在WLAN控制器的Web验证

目录

简介

本文解释Web验证的进程在无线局域网控制器(WLC)。

先决条件

要求

思科建议您有WLC配置基础知识。

使用的组件

本文档中的信息根据所有WLC硬件型号。

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。

Web验证内在进程

Web验证位置作为安全功能

Web验证(Webauth)是第3层安全。它允许在所有站点工作运行浏览器的用户友好安全。它可能与所有预先共享密钥(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不可能配置与802.1x/RADIUS (远程认证拨入用户服务)，直到WLC软件版本7.4安装可以同时的地方配置。然而，请注意客户端必须通过dot1x和Web验证。没有含义为访客，然而为一个Web门户的新增内容员工的(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)访客的。

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，您关联，但是不在WLC运转状态。当Web验证启用，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请求对网站的IP地址。请求并且返回**webauth**登录页，伪装网站IP地址的WLC截住。一旦包括您的网站IP地址并且阐明的一外部Webauth，与HTTP响应的WLC回复，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URL最初请求，默认情况下(除非牵强的重定向在WLC配置)。总之， WLC允许客户端解决DNS和在**WEBAUTH_REQD**状态自动地获得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。

> **关于HTTPS的重定向的注意**：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，您能启用HTTPS流量的重定向与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，万一许多HTTPS请求发送。并且请注意证书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地址发出的其自己的证书。这明显地不会匹配客户端请求的URL IP地址，并且证书不会委托，除非客户端强制在他的浏览器的例外。

被测量的预示性能下降：

Webauth	达到的速率
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由最终用户(用户要浏览对)的网站输入
- URL WLC重定向浏览器
- 最终凭证提交

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

如果需要配置与一个可操作的动态接口的一WLAN，客户端应该通过DHCP也收到DNS服务器IP地址。在您集所有**webauth**，您应该测试前您的WLAN适当地运作，您能解决DNS请求(**nslookup**)，并且您能浏览网页。然后，您能设置Web验证作为第3层安全功能。例如您能创建您的用户本地数据库的或外部RADIUS服务器的。参考无线局域网控制器Web身份验证配置示例文档。

如何配置与自定义页的自定义本地Webauth

自定义**webauth**可以配置与从**安全选项卡的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客户端请求并且显示重定向分配的页。

自定义功能允许您使用一个自定义HTML页面而不是默认登录页。上传您的html和镜像文件捆绑到控制器。在加载页，请寻找在tar格式的**webauth套件**。通常， PicoZip创建兼容与WLC一起使用的tar。对于Webauth套件的示例，参考无线控制器Webauth促销包的下载软件页。请务必选择您的WLC的适当的版本。一好建议是定制存在的套件;从头请勿创建套件。

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)

如果您的客户包不工作，用一个简单自定义包尝试。然后请添加文件和复杂性一次一个到达包客户设法使用。这应该帮助您识别问题。关于怎样的一示例配置一个自定义页，参考创建一个定制的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。

覆盖全局配置技术

对于每WLAN，您配置与集合的**覆盖global config命令**和每WLAN的一个Webauth类型。这意味着您能有与一自定义内部/默认Webauth的一内部/默认Webauth另一WLAN的。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上传他们到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套件内的一变量。请勿放置您牵强的重定向URL那里。对于在自定义Webauth的所有重定向问题，思科推荐检查套件。如果输入与**+=的**重定向URL在WLC GUI，这可能覆盖或添加到URL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验证与外部页一起使用

如已经简要地解释，一个外部Webauth服务器的利用率是登录页的一个外部信息库。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。这是为一外部Webauth执行的步骤：

