对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除

目录

简介

本文档提供了有关在无线 LAN 控制器 (WLC) 环境中排除 Web 身份验证故障的提示。

先决条件

要求

Cisco 建议您了解以下主题：

- 轻量级接入点协议(LWAPP) /Control和供应知识无线接入点(CAPWAP)
- 配置轻量接入点 (LAP) 和 WLC 的基本操作知识。
- WLC 中的 Web 身份验证及其配置的基础知识。有关配置 WLC 中的 Web 身份验证的详细信息，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 7.0.98.0 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。

相关产品

本文档也可用于以下硬件：

- 思科5500系列无线控制器

- Cisco 4400 系列无线局域网控制器
- Cisco 4100 系列无线局域网控制器
- 思科2500系列无线控制器
- Cisco 2100 系列无线局域网控制器
- Cisco 2000 系列无线局域网控制器
- Cisco Airespace 3500 系列 WLAN 控制器
- Cisco Airespace 4000 系列无线局域网控制器
- Cisco 无线局域网控制器模块
- Cisco Catalyst 6500 系列无线服务模块(Wism)
- Cisco Flex 7500系列无线控制器
- 思科无线服务模块2 (WiSM2)
- Cisco Catalyst 3750 系列集成无线局域网控制器

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

WLC 中的 Web 身份验证

Web 身份验证属于第 3 层安全功能，控制器可以使用该功能禁止来自特定客户端的 IP 数据流（DHCP/DNS 相关的数据包除外），直到该客户端正确提供有效的用户名和口令，但通过预身份验证 ACL 允许的数据流除外。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。

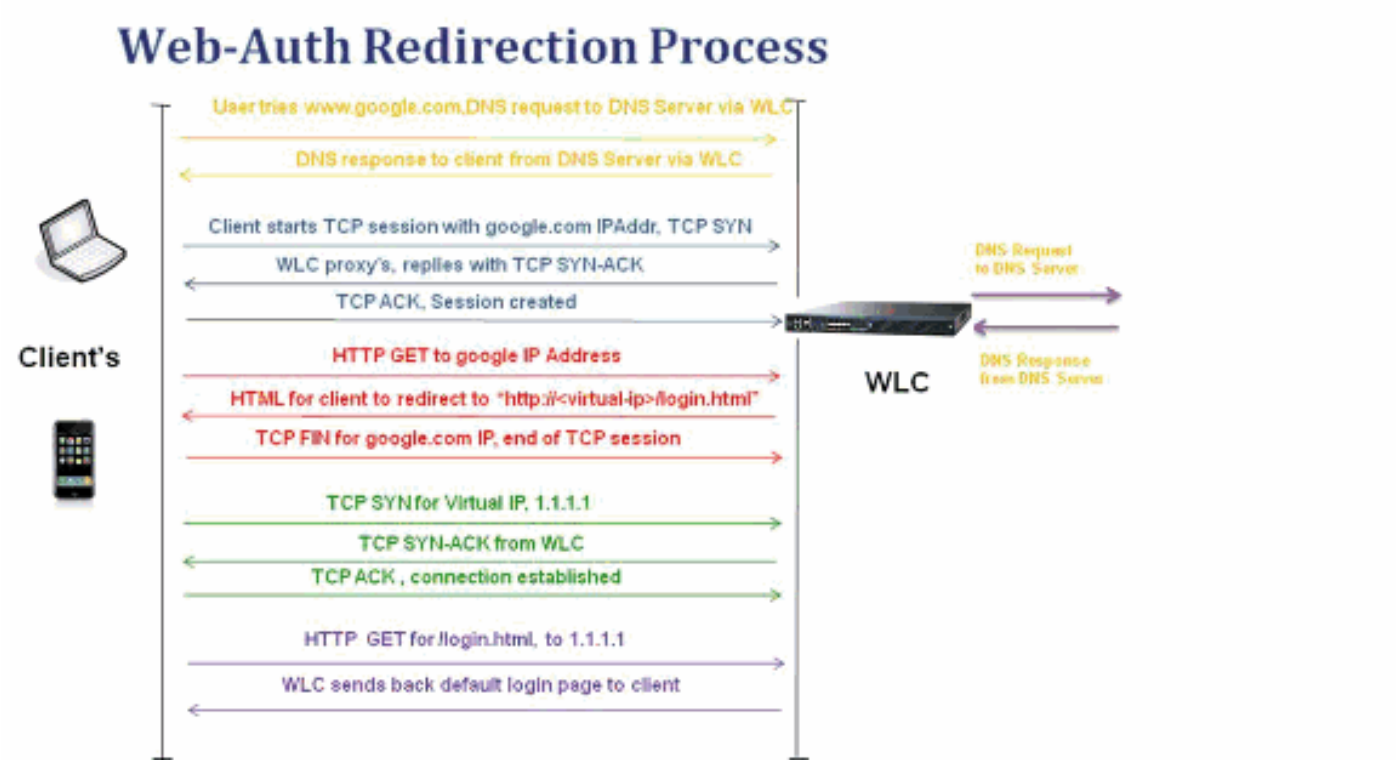
Web 身份验证在控制器拦截来自客户端的第一个 TCP HTTP（端口 80）GET 数据包时开始。为了使客户端的 Web 浏览器发送数据包，客户端必须首先获得 IP 地址，并为 Web 浏览器将 URL 转换为 IP 地址（DNS 解析）。这样，Web 浏览器就知道应向哪个 IP 地址发送 HTTP GET。

