Web 身份验证代理配置示例

Contents

Introduction

本文档介绍如何配置 Web 身份验证，以便使用代理设置。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 无线局域网控制器的基本配置
- Web 身份验证安全性

Components Used

本文档中的信息基于思科无线局域网控制器 7.0 版及更高版本。

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.

Configure

在网络中拥有代理服务器的网络管理员首先将 Web 流量发送到代理服务器，然后代理服务器将流量中继到互联网。客户端和代理服务器之间的连接可以使用端口 80 以外的 TCP 端口进行通信。此端口通常是 TCP 端口 3128 或 8080。默认情况下，Web 身份验证仅侦听端口 80。因此，计算机发出的 HTTP GET 请求传送到代理端口后，会被控制器丢弃。

本节介绍如何配置 Web 身份验证以使用代理设置：

1. 配置思科无线局域网控制器 (WLC) 以便侦听代理端口。
2. 配置代理自动配置 (PAC) 文件以直接返回虚拟 IP 地址。
3. 创建预先身份验证访问控制列表 (ACL)，以允许客户端在 Web 身份验证之前下载 PAC 文件。

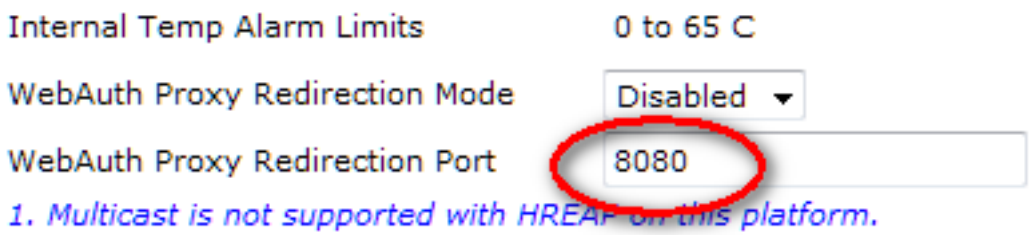
为了快速修复，您可以手动配置 Web 浏览器以返回 192.0.2.1。

有关这些流程的详细信息，请参阅下一小节。

配置 WLC

本程序介绍如何将控制器侦听的端口更改为代理服务器正在侦听的端口。

1. 导航到**控制器 > 常规**页面。

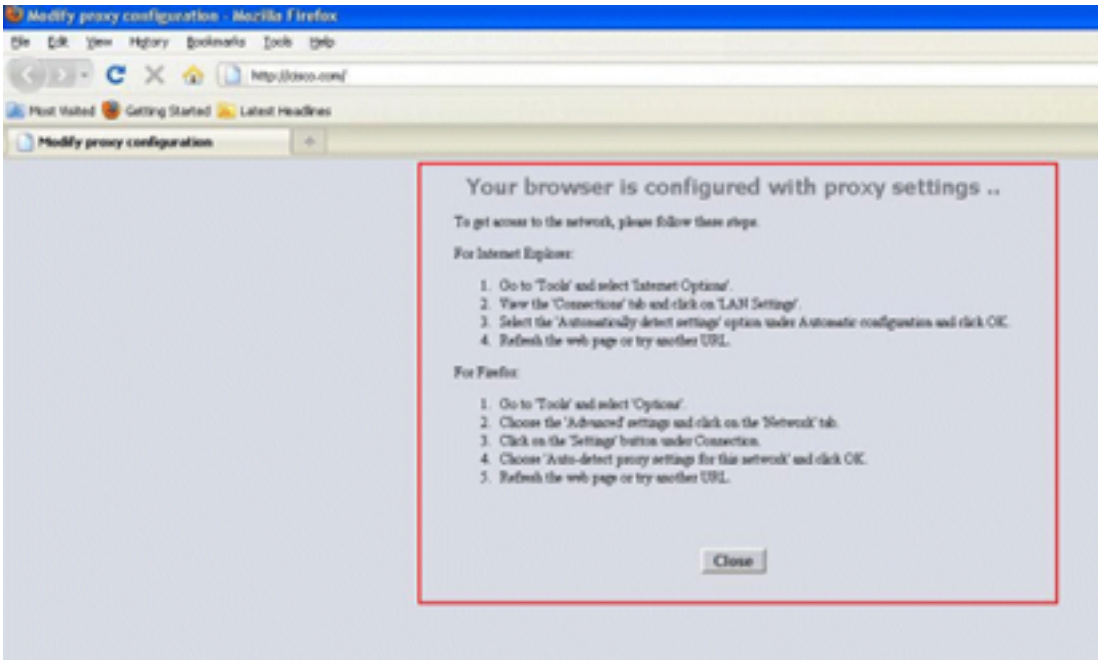


2. 在 WebAuth 代理重定向端口字段中，输入您希望 WLC 为了客户端重定向而侦听的端口。

3. 从 WebAuth 代理重定向模式下拉列表中选择已禁用或已启用：

   如果选择**已禁用**，客户端则会显示正常的 Web 身份验证页面以提供直通或进行身份验证。因此，如果您使用代理，则需要将所有客户端浏览器配置为不使用 192.0.2.1（或 WLC 使用的其他虚拟 IP 地址）的代理。请参阅配置 Web 浏览器。

