排除无线局域网控制器(WLC)上的Web身份验证故障

目录

简介

本文档介绍如何解决无线局域网控制器(WLC)环境中的Web身份验证问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 无线接入点的控制和调配(CAPWAP)。
- 如何为基本操作配置轻量接入点(LAP)和WLC。
- Web身份验证基础知识以及如何在WLC上配置Web身份验证。

有关如何在WLC上配置Web身份验证的信息，请参阅无线LAN控制器Web身份验证配置示例。

使用的组件

本文档中的信息基于运行固件版本 8.3.121 的 WLC 5500。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

本文档还可用于以下硬件：

- 思科 5500 系列无线控制器
- 思科 8500 系列无线控制器
- 思科 2500 系列无线控制器
- Cisco Airespace 3500 系列 WLAN 控制器
- Cisco Airespace 4000 系列无线局域网控制器

- 思科Flex 7500系列无线控制器
- 思科无线服务模块2(WiSM2)

WLC 中的 Web 身份验证

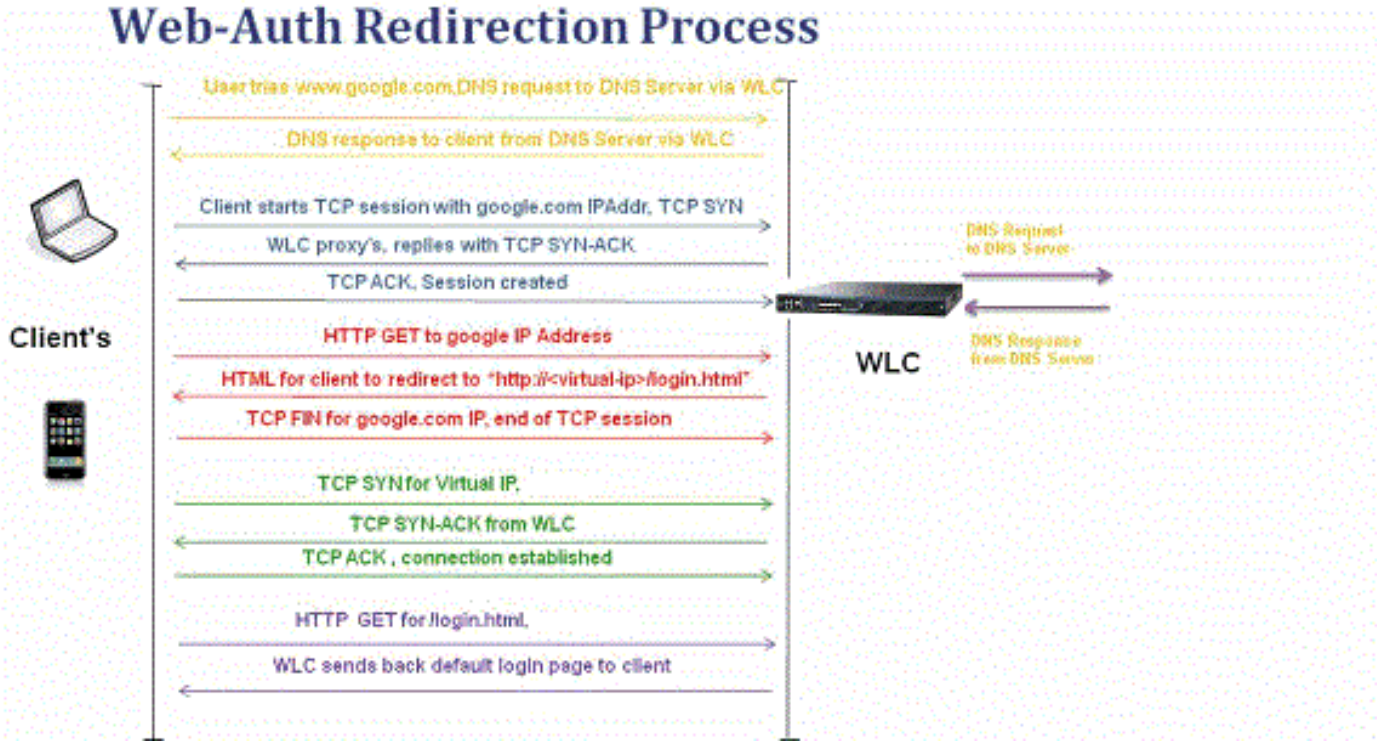
Web身份验证是第3层安全功能，它会导致控制器不允许来自特定客户端的IP流量(与DHCP相关的数据包/域名系统(DNS)相关的数据包除外)，直到该客户端正确提供了有效的用户名和密码(通过预身份验证访问控制列表(ACL)允许的流量除外)。Web 身份验证是唯一允许客户端在身份验证前获得 IP 地址的安全策略。它是一种不需要请求者或客户端实用程序的简单身份验证方法。Web 身份验证可以在 WLC 上本地执行，或通过 RADIUS 服务器执行。Web 身份验证通常由希望部署访客接入网络的客户使用。

