在WLAN控制器的Web认证

Contents

Introduction

本文解释Web认证的进程在无线局域网控制器(WLC)。

Prerequisites

Requirements

Cisco建议您有WLC配置基础知识。

Components Used

本文的信息根据所有WLC硬件型号。

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.

Web认证内在进程

Web认证位置作为安全功能

Web认证(WebAuth)是第3层安全。它允许在所有位置工作运行浏览器的用户友好安全。它可能与所有预共享密钥(PSK)安全(第2层安全策略)也一起。虽然WebAuth和PSK的组合极大减少用户友好部分和经常没有使用，仍然有加密的优点客户端的流量。没有加密， WebAuth是认证方法。

WebAuth不可能配置有802.1x/RADIUS (远程认证拨入用户服务)，直到安装WLC软件版本7.4可以同时的地方配置。然而，请注意客户端必须通过dot1x和Web认证。没有意味着为客户，然而为一个Web门户的添加员工的(谁使用802.1x)。没有dot1x员工的或Web门户的一一体化服务集标识(SSID)客户的。

WebAuth如何工作

802.11认证过程是开放的，因此您能验证和联合不出任何问题。在那以后，您是关联的，但是不在WLC运转状态。有Web认证功能，您在您不能访问任何网络资源的**WEBAUTH_REQD**被保留(没有ping，等等)。您必须收到与DNS服务器的地址的一个DHCP IP地址在选项的。

您必须键入在您的浏览器的有效URL。客户端通过DNS协议解决URL。客户端然后发送其HTTP请求到网站的IP地址。请求并且返回**webauth**登录页，伪装网站IP地址的WLC截住。一旦外部WebAuth， WLC回复以包括您的网站IP地址的HTTP回应并且阐明，页移动了。页被移动了向WLC使用的外部Web服务器。当您验证时，您获得访问到所有网络资源和重定向对最初被请求的URL，默认情况下(除非牵强的重定向在WLC被配置了)。总之， WLC在**WEBAUTH_REQD**状态允许客户端解决DNS和自动地获得IP地址。

提示：如果希望WLC观看另一个端口而不是端口80，您能使用**config network web-auth-port <port number>**也创建在此端口的重定向。示例是访问控制服务器(ACS) Web接口，在端口2002或其他相似的应用程序。

> **注释关于HTTPS重定向**：默认情况下和在7.x版本和前， WLC没有重定向HTTPS流量。这意味着，如果打开您的浏览器并且键入HTTPS地址，什么都不发生。您必须键入HTTP地址为了重新定向到在HTTPS服务的登录页。
>
> 在版本8.0和以上，您能HTTPS流量的enable (event)重定向与CLI命令**设置网络web-auth https重定向enable (event)的。**
>
> 注意这是消耗为WLC的资源，万一发送许多HTTPS请求。建议不在此功能可扩展性被提高的WLC版本8.7前使用此功能。并且请注意认证警告在这种情况下是不可避免的。的确，如果您的客户端要求任何URL (例如https://www.cisco.com)，仍然WLC存在为虚拟接口IP地址发行的其自己的认证。这明显地不会匹配客户端要求的URL IP地址，并且认证不会委托，除非客户端强制在他们的浏览器的例外。

WLC软件版本预示性能下降在被测量的8.7前的：

Webauth	达到的费率
3个URL - HTTP	140/第二
第1个URL - HTTP 第2个和第3个URL - HTTPS	20/第二
3个URL - HTTPS (大的部署)	<1/第二
3个URL - HTTPS (最多100个客户端)	10/第二

在此性能表里， 3个URL被称为：

- 原始URL由终端用户(用户要访问对)的网站进入了
- URL WLC重定向浏览器
- 最终证件提交

性能表提供WLC性能，万一全部3个URL是HTTP，万一全部3个URL是HTTPS，或者，如果客户端从HTTP移动到HTTPS (更多典型方案)。

如何做内部(本地) WebAuth与内部页一起使用

如果需要用一个可操作的动态接口配置WLAN，客户端应该通过DHCP也接受DNS服务器IP地址。在您设置所有**webauth前**，您应该测试您的WLAN适当地运作，您能解决DNS请求(**nslookup**)，并且您能访问网页。然后，您能设置Web认证作为第3层安全功能。例如您能创建您的用户本地数据库的或一个外部RADIUS服务器的。请参见无线局域网控制器Web身份验证配置示例文档。

