对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除

Contents

Introduction

本文在无线局域网控制器(WLC)环境里提供提示为了排除Web认证问题故障。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 控制知识和设置无线访问访问接入点(CAPWAP)。
- 知识如何配置轻量级基本操作的接入点(LAP)和WLC。
- Web认证基础知识和如何配置在WLCs的Web认证。关于如何配置在WLCs的Web认证的信息，请参见无线局域网控制器Web身份验证配置示例。

Components Used

本文的信息运行固件版本8.3.121的根据WLC 5500。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

相关产品

本文可能也与此硬件一起使用：

- 思科5500系列无线控制器
- Cisco 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

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

在WLCs的Web认证

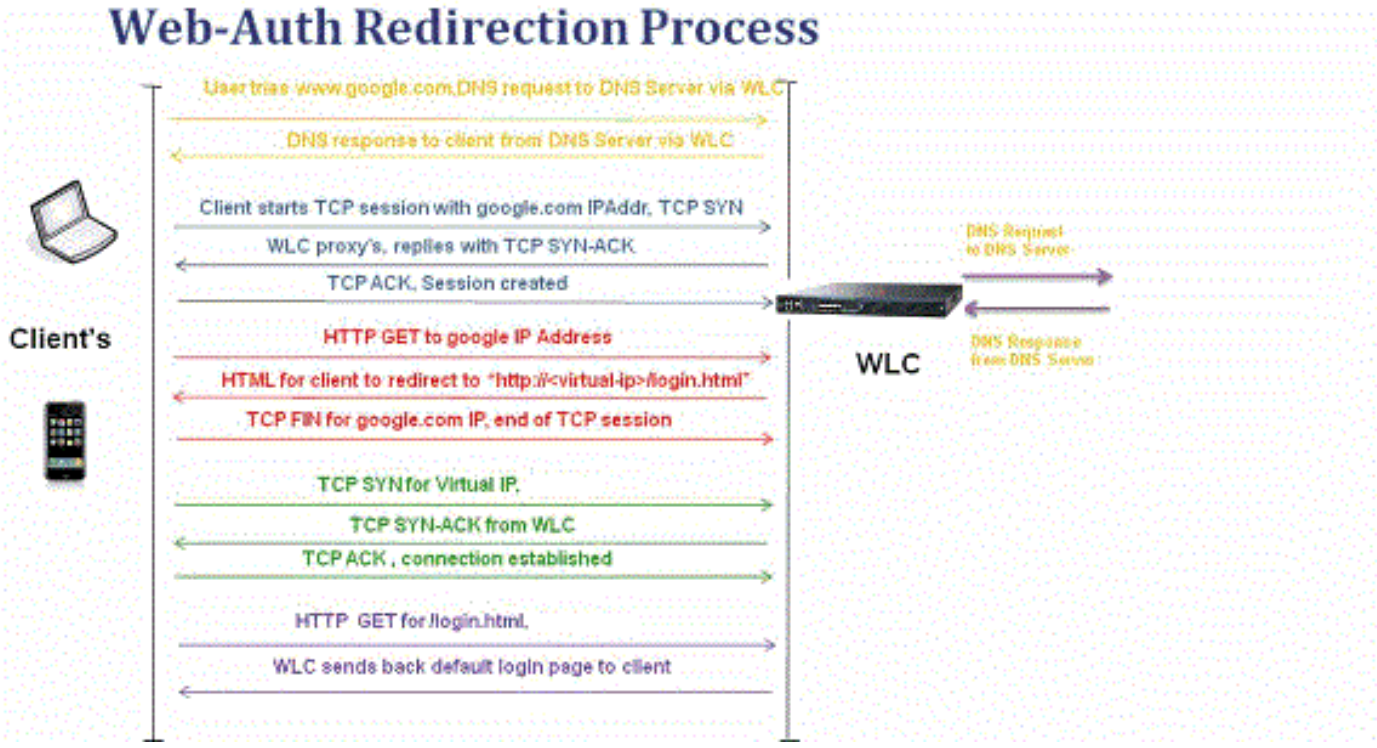
Web认证是造成控制器不允许IP数据流，除了与DHCP相关的信息包域名系统(DNS)有关的信息包，自一个特定的客户端的第3层安全功能，直到该客户端把允许的流量的例外正确地供给一个有效用户名和密码通过PREauth访问控制表(ACL)。Web认证是允许客户端在认证前获得IP地址的唯一的安全策略。没有需要对于请求方或客户端工具，它是一个简单验证方法。Web 身份验证可以在 WLC 上本地执行，或通过 RADIUS 服务器执行。Web 身份验证通常由希望部署访客接入网络的客户使用。

