Web身份验证代理配置示例

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[配置 WLC](#)
[配置PAC文件](#)
[创建预先身份验证ACL](#)
[快速修复：配置Web浏览器](#)
[Verify](#)
[Troubleshoot](#)

Introduction

本文描述如何配置Web认证为了与代理设置一起使用。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 无线局域网控制器基本配置
- Web认证安全

Components Used

本文的信息根据Cisco无线LAN控制器，版本7.0和以上。

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

安排在他们的网络的一个代理服务器首先发送Web数据流到代理服务器，然后传递数据流到互联网的网络管理员。客户端和代理服务器之间的连接能使用TCP端口除端口80之外通信。此端口通常是TCP端口3128或8080。默认情况下，Web认证在端口80只监听。因此，当HTTP GET留下计算机时，它被发送到代理端口，但是由控制器下降。

此部分描述如何配置Web认证为了与设置的代理一起使用：

1. 配置Cisco无线LAN控制器(WLC)为了监听在代理端口。
2. 配置代理自动配置(PAC)文件为了返回直接的虚拟IP地址。
3. 创建预先身份验证访问控制表(ACL)为了允许客户端在Web认证前下载PAC文件。

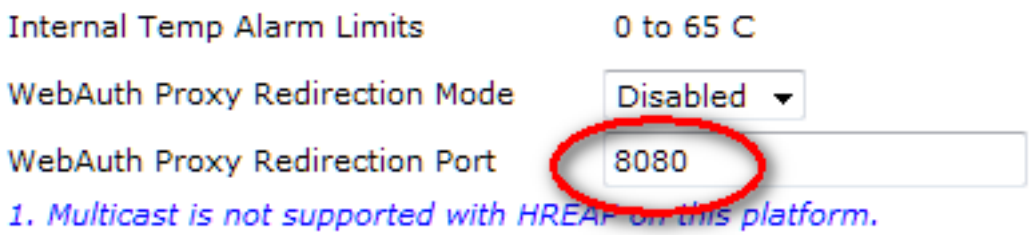
作为快速修复，您能手工配置Web浏览器为了返回192.0.2.1。

在这些进程中的每一个的详细资料在下小节。

配置 WLC

此程序描述如何更改控制器监听端口代理服务器监听的端口。

1. 连接对**Controller>常规**页。

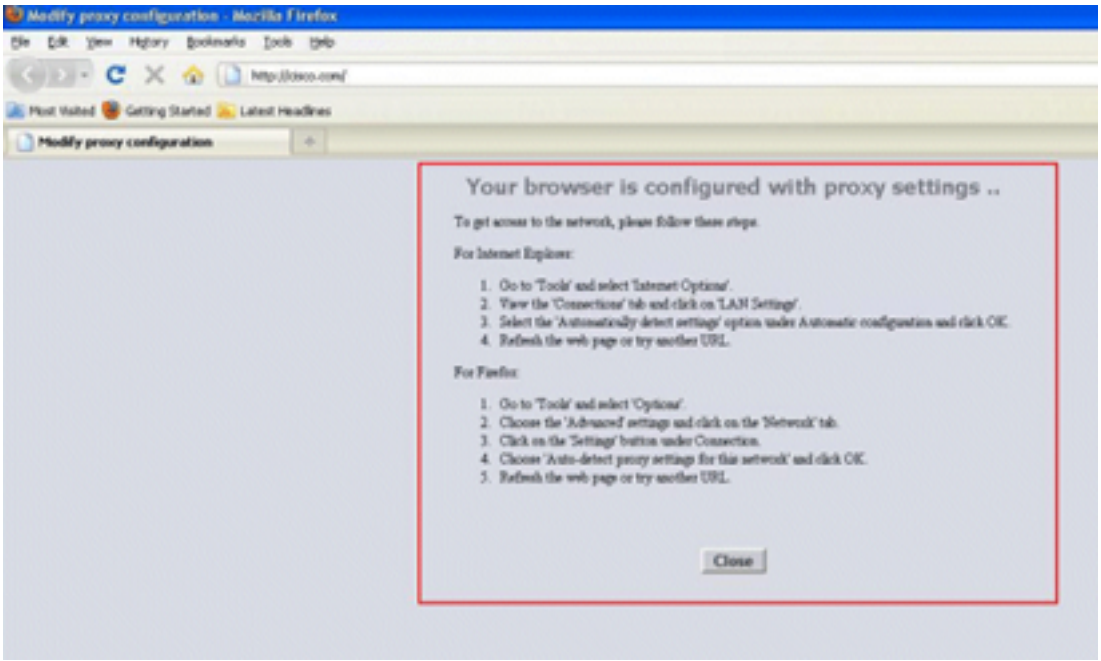


2. 在Port字段WebAuth代理的重定向，请输入端口您希望WLC细听客户端重定向。

3. 从WebAuth代理重定向模式下拉列表选择失效或启用：

   如果选择**失效**，提交客户端转接或认证的正常Web认证页。因此，如果使用一个代理，您需要配置所有客户端浏览器不使用代理192.0.2.1 (或其他虚拟IP地址WLC用途)。请参阅配置Web浏览器。