如何用自定义页配置自定义本地WebAuth

自定义**webauth**可以配置有从**安全**选项的**redirectUrl**。这强制重定向对您输入的一个特定网页。当用户验证时，它改写原始URL客户端被请求并且显示重定向分配的页。

自定义功能允许您使用自定义超文本标记语言页而不是默认登录页。加载您的html和图像文件捆绑到控制器。在加载页，请寻找**webauth套件**以tar格式。通常， PicoZip创建兼容与WLC一起使用的tar。关于WebAuth套件的示例，请参见无线控制器WebAuth套件的下载软件页。请务必为您的WLC选择适当的版本。好推荐是定制存在的套件;从头请勿创建一个套件。

有随版本和Bug变化与**自定义webauth的**一些限制。注意的事包括：

- .tar文件大小(没有更多比5MB)
- 文件的数量在.tar的
- 文件的文件名长度(应该是不大于30个字符)

如果您的用户程序包不工作，尝试与一个简单的自定义程序包。然后请添加文件和复杂性一次一个到达程序包用户设法使用。这应该帮助您识别问题。关于关于怎样的一个示例配置自定义页，请参见创建定制的Web认证登录页，在Cisco无线LAN控制器配置指南内的一个部分，版本7.0。

改写全局配置技术

对于每WLAN，您用集合的**覆盖**配置**global config命令**和每WLAN的一种WebAuth类型。这意味着您能有内部/默认值与一个自定义内部/默认值另一WLAN的WebAuth的WebAuth。这也允许您配置每

WLAN的不同的自定义页。您必须结合在同一个套件的所有您的页和加载他们到WLC。然后，您能设置您的与**覆盖的**自定义页**global config命令**在每WLAN和选择哪个文件是从所有的登录页在套件内的文件。您能选择不同的登录页在每WLAN的套件里面。

重定向问题

有在允许重定向的HTML套件内的一个变量。请勿放置您牵强的重定向URL那里。对于所有重定向在自定义WebAuth发出， Cisco推荐检查套件。如果在WLC GUI输入与**+=的**重定向URL，这可能重写或添加到URL被定义在套件里面。例如，在WLC GUI， **redirectURL**字段设置为 www.cisco.com;然而，在套件它显示：**redirectURL+=** 'www.google.com'。**+=**重定向用户对 www.cisco.comwww.google.com，是无效URL。

如何做外部(本地) Web认证与外部页一起使用

如已经简要地解释，外部WebAuth服务器的利用率是登录页的一间外部贮藏库。用户凭证由WLC仍然验证。外部Web服务器只允许您使用特殊或不同的登录页。这是为外部WebAuth执行的步骤：

1. 客户端(终端用户)打开Web浏览器并且输入URL。

2. 如果客户端没有验证，并且使用外部Web认证， WLC重定向用户对外部Web服务器URL。换句话说， WLC发送HTTP重定向到客户端用网站的被伪装的IP地址和点到外部服务器IP地址。外部Web认证登录URL带有参数例如**AP_Mac_Address**、**client_url** (www.website.com)和用户需求与交换机Web服务器联系的**action_URL**。

3. 外部Web服务器URL派遣用户到登录页。然后用户能使用预验证访问控制表(ACL)为了访问服务器。ACL为除了4400系列和Wism1的所有WLC型号是需要的。

4. 登录页采取被输入的用户凭证并且送回请求到**action_URL**，例如http://192.0.2.1/login.html， WLC Web服务器。这提供作为输入参数给用户重定向URL， 192.0.2.1是在交换机的虚拟接口地址。

