電信技術規範
檢驗規範

資通安全 0016 (IS0016-0)
訂定日期 102 年 2 月 7 日
通傳資技字第 10243004130 號

無線接取設備
資通安全檢測技術規範

國家通訊傳播委員會

目　次

圖　次

表　次

附　表　次

附　錄

無線接取設備檢測技術規範

1. 概說

無線接取設備 (Wireless Access Point，縮寫為 AP)是一個連接無線網路，亦可以連接有線網路的乙太網裝置。其主要功能為網路傳輸之中介點，使得有線及無線網路裝置可互相連接並傳輸資料。

2. 適用範圍

本規範適用於獨立式硬體架構，並使用嵌入式韌體或專屬軟體之區域網路無線接取設備，可支援開放系統介面 (OSI, Open System Interface)網路架構。

3. 安全等級

本規範之設備安全等級分為基礎型(Basic)與進階型(Advanced)。

3.1. 基礎型無線接取設備

基礎型設備安全功能測試項目包括稽核資料產出、外部稽核伺服器失去連線的應變措施、重送攻擊 (Replay Attacks) 偵測、可信賴更新、待測物安全功能自我測試、鑑別 (Authentication) 失敗控制功能、使用者識別及授權功能、檢查通行碼逾期功能、通行碼重新鑑別功能、登入畫面加密功能、802.1X 使用者識別及鑑別功能、安全功能行為管理、資源最大配額、登入連線之鎖定及登入連線之終止等 15 個主要測試；堅實測試項目包括異常或攻擊流量測試；穩定測試包括真實網路流量長時間測試。

3.2. 進階型無線接取設備

進階型設備除基礎型設備之測試項目外，另增加壓力測試包括吞吐量；堅實測試包括非正常關機恢復；穩定測試中的真實網路流量測試時間要求為基礎的兩倍。

4. 參考標準

ISO/IEC 15408 共同準則 (Common Criteria for Information TechnologySecurity Evaluation, CC)。

5. 用語釋義

RFC(Request For Comments)

由網際網路工程任務組(IETF)發行的一系列備忘錄。檔案收集了有關網際網路相關資訊，以及 UNIX 和網際網路社群的軟體檔案，以編號排定。目前 RFC 檔案是由網際網路協會 (ISOC) 贊助發行。

IEEE 802.1X

電機電子工程師學會 (IEEE) 制定關於用戶接入網路的鑑別標準，運行於網路中資料連結層。

IP 安全協定 （InternetProtocolSecurity, IPSec）

為建立在網路層上的安全協議，對所有通訊的 IP 封包使用鑑別和加密，並在雙方建立通訊時進行相互鑑別及金鑰交換。

SSH (Secure Shell)

為建立在應用層基礎上的安全協議，對所有傳輸的資料進行加密及壓縮，可以增加傳輸安全並加快傳輸速度。

傳送層安全 (TransportLayerSecurity, TLS)

為建立在傳輸層基礎上的安全協議，是為網路通信提供安全及數據完整性的一種安全協議。

安全接套層 (Secure Sockets Layer, SSL)

為 Netscape 公司推出 Web 瀏覽器首版時提出的協議。SSL 採用公開金鑰密碼技術，保證兩個應用程式間通信的保密性和可靠性，使客戶與伺服器之間的通信不被攻擊者竊聽。

安全的超文字傳送協定 (Hypertext Transfer Protocol Secure, HTTPS)

與 SSL/TLS 合併使用，用以提供加密通訊及對網路伺服器身分之鑑別。

RADIUS (Remote Authentication Dial In User Service)

包含驗證 (Authentication)、授權 (Authorization) 及計費 (Accounting) 三種

服務的通訊協議 (Protocol)，通常用於網路存取或浮動 IP 服務，亦適用於區域網或漫遊服務。

X.509

國際電信聯盟 (ITU-T) 制定的一種數位憑證標準，屬於公開金鑰密碼系統之通訊標準，可用於單一登入及權限管理架構用途。提供通信實體鑑別機制，並規範鑑別過程中廣泛適用的憑證語法及資料介面。

角色 (Role)

指預先定義之規則，以描述使用者與待測物間的操作權限。

最大同時連線數

指防火牆能同時處理之 TCP 連線數最大值。

吞吐量

指待測物處理網路流量的速度，通常的表示法為「Mbps」（每秒一百萬位元） 或 「Gbps」 （每秒十億位元）。

最大連線建立速度

指防火牆能處理的 TCP 連線建立速度，通常的表示法為 「TCP 連線數/每秒」。

共同準則 (Common Criteria, CC)

為國際資通安全產品評估及驗證之標準 (ISO/IEC 15408)，依其定義之評估保證等級 (Evaluation Assurance Level, EAL) 判定產品之安全等級，EAL 共有 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7，提供申請者/贊助者、檢測實驗室與驗證機關 (構) 評估及驗證資通安全產品安全與功能性。參考網址 http://www.commoncriteriaportal.org

無線網路存取系統保護剖繪 (U.S. Government Protection Profile for Wireless Local Area Network Access Systems)