   如果选择**启用**，默认情况下WLC在端口80， 8080和3128监听，因此您不必须在WebAuth代理重定向端口文本字段输入那些端口。如果客户端发送在这些端口的一HTTP GET，他们看到请求他们更改他们的代理设置到自动的屏幕。



4. 保存配置。

5. 重新启动控制器。

总之，请输入端口编号在WebAuth代理重定向端口为了定义WLC监听的端口。当重定向模式是启用的时，重定向客户端对setting屏幕的代理并且期望动态地推进Web代理自动发现(WPAD)或自动代理配置的PAC文件。当禁用，客户端重定向对正常Web认证页。

配置PAC文件

WLC的虚拟IP地址需要是返回的'直接的'为了Web正确验证用户的Auth。处理意味着代理服务器不代理请求，并且客户端有权限直接地提供援助到IP地址。这在WPAD或PAC文件的代理服务器通常被配置由代理服务器管理员。这是PAC文件的一个示例配置：

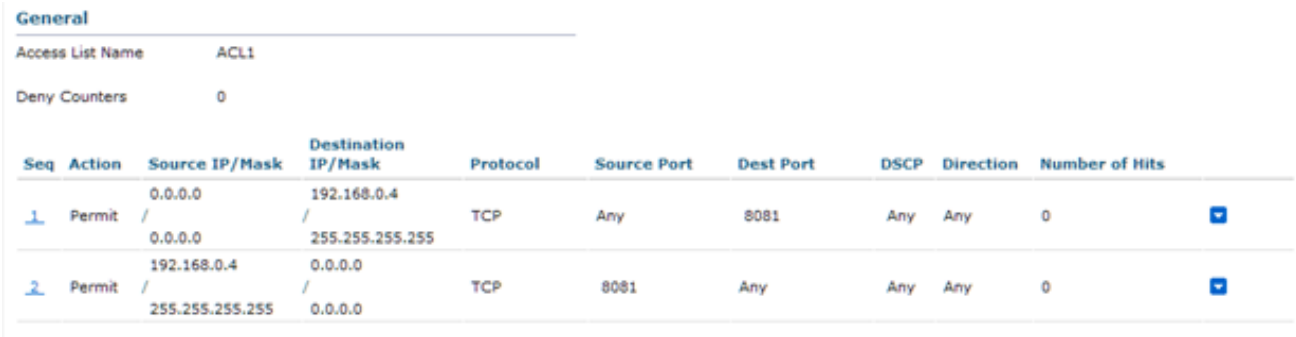
```
function FindProxyForURL(url, host) {
