无线局域网控制器 Web 身份验证配置示例

目录

简介

本文解释Cisco如何实现Web验证并且显示如何配置一个Cisco 4400系列无线局域网(WLAN)控制器(WLC)支持内部Web验证。

先决条件

要求

本文档假设您已对 4400 WLC 进行了初始配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本7.0.116.0的一4400系列WLC
- 思科安全访问控制服务器(ACS)版本4.2在Microsoft® Windows 2003服务器安装

- Cisco Aironet 1131AG系列轻量接入点
- Cisco Aironet 802.11 a/b/g运行版本4.0的CardBus无线适配器

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Web 身份验证

Web验证是造成控制器不允许IP数据流的第3层安全功能(除了DHCP和DNS相关的数据包)从特定的客户端，直到该客户端正确地供应了一个有效用户名和密码。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 身份验证通常由希望部署访客接入网络的客户使用。典型的部署可能包括如 T-Mobile 或 Starbuck 之类的“热点”位置。

请记住，Web 身份验证不提供数据加密。Web 身份验证通常用作仅关注连接性的“热点”或校园环境的简单访客接入。

Web验证可以执行使用：

- 在WLC的默认登录窗口
- 默认登录窗口的修正的版本在WLC的
- 您在外部 Web 服务器上配置的自定义登录窗口（外部 Web 身份验证）
- 您下载到控制器的自定义登录窗口

在本文中，内部Web验证的无线局域网控制器配置。

Web认证过程

这是什么发生，当用户连接对为Web验证配置的WLAN ：

- 用户打开Web浏览器并且输入URL，例如， http://www.cisco.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DNS服务器，并且DNS服务器响应有的上一步DNS回复，包含目的地www.cisco.com的IP地址。这，反过来，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，它派出TCP Syn信息包被注定对www.cisco.com的IP地址。
- WLC有为客户端配置的规则并且能作为www.cisco.com的一个代理。它退还TCP SYN-ACK数据包给有来源的客户端作为www.cisco.com的IP地址。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。
- 客户端发送被注定的HTTP GET数据包对www.cisco.com。WLC截断此数据包并且为重定向处理发送它。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使客户端去WLC的默认网页URL，例如， http:// <Virtual-Server-IP>/login.html。
- 客户端断开TCP连接用IP地址，例如， www.cisco.com。
- 现在客户端要去http://1.1.1.1/login.html。所以，客户端设法打开一TCP连接用WLC的虚拟IP地址。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。
- 客户端发送被注定的/login.html的一HTTP GET对1.1.1.1为了为登录页请求。
- 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。
这是链路到在解释Web 认证过程的Cisco支持社区的一个视频：

在Cisco无线LAN控制器(WLCs)的Web验证

网络设置

本文档使用以下网络设置：

配置用于 Web 身份验证的控制器

在本文中， WLAN为Web验证配置并且被映射对专用VLAN。以下是配置用于 Web 身份验证的 WLAN 所包含的步骤：

- 创建 VLAN 接口
- 配置内部Web验证的WLC
- 添加 WLAN 实例
- 配置认证类型(三种方式验证Web验证的用户)

本部分提供有关如何配置用于 Web 身份验证的控制器的信息。

以下是本文档中使用的 IP 地址：

- WLC的IP地址是10.77.244.204。
- ACS服务器的IP地址是10.77.244.196。

创建 VLAN 接口

完成这些步骤：

1. 从无线局域网控制器GUI，请从菜单选择**控制器**在顶部，从在左边的菜单选择**接口**，并且单击**新**在窗口的右上端创建一个新的动态接口。**接口>New**窗口出现。本示例使用 VLAN ID 为 90 的接口名称 *vlan90*：
2. 单击 **Apply** 以创建 VLAN 接口。**接口> Edit Window**出现要求您填装界面特殊化的信息。
3. 本文档使用以下参数：IP 地址 - 10.10.10.2子网掩码 - 255.255.255.0（24 位）网关 - 10.10.10.1端口号 - 2主 DHCP 服务器 - 10.77.244.204**注意：** 此参数应为您的 RADIUS 或 DHCP 服务器的 IP 地址。在本示例中，由于内部 DHCP 范围是在 WLC 上配置的，因此 WLC 的管理地址被用作 DHCP 服务器。辅助 DHCP 服务器 - 0.0.0.0**注意：** 本示例中没有辅助 DHCP 服务器，因此使用 0.0.0.0。如果您的配置中有辅助 DHCP 服务器，请在此字段中添加服务器 IP 地址。ACL 名称 - 无
4. 单击 **Apply** 以保存更改。