1. 客户端(最终用户)打开Web浏览器并且输入URL。
2. 如果客户端没有验证，并且验证使用外部Web， WLC重定向用户对外部Web服务器URL。换句话说， WLC发送HTTP重定向到对外部服务器IP地址的客户端用网站的被伪装的IP地址和点。外部Web认证登录URL带有参数例如**AP_Mac_Address**、**client_url** (www.website.com)和该的**action_URL**用户需求与交换机Web服务器联系。
3. 外部Web服务器URL派遣用户对登录页。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://1.1.1.1/login.html， WLC Web服务器。这提供作为输入参数给客户重定向URL， 1.1.1.1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启动RADIUS服务器请求或使用在WLC的本地数据库，然后验证用户。
7. 如果验证是成功的， WLC Web服务器二者之一转发用户对已配置的重定向URL或对URL客户端输入。
8. 如果验证发生故障，则WLC Web服务器重定向用户回到客户登录URL。

注意： 如果接入点(AP)在FlexConnect模式， **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。参考与无线局域网控制器配置示例的外部Web验证。

Web Passthrough

这是内部Web验证的变化。它显示与警告或一个提醒的语句的一个页，但是不提示输入凭证。用户应该点击OK键。您能启用电子邮件输入，并且用户能输入他们的电子邮件地址，变为他们的用户名。当用户连接时，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输入作为用户名。欲知更多信息，参考无线局域网控制器Web Passthrough配置示例。

有条件的Web重定向

如果启用有条件的Web重定向，用户有条件地重定向对一个特定的网页，在802.1x验证顺利地完成后。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，当用户需要付帐单继续使用/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授权并且能由预验证ACL只通过允许的流量。在客户端完成一特定的操作在指定的URL (例如，密码更改或账单付款)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已授权和允许通过流量。

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

在您配置RADIUS服务器后，您能然后配置在控制器的有条件的Web重定向有控制器GUI或CLI的。参考这些逐步指南：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

如果启用飞溅页Web重定向，用户重定向对一个特定的网页，在802.1x验证顺利后地完成。在重定向，用户有对网络后的完全权限。您能指定在您的RADIUS服务器的重定向页。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授权和允许通过流量，即使RADIUS服务器不返回**url重新定向**。

注意： 飞溅页Web重定向功能为为802.1x或WPA+WPA2第2层安全配置的WLAN是仅可用的。

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

在MAC过滤器失败的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验证出现。

注意：这不支持与Web转接。欲知更多信息，请跟随在增强请求CSCtw73512的活动 。

中央Web验证

中央Web验证是指WLC不再主机所有服务的一个方案。差异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1.1.1.1。登录页和整个门户被形象化。

中央Web验证发生，当您安排RADIUS网络准入控制(NAC)启用在WLAN的先进的设置，并且MAC过滤已启用。

整体概念是WLC发送RADIUS验证(通常MAC过滤器)对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给与授权(CoA)请求的崔凡吉莱的授权。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，因为访客门户不能返回加密的会话密钥，如执行与可扩展的认证协议(EAP)。

外部用户验证(RADIUS)

这为本地Webauth只是有效，当WLC处理凭证时，或者，当第3层Web策略启用时。您能本地然后验证用户在WLC或外部通过RADIUS。

有WLC检查用户的凭证的命令。

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，去在访客WLAN配置的RADIUS服务器(如果有配置的一个)。
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：

从GUI ：导航对**Controller> Web RADIUS验证**

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

注意： 美洲台访客服务器只使用PAP。

如何设置有线的访客WLAN

配置和非常close到无线访客配置是容易的。(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安置有线的来宾用户，例如的VLAN。当一有线的访客想要对互联网时的访问，请插入笔记本电脑对在为VLAN配置的交换机的端口50。此VLAN 50一定是允许和存在路径到WLC中继端口。在一案件两WLCs中(外国一的锚点和一个)，此有线的访客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流量对DMZ WLC (锚点，已命名WLC2)，发布在路由的网络的流量。

这是配置有线的访客访问的五个步骤：

1. **配置一个动态接口(VLAN)有线的来宾用户用户访问的。**

   在WLC1，请创建动态接口VLAN50。在**Interface Configuration页**，请检查**访客LAN**方框。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流量从VLAN 50路由。这些客户端是有线访客。