     // our local URLs from the domains below example.com don't need a proxy:
     if (shExpMatch(host, "*.example.com"))
     if (shExpMatch(host, "192.0.2.1"))   <-- (Line states return 1.1.1 directly)
      {
        return "DIRECT";
     }
```

```
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

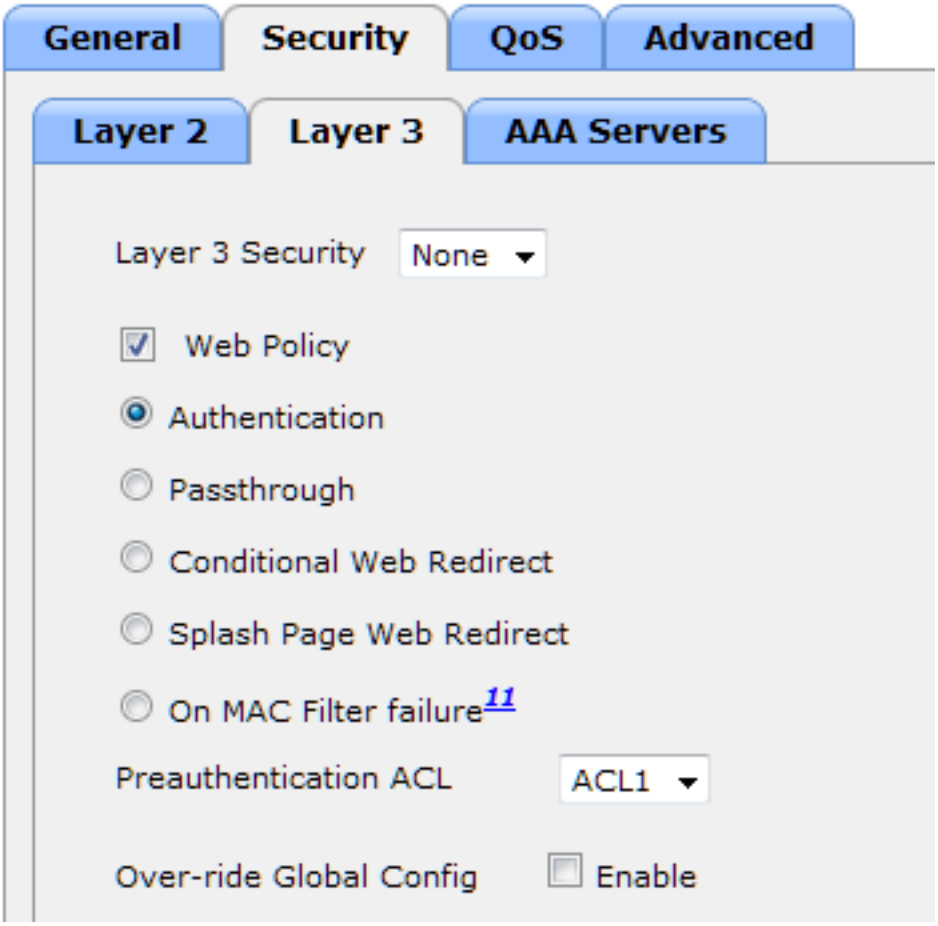
放置预先身份验证ACL在Web认证服务集标识(SSID)，以便无线客户端能在客户端日志前下载PAC文件到Web Auth。预先身份验证ACL仅需要允许对PAC文件打开的端口。对代理端口的访问允许客户端到达互联网，不用Web认证。

1. 连接对**安全>访问控制表**为了创建在控制器的ACL。
