在自治AP上为访客配置Web身份验证

目录

简介

本文档介绍如何使用嵌入在AP本身的内部网页在自主接入点(AP)上配置访客接入。

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：

- 如何为基本操作配置自治AP
- 如何在自治AP上配置本地RADIUS服务器
- Web身份验证作为第3层安全措施的工作原理

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®映像15.2(4)JA1的AIR-CAP3502I-E-K9
- Intel Centrino Advanced-N 6200 AGN无线适配器（驱动程序版本13.4.0.9）
- Microsoft Windows 7请求方实用程序

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身份验证是第3层(L3)安全功能，它使自治AP能够阻止IP流量(DHCP和域名服务器(DNS)相关数据包除外)，直到访客在打开浏览器时将客户端重定向到的Web门户中提供有效的用户名和密码。

使用Web身份验证时，必须为每个访客定义单独的用户名和密码。访客通过本地RADIUS服务器或外部RADIUS服务器使用用户名和密码进行身份验证。

此功能在Cisco IOS版本15.2(4)JA1中引入。

无线接入点配置

> **注意：**本文档假设AP上的网桥虚拟接口(BVI)1的IP地址为192.168.10.2 /24，并且DHCP池在AP上内部定义，用于IP地址192.168.10.10到192.168.10.254（排除IP地址192.168.10.1到192.168.10.10）。

要配置AP以访客访问，请完成以下步骤：

1. 添加新的服务集标识符(SSID)，将其命名为Guest，并将其配置为Web身份验证：

```
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. 创建身份验证规则，在该规则中必须指定代理身份验证协议，并将其命名为web_auth：

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

3. 将SSID(访客)和身份验证规则(web_auth)应用到无线电接口。本示例使用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. 定义指定用户凭证身份验证位置的方法列表。将方法列表名称与**web_auth身**份验证规则链接，并将其**命名为web_list**:

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

5. 要在AP和本地RADIUS服务器上配置身份验证、授权和记帐(AAA)，并将方法列表与AP上的本地RADIUS服务器链接：

   Enable 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，并指定其生存时间（以分钟为单位）。 使用用户名和密码user1创建一个用户**帐户**，并将生存期值设置为60分钟：