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。当客户端发送第一个 HTTP GET 至 TCP 端口 80 时，控制器将客户端重定向至 https:1.1.1.1/login.html 进行处理。此过程最终会启动登录网页。

注意： 当您使用一外部Web服务器Web验证时，某些WLC平台需要外部Web服务器的预验证ACL，包括Cisco 5500系列控制器，一个Cisco 2100系列控制器， Cisco 2000系列和控制器网络模块。对于其他WLC平台预验证ACL不是必须。

注意： 当您使用一外部Web验证时，但是，它是良好的做法配置外部Web服务器的预先身份验证ACL。

此部分详细说明了 Web 身份验证重定向过程。

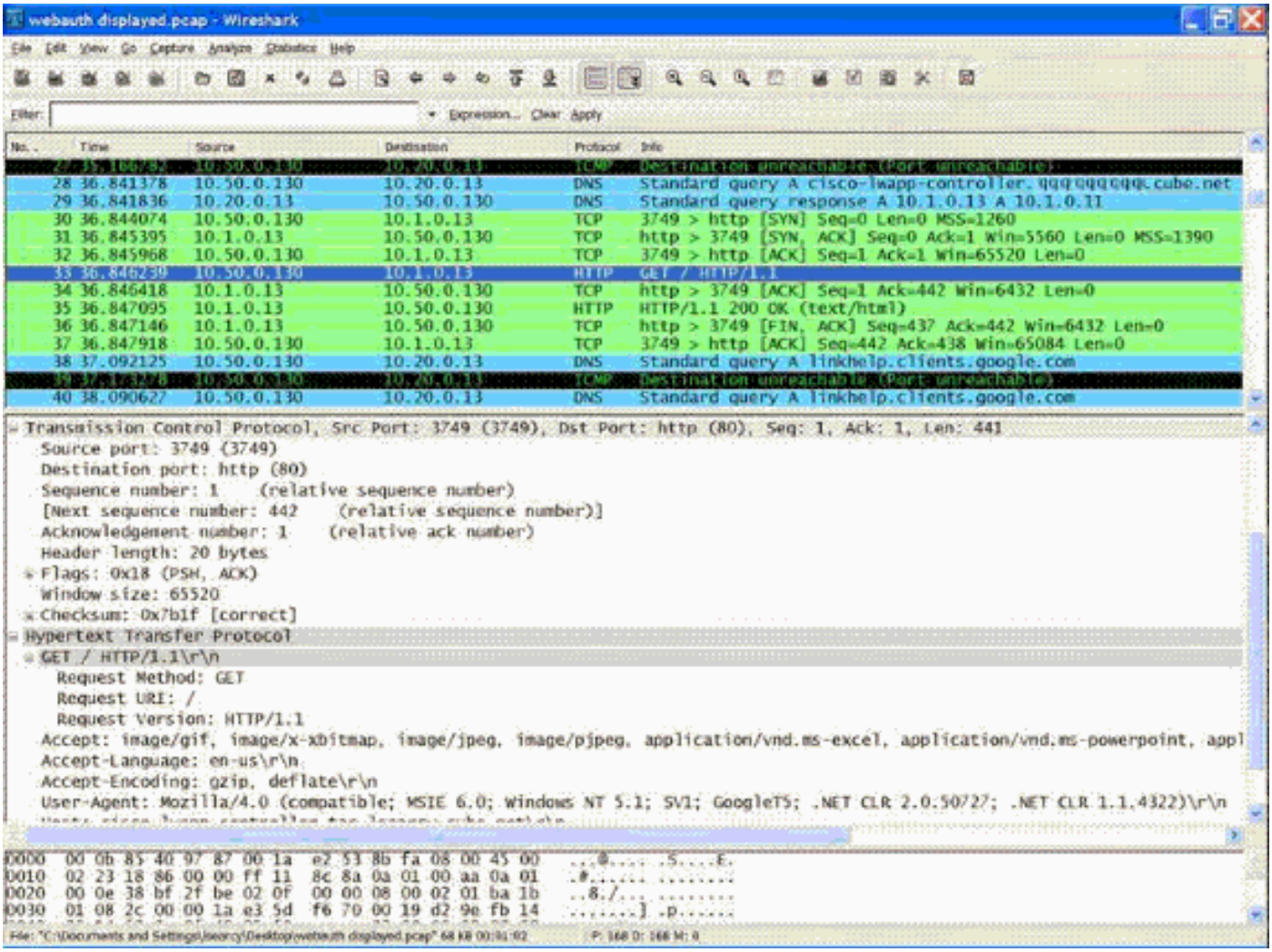


- 打开 Web 浏览器并输入 URL，例如，http://www.google.com。客户端将发出该 URL 的 DNS 请求，以获取目标 IP。WLC 绕过 DNS 请求到达 DNS 服务器，DNS 服务器返回 DNS 应答，其中包含目标 www.google.com 的 IP 地址，并进一步转发给无线客户端
- 然后，客户端尝试打开与目标 IP 地址之间的 TCP 连接，并将 TCP SYN 数据包发送至 www.google.com 的 IP 地址。
- WLC 配置了客户端规则，因此可作为 www.google.com 的代理，然后将 TCP SYN-ACK 数据包发回至客户端，其中包含 www.google.com 的 IP 地址源。客户端发回 TCP ACK 数据包，以完成三次 TCP 握手，从而完全建立 TCP 连接。
- 客户端向 www.google.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。该 HTML 可以使客户端转至 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.google.com）的 TCP 连接。
- 现在，客户端要转至 http://1.1.1.1/login.html，因此尝试打开与 WLC 的虚拟 IP 地址之间的 TCP 连接。它将 1.1.1.1 的 TCP SYN 数据包发送至 WLC。
- WLC 返回 TCP SYN-ACK，而客户端则发回 TCP ACK 至 WLC，以完成握手。
- 客户端向目的地为 1.1.1.1 的 /login.html 发送 HTTP GET，以请求登录页。
- 此请求由 WLC 的 Web 服务器确认允许，该服务器返回默认登录页。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。

