使用无线局域网控制器的外部 Web 身份验证配置示例

目录

简介

本文档介绍如何使用外部 Web 服务器设置无线 LAN 控制器 (WLC) 以进行 Web 身份验证。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解轻量接入点 (LAP) 和 Cisco WLC 配置的基础知识
- 基础知识轻量级接入点协议(LWAPP)和控制和供应无线接入点(CAPWAP)
- 有关如何设置和配置外部 Web 服务器的知识
- 有关如何设置和配置 DHCP 和 DNS 服务器的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本7.0.116.0的思科4400 WLC
- 思科1131AG系列LAP
- 运行固件版本3.6的思科802.11a/b/g无线客户端适配器
- 托管 Web 身份验证登录页面的外部 Web 服务器
- 用于地址解析和为无线客户端分配 IP 地址的 DNS 和 DHCP 服务器

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。

背景信息

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。没有需要对于请求方或客户端工具，Web验证是简单验证方法。

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

本文提供配置示例以说明如何配置 WLC 使用外部 Web 服务器上的登录脚本。

外部 Web 身份验证过程

使用外部Web验证，用于Web验证的登录页在外部Web服务器存储。下面是无线客户端尝试接入启用了外部 Web 身份验证的 WLAN 网络时的事件顺序：

1. 客户端(最终用户)连接对WLAN并且打开Web浏览器并且输入URL，例如www.cisco.com。
2. 客户端发送DNS请求到DNS服务器为了解决www.cisco.com到IP地址。
3. WLC寄请求给，反过来，解决www.cisco.com对IP地址并且发送DNS回复的DNS服务器。控制器寄回复给客户端。
4. 客户端设法通过发送TCP Syn信息包首次TCP连接用www.cisco.com IP地址对www.cisco.com IP地址。
5. 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。
6. 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。此HTML使客户端去WLC的默认网页URL，例如， http:// <Virtual-Server-IP>/login.html。
7. 客户端然后开始发送它对1.1.1.1对重定向URL的HTTPS连接。这是控制器的虚拟IP地址。客户端必须验证或忽略服务器证书，以建立 SSL 隧道。
8. 由于外部Web验证启用， WLC重定向客户端对外部Web服务器。

9. 外部Web验证登录URL带有参数例如AP_Mac_Address、client_url (www.cisco.com)和客户端需要与控制器Web服务器联系的action_URL。**注意：** action_URL告诉Web服务器用户名和密码在控制器存储。凭证一定被退还的到控制器为了得到验证。
10. 外部 Web 服务器 URL 可将用户定向到登录页。
11. 登录页采取用户凭证输入，并且送回请求到action_URL，示例http://1.1.1.1/login.html，WLC Web服务器。
12. WLC Web 服务器提交用于身份验证的用户名和口令。
13. WLC 启动 RADIUS 服务器请求或使用 WLC 上的本地数据库并对用户进行身份验证。
14. 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客户端开始与，例如www.cisco.com。
15. 如果身份验证失败，则 WLC Web 服务器会将用户重定向回客户登录 URL。