5. WLC Web 服务器提交用于身份验证的用户名和口令。

6. WLC起动RADIUS服务器请求或使用在WLC的本地数据库，然后验证用户。

7. 如果认证是成功的， WLC Web服务器二者之一转发用户到被配置的重定向URL或到URL客户端被输入。

8. 如果认证发生故障，则WLC Web服务器重定向用户回到用户登录URL。

   Note: 我们例如虚拟IP使用192.0.2.1在本文。因为是不可路由的， 192.0.2.x范围建议为虚拟IP的使用。更旧的文档可能是指"1.1.1.x"或那可能仍然是什么在您的WLC被配置和这曾经默认设置。然而，请注意当前此ip一个有效可路由IP地址并且192.0.2.x子网建议。

Note: 如果接入点(APs)在FlexConnect模式下， **preauth** ACL是毫不相关的。弹性ACL可以用于对Web服务器的允许未验证的客户端。请参见与无线局域网控制器配置示例的外部Web认证。

Web转接

这是内部Web认证的变化。它显示与警告或一个提醒的语句的页，但是不提示输入证件。用户应该点击OK键。您能enable (event)电子邮件输入，并且用户能输入他们的电子邮件地址，成为他们的用户名。当用户被联络时，请检查您的活动客户端列表;用户用电子邮件地址列出他们进入了作为用户名。欲知更多信息，请参见无线局域网控制器Web转接配置示例。

有条件的Web重定向

如果enable (event)有条件的Web重定向，用户有条件地重定向对一个特定的网页，在802.1x认证成功地完成后。您可以在您的 RADIUS 服务器上指定重定向页以及发生重定向的条件。情况能包括用户密码，当它到达有效期时或，当用户需要付帐单持续的使用/访问时。如果RADIUS服务器返回Cisco AV对**url重新定向**，则用户重定向对指定的URL，当他们打开浏览器时。如果服务器也返回Cisco AV对**url-redirect-acl**，则命名ACL安装作为此客户端的预验证ACL。客户端没有被认为这时充分地被核准并且能只通过允许的流量预验证ACL。在客户端完成一次特定的操作在指定的URL (例如，密码更改或票据付款)后，然后客户端必须重新鉴别。当RADIUS服务器不返回**url重新定向时**，客户端被认为充分地被核准和允许通过数据流。

Note: 有条件的Web重定向功能为为802.1x或WPA+WPA2第2层安全被配置的WLANs是仅可用的。

在您配置RADIUS服务器后，您能用控制器GUI或CLI然后配置在控制器的有条件的Web重定向。请参见这些逐步指南：使用配置的GUI Web重定向和使用CLI配置Web重定向。

飞溅页Web重定向

如果enable (event)飞溅页Web重定向，用户重定向对一个特定的网页，在802.1x认证成功后地完成。在重定向，用户有全部存取对网络后。您在您的RADIUS服务器能指定重定向页。如果RADIUS服务器返回Cisco AV对**url重新定向**，则用户重定向对指定的URL，当他们打开浏览器时。客户端被认为这时充分地被核准和允许通过数据流，即使RADIUS服务器不返回**url重新定向**。

Note: 飞溅页Web重定向功能为为802.1x或WPA+WPA2第2层安全被配置的WLANs是仅可用的。

在您配置RADIUS服务器后，您能用控制器GUI或CLI然后配置在控制器的飞溅页Web重定向。

在MAC过滤器故障的WebAuth

这要求您配置在第2层安全菜单的MAC过滤器。如果用户顺利地验证与他们的MAC地址，则他们去直接地运转状态。如果他们不是，则他们去**WEBAUTH_REQD**状态，并且正常Web认证出现。

Note:这没有用Web转接支持。欲知更多信息，请跟随在增强请求CSCtw73512的活动 。

中央Web认证

中央Web认证是指WLC不再主机所有服务的一个方案。区别位于事实客户端直接地派遣到ISE Web门户，并且不通过在WLC的192.0.2.1。登录页和整个门户被形象化。

当您安排RADIUS网络准入控制(NAC)被启用在被启用的WLAN和MAC过滤器的先进的设置中央Web认证发生。

整体概念是WLC发送RADIUS认证(通常MAC过滤器)到ISE，回复以重定向**URL**属性值(AV)对。用户在**POSTURE_REQD**状态然后放置，直到ISE产生与授权(CoA)请求的更改的授权。同一个方案在状