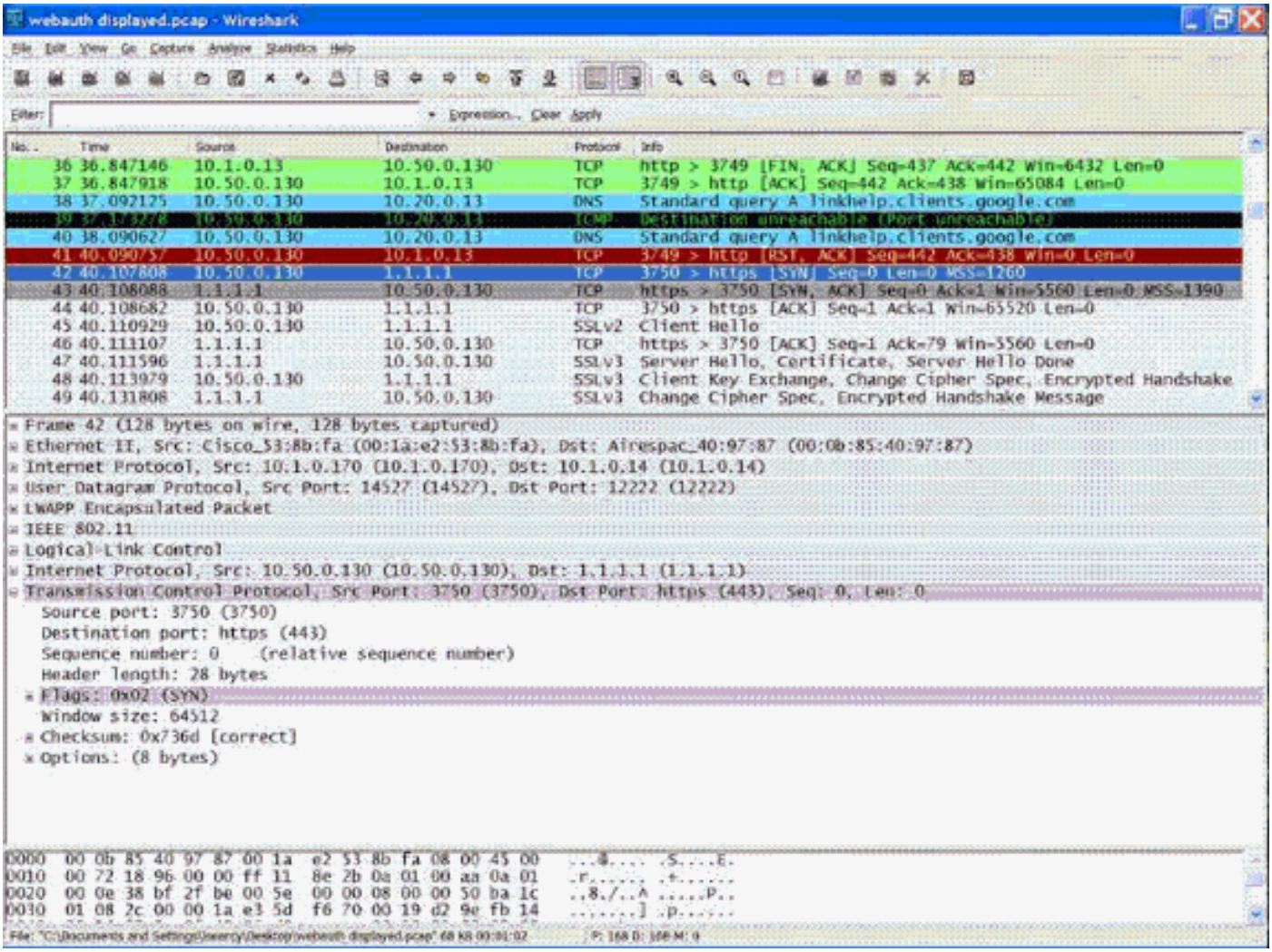
下面是一个示例。在本示例中，客户端的 IP 地址是 10.50.0.130。客户端将访问的 Web 服务器的 URL 解析为 10.1.0.13。如您所见，客户端进行三次握手并启动 TCP 连接，然后发送 HTTP GET 数据包，以数据包 30 为起始。控制器正在拦截数据包并以代码 200 回复。代码 200 数据包中含重定向 URL：

```
<HTML><HEAD><TITLE>Cisco Systems Inc. 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://1.1.1.1/login.html?redirect=cisco-lwapp-controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

然后通过三次握手关闭 TCP 连接。



接着，客户端启动 HTTPS 连接，以连接至重定向 URL，并将其发送至控制器的虚拟 IP 地址 1.1.1.1。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 42 开始处理。



您可以选择配置无线 LAN 控制器的虚拟 IP 地址的域名。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，您必须执行该域名的 DNS 解析，一旦获得 IP 地址后，它将尝试使用此 IP 地址（该 IP 配置在控制器的虚拟接口）打开 TCP 会话。

最终，网页通过隧道到达客户端，用户通过 SSL 隧道发回用户名/口令。

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）的 Web 身份验证。有关默认网页使用的详细信息，请参阅“选择默认 Web 身份验证登录页”。
- 使用自定义登录页的 Web 身份验证。有关如何使用自定义登录页的详细信息，请参阅“创建自定义 Web 身份验证登录页”。
- 使用外部 Web 服务器登录页的 Web 身份验证。有关如何使用外部 Web 服务器登录页的详细信息，请参阅“使用外部 Web 服务器的自定义 Web 身份验证登录页”。

注意： 定制的Web验证套件有文件名的30个字符限制。保证在套件内的文件名比30个字符不极大。