```
ap(config)#dot11 guest

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

ap(config-guest-mode)#exit

ap(config)#
```

   您可以使用相同的流程创建其他用户。

   注意：必须启用**radius-server local**才能创建访客帐户。
   将AP定义为RADIUS服务器：

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

   将Web身份验证列表与本地服务器链接：

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

   注意：您可以使用外部RADIUS服务器来托管访客用户帐户。为此，请配置**radius-server host**

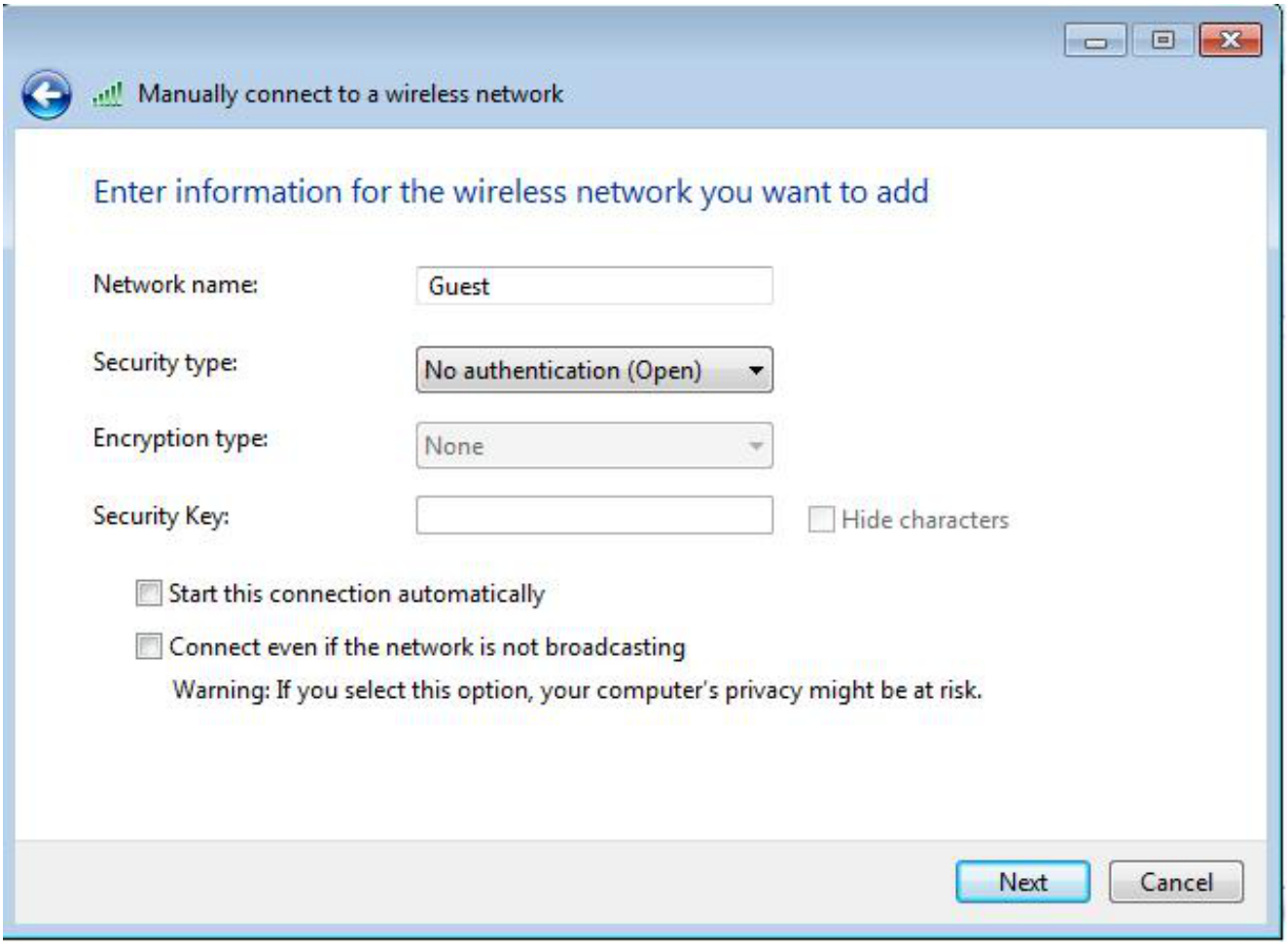
命令以指向外部服务器而不是AP IP地址。

配置无线客户端

要配置无线客户端，请完成以下步骤：

1. 要使用名为**Guest**的SSID配置Windows请求方实用程序上的无线网络，请导航到**Network and Internet > Manage Wireless Networks**，然后单击**Add**。

2. 选择**手动连接到无线网络**，然后输入所需信息，如下图所示：



3. 单击 **Next**。

验证

配置完成后，客户端可以正常连接到SSID，您在AP控制台上看到：

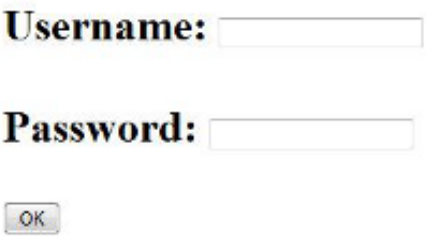
```
%DOT11-6-ASSOC: Interface Dot11Radio0, Station ap 0027.10e1.9880
```

```
 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
```

客户端的动态IP地址为192.168.10.11。但是，当您尝试ping客户端的IP地址时，该地址会失败，因为客户端未完全通过身份验证：

