在WLC上設定Web驗證代理

目錄

簡介

本檔案將提供在無線LAN控制器(WLC)上使用Web驗證代理功能的組態範例。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解輕型存取點(LAP)和Cisco WLC的配置。
- 瞭解輕量存取點協定(LWAPP)/無線存取點的控制和調配(CAPWAP)。
- 具備Web身份驗證知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行韌體版本7.0.116.0的Cisco 4400 WLC
- Cisco 1130AG系列LAP
- 執行韌體版本4.2的Cisco 802.11a/b/g無線使用者端配接器

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。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

WLC上的Web驗證Proxy

本文假設讀者事先瞭解了Web身份驗證以及在Cisco WLC上配置Web身份驗證所涉及的步驟。如果您是新使用者，請閱讀以下檔案，其中詳細說明了Web驗證程式：

- 無線 LAN 控制器 Web 驗證組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難

Web驗證代理功能是在WLC 7.0.116.0版中導入。

Web瀏覽器具有三種可由使用者配置的網際網路設定：

- 自動偵測
- 系統代理
- 手動

此功能可讓在瀏覽器中啟用手動Web代理的使用者端使用控制器進行Web驗證。

在設定為Web驗證的網路中，如果使用者端設定為手動代理伺服器設定，則控制器不會接聽這類代理伺服器連線埠，因此使用者端無法與控制器建立TCP連線。實際上，使用者無法存取任何登入頁面進行驗證，也無法存取網路。

當客戶端請求任何URL並且啟用Web驗證代理功能時，控制器以網頁作出響應，提示使用者更改網際網路代理設定以自動檢測代理設定。

此程式可防止瀏覽器的手動代理設定遺失。配置此功能後，使用者可透過Web身份驗證策略訪問網路。

預設情況下，此功能用於埠80、8080和3128，因為這些埠是Web代理伺服器最常用的埠。

在WLC上設定Web驗證代理

本節提供用於設定本文件中所述功能的資訊。

組態

完成以下步驟，以便使用控制器GUI設定Web驗證代理：

1. 從控制器GUI中，選擇Controller > General。
2. 若要啟用WebAuth Proxy，請從WebAuth Proxy Redirection Mode下拉式清單中選擇Enabled。

3. 在「WebAuth Proxy Redirection Port」文字方塊中，輸入Web驗證Proxy的連線埠號碼。此文字方塊包含控制器偵聽Web驗證Proxy重新導向的連線埠號碼。預設情況下，假設有三個埠80、8080和3128。如果將Web驗證重新導向連線埠設定為除了這些值以外的任何連線埠，則必須指定該值。
4. 按一下「Apply」。

若要從CLI設定WebAuth Proxy，請發出以下命令：

```
<#root>

config network web-auth proxy-redirect

 {enable | disable}
```

使用config network web-auth port <port-number>命令設定Web身份驗證埠號。

設定WLC後，儲存設定並重新啟動控制器，以便設定生效。

驗證

要檢視Web身份驗證代理配置的當前狀態，請發出show network summary或show running-config命令。

```
<#root>

(Cisco Controller) >

show network summary


RF-Network Name.............................. WLAN-LAB
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Forwarding................ Disable
Ethernet Broadcast Forwarding................ Disable
AP Multicast/Broadcast Mode.................. Unicast
IGMP snooping................................ Disabled
IGMP timeout................................. 60 seconds
IGMP Query Interval.......................... 20 seconds
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
Cisco AP Default Master...................... Disable
AP Join Priority............................. Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
```

```
--More-- or (q)uit
Mesh Full Sector DFS..................... Enable
Apple Talk .............................. Disable
AP Fallback ............................. Enable

Web Auth Redirect Ports ................. 80
Web Auth Proxy Redirect  ................ Enable

Fast SSID Change ........................ Disabled
802.3 Bridging .......................... Disable
IP/MAC Addr Binding Check ............... Enabled
```

現在，讓我們將無線客戶端連線到我們為Web身份驗證配置的訪客SSID。

假設您有內部DHCP伺服器，則客戶端連線到WLAN Guest1並獲取IP地址。當客戶端嘗試訪問URL(例如www.cisco.com)時，由於客戶端瀏覽器上啟用了手動代理，因此使用Web身份驗證代理功能的控制器會響應一個網頁，提示使用者更改網際網路代理設定以自動檢測代理設定。

此時，客戶端知道需要停用手動代理設定。在此，您可以看到如何在Firefox 3.6版上停用手動代理設定。

1. 從Firefox瀏覽器中，選擇工具 > 選項，然後選擇高級。
2. 按一下網路頁籤，然後選擇設定。
3. 在「Connection Settings」窗口中，選擇Auto-detect proxy settings for this network。

完成後，請重新整理瀏覽器，然後再次嘗試存取URL。這次會將您重新導向到「Web驗證」頁面。使用者端可以為您提供憑證，您也可以登入訪客網路。

相關資訊

- 無線 LAN 控制器 Web 驗證組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難
- 思科無線LAN控制器配置指南7.0.116.0版
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。