WLC第2層和第3層安全相容性矩陣

目錄

簡介

本檔案為無線LAN控制器(WLC)支援的第2層和第3層安全機制提供相容性矩陣。

必要條件

需求

思科建議您瞭解以下主題：

- 輕量AP和Cisco WLC配置的基本知識
- 輕量AP協定(LWAPP)基礎知識
- 無線安全解決方案基礎知識

採用元件

本檔案中的資訊是根據執行韌體版本7.0.116.0的Cisco 4400/2100系列WLC

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

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

思科整合無線網路安全解決方案

思科統一無線網路支援第2層和第3層安全方法。

- 第2層安全性
- 第3層安全（適用於WLAN）或第3層安全（適用於訪客LAN）

訪客LAN不支援第2層安全。

下表列出無線LAN控制器上支援的各種第2層和第3層安全方法。可從WLAN的**WLANs > Edit**頁面上的**Security**索引標籤啟用這些安全方法。

第2層安全機制		
引數		**說明**
第2層安全	無	未選擇第2層安全性。
	WPA+WPA2	使用此設定可啟用Wi-Fi保護訪問。
	802.1X	使用此設定可啟用802.1x身份驗證。
	靜態WEP	使用此設定可啟用靜態WEP加密。
	靜態WEP + 802.1x	使用此設定可同時啟用靜態WEP和802.1x引數。
	CKIP	使用此設定可啟用Cisco Key Integrity Protocol(CKIP)。在AP型號1100、1130和1200上工作正常，但在AP 1000上不起作用。需要啟用Aironet IE才能使用此功能。CKIP將加密金鑰擴展為16位元組。
MAC過濾	選擇以按MAC地址過濾客戶端。在MAC Filters（MAC過濾器）> New（新建）頁面中按MAC地址本地配置客戶端。否則，在RADIUS伺服器上設定使用者端。	
第3層安全機制（適用於WLAN）		
引數		**說明**
第3層安全	無	未選擇第3層安全性。
	IPSec	使用此設定可啟用IPSec。在實施IPSec之前，您需要檢查軟體可用性和客戶端硬體相容性。 **注意**：您必須安裝可選的VPN/增強型安全模組（加密處理器卡）才能啟用IPSec。驗證控制器上是否已在「清單」頁面上安裝。
	VPN傳輸	使用此設定可啟用VPN傳輸。 **注意**：此選項在Cisco 5500系列控制器和Cisco 2100系列控制器上不可用。但是，您可以使用ACL建立開放式WLAN，在Cisco 5500系列控制器或Cisco 2100系列控制器上

		複製此功能。
Web策略	選中此覈取方塊可啟用Web策略。驗證之前，控制器會將DNS流量轉送到無線客戶端或從無線客戶端轉送。 **注意**：Web策略不能與IPsec或VPN直通選項結合使用。 將顯示以下引數： • Authentication — 如果選擇此選項，則在將客戶端連線到無線網路時，系統會提示使用者輸入使用者名稱和密碼。 • Passthrough — 如果選擇此選項，則使用者無需使用者名稱和密碼身份驗證即可直接訪問網路。 • 條件式Web重新導向 — 如果選擇此選項，則在802.1X驗證成功完成後，可以有條件地將使用者重新導向到特定網頁。您可以指定重新導向頁面，以及在 RADIUS 伺服器上進行重新導向的條件。 • 啟動顯示頁面Web重新導向 — 如果選擇此選項，則802.1X驗證成功完成後，使用者將被重新導向到特定網頁。重新導向後，使用者會獲得網路的完整存取權限。您可以在RADIUS伺服器上指定啟動顯示網頁。 • On MAC Filter failure — 啟用Web身份驗證MAC過濾器故障。	
預先驗證ACL	選擇要用於客戶端和控制器之間流量的ACL。	
搭載全域性配置	如果選擇「身份驗證」，則顯示。選中此框可覆蓋Web登入頁面上設定的全域性身份驗證配置。	
Web身份驗證型別	如果您選擇Web Policy和Over-ride Global Config，則顯示。選擇一種Web驗證型別： • 內部 • 定製（下載）Login Page — 從下拉選單中選擇登入頁。Login Failure page — 選擇在Web身份驗證失敗時顯示到客戶端的登入頁。註銷頁面 — 選擇當使用者註銷系統時顯示給客戶端的登入頁面。 • 外部（重定向到外部伺服器）URL — 輸入外部伺服器的URL。	
電子郵件輸入	如果選擇「傳遞」(Passthrough)，則顯示。如果選擇此選項，則在連線到網路時，系統會提示您輸入電子郵件地址。	
第3層安全機制（適用於訪客LAN）		
引數		**說明**
第3層	無	未選擇第3層安全性。