```
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)
```

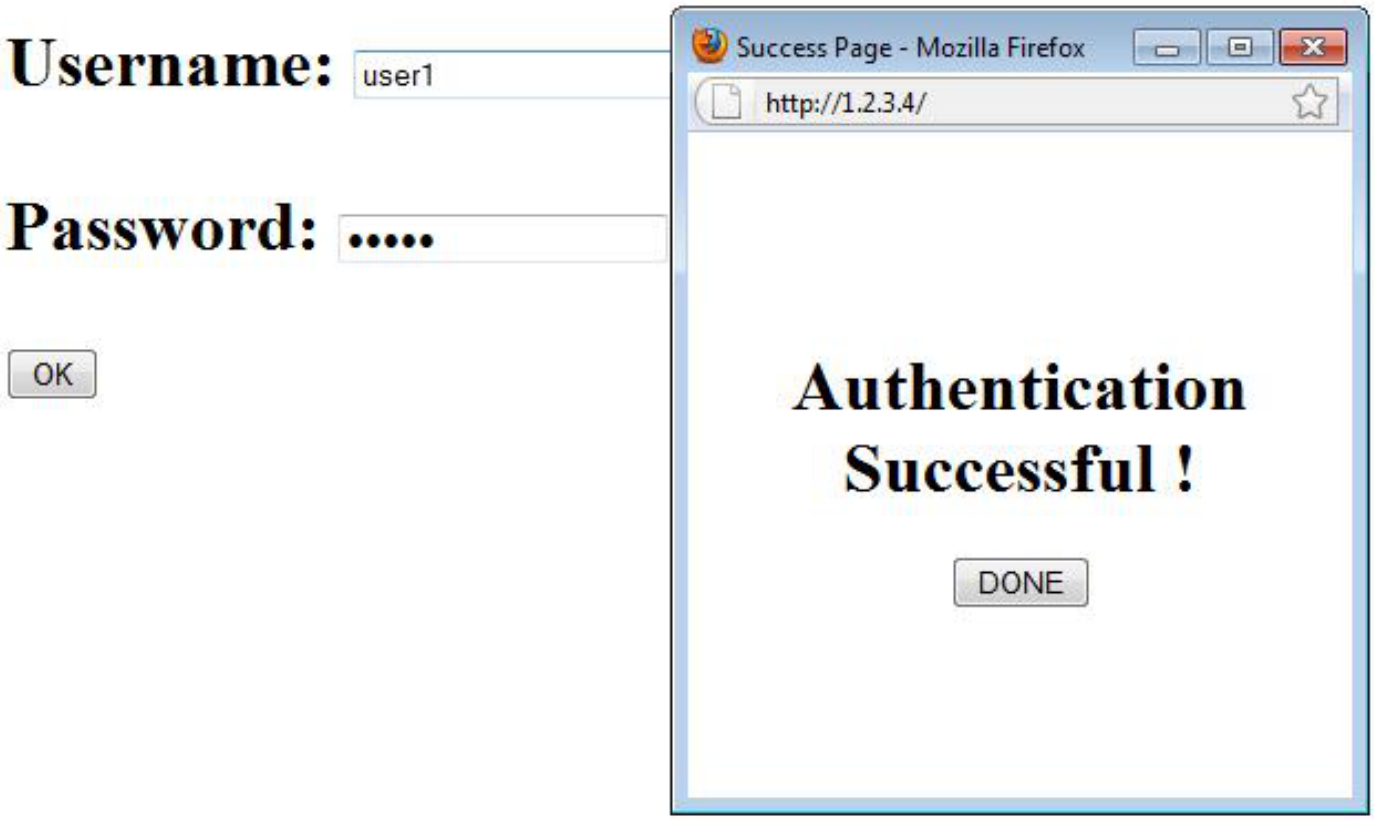
例如，如果客户端打开浏览器并尝试访问**http://1.2.3.4**，则客户端将重定向到内部登录页：



注意：此测试完成时直接输入随机IP地址(此处输入的URL为**1.2.3.4**)，无需通过DNS转换URL，因为测试中未使用DNS。在正常情况下，用户输入主页URL，并允许DNS流量，直到客户端向解析地址发送HTTP GET消息，该地址被AP拦截。AP欺骗网站地址，并将客户端重定向到内部存储的登录页。

一旦客户端重定向到登录页面，用户凭证将根据AP配置输入并根据本地RADIUS服务器进行验证。身份验证成功后，将完全允许从客户端发往客户端的流量。

以下是身份验证成功后发送给用户的消息：



身份验证成功后，您可以查看客户端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
```

在成功完成身份验证后，应该能正确地ping通客户端：

```
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**：在Web身份验证期间，AP之间的漫游无法提供流畅的体验，因为客户端必须登录到其连接的每个新AP。

定制

与路由器或交换机上的IOS类似，您可以使用自定义文件自定义页面；但是，无法重定向到外部网页。

使用以下命令自定义门户文件：

- IP Admission Proxy HTTP登录页文件
- ip admission proxy http expired page file
- IP Admission Proxy HTTP Success Page文件
- IP Admission Proxy HTTP Failure页面文件