指美國政府機關採購無線網路存取系統之技術參考指引。

評估標的 (Target of Evaluation, TOE)

指待測物及其相關之手冊。

保護剖繪 (Protection Profile, PP)

指滿足資通安全產品評估標的 (TOE) 製作之安全基本需求文件。

安全標的 (Security Target, ST)

指資通安全產品能符合保護剖繪 (PP) 或特定安全需求製作之規格文件。

安全功能 (TOE Security Functions, TSF)

指資通安全產品用於實現安全標的 (ST) 所要求安全功能需求之相關功能。

安全功能需求 (Security Functional Requirement, SFR)

指共同準則第二部份 (Common Criteria, Part 2) 所定義之安全相關需求條文，用以描述一資通安全產品之 TSF 所需滿足的各項要求。此要求條文會被引用於保護剖繪及安全標的中，用以具體陳述該產品功能的安全方面的需求。

安全功能介面 (TOE Security Functions Interface, TSFI)

為評估標的 (TOE) 用於實現安全功能需求 (SFR) 之對外溝通介面。

安全領域 (Security Domain)

指一個主動式個體 (人或機器) 被授權存取的資源集合，為安全架構的屬性之一。

自我保護 (Self-Protection)

指安全功能無法被無關的程式碼或設施破壞，為安全架構的屬性之一。

6. 技術要求

6.1. 書面審查類別

6.1.1. 安全標的

審查待測物之設備規格及安全功能需求。

6.1.2. 安全功能設計

審查待測物之設計安全性、安全架構及安全指引。

6.2. 書面審查類別之項目及判定標準

申請者應依基礎型或進階型之安全等級，提供符合該等級之安全標的及安全功能設計類別相關文件 (如：表 1)。

表 1　書面審查之類別、項目及審查內容

類別	項目	審查內容	檢附文件	基礎型	進階型
安全標的	設備規格	附表 1-1	設備規格說明書	Π	Π
	安全功能需求	附表 1-2	設備規格說明書	Π	Π
安全功能設計	安全功能規格	附表 1-3	附件一、安全功能介面表	Π	Π
	設計安全性	附表 1-4	附件二、子系統描述與分類表		Π
	安全架構	附表 1-5	附件三、安全架構描述表	Π	Π
	安全指引	附表 1-6	指引文件	Π	Π

6.2.1. 安全標的

申請者應提供待測物之設備規格說明書，包含設備規格 (附表 1-1) 及該設備可執行的安全功能需求 (附表 1-2)。

6.2.1.1. 設備規格說明

本項書面審查內容依申請者提供之設備規格說明書，檢視設備規格是

否符合附表 1-1 設備規格之書面審查內容：

附表 1-1 設備規格之書面審查內容

類別	項目	子項目	審查標準	基礎型	進階型
安全標的	設備規格	1.設備識別	應標示下列內容： (1) 名稱、廠牌、型號及版本。 (2) 申請者名稱 (製造商或代理商)。 (3) 製造商名稱。 (4) 設備形式 (硬體、韌體或軟體)。	Π	Π
		2.範圍	應說明下列內容： (1) 待測物之實體範圍：包含待測物外觀、尺寸、主要零組件及執行必須之相關週邊設施。 (2) 待測物之邏輯範圍：包含待測物安全功能以及功能之間相互關係。	Π	Π
		3.安全功能	應說明待測物之安全功能如何滿足本規範之安全功能需求。	Π	Π

6.2.1.2. 安全功能需求 (SFR)