态或中央WebAuth发生。中央WebAuth不是与WPAEnterprise/802.1x兼容，因为客户门户不能返回加密的对话键，如执行与可扩展的认证协议(EAP)。

外部用户认证(RADIUS)

这为本地WebAuth只是有效的，当WLC处理证件时，或者，当第3层Web策略是启用的时。您能本地然后验证用户在WLC或外部通过RADIUS。

有WLC检查用户的证件的命令。

1. 无论如何，它在其自己的数据库首先查找。
2. 如果它不找到用户那里，去在客户WLAN配置的RADIUS服务器(如果有被配置的一个)。
3. 它根据**网络用户**被检查的RADIUS服务器然后检查全局RADIUS服务器列表。

此第三个点是非常重要的并且应答不配置该WLAN的RADIUS许多的问题，但是注意仍然检查RADIUS，当用户在控制器时没有找到。这是因为**网络用户**根据您的在全局列表的RADIUS服务器核对。

WLC能验证用户到有密码认证协议的RADIUS服务器，质询握手验证协议(CHAP)或者EAP-MD5 (消息Digest5)。这是一个全局参数并且从GUI或CLI是可配置的：

从GUI ：连接对**Controller> Web RADIUS认证**

从CLI ：输入**设置自定义Web RADIUSauth <pap|chap|md5chap>**

Note: NAC客户服务器只使用PAP。

如何设置有线客户WLAN

配置和非常close到无线客户配置是容易的。(只有当一个是自动锚点)，您能用一两个控制器配置它。

选择VLAN作为您在VLAN 50安置有线客人身份的用户，例如的VLAN。当一个有线客户想要对互联网时的访问，请插入膝上型计算机对在为VLAN配置的交换机的端口50。此VLAN 50一定是准许和存在路径到WLC中继端口。在两WLCs案件(外国一的锚点和一个)，此有线客户VLAN必须导致外国WLC (已命名WLC1)和不锚点。WLC1然后照料以隧道传输数据流对DMZ WLC (锚点，已命名WLC2)，发布在路由的网络的数据流。

这是配置有线访客访问的五个步骤：

1. **配置有线客户用户访问的一动态interface (VLAN)。**

   在WLC1，请创建一个动态接口VLAN50。在**Interface Configuration页**，请检查**客户LAN**机箱。然后，字段例如**IP地址**和**网关**消失。唯一的事您的WLC需要知道关于此接口是数据流从VLAN 50被路由。这些客户端是有线客户。

2. **创建客户用户访问的一个有线LAN。**

   在控制器上，使用接口，当联合对WLAN。第二步将创建在您的总部控制器的一WLAN。连接对**WLANs**并且点击**新**。在**WLAN类型**，请选择**客户LAN**。

在**配置文件名字**和**WLAN SSID**，请输入识别此WLAN的名字。这些名字是不同的，但是不能包含空间。使用术语WLAN，但是此网络配置文件没有与无线网络配置文件有关。

一般选项提供两张下拉列表：**入口**和**出口**。入口是用户来的VLAN (VLAN 50);出口是您要发送他们的VLAN。

对于**入口**，请选择**VLAN50**。

对于**出口**，它是不同的。如果只有一个控制器，您需要创建另一个动态接口，一**标准**一个这次(不是客户LAN)，并且您派遣您的有线用户到此接口。在这种情况下，请发送他们到DMZ控制器。所以，对于输出接口，请选择**管理接口**。

此客户LAN的"WLAN"**安全模式**是WebAuth，是可接受的。点击OK键为了验证。

3. **配置外国控制器(总部)。**

从**WLAN列表**，请点击**移动性锚点**在**客户LAN**线路尽头，并且选择您的DMZ控制器。被假设得这里两个控制器彼此了解。如果他们不彼此了解，请去**Controller>移动性Management>移动组**，并且添加在WLC1的**DMZWLC**。然后请添加在DMZ的**WLC1**。两个控制器不应该在同样移动组。否则，基本安全规则是残破的。

4. **配置锚点控制器(DMZ控制器)。**

您的总部控制器准备好。您当前需要准备您的DMZ控制器。对您的DMZ控制器开始Web浏览器会话并且连接对**WLANs**。创建一新的WLAN。在**WLAN类型**，请选择**客户LAN**。