Web认证开始，当控制器截断自客户端的第一个TCP HTTP (端口80) GET信息包。为了客户端的Web浏览器能获得此更，客户端必须首先获得IP地址，并且执行URL的转换对IP地址(DNS解析)Web浏览器的。这告诉Web浏览器发送HTTP GET的哪个IP地址。

当Web认证在WLAN时被配置，控制器阻塞所有数据流(直到认证过程完成)从客户端，除了DHCP和DNS数据流。当客户端发送第一HTTP GET到TCP端口80时，控制器重定向客户端对 https://192.0.2.1/login.html (如果配置)的这是虚拟IP处理的。此进程最终带动登录网页。

Note:当您使用一外部Web服务器Web认证时， WLC平台需要外部Web服务器的预验证ACL。

此部分详细说明Web认证重定向过程。



- 您打开Web浏览器并且输入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通过DNS请求到DNS服务器，并且DNS服务器回应DNS回复，包含目的地www.google.com的IP地址，反过来转发到无线客户端。
- 然后，客户端尝试打开与目标 IP 地址之间的 TCP 连接，它派出TCP Syn信息包被注定对www.google.com的IP地址。

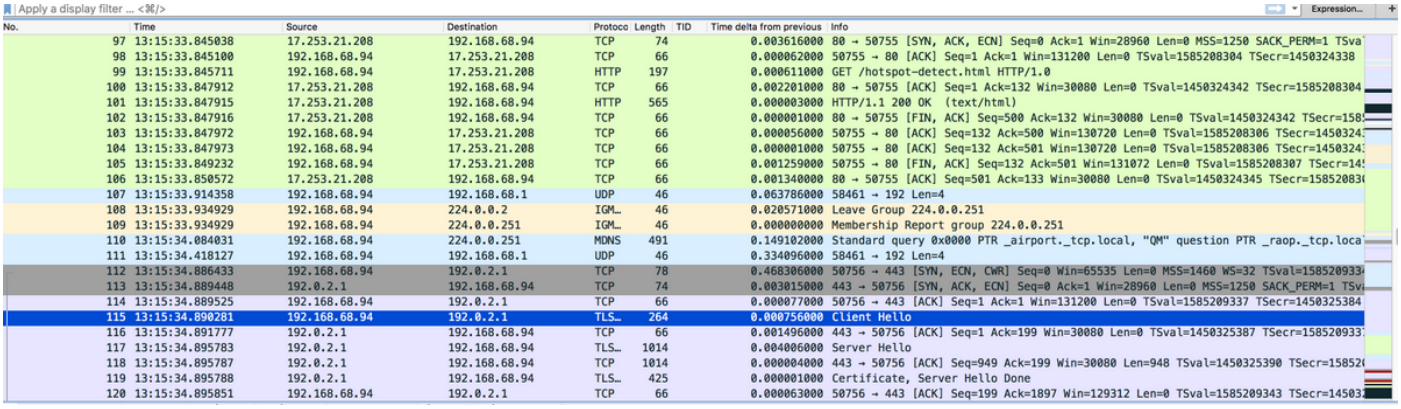
- WLC有为客户端配置的规则并且能作为www.google.com的一个代理。它退还一个TCP SYN-ACK信息包到有来源的客户端作为www.google.com的IP地址。客户端退还一TCP ACK数据包为了完成三向交握，并且TCP连接充分地被建立。
- 客户端发送被注定的一个HTTP GET信息包到www.google.com。WLC 拦截此数据包并发送以进行重定向处理。HTTP 应用程序网关准备 HTML 主体并将其作为客户端 HTTP GET 请求的应答返回。此 HTML 使客户端前往 WLC 的默认网页 URL，例如 http://<Virtual-Server-IP>/login.html。
- 客户端断开与IP地址的TCP连接，例如www.google.com。
- 现在客户端要去http:// <virtualip>/login.html和，因此设法打开与WLC的虚拟IP地址的TCP连接。它发送(一个TCP Syn信息包我们的虚拟IP在这里)的192.0.2.1的到WLC。
- WLC 返回 TCP SYN-ACK，而客户端则发回 TCP ACK 至 WLC，以完成握手。
- 客户端发送被注定的/login.html的一HTTP GET到192.0.2.1为了请求登录页。
- 此请求允许至WLC的Web服务器，并且服务器回应默认登录页。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。