安全	Web驗證	如果選擇此選項，則在將客戶端連線到網路時，系統會提示您輸入使用者名稱和密碼。
	USB傳輸	如果選擇此選項，可以直接訪問網路，而無需使用者名稱和密碼身份驗證。
預先驗證ACL		選擇要用於客戶端和控制器之間流量的ACL。
搭載全域性配置		選中此框可覆蓋Web登入頁面上設定的全域性身份驗證配置。
Web身份驗證型別		如果選擇Over-ride Global Config，則顯示。選擇一種Web驗證型別： • 內部 • 定製（下載）Login Page — 從下拉選單中選擇登入頁。Login Failure page — 選擇在Web身份驗證失敗時顯示到客戶端的登入頁。註銷頁面 — 選擇當使用者註銷系統時顯示給客戶端的登入頁面。 • 外部（重定向到外部伺服器）URL — 輸入外部伺服器的URL。
電子郵件輸入		如果選擇「USB傳輸」，則顯示。如果選擇此選項，則在連線到網路時，系統會提示您輸入電子郵件地址。

註：在控制器軟體版本4.1.185.0或更高版本中，僅支援與靜態WEP結合使用的CKIP。不支援將其用於動態WEP。因此，配置為將CKIP與動態WEP配合使用的無線客戶端無法與為CKIP配置的無線LAN關聯。思科建議您使用不帶CKIP的動態WEP（安全性較低）或帶TKIP或AES的WPA/WPA2（安全性較高）。

無線LAN控制器第2層 — 第3層安全相容性矩陣

在無線LAN上設定安全性時，第2層和第3層安全性方法可以結合使用。但是，並非所有第2層安全方法都可與所有第3層安全方法一起使用。下表顯示無線LAN控制器上支援的第2層和第3層安全方法的相容性矩陣。

第2層安全機制	第3層安全機制	相容性
無	無	有效
WPA+WPA2	無	有效
WPA+WPA2	Web驗證	無效
WPA-PSK/WPA2-PSK	Web驗證	有效
WPA+WPA2	USB 傳輸	無效
WPA-PSK/WPA2-PSK	USB 傳輸	有效
WPA+WPA2	條件式 Web 重新導向	有效
WPA+WPA2	啟動顯示頁面 Web 重新導向	有效

WPA+WPA2	VPN傳輸	有效
802.1x	無	有效
802.1x	Web驗證	無效
802.1x	USB 傳輸	無效
802.1x	條件式 Web 重新導向	有效
802.1x	啟動顯示頁面 Web 重新導向	有效
802.1x	VPN傳輸	有效
靜態WEP	無	有效
靜態WEP	Web驗證	有效
靜態WEP	USB 傳輸	有效
靜態WEP	條件式 Web 重新導向	無效
靜態WEP	啟動顯示頁面 Web 重新導向	無效
靜態WEP	VPN傳輸	有效
靜態WEP+ 802.1x	無	有效
靜態WEP+ 802.1x	Web驗證	無效
靜態WEP+ 802.1x	USB 傳輸	無效
靜態WEP+ 802.1x	條件式 Web 重新導向	無效
靜態WEP+ 802.1x	啟動顯示頁面 Web 重新導向	無效
靜態WEP+ 802.1x	VPN傳輸	無效
CKIP	無	有效
CKIP	Web驗證	有效
CKIP	USB 傳輸	有效
CKIP	條件式 Web 重新導向	無效
CKIP	啟動顯示頁面 Web 重新導向	無效
CKIP	VPN傳輸	有效

相關資訊

- 無線LAN控制器和輕量型存取點基本組態範例
- 輕量AP(LAP)註冊到無線LAN控制器(WLC)
- 思科無線LAN控制器配置指南7.0.116.0版
- 無線 LAN 控制器 (WLC) 常見問題
- 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）。