Web 身份验证在控制器拦截来自客户端的第一个 TCP HTTP（端口 80）GET 数据包时开始。要使客户端Web浏览器达到此目的，客户端必须首先获取IP地址，然后为Web浏览器执行URL到IP地址的转换（DNS解析）。这样，Web 浏览器就知道应向哪个 IP 地址发送 HTTP GET。

在 WLAN 上配置 Web 身份验证时，控制器将阻止所有数据流（DHCP 和 DNS 数据流除外），直到身份验证过程完成。当客户端将第一个HTTP GET发送到TCP端口80时，控制器将客户端重定向到https://192.0.2.1/login.html（如果这是配置的虚拟IP）进行处理。此过程最终会启动登录网页。

> **注意**：使用外部Web服务器进行Web身份验证时，WLC平台需要外部Web服务器的预身份验证ACL。

此部分详细说明了 Web 身份验证重定向过程。



- 打开 Web 浏览器并输入 URL，例如，http://www.site.com。客户端将发出该 URL 的 DNS 请求，以获取目标 IP。WLC将DNS请求传递给DNS服务器，DNS服务器通过DNS应答进行响应，其中包含目标www.site.com的IP地址，然后转发给无线客户端。
- 然后，客户端尝试打开与目标 IP 地址之间的 TCP 连接，并将 TCP SYN 数据包发送至

www.site.com 的 IP 地址。

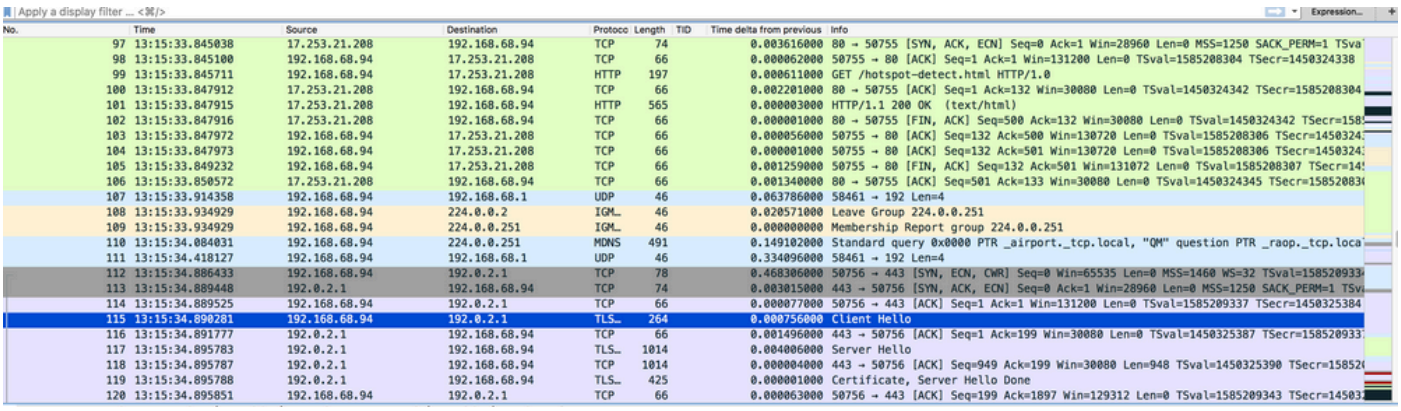
- WLC 配置了客户端规则，因此可作为 www.site.com 的代理，然后将 TCP SYN-ACK 数据包发回至客户端，其中包含 www.site.com 的 IP 地址源。客户端发回TCP ACK数据包以完成三次TCP握手，并且TCP连接已完全建立。
- 客户端向 www.site.com 发送 HTTP GET 数据包。 WLC 拦截此数据包并发送以进行重定向处理。 HTTP 应用程序网关准备 HTML 主体并将其作为客户端 HTTP GET 请求的应答返回。此 HTML 使客户端前往 WLC 的默认网页 URL，例如 http://<Virtual-Server-IP>/login.html。
- 客户端关闭与IP地址(例如www.site.com)的TCP连接。
- 现在，客户端要转到http://<virtualip>/login.html，因此它尝试打开与WLC的虚拟IP地址的TCP连接。它向WLC发送用于192.0.2.1（此处是我们的虚拟IP）的TCP SYN数据包。
- WLC 返回 TCP SYN-ACK，而客户端则发回 TCP ACK 至 WLC，以完成握手。
- 客户端向/login.html发送目的地为192.0.2.1的HTTP GET以请求登录页。
- 此请求被允许到WLC的Web服务器，并且服务器使用默认登录页进行响应。客户端将在浏览器窗口接收登录页，用户可以前往该窗口并登录。