2. 创建规则允许在PAC下载端口的数据流到在两个方向的代理。



Note:请勿允许代理HTTP端口。

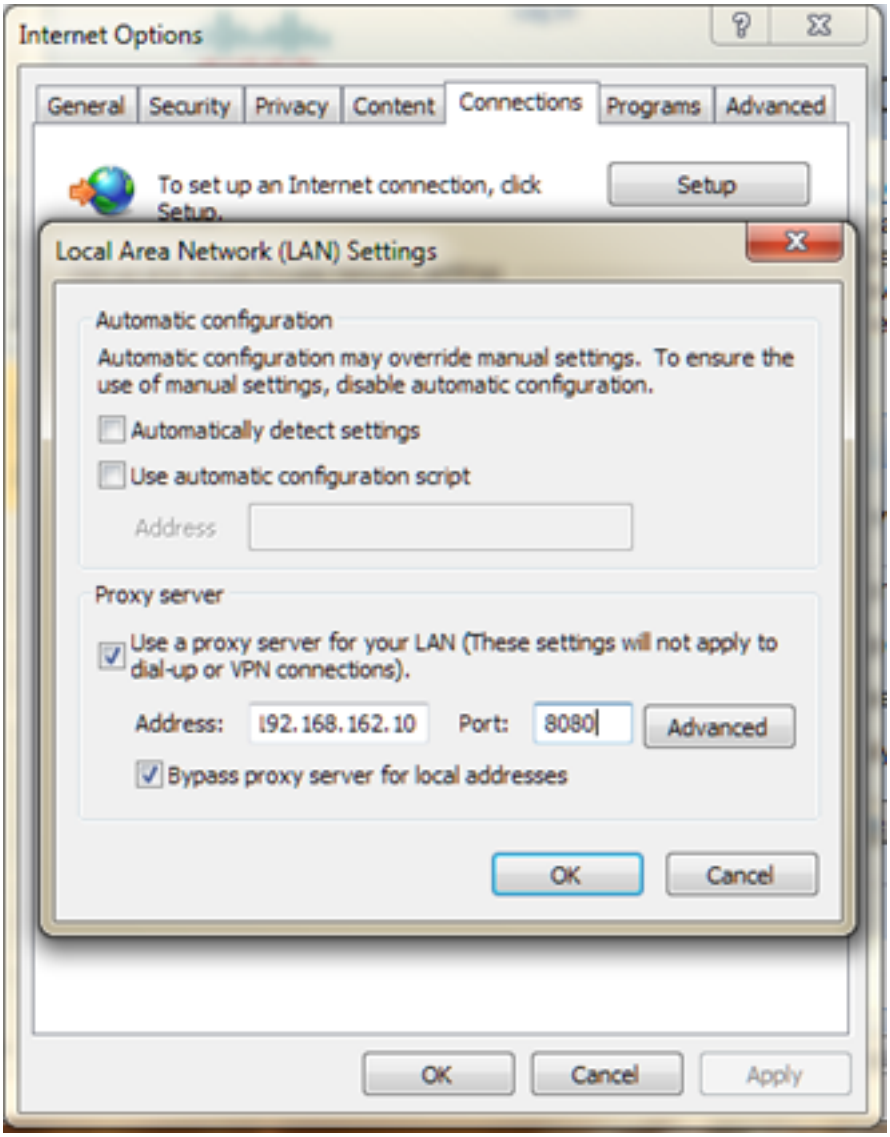
3. 在控制器的WLAN配置中，请勿忘记选择您创建作为预先身份验证ACL的ACL。



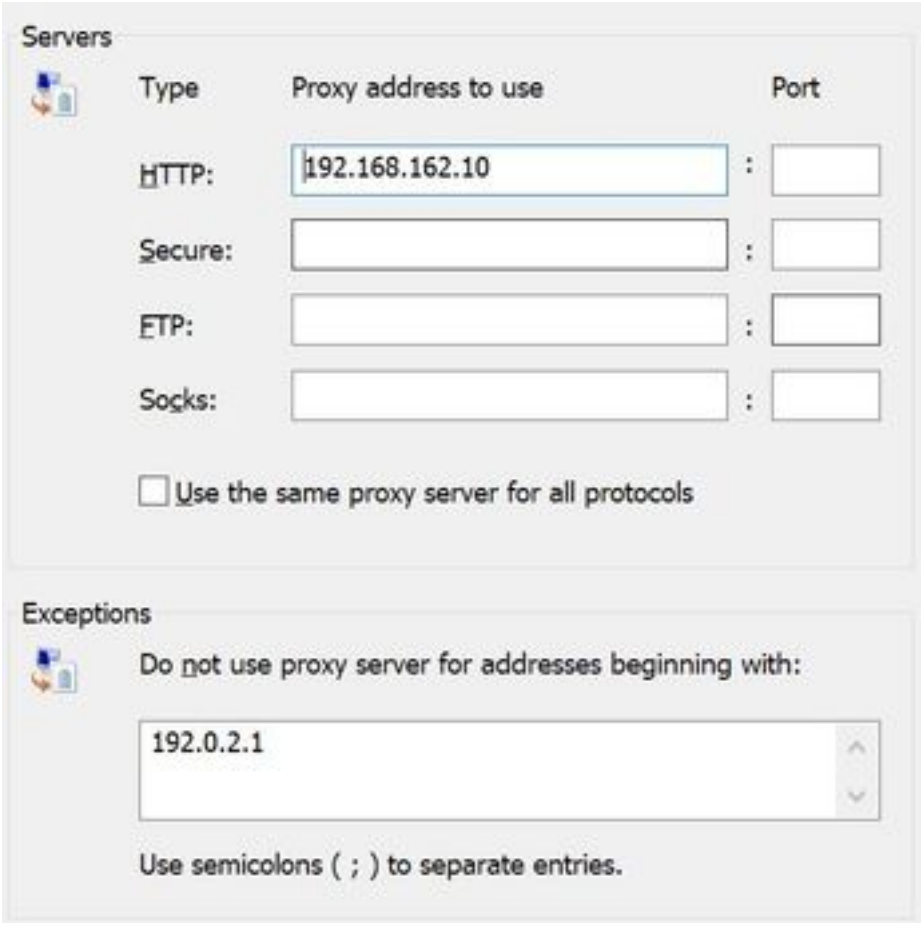
快速修复：配置Web浏览器

此程序描述如何手工配置例外，以便客户端Web浏览器提供援助直接地对192.0.2.1。

1. 在Internet Explorer，请连接对**工具> Internet选项**。
2. 点击**Connections选项**，然后**LAN Settings按钮**。
3. 在代理服务器地区中，请检查**使用代理服务器您的LAN**复选框，并且输入(IP)地址，并且端口服务器监听。



4. 点击**先进**并且输入WLC的虚拟IP地址在例外地区。



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。