透過Web-auth設定HTTPS重新導向

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>證書錯誤</u> <u>設定</u> <u>設定WLC以進行HTTPS重新導向</u> <u>驗證</u> <u>疑難排解</u>

簡介

本檔案介紹有關透過HTTPS進行Web驗證重新導向的組態。這是思科整合無線網路(CUWN)版本8.0中引入的功能。

必要條件

需求

思科建議您瞭解以下主題:

- 無線LAN控制器(WLC)Web驗證的基礎知識
- 如何設定WLC以進行Web驗證。

採用元件

本檔案中的資訊是根據執行CUWN韌體版本8.0的Cisco 5500系列WLC。

附註:本文提供的設定和web-auth說明適用於所有WLC型號和任何等於或高於8.0.100.0的 CUWN映像。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

Web驗證是第3層安全功能。它會阻止來自特定客戶端的所有IP/資料流量(DHCP相關資料包 /DNS相關資料包除外),直到無線客戶端提供了有效的使用者名稱和密碼。希望部署訪客接入網路 的客戶通常使用Web身份驗證。當控制器從客戶端截獲第一個TCP HTTP(埠80)GET資料包時 ,Web身份驗證啟動。

為了讓使用者端的Web瀏覽器達到此目的,使用者端必須首先取得IP位址,然後對Web瀏覽器執行 URL到IP位址(DNS解析)的轉換。這使Web瀏覽器知道要傳送HTTP GET的IP地址。當客戶端將 第一個HTTP GET傳送到TCP埠80時,控制器將客戶端重定向到https:<virtual IP>/login.html進行處 理。此程式最終會啟動登入網頁。

在CUWN 8.0之前的版本(即7.6之前)之前,如果無線客戶端顯示HTTPS頁面(TCP 443),則頁面 不會重定向到Web驗證門戶。隨著越來越多的網站開始使用HTTPS,CUWN 8.0及更高版本中會包 含此功能。具有此功能後,如果無線使用者端嘗試使用https://<website>,系統會將它重新導向到 web-auth登入頁面。此外,此功能對於使用應用程式(而不是瀏覽器)傳送https請求的裝置非常有 用。

證書錯誤

警告消息「證書不是由受信任的證書頒發機構頒發。」 設定https重新導向功能後顯示在瀏覽器上。 即使控制器上有有效的根憑證或鏈結憑證(如圖1和圖2所示),系統也會顯示此情況。這是因為控 制器上安裝的憑證已核發給您的虛擬IP位址。

附註:如果您嘗試HTTP-redirect並在WLC上擁有此憑證,就不會收到此憑證警告錯誤。 但是 在HTTPS-redirect的情況下,會出現此錯誤。

當客戶端嘗試訪問HTTPS://<web-site>時,瀏覽器期望向通過DNS解析的站點IP地址頒發的證書。 但是,他們收到的是頒發給WLC內部Web伺服器(虛擬IP位址)的憑證,這會導致瀏覽器發出警告 。這完全是由於HTTPS的運作方式,如果您嘗試擷取HTTPS作業階段,以使Web-auth重新導向正 常運作,就會一律發生這種情況。

在不同的瀏覽器中,您可能會看到不同的證書錯誤消息,但所有消息都與上述同一問題有關。

圖1

Contraction (acebook.com)	0 0 0 × 0
Cetificate Error Navigation ×	
File Edit View Favorites Tools Help 🎪 📴 Suggested Sizer 🕶 🏥 Web Monitor C3 for HTTS 🏥 Add to, view, and organiz 🛐 Google 🍰 SoftStub 🗿 Web Size Gallery 🕶	🏠 • 🔯 - 🖙 👼 • Page • Safety • Tools • 📦 •
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.	
Continue to this website (not recommended).	
More information	

以下範例說明錯誤如何在Chrome中顯示:

圖2

CSCut21t	20 - x X SCup92877 - x 2 Global Technic X Cases - Consc X X CAPWAP Frag X Chetps://cisco.c X D Privacy error	
	Your connection is not private	
	Attackers might be trying to steal your information from facebook.com (for example, passwords, messages, or credit cards).	
	Advanced Released	
	NET:ERR_CERT_COMMON_NAME_INVALID	

設定

設定WLC以進行HTTPS重新導向

此組態假設無線LAN(WLAN)已設定為第3層Web驗證安全。若要在此Web-auth WLAN上啟用或停用HTTPS重新導向:

(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
如範例組態所示,這可能會影響HTTPS重新導向的輸送量,但不會影響HTTP重新導向

有關Web驗證WLAN的詳細資訊和組態,請參閱WLAN控制器上的Web驗證。

驗證

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸 出的分析。

(WLC) > show network summary

Web Auth Secure Web Enable Web Auth Secure Redirection Enable 1. 啟用以下調試:

(WLC) debug client

```
(WLC) > debug web-auth redirect enable
2. 驗證調試:
  (WLC) >show debug
  MAC Addr 1..... 24:77:03:52:56:80
  Debug Flags Enabled:
  webauth redirect enabled.
3. 將客戶端與啟用Web-auth的SSID關聯。
4. 尋找以下調試:
  *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
  附註:確保啟用Secure Web(config network secureweb enable/disable)或web-auth
  secure(config network web-auth secureweb enable/disable),以使HTTPS重新導向生效。另
```

secure(coming network web-auth secureweb enable/disable),以使HTT 請注意,使用HTTPS重新導向時,輸送量可能會輕微下降。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。