在本示例中，客户端IP地址为192.168.68.94。客户端解析了所访问的Web服务器10.1.0.13的URL。您可以看到，客户端进行了三次握手以启动TCP连接，然后发送了一个以数据包96开始的HTTP GET数据包（00是HTTP数据包）。这不是由用户触发，而是操作系统自动的门户检测触发（我们可以从请求的URL中猜测）。控制器拦截数据包并使用代码200进行回复。代码 200 数据包中含重定向 URL：

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1;
URL=https://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

然后，它通过三次握手关闭TCP连接。

然后，客户端启动与重定向URL的HTTPS连接，重定向URL将其发送到192.0.2.1，这是控制器的虚拟IP地址。客户端必须验证或忽略服务器证书，以建立 SSL 隧道。在这种情况下，这是一种自签名证书，因此客户端可以忽略。登录网页通过此 SSL 隧道发送。数据包 112 开始处理。



您可以选择为WLC的虚拟IP地址配置域名。如果选择配置虚拟 IP 地址的域名，此域名将包含在控制器返回的 HTTP OK 数据包中，以响应来自客户端的 HTTP GET 数据包。然后您必须对此域名执行DNS解析。从DNS解析获取IP地址后，它会尝试使用该IP地址打开TCP会话，该IP地址是在控制器的虚拟接口上配置的IP地址。

最终，网页通过隧道传递到客户端，用户通过安全套接字层(SSL)隧道发回用户名/密码。

Web 身份验证可以通过以下三种方式执行：

- 使用内部网页（默认）。
- 使用自定义登录页。
- 使用来自外部Web服务器的登录页。

注意：
— 自定义Web身份验证捆绑包的文件名限制为30个字符。确保捆绑包内的文件名不超过30个字符。

— 从WLC版本7.0开始，如果在WLAN上启用了Web身份验证，并且您还具有CPU ACL规则，则只要客户端在WebAuth_Reqd状态下未进行身份验证，基于客户端的Web身份验证规则始终具有更高的优先级。一旦客户端变为 RUN 状态，就应用 CPU ACL 规则。

— 因此，如果在WLC中启用了CPU ACL，则在以下情况下需要虚拟接口IP的允许规则（在ANY方向）：
-CPU ACL 不包含两个方向的“全部允许”规则。
-存在“全部允许”规则，但还存在优先级较高的端口 443 或 80 的拒绝规则。

— 如果禁用secureweb，虚拟IP的允许规则必须用于TCP协议和端口80，如果启用secureweb，则必须用于端口443。这是为了在启用 CPU ACL 并成功进行身份验证后，允许客户端访问虚拟接口 IP 地址。

