通过 Web 身份验证配置 HTTPS 重定向

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 <u>背景信息</u> <u>证书错误</u> 配置 <u>为HTTPS重定向配置WLC</u> <u>验证</u> 故障排除

简介

本文档介绍有关通过 HTTPS 进行 Web 身份验证重定向的配置。这是思科统一无线网络 (CUWN) 版本 8.0 中引入的一项功能。

先决条件

要求

Cisco 建议您了解以下主题:

- •无线LAN控制器(WLC)Web身份验证的基本知识
- 如何配置WLC进行Web身份验证。

使用的组件

本文档中的信息基于运行CUWN固件版本8.0的Cisco 5500系列WLC。

注意:本文档中提供的配置和网络身份验证说明适用于所有WLC型号和等于或高于 8.0.100.0的任何CUWN映像。

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身份验证是第3层安全功能。在无线客户端提供有效的用户名和密码之前,它会阻止来自特定 客户端的所有IP/数据流量(DHCP相关数据包/DNS相关数据包除外)。Web身份验证通常由想要部 署访客接入网络的客户使用。当控制器拦截来自客户端的第一个TCP HTTP(端口80)GET数据包 时,Web身份验证开始。

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浏览器就知道要发送HTTP GET的IP地址。当客户端将 第一个HTTP GET发送到TCP端口80时,控制器将客户端重定向到https:<virtual IP>/login.html进行 处理。此过程最终会启动登录网页。

在CUWN 8.0(即最高7.6)之前的版本中,如果无线客户端显示HTTPS页面(TCP 443),则该页面 不会重定向到Web身份验证门户。随着越来越多的网站开始使用HTTPS,CUWN 8.0及更高版本中 包含了此功能。如果此功能就位,则如果无线客户端尝试https://<website>,则会将其重定向到 Web身份验证登录页。此外,此功能对于通过应用(但不通过浏览器)发送https请求的设备非常有 用。

证书错误

警告消息"证书未由受信任证书颁发机构颁发。" 在配置https-redirect功能后显示。即使您在控制器 上具有有效的根证书或链接证书,也会出现此情况,如图1和图2所示。原因是您在控制器上安装的 证书已颁发给您的虚拟IP地址。

注意:如果尝试HTTP重定向并在WLC上具有此证书,则不会收到此证书警告错误。 但是 ,在HTTPS重定向的情况下,出现此错误。

当客户端尝试HTTPS://<website>时,浏览器会期待颁发给DNS解析的站点IP地址的证书。但是 ,他们收到的是颁发给WLC(虚拟IP地址)的内部Web服务器的证书,导致浏览器发出警告。这纯 粹是因为HTTPS的工作方式,如果您尝试截取HTTPS会话以使Web身份验证重定向工作,则始终 会发生。

您可能会在不同的浏览器中看到不同的证书错误消息,但都与前面描述的相同问题有关。

图 1

()	B https://facebook.com/	D+0 0+0	
Cetific	ate Error Navigation×		
Får Edit View Favorites Tools Help 🎪 📴 Suggested Sites 🔹 🕮 Web Monitor CB for HTTS 🟥 Add to, view, and organiz 🛐 Google 🍰 SoftStub 🗿 Web Sice Gallery 🔹		🦓 = 🔯 - 🖙 👼 = Page = Safety = Tools = 🕯	
8	There is a problem with this website's security certificate.		
	The security certificate presented by this website was issued for a different website's address.		
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.		
	We recommend that you close this webpage and do not continue to this website.		
	Click here to close this webpage.		
	Secontinue to this website (not recommended).		
	More information		

图 2

CCCu/2020 ← → C	ie - T. × (📅 Unified: Conto: × 🤇 🖷 CSCut21020 - o × 🤇 🖷 CSCup82877 - × 🤇 😫 Global Technic: × (📿 Cases - Consol × 🤇 🚡 CAPWAP File; × 🤇 🗅 https://cisco.or × 💙 🗅 Priva ()s batpS://facebook.com	
	Δ	
	×	
	Your connection is not private	
	Attackers might be trying to steal your information from facebook.com (for example, passwords, messages, or credit cards).	
	Advanced Reford	
	NET-ERR_CERT_COMMON_NAME_INVALID	

配置

为HTTPS重定向配置WLC

此配置假设已为第3层Web身份验证安全配置了无线LAN(WLAN)。要在此网络身份验证WLAN上启 用或禁用HTTPS重定向,请执行以下操作:

(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
如示例配置所示,这可能会影响HTTPS重定向的吞吐量,但不会影响HTTP重定向

有关Web身份验证WLAN的详细信息和配置,请参阅<u>WLAN控制器上的Web身份验证</u>。

验证

使用本部分可确认配置能否正常运行。

<u>命令输出解释程序工具(仅限注册用户)支持某些 show</u> 命令。使用输出解释器工具来查看 show 命令输出的分析。

(WLC) > show network summary

Web Auth Secure Web Enable Web Auth Secure Redirection Enable

1. 启用以下调试: (WLC) **debug client**

```
(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. 将客户端关联到启用网络身份验证的SSID。
4. 查找以下调试:
  *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(wirelessquest.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:确保启用Secure Web(config network secureweb enable/disable)或Web-auth
  secure(config network web-auth secureweb enable/disable),以使HTTPS重定向工作。另请
```

```
注意,使用HTTPS重定向时,吞吐量可能会略有下降。
```

故障排除

目前没有针对此配置的故障排除信息。