在**配置文件名字**和**WLAN SSID**，请输入识别此WLAN的名字。请使用值和被输入一样在总部控制器。

这里入口接口是**无**。实际上不重要，因为数据流通过在IP (EoIP)隧道的以太网收到。这就是为什么您不需要指定任何入口接口。

输出接口是客户端应该被发送的那个。例如， **DMZ VLAN**是VLAN 9.创建VLAN9的一个标准的动态接口在您的DMZWLC，然后选择**VLAN9**作为输出接口。

您需要配置移动性锚点隧道的末端。从**WLAN列表**，请选择**客户LAN的移动性锚点**。发送数据流到LocalDirector， **DMZWLC**。两端当前准备好。

5. **优化客户LAN。**

您能也优化在两端的WLAN设置。小心，设置一定是相同的在两端。例如，如果在**WLAN高级选项卡。**选择点击，请**允许**在WLC1的**AAA覆盖**，您需要检查在DMZWLC的同一个机箱。如果在任何一方有在选择上的任何区别在WLAN，隧道中断。DMZWLC拒绝数据流;您能看到，当您**运行调试移动性**。

记住所有值从DMZWLC实际上得到：IP地址， VLAN值，等等。相等地配置WLC1边，因此传递请求对WLCDMZ。

登录页的证书

此部分提供您需要按照的进程，如果在WebAuth页上要把您自己的认证放，或者，如果要隐藏192.0.2.1 WebAuth URL和显示已命名URL。

加载控制器Web认证的认证

通过GUI (**WebAuth >认证**)或CLI (转移类型**webauthcert**)您能加载在控制器的一个认证。它是否是您用您的Certificate Authority (CA)或一个第三方正式证书创建的认证，必须以.pem格式。在您发送前，您必须也输入认证的键。

在加载以后，重新启动要求为了认证到位。一旦重新启动，请去在GUI的WebAuth认证页，并且显示您您加载认证的详细资料(正确性等等)。重要字段是共同名称(CN)，是名字发出对认证。此字段在部分“认证机关和其他证书下的本文讨论在控制器”。

在您重新启动并且验证了认证的详细资料后，向您介绍关于WebAuth登录页的新的控制器认证。然而，可以有两个情况。

1. 如果您的认证由之一少量发行了每台计算机委托的主要根CAs，则是好的。示例是VeriSign，但是您由Verisign SUB CA而不是根CA通常签字。如果看到如委托，被提及的那里CA您能登记您的浏览器证书存储。

2. 如果从更小的company/CA获得了您的认证，所有计算机不委托他们。您应该提供company/CA认证给客户端，并且有希望地一个根CAs将发行该认证。最终，以一系列结束例如“认证CA发出了x > CA x认证CA发出了y > CA y认证此可信的根CA发出了您”。结尾目标是到达客户端委托的CA。

认证机关和其他证书在控制器

为了是“此认证没有委托”警告的rid，您必须也进入发行在控制器的控制器认证CA的认证。然后控制器提交两证书(控制器的认证和其CA证书)。CA证书应该是委托的CA或有验证的资源CA。您能实际上构件的CA证书一系列导致在上面的委托的CA。

您在同一个文件必须安置整个一系列。这意味着您的文件包含内容例如此示例：

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

如何造成认证匹配URL

WebAuth URL设置为192.0.2.1为了验证自己，并且发行认证(这是WLC认证的CN字段)。如果要更改WebAuth URL到‘myWLC.com’，例如，请进入virtualinterface**配置(**192.0.2.1接口)，并且那里您能进入一个virtualDNS**主机名-，例如**myWLC.com。这替换在您的URL栏的192.0.2.1。此名字一定也是可溶解的。嗅探器跟踪显示全部如何工作，但是，当WLC发送登录页时， WLC显示myWLC.com地址，并且客户端解析此名字用他们的DNS。此名字应该解决作为192.0.2.1。这意味着，如果也使用一个名字WLC的管理，您应该使用不同的名称WebAuth。换句话说，如果使用myWLC.com被映射对WLC管理IP地址，您必须使用不同的名称WebAuth，例如myWLCwebauth.com。