配置内部Web验证的WLC

下一步是配置内部Web验证的WLC。内部Web验证是在WLCs的默认Web认证类型。如果此参数未更改，配置没有要求启用内部Web验证。如果Web验证参数以前更改，请完成这些步骤配置内部Web验证的WLC ：

1. 从控制器GUI，请选择**安全> Web验证> Web登录页**为了访问Web登录页。
2. 从Web认证类型下拉框，请选择**内部Web验证**。
3. **在登录**字段以后的**重定向URL中**，请输入最终用户将重定向对在成功认证以后页的URL。**注意**：在WLC版本5.0和以上， logout页Web验证的可能也定制。有关如何进行配置的更多信息，请参阅无线局域网控制器配置指南的为每个 WLAN 分配登录、登录失败和注销页一节中的5.2。

添加 WLAN 实例

即然内部Web验证启用，并且有为Web验证投入的VLAN接口，您必须提供一新的WLAN/SSID为了支持Web认证用户。

完成以下步骤以创建新的 WLAN/SSID：

1. 从WLC GUI，请在顶部单击在菜单的**WLAN**，并且点击**新**在右上端。选择 **WLAN** 作为“Type”。选择用于 Web 身份验证的配置文件名和 WLAN SSID。本示例对“Profile Name”和“WLAN SSID”都使用 **Guest**。
2. 单击 **Apply**。一新的WLAN > Edit Window出现。
3. 选中 WLAN 的状态框以启用 WLAN。从“Interface”菜单中，选择您以前创建的 VLAN 接口的名称。在本示例中，接口名称为 *vlan90*。**注意：** 请保留此屏幕中其他参数的默认值。
4. 单击 **Security** 选项卡。完成以下步骤以配置 Web 身份验证：单击“Layer 2”选项卡并且将安全模式设置为 ***None***。**注意：** 您不能将 Web 穿透功能配置为使用 802.1x 的第 3 层安全，或将 WPA/WPA2 配置为 WLAN 的第 2 层安全。有关无线局域网控制器第 2 层和第 3 层安全兼容性的详细信息，请参阅无线局域网控制器第 2 层和第 3 层安全兼容性列表。单击“Layer 3”选项卡。检查**Web策略**方框并且选择***认证选项***，如显示此处：单击“Apply”以保存 WLAN。此时将返回到“WLAN Summary”窗口。请确保 WLAN 表的“Security Policies”列下的“Web-Auth”对于 SSID 访客处于启用状态。

三种方式验证Web验证的用户

当您使用Web验证时，有三种方式验证用户。使用本地身份验证可在 Cisco WLC 中对用户进行身份验证。您能也使用外部RADIUS服务器或LDAP服务器，一个后端数据库为了验证用户。

本文为所有三个方法提供一配置示例。

本地 认证

来宾用户的用户数据库在WLC's本地数据库存储。用户由此数据库的WLC验证。

1. 从 WLC GUI 中，请选择 **Security**。
2. 在左侧的 AAA 菜单中单击 **Local Net Users**。
3. 单击 **New** 以创建一个新用户。此时将显示一个新窗口，要求提供用户名和口令信息。
4. 输入用户名和口令以创建新用户，然后确认要使用的口令。本示例创建名为 **User1** 的用户。
5. 如果需要，可添加说明。此示例使用**访客User1**。
6. 单击 **Apply** 以保存新的用户配置。
7. 重复步骤 3-6 以向数据库中添加更多用户。

用于 Web 身份验证的 RADIUS 服务器

本文档使用 Windows 2003 Server 上的无线 ACS 作为 RADIUS 服务器。您可以使用当前部署在网络中的任何可用的 RADIUS 服务器。

注意： 可以在 Windows NT 或 Windows 2000 Server 上设置 ACS。要从 Cisco.com 上下载 ACS，请参阅软件中心（下载）- Cisco 安全软件（仅限注册用户）。您需要 Cisco Web 帐户才能下载该软件。

