

配置在Web-auth的HTTPS重定向

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[验证错误](#)

[配置](#)

[配置HTTPS的重定向的WLC](#)

[验证](#)

[故障排除](#)

简介

本文描述关于Web验证重定向的配置在HTTPS。这是在Cisco Unified无线网络(CUWN)版本介绍的功能8.0。

先决条件

要求

Cisco 建议您了解以下主题：

- 无线局域网控制器(WLC) Web验证基础知识
- 如何配置Web验证的WLC。

使用的组件

运行CUWN固件版本8.0的本文档中的信息根据Cisco 5500系列WLC。

注意：在本文提供的配置和web-auth说明比8.0.100.0是可适用的对所有WLC型号和所有CUWN镜像相等与或以后。

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。

背景信息

Web验证是第3层安全功能。它阻塞所有IP/data流量，除了与DHCP相关的信息包DNS相关的数据包，从特定的客户端，直到无线客户端供应了一个有效用户名和密码。Web身份验证通常由希望部署访客接入网络的客户使用。Web身份验证在控制器拦截来自客户端的第一个TCP HTTP (端口80) GET数据包时开始。

为了使客户端的Web浏览器发送数据包，客户端必须首先获得IP地址，并为Web浏览器将URL转换为IP地址(DNS解析)。这样，Web浏览器就知道应向哪个IP地址发送HTTP GET。当客户端发送第一HTTP GET对TCP端口80时，控制器重定向客户端对https:处理的<virtual IP>/login.html。此过程最终会启动登录网页。

在版本之前早于CUWN 8.0 (即7.6)，如果无线客户端提交一个HTTPS页(TCP 443)，页没有重定向到Web验证门户。当越来越多的网站开始使用HTTPS，此功能在版本CUWN 8.0包括及以后。使用到位此功能，如果无线客户端试https:// <website>，它重定向对web-auth登录页。并且此功能为发送与应用程序的https请求的设备是非常有用的(但是不用浏览器)。

验证错误

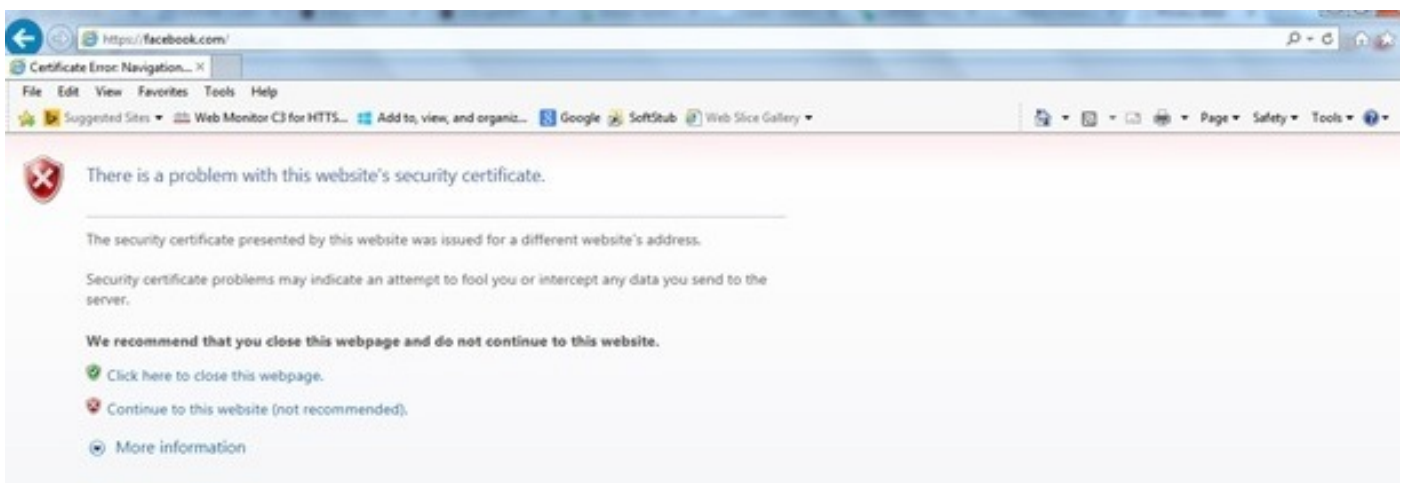
警告消息“证书没有由委托发出认证机关”。在您配置https重定向功能后，出现在浏览器。这被看到如图1和图2所显示，即使您有一有效根或被串连的证书在控制器。原因是您在控制器安装的certificiate发出对您的虚拟IP地址。