   如果选择**已启用**，则 WLC 默认侦听端口 80、8080 和 3128，因此您无需在 WebAuth 代理重定向端口文本字段中输入这些端口。如果客户端在这些端口上发送 HTTP GET 请求，用户将看到要求将代理设置更改为自动的屏幕。



4. 保存配置。

5. 重启控制器。

总之，在 WebAuth 代理重定向端口中输入端口号，以便定义 WLC 侦听的端口。当重定向模式为已启用时，它会将客户端重定向到代理设置屏幕，并期望动态推送Web 代理自动发现 (WPAD) 或 PAC 文件以进行自动代理配置。当禁用时，客户端将重定向到正常的 Web 身份验证页面。

配置 PAC 文件

WLC 的虚拟 IP 地址需要“直接”返回，以便 Web Auth 正确验证用户身份。直接意味着代理服务器不代理请求，并且客户端有权直接连接到 IP 地址。这通常由代理服务器管理员在 WPAD 或 PAC 文件中的代理服务器上配置。这是 PAC 文件的示例配置：

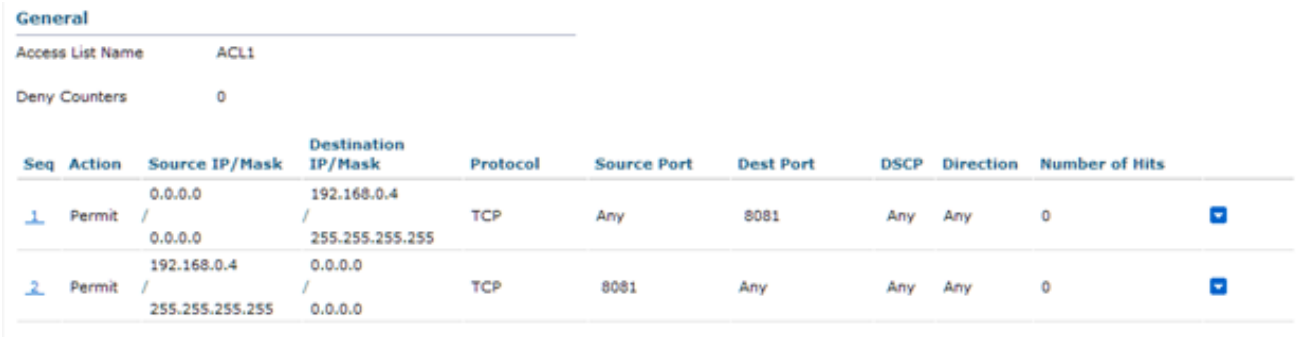
```
function FindProxyForURL(url, host) {
     // our local URLs from the domains below example.com don't need a proxy:
     if (shExpMatch(host, "*.example.com"))
     if (shExpMatch(host, "192.0.2.1"))   <-- (Line states return 1.1.1 directly)
      {
        return "DIRECT";
     }

function FindProxyForURL(url, host) {
     // our local URLs from the domains below example.com don't need a proxy:
     if (shExpMatch(host, "*.example.com"))
     if (shExpMatch(host, "192.0.2.1"))   <-- (Line states return 1.1.1 directly)
      {
        return "DIRECT";
     }
```