注意： 从 WLC 版本 7.0 开始，如果 WLAN 上启用了 Web 身份验证且具备 CPU ACL 规则，只要客户端在 WebAuth_Reqd 状态中未进行身份验证，则基于客户端的 Web 身份验证规则的优先级始终较高。一旦客户端变为 RUN 状态，就应用 CPU ACL 规则。

注意： 因此，如果 CPU ACL 已在 WLC 中启用，则在以下情况下需要虚拟接口 IP 的允许规则（任何方向）：

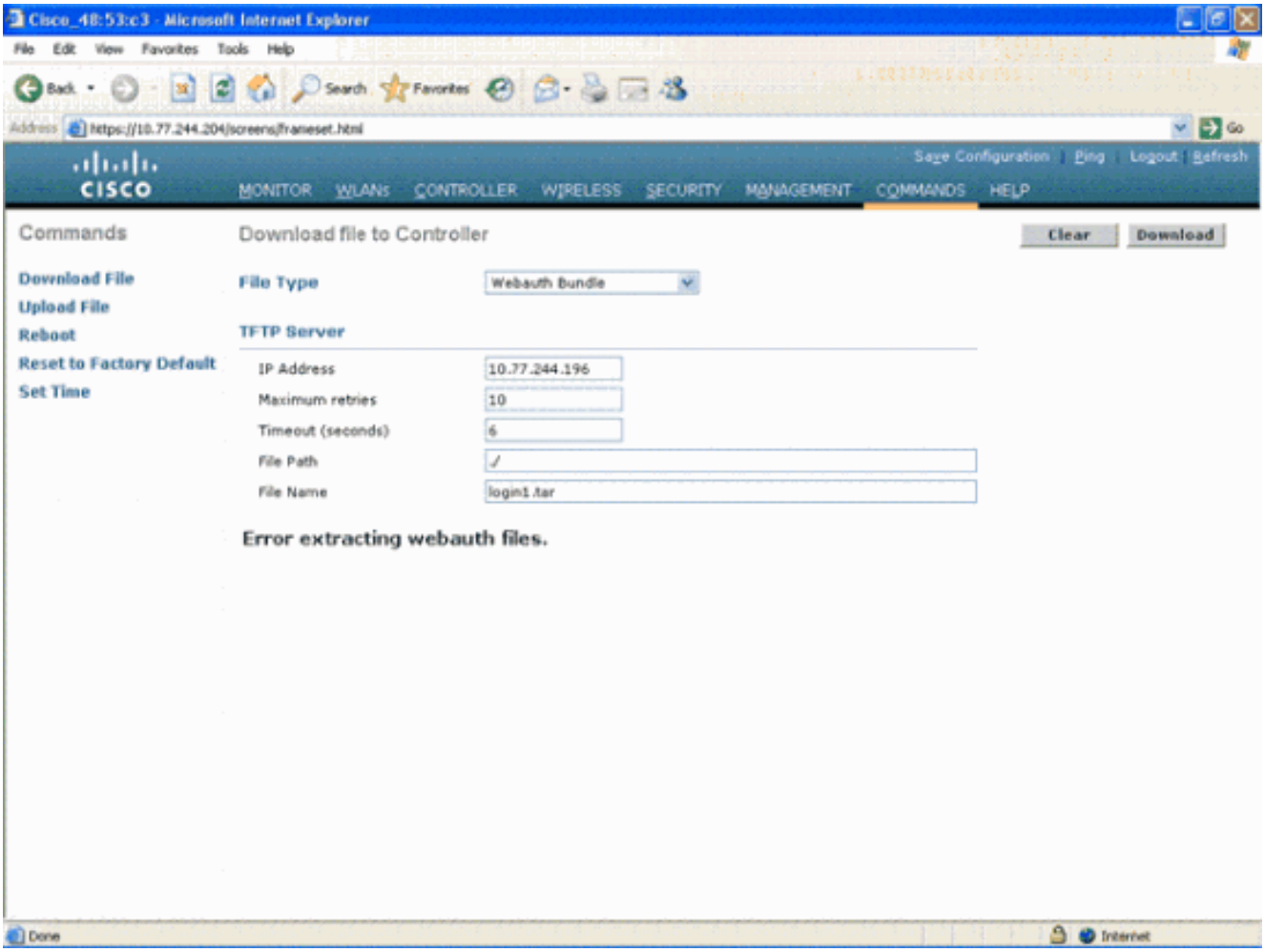
- CPU ACL 不包含两个方向的“全部允许”规则。
- 存在“全部允许”规则，但还存在优先级较高的端口 443 或 80 的拒绝规则。

注意： 如果已禁用安全 Web，虚拟 IP 的允许规则应用于 TCP 协议和端口 80，如果已启用安全 Web，则应用于端口 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，如果该功能无法发挥预期作用，请完成以下故障排除步骤：

1. 检查客户端是否已获得 IP 地址。如果未获得，用户可以取消选中 WLAN 上的 **DHCP Required** 并给无线客户端一个静态 IP 地址。这样将与接入点建立关联。*有关 DHCP 故障排除的相关问题*，请参阅*“Cisco 统一无线网络的客户端问题故障排除”中的“IP 编址问题”*部分。
2. 对于版本早于 3.2.150.10 的 WLC，必须手动输入 **https://1.1.1.1/login.html**，以导航到 Web 身份验证窗口。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 Windows 上，选择“开始”>“运行”，输入 **CMD** 打开命令窗口，然后执行“nslookup www.cisco.com”并查看是否返回 IP 地址。在 Mac/Linux 上：打开终端窗口，执行“nslookup www.cisco.com”并查看是否返回 IP 地址。如果您认为客户端没有进行 DNS 解析，可以执行以下操作：输入 URL 的 IP 地址（例如，http://www.cisco.com 的 IP 地址是 http://198.133.219.25）尝试使用 https://<Virtual_interface_IP_Address>/login.html 直接到达控制器的 Web 身份验证页。通常是 http://1.1.1.1/login.html。输入此 URL 是否可以打开网页？如果可以，很可能是 DNS 问题。也可能是证书问题。默认情况下，控制器使用自签名证书，而多数 Web 浏览器会对此提出相应的警告。