注意：如果尝试HTTP重定向并且有在WLC的此certificate，您不收到此证书警告错误。然而一旦HTTPS重定向，此错误出现。

当客户端试HTTPS:// <website>时，浏览器期待证书发出对DNS解决的站点的IP地址。然而，什么他们接收是发出到造成浏览器发布警告。WLC的证书(虚拟IP地址)的内部网络服务器这纯粹地是由于方式HTTPS工作和总是发生，如果设法拦截HTTPS会话为了web-auth重定向能工作。

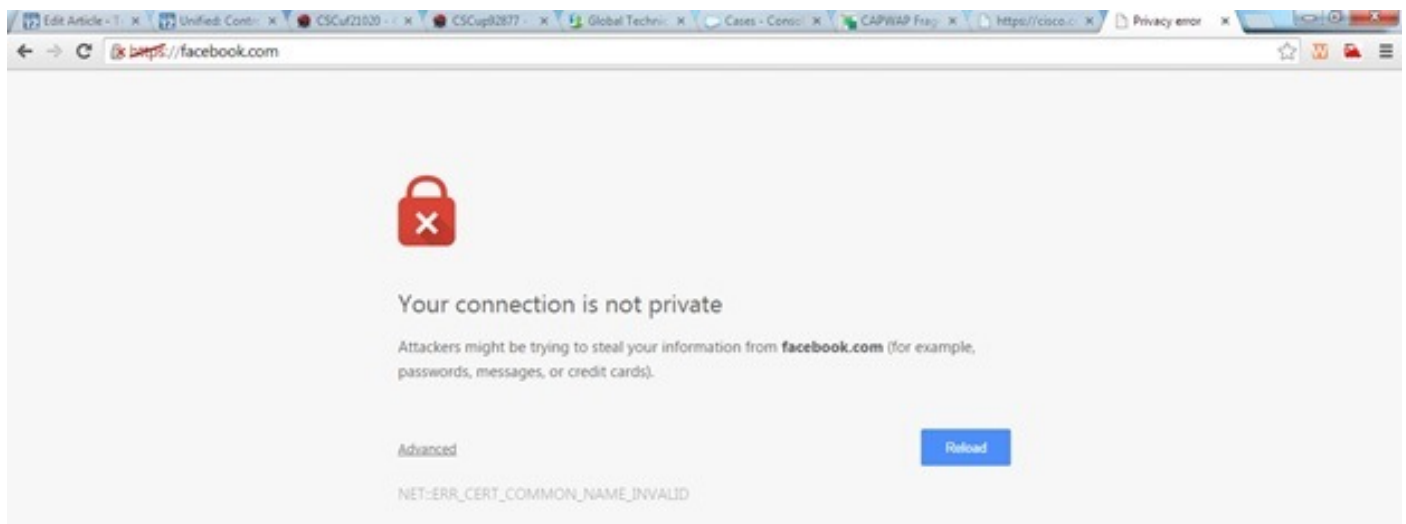
您也许发现不同的身份验证错误消息用不同的浏览器，但是全部与同一问题如前所述关连。

图 1



这是示例错误如何在镀铬物能出现：

图 2



配置

配置HTTPS的重定向的WLC

此配置假设，无线局域网(WLAN)为第3层Web authentication安全已经配置。为了启用或禁用在此Web-auth WLAN的HTTPS重定向：

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

因为配置示例显示，这也许影响不是HTTPS的重定向，但是HTTP重定向的吞吐量

欲知更多信息和Web验证WLAN的配置，请参阅[在WLAN控制器的Web验证](#)。

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

```
(WLC)>show network summary
```

```
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

1. 启用这些调试：(WLC) **debug client <MAC address>**

```
(WLC)> debug web-auth redirect enable
```

2. 验证调试：(WLC) **>show debug**

```
MAC Addr 1..... 24:77:03:52:56:80
```

```
Debug Flags Enabled:
```

webauth redirect enabled.

3. 关联客户端对web-auth启用的SSID。

4. 寻找这些调试：*webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received connection.

client socket = 9

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204

*webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled, checking for wispr in HTTP GET, client mac=24:77:3:52:56:80

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect URL according to configured Web-Auth type

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName for virtual IP(wirelessguest.test.com)

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web config for WLAN ID:10

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is enabled, checking on web-auth type

*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,

using URL:https://wirelessguest.test.com/fs/customwebauth/login.html**注意：保证或者安全Web (设置网络secureweb启用/禁用)或安全的web-auth (设置网络web-auth secureweb启用/禁用)启用为了做HTTPS重定向工作。并且请注意也许有对吞吐量的轻微的减少，当使用时在HTTPS的重定向。**

故障排除

目前没有针对此配置的故障排除信息。