设置 ACS 部分说明了如何配置 RADIUS 的 ACS。您必须具有使用域名系统 (DNS) 和 RADIUS 服务器的全功能网络。

设置 ACS

本部分提供有关如何设置 RADIUS 的 ACS 的信息。

设置在您的服务器的ACS然后完成这些步骤为了创建验证的一个用户：

1. 当 ACS 询问您是否要在浏览器窗口中打开 ACS 以进行配置时，请单击 **Yes**。**注意：** 设置 ACS 之后，您的桌面上还会显示一个图标。
2. 在左侧的菜单中单击 **User Setup**。此操作把您带对User Setup屏幕如显示此处：
3. 输入要用于 Web 身份验证的用户，然后单击 **Add/Edit**。在用户创建后，第二个窗口打开如显示此处：
4. 保证在顶部的**帐户禁用的**方框没有被检查。
5. 选择密码验证选项的**ACS内部数据库**。
6. 输入密码。Admin有一个选项配置PAP/CHAP或MD5-CHAP验证，当添加ACS内部数据库的时一个用户。PAP是web-auth用户的默认验证类型控制器的。使用此CLI命令， Admin有灵活性更改认证方法到chap/md5-chap ：
   ```
   config custom-web radiusauth <auth method>
   ```
7. 单击 **submit**。

将您的 RADIUS 服务器信息输入到 Cisco WLC 中

完成这些步骤：

1. 在顶部的菜单中单击 **Security**。
2. 在左侧的菜单中单击 **Radius Authentication**。
3. 单击 **New**，并且输入 ACS/RADIUS 服务器的 IP 地址。在本例中， ACS服务器的IP地址是 **10.77.244.196**。
4. 输入 RADIUS 服务器的共享密钥。确保此密钥是相同的象那个您在WLC的RADIUS服务器输入。
5. 保留端口号为默认值 1812。
6. 确保已启用 **Server Status** 选项。
7. 检查**网络用户Enable复选框，**以便此RADIUS服务器使用验证您的无线网络的用户。
8. 单击 **Apply**。

确保*网络用户*方框被检查，并且*管理状态*启用。

配置使用 RADIUS 服务器的 WLAN

即然已在 WLC 上配置 RADIUS 服务器，您需要配置 WLAN 以使用此 RADIUS 服务器进行 Web 身份验证。完成以下步骤以配置使用 RADIUS 服务器的 WLAN。

1. 打开您的 WLC 浏览器并单击 **WLANs**。这显示配置列表在WLC的。点击为Web验证创建的WLAN**访客**。
2. 在**WLAN > Edit**页请点击**Security菜单**。单击**AAA服务器**选项卡在安全下。然后，请选择是在本例中的10.77.244.196的RADIUS服务器：
3. 单击 **Apply**。

验证 ACS

当您设置ACS时，请切记下载所有当前补丁程序和最新的代码。这应该能够解决迫在眉睫的问题。万一使用RADIUS验证请确保您的WLC列出作为其中一个AAA客户端。点击**Network Configuration菜单**在左手边检查此。点击AAA客户端，然后验证配置的密码和认证类型。有关如何配置 AAA 客户端的详细信息，请参阅“Cisco 安全访问控制服务器 4.2 用户指南”的配置 AAA 客户端部分。

当您选择用户设置时，再请验证您的用户实际上存在。点击**列表所有用户**。一个窗口如显示出现。请确保在该列表中存在已创建的用户。

LDAP 服务器

此部分说明如何配置轻量级目录访问协议(LDAP)服务器作为一个后端数据库，类似于RADIUS或本地用户数据库。LDAP 后端数据库允许控制器向 LDAP 服务器查询特定用户的凭证（用户名和密码）。然后使用这些凭证对用户进行身份验证。