2. **创建来宾用户用户访问的一个有线LAN。**

   在控制器上，使用接口，当关联对WLAN。第二步将创建在您的总部控制器的一WLAN。导航对**WLAN**并且点击**新**。在**WLAN类型**，请选择**访客LAN**。

   在**配置文件名称**和**WLAN SSID**，请输入识别此WLAN的名称。这些名称不同的，但是不能包含空间。使用期限WLAN，但是此网络配置文件与无线网络配置文件没有涉及。

   常规选项卡提供两张下拉列表：**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(不是访客LAN)，并且您派遣您的有线的用户对此接口。在这种情况下，请发送他们到DMZ控制器。所以，对于**出口接口**，请选择**管理接口**。

此访客LAN的"WLAN"**安全模式**是Webauth，是可接受。点击OK键为了验证。

3. **配置外国控制器(总部)。**

   从**WLAN列表**，请单击**移动性锚点**在**访客LAN**线路尽头，并且选择您的DMZ控制器。被假设得此处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。开始Web浏览器会话到您的DMZ控制器并且导航对**WLAN**。创建一新的WLAN。在**WLAN类型**，请选择**访客LAN**。

   在**配置文件名称**和**WLAN SSID**，请输入识别此WLAN的名称。请使用同样值作为输入在总部控制器。

   此处**入口接口**是**无**。实际上不重要，因为流量通过在IP (EoIP)通道的以太网接收。这就是为什么您不需要指定任何入口接口。

   出口接口是客户端应该发送的那个。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**作为出口接口。

   您需要配置移动性锚点通道的末端。从**WLAN列表**，请选择**访客LAN的移动性锚点**。发送流量对LocalDirector， **DMZWLC**。两端当前准备好。

5. **优化访客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。**选择单击，请**允许**在WLC1的**AAA覆盖**，您需要检查在DMZWLC的同一个方框。如果在任何一方有在选择的任何差异在WLAN，通道中断。DMZWLC拒绝流量;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侧，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页上要把您自己的证书放，或者，如果要隐藏1.1.1.1 Webauth URL和显示已命名URL。

上传控制器Web验证的证书

通过GUI (**Webauth >证书**)或CLI (转移类型**webauthcert**)您能上传在控制器的一证书。它是否是您创建与您的Certificate Authority (CA)或一个第三方正式证书的证书，必须在.pem格式。在您发送前，您必须也输入证书的密钥。

在加载，重新启动要求为了证书到位后。一旦重新启动，请去在GUI的Webauth证书页，并且显示您您上传证书的详细信息(正确性等等)。重要字段是共同名称(CN)，是名称发出对证书。此字段在部分下的本文“认证机关和在控制器的其他证书讨论”。

在您重新启动并且验证证书的详细信息后，您提交与在Webauth登录页的新的控制器证书。然而，可以有两个情况。

1. 如果您的证书由之一少量发出每台计算机委托的主要根CA，则是好的。示例是Verisign，但是您由Verisign SUB CA而不是根CA通常签字。如果看到作为委托，被提及的那里CA您能登记您的浏览器证书存储。

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

认证机关和在控制器的其他证书

为了是“此证书没有委托”警告的rid，您必须也进入发出在控制器的控制器证书CA的证书。然后控制器提交两证书(控制器的证书和其CA证书)。CA证书应该是委托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 ------
```

如何造成证书匹配URL

Webauth URL设置为1.1.1.1为了验证，并且证书发出(这是WLC证书的CN字段)。如果要更改Webauth URL到‘myWLC.com’，例如，请进入virtualinterface**配置(**1.1.1.1接口)，并且那里您能进入一virtualDNS**主机名，例如**myWLC.com。这替换在您的URL栏的1.1.1.1。此名称一定也可解决。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称用他们的DNS。此名称应该解决作为1.1.1.1。这意味着，如果也使用一名称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。

排除故障证书问题

此部分检查如何说明，并且什么排除故障证书问题。

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。

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

为了得到关于证书的一般信息和检查它，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
```