在本例中，客户端IP地址是192.168.68.94。客户端解决了访问的URL到Web服务器， 10.1.0.13。正如你看到的客户端执行三通的握手开始TCP连接然后发送了开始从信息包96的HTTP GET信息包(00是HTTP数据包)。(我们能从被请求的URL猜测)，这未由用户触发，然而是操作系统自动化的门户检测触发。控制器拦截信息包和回复与代码200。代码200信息包有重定向URL在它：

```
<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>
```

它通过三通的握手然后断开TCP连接。

客户端然后开始发送它到192.0.2.1，是控制器的虚拟IP地址与重定向URL的HTTPS连接。客户端必须验证服务器证明或忽略它为了提出SSL隧道。在这种情况下，它是自签证书，因此客户端忽略了它。登录网页通过此SSL隧道被发送。信息包112开始处理。



No.	Time	Source	Destination	Protoco	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=145
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=158520830
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=158520933
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=158520
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=145033

您有配置的选项WLC的虚拟IP地址的域名。如果配置虚拟IP地址的域名，此域名在HTTP OK信息包返回从控制器以回应HTTP GET信息包从客户端。您必须然后执行此域名的DNS解析。一旦它从DNS解析获得IP地址，尝试开始一次TCP会话用该IP地址，是在控制器的虚拟接口配置的IP地址。

最终，网页通过隧道给客户端，并且用户通过安全套接字协议层(SSL)隧道退还用户名/密码。

Web认证由这三个方法之一进行：

- 请使用一个内部网页(默认值)。参考选择默认Web认证登录页关于使用默认网页的更多信息。
- 请使用定制的登录页。参考创建定制的Web认证登录页关于如何使用定制的登录页的更多信息。
- 请使用从外部Web服务器的登录页。请参见使用从外部Web服务器的定制的Web认证登录页关于如何使用从外部Web服务器的登录页的更多信息。

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

-从WLC版本7.0向前，如果Web认证在WLAN被启用，并且也有CPU ACL规则，基于客户的Web认证规则总是获得更高的优先权，只要客户端是未经鉴定的在Webauth_Reqd状态。一旦客户端去运转状态， CPU ACL规则得到应用。

所以-，如果CPU ACL在WLC被启用，虚拟接口IP的一个允许规则在这些情况需要(在ANY方向)：
-，当CPU ACL没有一允许两个方向的所有规则。
-，当那里存在允许所有规则时，但是那里也存在端口的443或80一个拒绝规则更高的优先次序。

-虚拟IP的允许规则应该是为TCP协议和端口80，如果secureweb是失效的，或者端口443，如果secureweb是启用的。当CPU ACL到位时，这是需要的为了允许客户端的访问对虚拟接口IP地址过帐成功的验证。