使用控制器GUI，完成这些步骤配置LDAP ：

1. 点击**安全**>AAA > **LDAP**为了打开LDAP服务器。此页列出已经配置的所有LDAP服务器。如果要删除一个现有LDAP服务器，请移动您的在蓝色下拉箭头的光标该服务器的并且选择**删除**。如果要确保，控制器能到达特定服务器，盘旋您的在蓝色下拉箭头的光标该服务器的并且选择**Ping**。
2. 执行下列操作之一：要编辑一个现有LDAP服务器，请点击该服务器的索引编号。LDAP服务器> Edit页出版。添加LDAP服务器，点击**新**。这会显示 **LDAP Servers > New** 页。
3. 如果添加一个新的服务器，请从服务器索引(优先级)下拉框选择编号关于所有其他已配置的LDAP服务器指定此服务器优先级顺序。最多可以配置 17 个服务器。如果控制器不能到达第一个服务器，则尝试第二个从列表等等。
4. 如果添加一个新的服务器，请在服务器IP地址字段输入LDAP服务器的IP地址。
5. 如果添加一个新的服务器，请进入在Port Number字段的LDAP服务器的TCP端口号。有效范围是 1 到 65535，默认值是 **389**。
6. 检查**Enable (event)服务器状态**复选框启用此LDAP服务器或者不选定它禁用它。默认值是禁用。
7. 从简单捆绑下拉框，请选择**匿名**或**已验证**指定LDAP服务器的本地认证捆绑方法。匿名方法允许对LDAP服务器的匿名访问，而已验证方法要求用户名和密码输入对安全访问。默认值是匿名的。
8. 如果选择已验证在步骤7，请完成这些步骤：在捆绑用户名字段，请输入将用于本地认证用户名对LDAP服务器。在捆绑密码和确认捆绑密码字段，请输入将用于本地认证密码对LDAP服务器。
9. 在用户群DN字段，请进入子树的特有名(DN)在包含所有用户列表的LDAP服务器的。例如，ou=组织单位，.ou=下一个组织单位，o=corporation.com。如果包含用户的树是基础DN、类型o=corporation.com或dc=corporation， dc=com。
10. 在 **User Attribute** 字段中，输入包含用户名的用户记录中的属性名称。您能从您的目录服务器

得到此属性。

11. 在 **User Object Type** 字段中，输入将记录标识为用户的 LDAP objectType 属性的值。通常，用户记录具有多个 objectType 属性值，其中有些对用户是唯一的，而另一些则与其他对象类型共享。
12. 在服务器超时字段，请进入秒钟数量在重发之间。有效范围是 2 到 30 秒，默认值是 2 秒。
13. 单击 **Apply** 以提交更改。
14. 点击**保存配置**保存您的更改。
15. 如果希望分配特定LDAP服务器对WLAN，请完成这些步骤：单击“WLANs”以打开“WLANs”页。点击希望的WLAN的ID号码。当WLAN > Edit页出版时，请点击**安全**>AAA**服务器**选项卡打开WLAN > Edit (安全>AAA服务器)页。从LDAP服务器下拉框，请选择您要以此WLAN使用的LDAP服务器。您能选择三个LDAP服务器，按优先级顺序尝试。单击 **Apply** 以提交更改。点击**保存配置**保存您的更改。

配置您的WLAN客户端使用Web验证

一旦WLC配置，客户端必须为Web验证配置适当地。本部分提供有关如何配置用于 Web 身份验证的 Windows 系统的信息。

客户端配置

对此用户而言，Microsoft 无线客户端配置保持大致不变。您只需要添加适当的 WLAN/SSID 配置信息。完成这些步骤：

1. 从 Windows“开始”菜单中选择**设置 > 控制面板 > 网络和 Internet 连接**。
2. 单击**网络连接**图标。
3. 右键单击 **LAN 连接**图标并选择“禁用”。
4. 右键单击**无线连接**图标并选择“启用”。
5. 再次右键单击**无线连接**图标并选择“属性”。
6. 从“无线网络连接属性”窗口中，单击**无线连接**选项卡。
7. 在首选网络区域下单击**添加**以配置 Web 身份验证 SSID。
8. 在“关联”选项卡下，输入要用于 Web 身份验证的网络名称 (WLAN/SSID) 值。**注意：** 默认情况下，数据加密为有线等效加密 (WEP)。请禁用数据加密以使 Web 身份验证能够正常运行。
9. 在窗口底部单击**确定**以保存配置。当您与 WLAN 通信时，您会在“首选网络”框中看到一个信号图标。

这表示对Web验证的成功的无线连接。WLC 已为您的无线 Windows 客户端提供 IP 地址。

注意： 如果您的无线客户端也是VPN端点，并且有作为WLAN的一个安全功能配置的Web验证，则VPN通道没有设立，直到您通过解释的Web认证过程此处。为了设立VPN通道，客户端必须首先通过Web验证进程与成功的。只有在那时才能成功建立 VPN 隧道。