注意： 要将外部 Web 身份验证配置为使用 HTTP 和 HTTPS 以外的端口，请发出此命令：

```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

网络设置

配置示例使用此设置。WLC 上已注册 LAP。您需要为来宾用户配置一个 WLAN 来宾并必须为用户启用 Web 身份验证。您也需要保证控制器重定向用户对外部Web服务器URL (外部Web验证)。外部 Web 服务器托管用于身份验证的 Web 登录页。

必须对照控制器上维护的本地数据库来验证用户凭证。在成功进行身份验证后，应该允许用户访问 WLAN 来宾。控制器和其它设备需要为此设置配置。

注意： 对于用于进行 Web 身份验证的登录脚本，您可以使用自定义版本。您能下载从Cisco软件下载页的一份示例Web验证脚本。例如，对于4400个控制器，请导航对**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**。

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： 本文假定已配置 DHCP、DNS 和外部 Web 服务器。有关如何配置 DHCP、DNS 和外部 Web 服务器的信息，请参阅相应的第三方文档。

配置

在您为外部 Web 身份验证配置 WLC 之前，您必须针对基本操作来配置 WLC 并将 LAP 注册到该 WLC。本文档假设已配置 WLC 进行基本操作，并且已在 WLC 中注册 LAP。对无线局域网控制器(WLC)的参考的轻量AP (LAP)注册，如果是尝试的新用户设置基本操作的WLC与拉普。

若要针对此设置配置 LAP 和 WLC，请完成以下步骤：

1. 为来宾用户创建动态接口
2. 创建预先身份验证ACL
3. 在 WLC 上为来宾用户创建本地数据库
4. 配置外部 Web 身份验证的 WLC
5. 为来宾用户配置 WLAN

为来宾用户创建动态接口

要为来宾用户创建动态接口，请完成以下步骤：

1. 从 WLC GUI 中，选择 **Controllers > Interfaces**。此时会显示“Interfaces”窗口。此窗口中会列出在控制器上配置的接口。这包括默认接口，包括管理接口、ap-manager 接口、虚拟接口和服务端口接口以及用户定义的动态接口。
2. 单击 **New** 创建新的动态接口。
3. 在**接口>New**窗口，请输入接口名称和VLAN Id。然后，单击 **Apply**。在本例中，动态接口被命名为 **guest**，并为 VLAN Id 分配 10。
4. 对于动态接口，在 Interfaces > Edit 窗口中输入 IP 地址、子网掩码和默认网关。将它分配到 WLC 上的某个物理端口，再输入 DHCP 服务器的 IP 地址。然后，单击 **Apply**。

创建预先身份验证ACL

当使用外部Web服务器Web验证时，某些WLC平台需要外部Web服务器的(Cisco 5500系列控制器预验证ACL，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。

然而，当曾经外部Web验证时，它是良好的做法配置外部Web服务器的预先身份验证ACL。

完成以下这些步骤，以便为 WLAN 配置预身份验证 ACL：

1. 从 WLC GUI 中，选择 **Security > Access Control Lists**。此窗口允许您查看类似于标准防火墙 ACL 的当前 ACL。
2. 单击 **New** 以创建新的 ACL。
3. 输入 ACL 的名称并单击 **Apply**。在本例中， ACL被命名PRE验证为外部Web**服务器**。
4. 对于创建的新 ACL，单击 **Edit**。此时将显示 ACL > Edit 窗口。此窗口允许用户定义新规则或修改现有 ACL 的规则。
5. 单击 **Add New Rule**。
6. 定义允许客户端访问外部 Web 服务器的 ACL 规则。在本例中，172.16.1.92 是外部 Web 服务器 IP 地址。
7. 单击 **Apply** 以提交更改。

在 WLC 上为来宾用户创建本地数据库

来宾用户的用户数据库在无线局域网控制器的本地数据库存储或者也许是控制器的存储的外部。

在本文中在控制器的本地数据库用于验证用户。您必须创建一个本地净用户和定义Web验证客户端登录的一个密码。要在 WLC 上创建用户数据库，请完成以下步骤：

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。

配置外部 Web 身份验证的 WLC

下一步是配置外部Web验证的WLC。完成这些步骤：

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 Authentication Type 下拉框中，选择 **External (Redirect to external server)**。
3. 在**外部Web服务器**部分，请添加新的外部Web服务器。
4. **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页的URL。在**外部Web验证URL字段**，请输入登录页在外部Web服务器存储的URL。**注意：** 在WLC版本5.0和以上， logout页Web验证的可能也定制。*参考分配洛金，登录失败和注销页每个无线局域网控制器配置Guide,5.2的*WLAN部分关于如何配置它的更多信息。

为来宾用户配置 WLAN