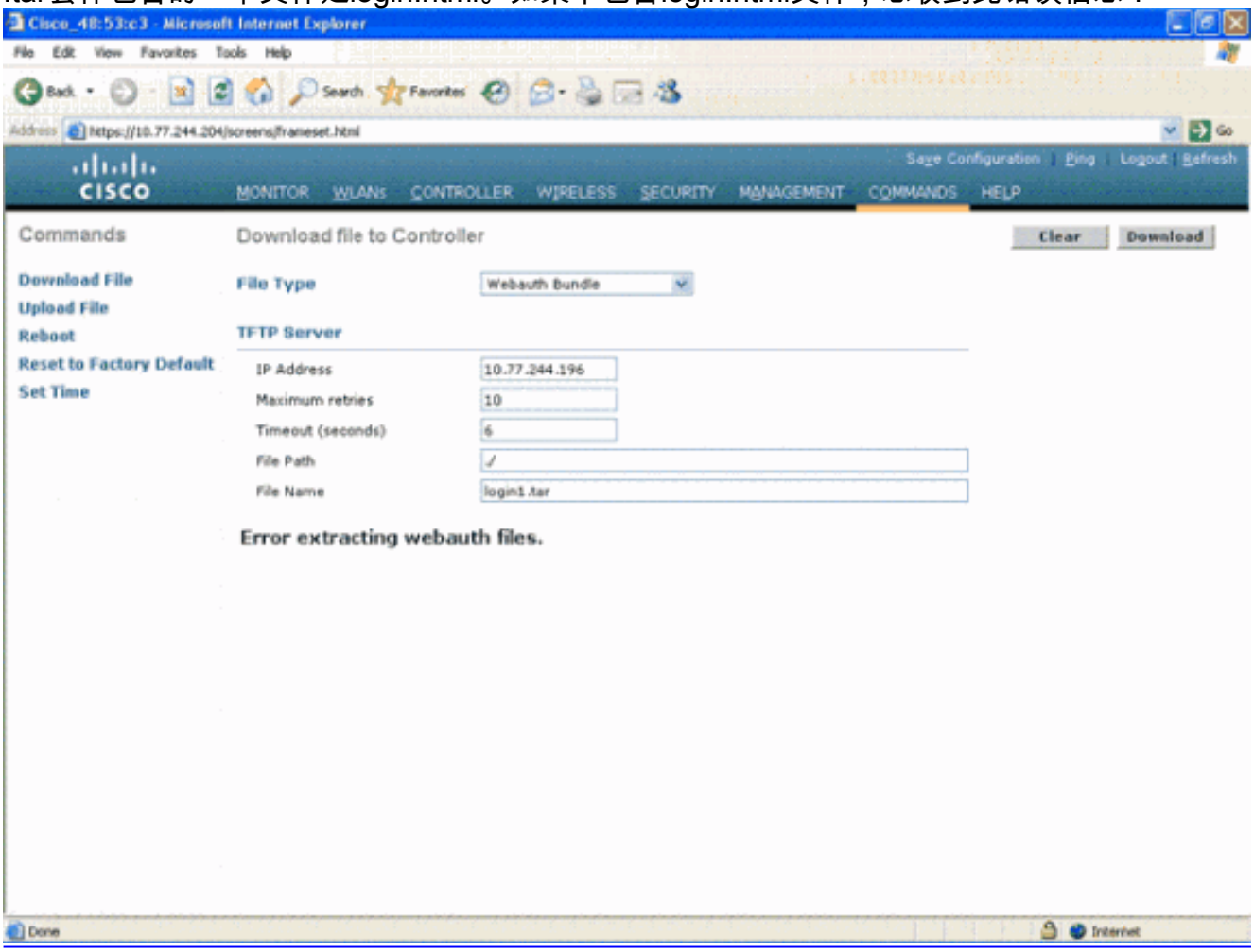
Web 身份验证故障排除

在您配置Web认证后，并且，如果功能不运作得正如所料，请完成这些步骤：

1. 检查客户端是否获得IP地址。否则，用户能不选定**DHCP要求了**在WLAN的复选框并且产生无线客户端静态IP地址。这假设关联用接入点。
2. 下一步在进程中是URL的DNS解析在Web浏览器的。当WLAN客户端连接到为Web认证时配置的WLAN，客户端获得从DHCP服务器的一个IP地址。用户打开Web浏览器并且输入网址。客户端然后执行DNS解析获得网站的IP地址。现在，当客户端设法到达网站时， WLC拦截客户端的HTTP GET会话并且重定向用户对Web认证登录页。
3. 所以，请保证客户端能执行重定向的DNS解析能工作。在微软视窗中，请选择**Start > Run**，输入**CMD**为了打开命令窗口，并且执行“nslookup www.cisco.com”并且检查IP地址是否回来。在橡皮防水布/Linux中，请打开终端窗口并且执行“nslookup www.cisco.com”并且检查IP地址是否回来。如果相信客户端没获得DNS解析，您能：输入或者URL的IP地址(例如，http://www.cisco.com是http://198.133.219.25)。设法键入应该通过无线适配器解决的所有(甚而非存在的) IP地址。输入此URL带动网页？如果是，是很可能DNS问题。它也许也是认证问题。默认情况下，控制器使用一自签证书，并且多数Web浏览器对他们的使用提出警告。
4. 对于与一个定制的网页的Web认证，请保证定制的网页的HTML代码是适当的。 您能从Cisco软件下载下载示例Web认证脚本。例如，对于5508个控制器，请选择**产品>无线>无线局域网Controller>独立控制器> Cisco 5500系列无线局域网控制器> Cisco 5508无线局域网在机箱>无线局域网控制器Web认证套件的Controller>软件**并且下载**webauth_bundle.zip文件**。当用户的互联网浏览器重定向对定制的登录页时，这些参数被添加到URL ：ap_mac -无线用户是关联的接入点的MAC地址。switch_url -用户凭证应该张贴控制器的URL。重定向-用户重定向的URL，在认证是成功的以后。状态代码-从控制器的Web认证服务器返回的状态码。
WLAN -无线用户是关联的WLAN SSID。这些是可用的状态码：状态码1 - “您已经登陆。进一步动作在您的部分没有需要”。状态码2 - “没有配置您验证Web门户。进一步动作在您的部分没

有需要”。状态码3 - “指定的用户名不可能此时使用。或许用户名已经被记录到系统？”状态码4 - “您被排除了”。状态码5 - “您输入的用户名和密码组合无效。请再试试”。

5. 需要出现在定制的网页的所有文件和图片应该捆绑到.tar文件，在被加载到WLC前。保证在.tar套件包含的一个文件是login.html。如果不包含login.html文件，您收到此错误信息：