注意： 在成功登录以后，如果无线客户端是空闲，并且不通信与任何其它设备，客户端是已取消验证在空闲超时期限之后。使用此CLI命令，默认情况下超时周期是300秒并且可以更改：`usertimeout <seconds>`。当这发生时，客户端条目从控制器删除。如果客户端再联合，它将移动回到Webauth_Reqd状态。

注意： 如果客户端在成功登录以后是活跃的，他们将获得已取消验证，并且条目可能从控制器仍然删除在该WLAN配置的会话超时期限之后使用此CLI命令，(在example,1800秒钟默认情况下和能更改：`WLAN session-timeout <WLAN ID> <seconds>`)。当这发生时，客户端条目从控制器删除。如果客户端再联合，它在Webauth_Reqd状态将移动上一步。

如果客户端在Webauth_Reqd状态，没有问题，如果他们活跃或空闲，客户端在一个**web-auth要求的超时周期之后将**获得已取消验证(例如， 300秒和这次是可配置的非使用者)。(允许通过PRE验证ACL)将阻碍从客户端的所有流量。如果客户端再联合，它将移动回到Webauth_Reqd状态。

客户端登录

完成这些步骤：

1. 打开浏览器窗口并输入所有 URL 或 IP 地址。这将从 Web 身份验证页转到客户端。如果控制器运行任何的版本早于3.0，用户必须输入https://1.1.1.1/login.html启动Web验证页。此时将显示安全警报窗口。
2. 单击 **Yes** 以继续操作。
3. 当登录窗口出现时，请输入该本地净的用户的用户名和密码您创建。如果登录成功，您将看到两个浏览器窗口。更加大的窗口指示成功登录和您能浏览此的窗口互联网。完成对访客网络的使用时，可使用较小的窗口注销。屏幕画面显示Web验证的成功的重定向。下张屏幕画面显示洛金成功的窗口，显示，当验证出现。

思科4404/WiSM控制器可以支持125同时Web验证用户登录，并且扩展5000个Web验证客户端。

Cisco 5500控制器可以支持150同时Web验证用户登录。

Web 身份验证故障排除

ACS 故障排除

如果口令验证存在问题，请单击 ACS 左下方的 **Reports and Activity** 以打开所有可用的报告。打开报告窗口后，可以通过相应选项打开 RADIUS 记账、失败的尝试登录、通过的验证、已登录用户和其他报告。这些报告为 .csv 文件，您可以在计算机上本地打开这些文件。这些报告有助于揭示身份验证存在的问题，如用户名和/或口令不正确。ACS 还附带联机文档。如果未连接到真实网络并且未定义服务端口，ACS 将使用以太网端口的 IP 地址作为服务端口。如果您的网络未建立连接，您很可能最终使用 Windows 默认 IP 地址 169.254.x.x。

注意： 如果键入任何外部 URL，WLC 会自动将您连接到内部 Web 身份验证页。如果自动连接不起作用，您可以在 URL 栏中输入 WLC 的管理 IP 地址以排除故障。在浏览器顶部查找说明 Web 身份验证重定向的消息。

参考故障排除在无线局域网控制器(WLC)的Web验证关于故障排除Web验证的更多信息。

与IPv6桥接的Web验证

为了配置桥接，从控制器GUI的IPv6的一WLAN，请导航对**WLAN**。然后，请选择希望的WLAN并且从**WLAN** > Edit页选择**先进**。

请选择**IPv6 Enable复选框，**如果要启用连接对此WLAN接受IPv6数据包的客户端。否则，请留下复选框取消选择，是默认值。如果禁用(或请不选定) IPv6复选框， IPv6在验证以后只将允许。启用IPv6意味着控制器能通过IPv6流量，不用客户端验证。

关于IPv6桥接和**指南的更详细信息为使用此功能**，参考桥接Cisco无线LAN控制器配置指南的部分的配置的IPv6，版本7.0。

相关信息

- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除
- Cisco 无线 LAN
- 使用 Cisco WLAN 控制器的有线访客接入配置示例
- Cisco无线LAN控制器配置指南，版本7.0 -管理用户帐户
- 通过 RADIUS 服务器对无线局域网控制器的公用入口管理员执行身份验证
- 技术支持和文档 - Cisco Systems