最后一步将创建来宾用户的WLAN。完成这些步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。在本例中，WLAN 被命名为 **Guest**，并且 WLAN ID 是 1。
3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。对于访客WLAN，在常规选项卡，请从接口名称字段选择适当的接口。本示例将先前创建的动态接口 **guest** 映射到 WLAN 来宾。转到**安全**选项卡。在第2层安全下，**什么都没有**在本例中选择。**注意：** 不支持与 802.1x 身份验证一起使用 Web 身份验证。这意味着在使用 Web 身份验证时，您不能选择 802.1x 或使用 802.1x 的 WPA/WPA2 作为第 2 层安全方法。支持 Web 身份验证使用所有其他的第 2 层安全参数。在 Layer 3 Security 字段中，选中 **Web Policy** 复选框并选择 Authentication 选项。选择此选项是因为将使用 Web 身份验证对无线来宾客户端进行身份验证。从下拉菜单选择相应的预身份验证 ACL。在本例中，使用先前创建的预身份验证 ACL。单击 **Apply**。

验证

无线客户端出现，并且用户输入URL，例如www.cisco.com，在Web浏览器。由于尚未对用户进行身份验证，因此，WLC 会将用户重定向到外部 Web 登录 URL。

将会提示用户输入用户凭证。一旦用户提交了用户名和口令，登录页将接收用户凭证输入，并在提交后将请求发送回 WLC Web 服务器的 action_URL（例如 http://1.1.1.1/login.html）。它以输入参数形式提供给客户重定向 URL，其中 1.1.1.1 是交换机上的虚拟接口地址。

WLC 将按照 WLC 上配置的本地数据库对用户进行身份验证。在成功认证以后， 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客户端开始与，例如www.cisco.com。

故障排除

使用下面这些调试命令可排除配置的故障。

- **debug mac addr <client-MAC-address xx:** xx : xx : xx : xx : xx>
- debug aaa all enable
- debug pem state enable

- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

使用本部分可排除配置故障。

重定向到外部 Web 身份验证服务器的客户端收到证书警告

问题：在将客户端重定向到 Cisco 的外部 Web 身份验证服务器时，客户端会收到证书警告。服务器上有一个有效证书，如果您直接连接到外部 Web 身份验证服务器，则不会收到证书警告。这是否是因为 WLC 的虚拟 IP 地址 (1.1.1.1) 被提交给客户端而不是提交给与证书相关联的外部 Web 身份验证服务器的实际 IP 地址？

解决方案：可以。不管您是执行本地 Web 身份验证还是外部 Web 身份验证，您都将在控制器上使用内部 Web 服务器。当您重定向到外部 Web 服务器时，您仍会从控制器收到证书警告，除非控制器上具有一个有效证书。如果重定向被发送到 https，您会收到来自控制器和外部 Web 服务器的证书警告，除非这两者都具有一个有效证书。

为了同时消除证书警告，您需要发布一个根级证书并下载到控制器上。该证书针对主机名进行发布，您需要在控制器上将该主机名放在虚拟接口下面的 DNS 主机名框中。您还需要将该主机名添加到您的本地 DNS 服务器，并使其指向 WLC 的虚拟 IP 地址 (1.1.1.1)。

参考一第三方证书的证书签名请求(CSR)生成在一个WLAN控制器(WLC)欲知更多信息。

Error:“page cannot be displayed”

问题：当控制器升级到 4.2.61.0 后，在您使用下载的网页进行 Web 身份验证时，会显示“page cannot be displayed”错误信息。在升级之前，此操作可以顺利执行。默认的内部网页可以顺利加载而不出现任何问题。

解决方案：自 WLC 版本 4.2 和更高版本以后，引入了一项新功能，即您可以有多个用于 Web 身份验证的自定义登录页。

为了能够正确加载网页，在 Security > Web Auth > Web login page 中将 Web 身份验证类型全局设置为 **customized** 并不足以解决问题。还必须在特定的 WLAN 上进行配置。为此，请完成以下步骤：

1. 登录到 WLC 的 GUI。
2. 单击 **WLANs** 选项卡，查看为进行 Web 身份验证而配置的 WLAN 的配置文件。
3. 在 WLAN > Edit 页上，单击 **Security** 选项卡。然后，选择 **Layer 3**。
4. 在此页上，为 Layer 3 Security 选择 **None**。
5. 选中 **Web Policy** 框，并选择 Authentication 选项。
6. 选中 **Over-ride Global Config Enable** 框，为 Web Auth Type 选择 Customized (Downloaded)，然后从 Login Page 下拉菜单中选择所需的登录页。单击 **Apply**。

相关信息

- 无线局域网控制器 Web 身份验证配置示例

- 视频：在Cisco无线LAN控制器(WLCs)的Web验证
- 无线局域网控制器上的 VLAN 配置示例
- 无线 LAN 控制器和轻量接入点基本配置示例
- 技术支持和文档 - Cisco Systems