检查的内容

您能看到什么证书发送给客户端，当它连接时。读设备证书— CN应该是网页可及的URL。读”设备证书的线路“发出的。这必须匹配第二证书的CN。然后此第二证书“发出由”必须匹配下证书的CN，等等。否则，它不做实时一系列。在输出显示的Openssl此处，您能看到**openssl不**能验证设备证书，因为其“发出由”不匹配提供的CA证书的名称。

SSL输出

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
```

```
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

另一个可能的问题是证书不可能上传对控制器。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)连接和设法转接配置文件。然后，如果参与**所有enable命令调试的转移**，您看到问题是证书的安装。这能归结于错误的密钥与证书一起使用。可能也是证书是在一个错误的格式或是损坏的。

思科建议您比较证书内容对知道，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，应该然后再转变证书。有允许您从.pem返回到.p12与Openssl的两命令，然后补发与您的选择密钥的一.pem。

PRE STEP ：如果包含密钥跟随的证书的接收.pem，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 -出口-在certificate.pem - inkey key.pem - newcert.p12 ？您**用密钥提示;回车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**停住的访客**情况，请确保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：

- **用户不能联合到访客WLAN。**

  这与Webauth没有涉及。检查客户端配置，在WLAN的安全设置，如果启用，和无线电是否是活跃和有效的，等等。

- **用户不获取IP地址。**

  在访客锚点情况下，这经常是，因为外国和锚点未配置同一个方式。否则，请检查DHCP配置，连接，等等。确认其他WLAN是否能使用同样DHCP服务器不出问题。这与Webauth仍然没有涉及。

- **用户没有重定向对登录页。**

  这是多数常见的症状，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1.1.1.1，但是页不显示。

此情况是很可能WLC问题(bug)或一客户端问题。可能是客户端有某防火墙或阻塞软件或策略。可能也是他们配置他们的Web浏览器的一个代理。

建议：采取在客户端PC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：或者没有从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://1.1.1.1的一个普通的步骤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://1.1.1.1，它不使您在Web重定向附近工作。如果输入https://1.1.1.1 (请巩固)，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://1.1.1.1/login.html。

- **用户不能验证。**

  请参阅讨论验证本文的部分。检查凭证本地在RADIUS。

- **用户能通过Webauth成功验证，但是他们之后不访问互联网访问。**

  您能从WLAN的安全删除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，一共请取消Webauth设置并且检查您的接口配置。

有关详细信息，请参阅：排除故障在无线局域网控制器(WLC)的Web验证。

HTTP代理服务器，并且如何工作

您能使用HTTP代理服务器。如果在其浏览器需要客户端添加例外1.1.1.1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称对IP用DNS，它然后要求网页到Web服务器。进程应该总是发送页的HTTP请求对代理。(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。代理是否获取实时网页与客户端是毫不相关的。

这是Web认证过程：

- 用户类型URL。
- 对代理服务器的客户端PC发送。
- WLC截住和欺骗代理服务器IP;它回复有重定向的PC 1.1.1.1。

在此阶段，如果PC没有为它配置，它请求1.1.1.1 Webauth页给代理，因此不工作。PC必须做1.1.1.1的一例外;然后它发送HTTP请求对1.1.1.1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配置选项可以启用。当启用，WLC检查客户端是否配置手工使用代理。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。Webauth代理重定向在各种各样的端口可以配置工作并且是与中央Web验证兼容。

对于在Webauth代理重定向的一示例，参考在无线局域网控制器配置示例的Web认证代理。

在HTTP的Web验证而不是HTTPS

您在HTTP的Web验证能登陆而不是HTTPS。如果在HTTP登陆，您不收到证书警报。

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验证而不是管理的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。

相关信息

- **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促销包的软件**
- **创建一个定制的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)**
- **技术支持和文档 - Cisco Systems**