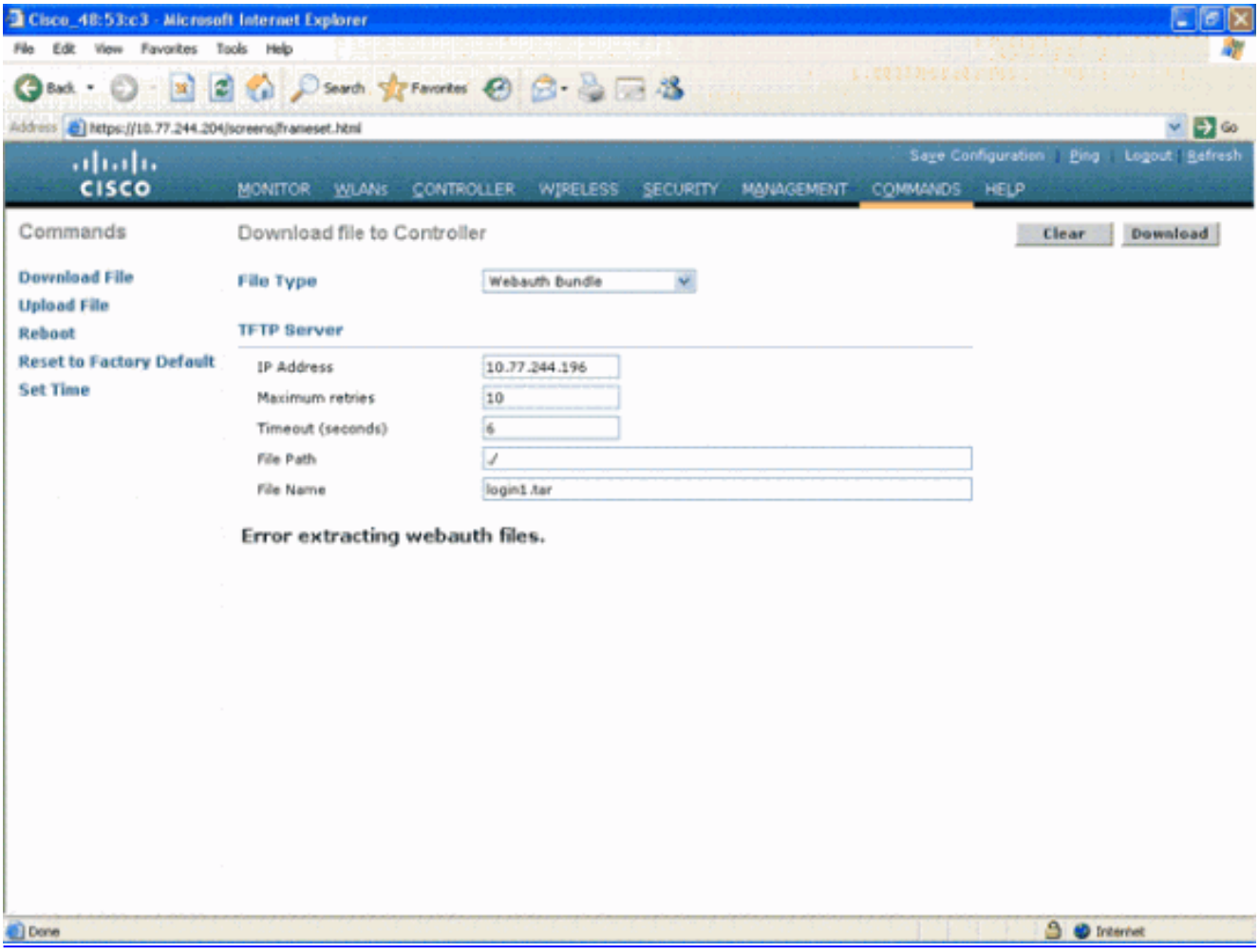
Web 身份验证故障排除

配置Web身份验证后，如果功能未按预期运行，请完成以下步骤：

1. 检查客户端是否已获得 IP 地址。否则，用户可以取消选中WLAN上的**DHCP Required**复选框，并为无线客户端提供静态IP地址。这样将与接入点建立关联。
2. 然后在 Web 浏览器中对 URL 进行 DNS 解析。当 WLAN 客户端连接至为了 Web 身份验证而配置的 WLAN 时，客户端会从 DHCP 服务器获得一个 IP 地址。用户打开 Web 浏览器并输入网站地址。然后，客户端就会执行 DNS 解析，以获得该网站的 IP 地址。当客户端尝试到达网站时，WLC 会拦截客户端的 HTTP Get 会话并将用户重定向至 Web 身份验证登录页。
3. 因此，需要确保客户端可以执行 DNS 解析，以实现重定向。在Microsoft Windows中，选择**开始>运行**，输入**CMD**以打开命令窗口，然后执行“nslookup www.cisco.com”并查看IP地址是否返回。 在Mac/Linux中，打开一个终端窗口，然后执行“nslookup www.cisco.com”，并查看IP地址是否返回。如果您认为客户端无法获得DNS解析，您可以：输入URL的IP地址(例如，http://www.cisco.com是http://192.168.219.25)。尝试键入必须通过无线适配器解析的任何（即使不存在）IP地址。当您输入此URL时，它是否显示网页？如果可以，很可能是 DNS 问题。这也可能是证书问题。默认情况下，控制器使用自签名证书，大多数Web浏览器会警告其不要使用。
4. 对于使用自定义网页的Web身份验证，请确保自定义网页的HTML代码适当。 您可以从Cisco Software Downloads下载Web身份验证脚本示例。例如，对于5508控制器，请选择**Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle**，然后下载**webauth_bundle.zip**文件。当用户的Internet浏览器重定向到自定义登录页面时，这些参数将添加到URL:ap_mac — 无线用户关联的接入点的MAC地址。switch_url — 必须向其发布用户凭据的控制器的URL。redirect — 身份验证成功后用户重定向到的URL。statusCode — 从控制器Web身份验证服务器返回的状态代