创建预先身份验证 ACL

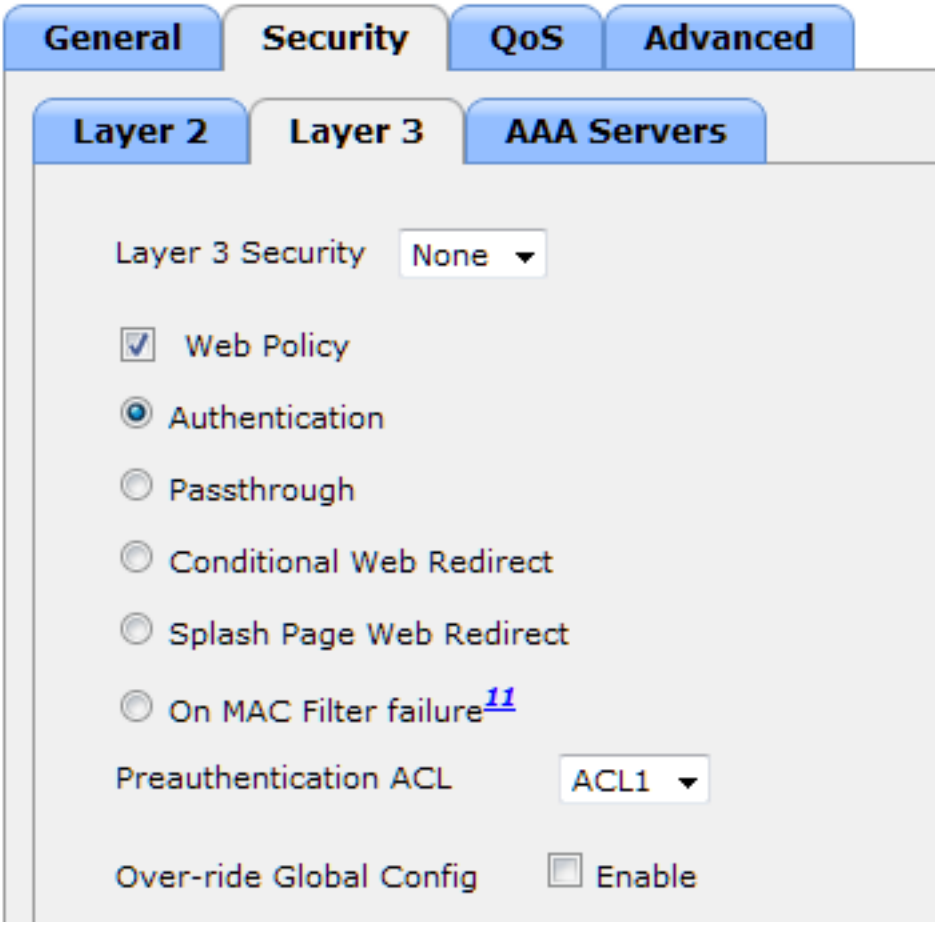
在 Web 身份验证服务集标识符 (SSID) 上放置预先身份验证 ACL，以便无线客户端可以在客户端登录 Web Auth 之前下载 PAC 文件。预先身份验证 ACL 需要仅允许访问 PAC 文件所在的端口。访问代理端口允许客户端无需进行 Web 身份验证即可连接到互联网。

1. 导航到**安全 > 访问控制列表**以便在控制器上创建 ACL。
2. 创建规则以允许 PAC 下载端口上的流量与代理之间进行双向传输。



Note:不允许代理 HTTP 端口。

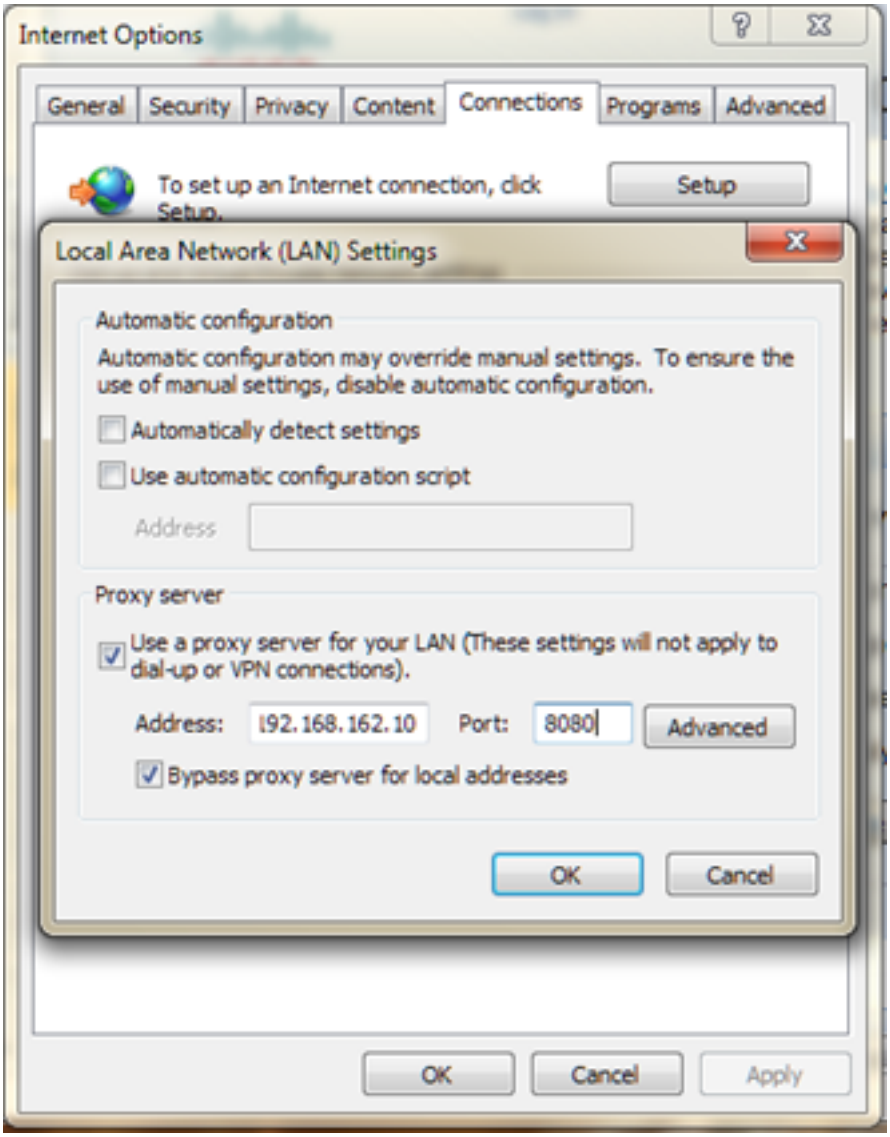
3. 在控制器上的 WLAN 配置中，不要忘记选择将刚刚创建的 ACL 作为预先身份验证 ACL。



