在WLC上配置Web身份验证代理

目录

简介

先决条件

- 要求
- 使用的组件
- 规则

WLC上的Web身份验证代理

在WLC上配置Web身份验证代理

- 配置

验证

相关信息

简介

本文档提供在无线局域网控制器(WLC)上使用Web身份验证代理功能的配置示例。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解轻量接入点(LAP)和Cisco WLC的配置。
- 了解轻量接入点协议(LWAPP)/无线接入点的控制和调配(CAPWAP)。
- 具有Web身份验证知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 7.0.116.0 的 Cisco 4400 WLC
- Cisco 1130AG系列LAP
- 运行固件版本4.2的Cisco 802.11a/b/g无线客户端适配器

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。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

WLC上的Web身份验证代理

本文档假设读者事先了解Web身份验证以及在Cisco WLC上配置Web身份验证所涉及的步骤。如果您是新用户，请阅读以下文档，其中详细解释了Web身份验证过程：

- 无线局域网控制器 Web 身份验证配置示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除

在WLC版本7.0.116.0中引入了Web身份验证代理功能。

Web浏览器有三种可由用户配置的Internet设置：

- 自动检测
- 系统代理
- 手动

此功能使在浏览器中启用了手动Web代理的客户端能够使用控制器进行Web身份验证。

在配置为Web身份验证的网络中，如果客户端配置为手动代理设置，则控制器不会侦听此类代理端口，因此客户端将无法与控制器建立TCP连接。实际上，用户无法访问任何用于身份验证的登录页面和访问网络。

当客户端请求任何URL并启用Web身份验证代理功能时，控制器会以网页做出响应，提示用户更改Internet代理设置以自动检测代理设置。

此过程可防止浏览器的手动代理设置丢失。配置此功能后，用户可通过Web身份验证策略访问网络。

默认情况下，此功能针对端口80、8080和3128提供，因为这些端口是Web代理服务器最常用的端口。

在WLC上配置Web身份验证代理

本部分提供有关如何配置本文档所述功能的信息。

配置

完成以下步骤以使用控制器GUI配置Web身份验证代理：

1. 从控制器GUI中，选择Controller > General。
2. 要启用WebAuth代理，请从WebAuth代理重定向模式下拉列表中选择Enabled。

3. 在WebAuth代理重定向端口(WebAuth Proxy Redirection Port)文本框中，输入Web身份验证代理的端口号。此文本框包含控制器侦听Web身份验证代理重定向的端口号。默认情况下，假定为三个端口80、8080和3128。如果将Web身份验证重定向端口配置为这些值以外的任何端口，则必须指定该值。

4. 单击 Apply。

要从CLI配置WebAuth代理，请发出以下命令：

```
<#root>

config network web-auth proxy-redirect

 {enable | disable}
```

使用config network web-auth port <port-number>命令设置Web身份验证端口号。

配置WLC后，保存配置并重新启动控制器以使配置生效。

验证

要查看Web身份验证代理配置的当前状态，请发出show network summary或show running-config命令。

```
<#root>

(Cisco Controller) >

show network summary


RF-Network Name............................. WLAN-LAB
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
AP Multicast/Broadcast Mode................. Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
```

```
--More-- or (q)uit
Mesh Full Sector DFS..................... Enable
Apple Talk .............................. Disable
AP Fallback ............................. Enable

Web Auth Redirect Ports ................. 80
Web Auth Proxy Redirect  ................ Enable

Fast SSID Change ........................ Disabled
802.3 Bridging .......................... Disable
IP/MAC Addr Binding Check ............... Enabled
```

现在，我们将无线客户端连接到我们已为Web身份验证配置的访客SSID。

假设您有内部DHCP服务器，客户端将连接到WLAN Guest1并获取IP地址。当客户端尝试访问URL(例如www.cisco.com)时，由于客户端浏览器上启用了手动代理，因此使用Web身份验证代理功能的控制器会以网页做出响应，提示用户更改Internet代理设置以自动检测代理设置。

此时，客户端知道需要禁用手动代理设置。在这里，您可以看到如何禁用Firefox版本3.6上的手动代理设置。

1. 从Firefox浏览器中，选择工具 > 选项，然后选择高级。
2. 单击网络选项卡，然后选择设置。
3. 在“Connection Settings”窗口中，选择Auto-detect proxy settings for this network。

完成此操作后，请刷新浏览器并尝试再次访问URL。这次会将您重定向到Web身份验证页面。客户端可以向您提供凭证，您可以登录到访客网络。

相关信息

- 无线局域网控制器 Web 身份验证配置示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除
- Cisco 无线 LAN 控制器配置指南 7.0.116.0 版
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。