码。wlan — 无线用户关联的WLAN SSID。以下是可用的状态代码：状态代码1 — “您已登录。无需再执行任何操作。”状态代码2 — “您未配置为根据Web门户进行身份验证。无需再执行任何操作。”状态代码3 — “此时无法使用指定的用户名。是否已使用该用户名登录系统？”状态代码4 — “You have been excluded.”状态代码5 — “您输入的用户名和密码组合无效。请重试。

5. 所有需要显示在自定义网页上的文件和图片必须捆绑到.tar文件中，然后才能将其上传到WLC。确保.tar捆绑包中包含的文件之一为login.html。如果没有包含 login.html 文件，您将收到以下错误消息：



有关如何创建自定义 Web 身份验证窗口的详细信息，请参阅“无线 LAN 控制器 Web 身份验证配置示例”中的“自定义 Web 身份验证”部分。**注**：大文件和长名称文件可能导致提取错误。建议的图片格式是 .jpg。

6. 确保客户端浏览器上的 **Scripting 选项未被阻止，因为 WLC 上的自定义网页基本上是 HTML 脚本。**
7. 如果您为 WLC 的**虚拟接口配置了主机名，确保可以对虚拟接口的主机名进行 DNS 解析。 注**意：从WLC GUI导航到**Controller > Interfaces**菜单，以向虚拟接**口分**配DNS主机名。
8. 有时，客户端计算机安装的防火墙会阻止 Web 身份验证登录页。尝试访问登录页前，禁用防火墙。Web 身份验证完成后，可以再次启用防火墙。
9. 拓扑/解决方案防火墙可以放置在客户端和Web身份验证服务器之间，具体取决于网络。对于实施的每个网络设计/解决方案，最终用户必须确保网络防火墙上允许这些端口。

10. 要进行Web身份验证，客户端必须首先关联到WLC上的相应WLAN。导航至 WLC GUI 上的 **Monitor> Clients 菜单，查看客户端是否已与 WLC 关联。**检查客户端是否具有有效的 IP 地址。
11. 禁用客户端浏览器上的代理设置，直到 Web 身份验证完成。

12. 默认Web身份验证方法是密码身份验证协议(PAP)。确保 RADIUS 服务器允许 PAP 身份验证，以保证其正常进行。要检查客户端身份验证状态，可以检查 RADIUS 服务器的调试程序和日志消息。您可以在WLC上使用**debug aaa all**命令查看来自RADIUS服务器的调试。
13. 将计算机上的硬件驱动程序更新为制造商网站中的最新代码。
14. 验证请求方的设置（笔记本电脑上的程序）。
15. 如果使用 Windows 内置的 Windows Zero Config 请求方，则： 验证用户安装了最新的修补程序。对请求方运行调试。
16. 在客户端上，从命令窗口打开EAPOL(WPA+WPA2)和RASTLS日志。选择**开始>运行> CMD**:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    为了禁用日志，可运行同一命令，但需要将“enable”改为“disable”。对于XP，所有日志都可以位于C:\Windows\tracing。
17. 如果仍然没有出现登录页，收集并分析单个客户端的以下输出：
    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
18. 如果完成这些步骤后仍未解决问题，请收集这些调试并使用Support Case Manager以提交服务请求。
    ```
    debug pm ssh-appgw enable
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

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**
- **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）。