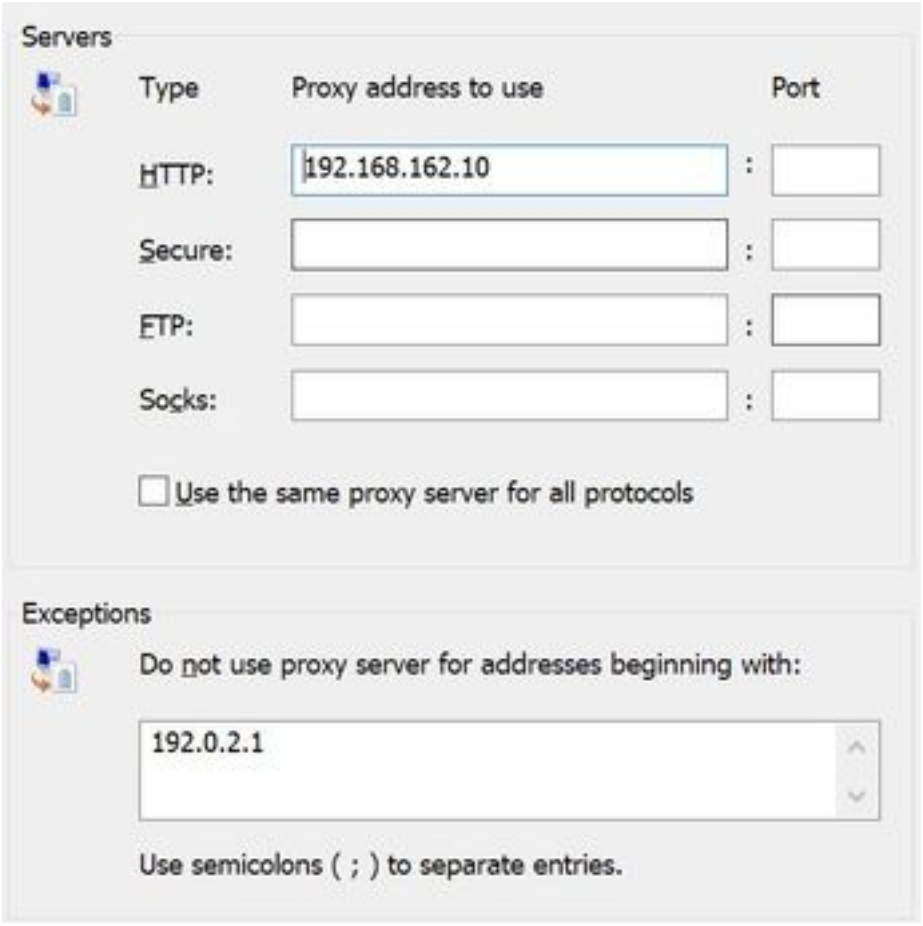
快速修复：配置 Web 浏览器

本程序介绍如何手动配置例外，以便客户端 Web 浏览器直接连接到 192.0.2.1。

1. 在 Internet Explorer 中，导航到**工具 > Internet 选项**。
2. 点击**“连接”选项卡**，，然后点击**“局域网设置”按钮**。
3. 在“代理服务器”区域中，选中 **为 LAN 使用代理服务器**复选框，然后输入服务器侦听的 (IP) 地址和端口。



4. 单击 **高级** ，并在“例外”区域中输入 WLC 的虚拟 IP 地址。



Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。