排除认证问题故障

此部分检查如何说明，并且什么排除认证问题故障。

如何检查

您能下载Openssl (Windows，搜索Openssl Win32)和安装它。没有任何配置，您在二进制文件目录和**s_client**尝试的**openssl**可以进来**–请连接**www.mywebauthpage.com:443，如果此URL是您的WebAuth页在您的DNS连接的URL。参考“检查”本文的部分什么示例。

如果您的证书使用专用的CA，您在目录需要安置根CA证书在一个本地设备和使用openssl选项**-CApath**。如果有中间CA，您必须放它到同一个目录。

为了得到关于认证的概要和检查它，请使用：

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

转换与使用的证书openssl也许也是有用的：

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

检查什么

您能看到什么证书被发送到客户端，当它连接时。读设备认证— CN应该是网页可及的URL。读”设备认证的线路“发出的。这必须匹配第二个认证的CN。然后此第二个认证“发行由”必须匹配下个认证的CN，等等。否则，它不做实际一系列。在输出显示的Openssl这里，您能看到**openssl不**能验证设备认证，因为其“发出由”不匹配提供的CA证书的名字。

SSL输出

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

另一个可能的问题是认证不可能被加载到控制器。在这种情况下没有正确性的问题， CA，等等。为了验证此，您能首先检查简单文件传输协议(TFTP)连接和设法调用配置文件。然后，如果参与**所有enable命令调试的转移**，您看到问题是认证的安装。这能归结于错误的键与认证一起使用。可能也是认证是以一种错误的格式或是损坏的。

Cisco建议您与知道比较认证内容，有效证书。这允许您发现**LocalkeyID**属性是否显示所有0s (已经发生)。如果那样，应该然后再转变认证。有允许您从.pem回来到.p12与Openssl的两个命令，然后补发一.pem用您的选择键。

PRE STEP ：如果包含键跟随的一个认证的接受了一.pem，请复制/粘贴关键部分：**----开始KEY----直到-------结束键------**从.pem到“key.pem里”。

1. **openssl pkcs12 -导出-在certificate.pem - inkey key.pem - newcert.p12 ？您**用键提示;输入check123**。**
2. **openssl pkcs12 -在newcert.p12 - workingnewcert.pem - passin pass:check123 - passout pass:check123这**导致与密码check123的一可操作的.pem**。**

排除故障的其他情况

虽然**移动性锚点**在本文未讨论，如果是在一个**停住的客户**情况，请确定移动性交换正确地发生，并且您看到的那客户端在锚点到达。任何另外WebAuth问题需要在锚点排除故障。

这是您能排除故障的一些常见问题：

- **用户不能联合到客户WLAN。**

  这没有与WebAuth有关。检查客户端配置，在WLAN的安全设置，如果是启用的，和无线电是否是活跃和有效的，等等。

- **用户不获得IP地址。**

  在客户锚点情况下，这经常是，因为未配置外国和锚点同一个方式。否则，请检查DHCP配置，连接，等等。确认其他WLANs是否能使用同一个DHCP服务器不出问题。这仍然没有与WebAuth有关。

- **用户没有重定向对登录页。**

  这是常见的症状，但是更加准确的。有两个可能的情况。

  用户没有重定向(用户输入URL和从未到达WebAuth页)。对于此情况，请检查：

  一个有效DNS服务器分配到客户端通过DHCP (**ipconfig /all**)，

  DNS从客户端(**nslookup** www.website.com)是可及的，

  用户输入有效URL为了重定向，

  用户在端口80的HTTP URL去(例如，到达与http://localhost:2002的一ACS不重定向您，因为您传送了端口2002而不是80)。

  用户正确地重定向对192.0.2.1，但是页不显示。

  此情况是很可能WLC问题(Bug)或一个客户端问题。可能是客户端有若干防火墙或阻塞软件或者策略。可能也是他们配置了在他们的Web浏览器的一个代理。

  推荐：采取在客户端PC机的嗅探器跟踪。没有对特殊无线软件的需要，只有Wireshark，在无线适配器运行并且显示您，如果WLC回复并且设法重定向。您有两种可能性：或者没有自WLC的无响应，或者某事在WebAuth页的SSL握手是错误的。对于SSL握手问题，您能证实用户浏览器是否允许SSLv3 (一些只允许SSLv2)，并且，如果是太积极的在证书验证。

