且指定他们的寿命(以分钟)。创建与**user1**用户名和密码的一个用户帐户，并且设置寿命值为60分钟：

   ```
   ap(config)#dot11 guest

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

   ap(config-guest-mode)#exit

   ap(config)#
   ```
   您能创建有同一进程的其他用户。

   注意：您必须使**radius-server local**为了创建访客帐户。
   定义AP作为RADIUS服务器：

   ```
   ap(config)#radius-server host 192.168.10.2 auth-port 1812
    acct-port 1813 key cisco
   ```
   与当地服务器连接Web认证列表：

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

   注意：您能使用外部RADIUS服务器为了主机来宾用户用户帐号。为了执行此，请配置**radius-server host命令**指向外部服务器而不是AP IP地址。

配置无线客户端

完成这些步骤为了配置无线客户端：

1. 为了配置在您的windows请求方工具的无线网络有SSID的命名了**Guest**，导航对**网络，并且互联网>管理无线网络**，并且单击**添加**。

2. 如此镜像所显示，选择**手工连接对无线网络**，并且输入必填信息， ：

3. 单击 **Next**。

验证

在配置完成后，客户端能通常连接到SSID，并且您在AP控制台看到此：

```
%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
```

客户端有192.168.10.11动态IP地址。然而，当您尝试ping客户端时的IP地址，它失败，因为客户端不充分地验证：

```
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)
```

如果客户端打开浏览器和尝试到达例如**http://1.2.3.4**，客户端重定向对内部登录页：

> **注意**：此测验完成用一个随机的IP地址直接地被输入(在这里被输入的URL **1.2.3.4**)，不用对URL的转换的需要通过DNS，因为DNS未用于测验。在正常方案中，用户输入主页URL，并且DNS流量允许，直到客户端传送HTTP GET信息对解决的地址， AP拦截。AP伪装网址，并且重定向客户端对存储的登录页内部地。

一旦客户端重定向对登录页，用户凭证被输入并且验证本地RADIUS服务器，根据AP配置。在成功认证以后，来自并且去客户端的流量充分地允许。

这是传送给用户在成功认证以后的信息：

在成功认证以后，您能查看客户端IP信息：

```
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
```

对客户端的Ping，在成功认证完成以后应该适当地运作：

```
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
```

故障排除

目前没有针对此配置的故障排除信息。

> **注意**：漫游在AP之间在Web验证时不提供一平稳的体验，因为客户端必须登陆到其中每一他们连接的新建的AP。

自定义

类似于在路由器或交换机的IOS，您能定制您的页用一个自定义文件;然而，重定向到外部网页是不可能的。

请使用这些命令为了定制门户文件：

- **ip admission代理http登录页页文件**
- **ip admission代理http已到期页面文件**
- **ip admission代理http成功页面文件**
- **ip admission代理http失败页面文件**