4. 对于使用自定义网页的 Web 身份验证，确保使用合适的自定义网页 HTML 代码。您能下载从Cisco软件下载的一份示例Web验证脚本。例如，对于4400个控制器，请选择**产品>无线>无线局域网Controller>独立控制器>思科4400系列无线局域网控制器> Cisco 4404无线局域网在机箱>无线局域网控制器Web验证Bundle-1.0.1的Controller>软件**并且下载**webauth_bundle.zip文件**。当用户的 Internet 浏览器重定向至自定义登录页时，下列参数将添加至 URL：ap_mac — 无线用户关联接入点的 MAC 地址。switch_url — 应发布用户凭证的控制器的 URL。redirect — 身份验证成功后用户重定向的目标 URL。statusCode — 从控制器的 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：“您未进行配置，无法对 Web 门户进行身份验证。无需再执行任何操作。”状态代码 3：“指定的用户名不可用。是否已使用该用户名登录系统？”状态代码 4：“您不在范围内。”状态代码 5：“您输入的用户名和口令组合无效。请重试。
5. 需要出现在自定义网页上的所有文件和图片应在上载至 WLC 前捆绑到 .tar 格式文件中。确保 tar 捆绑文件中包含 login.html 文件。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。**注意：** 较大的文件和名称较长的文件在提取时会发生错误。建议的图片格式是 .jpg。

6. 建议使用 Internet Explorer 6.0 SP1 或更高版本的浏览器进行 Web 身份验证。其他浏览器可能不适用。
7. 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。出于安全考虑，IE 6.0 上的该选项在默认情况下禁用。**注意：** 如果您已为用户配置了弹出消息，则需要在浏览器上禁用弹出窗口拦截器。**注意：** 如果您浏览 **https** 站点时无法重定向，请参阅 Cisco Bug ID CSCar04580（仅限注册用户），以获得更多详细信息。