  它是手工输入http://的一个普通的步骤192.0.2.1为了检查网页是否出版，不用DNS。实际上，您能键入http://6.6.6.6和获得同样效果。WLC重定向您输入的所有IP地址。所以，如果输入http:// 192.0.2.1，它不使您在Web重定向附近工作。如果输入https:// 192.0.2.1(secure)，这不工作，因为WLC不重定向HTTPS流量(默认情况下，这实际上是可能的在版本8.0和以上)。装载页的最佳方法直接地没有重定向是输入https:// 192.0.2.1/login.html。

- **用户不能验证。**

  请参阅讨论认证本文的部分。检查证件本地在RADIUS。

- **用户能通过WebAuth成功验证，但是他们之后没有互联网访问。**

  您能从WLAN的安全去除WebAuth，您应该然后有一开放WLAN。您能然后设法访问Web，DNS等等。如果遇到问题那里，一共请去除WebAuth设置并且检查您的接口配置。

欲知更多信息，请参见以下：排除在无线局域网控制器(WLC)的Web认证故障。

HTTP代理服务器，并且如何工作

您能使用HTTP代理服务器。如果需要客户端添加在其浏览器的例外192.0.2.1不是通过代理服务器，您在代理服务器(通常8080)的端口能做WLC细听HTTP数据流。

为了了解此方案，您需要了解什么HTTP代理。它是您在客户端配置的事(IP地址和端口)在浏览器。

通常方案，当用户访问一个网站时是解决名字对IP用DNS，它然后要求网页到Web服务器。进程应该总是发送HTTP请求页到代理。(如果页在代理已经没有被缓存)，代理处理DNS，如果必须，并且转发到Web服务器。讨论是仅客户端对代理。代理是否获得实际网页与客户端是毫不相关的。

这是Web认证过程：

- 用户类型URL。
- 客户端PC机发送到代理服务器。
- WLC拦截并且伪装代理服务器IP;它回复有重定向的PC到192.0.2.1

在此阶段，如果PC没有为它被配置，它请求192.0.2.1 WebAuth页对代理，因此不工作。PC必须做192.0.2.1的例外;然后它发送一个HTTP请求到192.0.2.1并且继续进行WebAuth。当验证，所有通信再通过代理。例外配置通常在接近代理服务器的配置的浏览器。您应该看到消息："请勿使用代理那些IP地址"。

使用WLC版本7.0及以后，功能**webauth代理重定向**在全局WLC配置选项可以被启用。当启用，WLC检查是否配置客户端手工使用代理。在那种情况下，他们重定向客户端对显示他们如何修改他们的代理设置使一切工作的页。可以配置WebAuth代理重定向在各种各样的端口工作并且是与中央Web认证兼容。

关于在WebAuth代理重定向的一个示例，请参见在无线局域网控制器配置示例的Web认证代理。

在HTTP的Web认证而不是HTTPS

您在HTTP的Web认证能登陆而不是HTTPS。如果在HTTP登陆，您不收到认证戒备。

对于早于WLC版本7.2代码，您必须禁用WLC的HTTPS管理和留下HTTP管理。然而，这只允许WLC的Web管理在HTTP的。

对于WLC版本7.2代码，请使用**disable命令设置网络web-auth的secureweb**禁用。这只禁用Web认证而不是管理的HTTPS。注意这要求控制器的重新启动!

在WLC版本7.3及以后代码，您能通过GUI和CLI仅启用/禁用WebAuth的HTTPS。

Related Information

- 无线局域网控制器 Web 身份验证配置示例
- 下载无线控制器WebAuth套件的软件
- 创建定制的Web认证登录页
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 无线局域网控制器Web转接配置示例
- 使用配置的GUI Web重定向
- 使用配置的CLI Web重定向
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除
- 在无线局域网控制器配置示例的Web认证代理
- 请求注解 (RFC)
- Technical Support & Documentation - Cisco Systems