请参见[无线局域网控制器Web身份验证配置示例的定制的Web Authentication部分指南]关于如何创建一个定制的Web认证窗口的更多信息。**Note**:大安排长名字发生在提取错误的文件和文件。建议图片以.jpg格式。

6. 保证**写脚本的**选项在客户端浏览器没有被阻拦，因为在WLC的定制的网页基本上是HTML脚本。
7. 如果有为WLC的**虚拟接口**配置的一个**主机名**，请切记DNS解析为虚拟接口的主机名是可用的。 **Note**:连接对从WLC GUI的**Controller>接口**菜单为了分配**DNS主机名**-到虚拟接口。
8. 有时在客户端计算机上安装的防火墙阻拦Web认证登录页。在您设法访问登录页前，请禁用防火墙。一旦Web认证完成，防火墙可以再被启用。
9. 拓扑/解决方案防火墙可以被放置在客户端和认证服务器之间，取决于网络。关于实现的每个网络设计/解决方案，终端用户应该确定这些端口在网络防火墙允许。

10. 为了使发生Web的认证，客户端应该首先联合到在WLC的适当的WLAN。连接对在WLC GUI的**监控程序>客户端**菜单为了看到客户端是否被关联对WLC。检查客户端是否有一个有效IP地址。
11. 请禁用在客户端浏览器的代理设置，直到Web认证完成。
12. 默认Web认证方法是密码认证协议。保证PAP认证在此的RADIUS服务器允许能工作。为了检查客户端验证的状况，请检查调试和日志消息从RADIUS服务器。您能使用**debug aaa all命令**在WLC为了查看从RADIUS服务器的调试。
13. 更新在计算机的硬件驱动程序对从制造商的网站的最新的代码。

14. 验证在请求方(膝上型计算机的程序的设置)。
15. 当您使用Windows零设置请求方被构件到Windows ： 验证安排最新的补丁程序安装用户。运行在请求方的调试。
16. 在客户端，请打开从命令窗口的EAPOL (WPA+WPA2)和RASTLS日志。选择**Start > Run > CMD** ：
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    为了禁用日志，请运行同一个命令，但是用功能失效替换enable (event)。对于XP，所有日志位于C:\Windows\tracing。
17. 如果仍然没有登录网页，请收集并且分析单个客户端的此输出：
    ```
    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. 如果问题不是解决的，在您完成这些步骤后，请收集这些调试并且请使用支持案件管理器为了打开服务请求。
    ```
    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>
    ```

Related Information

- **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**
- Technical Support & Documentation - Cisco Systems