8. 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，将 **DNS 主机名**分配给虚拟接口。
9. 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。
10. 根据网络的不同，可以将拓扑/解决方案防火墙置于客户端和 Web 身份验证服务器之间。对于实现的每个网络设计/解决方案，最终用户应确保网络防火墙允许使用这些端口。
11. 为了进行 Web 身份验证，客户端应首先与 WLC 上合适的 WLAN 建立关联。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。
12. 禁用客户端浏览器上的代理设置，直到 Web 身份验证完成。
13. 默认的 Web 身份验证方法是 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。可以使用 WLC 上的 **debug aaa all** 命令查看 RADIUS 服务器的调试程序。
14. 将计算机上的硬件驱动程序代码更新为制造商网站上的最新版。
15. 验证请求方的设置（笔记本电脑上的程序）。

16. 如果使用 Windows 内置的 Windows Zero Config 请求方，则：确认用户安装了最新的补丁程序。在请求方运行调试程序。
17. 在客户端上，从命令窗口打开 EAPOL (WPA+WPA2) 和 RASTLS 日志，运行 Start > Run > 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，所有日志都位于 C:\Windows\tracing 目录下。
18. 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
    ```
19. 如果完成这些步骤后仍未解决问题，收集以下调试程序并使用 TAC 服务请求工具（仅限注册用户）打开服务请求。`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**