本項書面審查內容依申請者提供之設備規格說明書，檢視安全功能需求 (SFR) 之執行內容是否符合附表 1-2 (安全功能需求之書面審查內容)。

附表 1-2 安全功能需求之書面審查內容

類別	項目	子項目	審查標準	基礎型	進階型
安全標的	安全功能	1.稽核紀錄	待測物應具備以下稽核紀錄： (1) 待測物應依下列事件產生其稽核紀錄，並存於資料庫中： A. 啟閉稽核功能。 B. 管理者透過管理介面操作待測物的所有行為。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
	需求		C. 使用者之識別與鑑別活動。 D. 待測物系統時間變更。 E. 軟韌體更新。 F. 解除交談鎖定之活動。 G. 終止登入連線之活動。 H 啟動、終止或失敗之可信任通道連結。 (2) 每筆稽核紀錄至少包含下列資訊： A. 事件識別碼。 B. 事件日期及時間。 C. 事件類型 D. 事件成功或失敗 (3) 每筆稽核事件需可識別是因何使用者所產生。		
		2.稽核紀錄之查詢	待測物應具備以下稽核紀錄之查詢： (1) 管理者的身分。 (2) 事件類型。 (3) 成功之稽核事件。 (4) 失敗之稽核事件。 (5) 或其他屬性。	Π	Π
		3.稽核資料儲存保護	待測物應具備以下稽核資料之保護： (1) 待測物應防止非授權人員透過安全功能介面竄改或刪除稽核資料。 (2) 待測物應將稽核資料儲存於外部的稽核資料儲存裝置；存取外部的稽核資料儲存裝置時需透過 IPsec、SSH、TLS 或 TLS/HTTPS 等可信賴通道。 (3) 如外部的稽核資料儲存裝置失聯，待測物應停止將稽核資料傳遞到外部的稽核資料儲存裝置，並即刻通知管理者。	Π	Π
		4.加解密金鑰管理	待測物應具備以下加解密金鑰管理功能： (1) 待測物應以加解密演算法 (Cryptographic Algorithm) 產生、分配、儲存及銷毀金鑰。 (2) 任何明文或金鑰在不需要使用時，必須將資料清除。	Π	Π
		5.加解密演算法操作	待測物應具備以下加解密演算法操作功能： (1) 待測物應以加解密演算法保護遠端管理連線。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
			(2) 應提供 WPA2 或相同安全等級之保密機制。 (3) 與 Radius Server 之間的連線應以 IPSec 或其他相同等級之安全協定加密保護。		
		6. 殘餘資訊保護	當待測物配置系統資源 (如：資料暫存區) 用之於處理通過之資料封包，應確保該新配置之系統資源的內容已於前次使用歸還時清除，或於本次使用前清除，不致將前次使用之殘餘資訊外洩。	Π	Π
		7. 鑑別失敗處理	待測物應具備以下鑑別失敗處理能力： (1) 可偵測出連續鑑別失敗次數。 (2) 當使用者進行登入，連續鑑別失敗次數達到指定值時，待測物應拒絕該使用者後續之任何登入鑑別要求；該使用者須經管理者解除鎖定後，始可重新登入。	Π	Π
		8. 通行碼管理	待測物應提供下列通行碼管理功能： (1) 通行碼可以由大小寫字元、數字或特殊字元組成。 (2) 通行碼最短長度可由管理人員設定，產品需支援 15 字元以上長度。 (3)通行碼需定期更換；管理者可設定更換週期。 (4) 通行碼更換時至少需有 4 個以上字元更動。	Π	Π
		9. 鑑別機制	待測物應具備以下鑑別機制： (1) 列舉使用者成功完成身分鑑別前，可執行的安全功能 (如：DHCP 或 Show Status 等)。 (2) 除前列之安全功能，使用者應成功完成身分鑑別後，始可執行被授權的安全功能。 (3) 應提供管理者本地通行碼 (Local Password) 鑑別機制。 (4) 通行碼過期時，待使用者成功登入後，待測物應要求使用者立即更新通行碼。 (5) 當使用者更改通行碼時，需重新登入。 (6) 鑑別過程中應避免在顯示器上顯示相關鑑別資訊 (如輸入的通行碼等)。 (7) 需支援 IEEE 802.1X 標準與外界 RADIUS 鑑別伺服器溝通，執行相關鑑別工作。 (8) 與 RADIUS 鑑別伺服器溝通需符合 RFC	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
			2865 和 3579 規範。 (9) 應確保無線用戶在成功完成身分鑑別前，無法透過待測物接取網路。 (10) IPSec 或其他傳輸協議應支援共享金鑰(Pre-shared Key)。 (11) 續上，待測物應支援長度為 22 字元的共享金鑰（可由大小寫英文字母及 “!”、 “@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、和 “)” 等特殊字元所組成）。 (12) 續上，待測物應具備由安全雜湊演算法(Secure Hash Algorithm, SHA) 轉換字元的共享金鑰。 (13) 續上，待測物應有接受或產生亂數位元的共享金鑰功能。 (14) 應支援 RFC 5280 所規範之 X.509 v3 數位憑證功能，協助 IPsec、TLS、SSH 或其他通訊協定進行身分鑑定。 (15) 待測物應儲存並保護憑證使之免於遭受未授權之刪除與修改。 (16) 待測物應支援授權之管理者匯入 X.509 v3 數位憑證功能。		
		10. 安全功能行為管理	只有授權之管理者可管理安全功能相關之資料，以及對任何安全功能進行更動與設定。	Π	Π
		11. 管理功能規格	待測物應具備以下管理功能規格： (1) 提供遠端或本機登入管理功能。 (2) 提供更新待測物韌體之能力，並於韌體更新前能驗證其真偽。	Π	Π
		12. 安全角色	待測物應具備及設定以下安全角色： (1) 經授權的管理者。 (2) 可以賦予使用者管理者之角色。 (3) 管理者可以透過遠端或本機登入系統。但 預設值應禁止遠端登入。	Π	Π
		13. 失效	當待測物於電源啟動後，若自我測試發生錯誤時，應確保金鑰與使用者資料仍處於保護狀態。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
		保全			
		14. 重送攻擊偵測	待測物應具備以下偵測功能： (1) 對通過待測物的網路封包進行重送攻擊偵測。 (2) 當發現重送之封包，應拒絕接收該資料。	Π	Π
		15. 管理者通行碼保護	待測物應具備以下管理者通行碼保護功能： (1) 應避免以明文 (Plaintext) 方式展示通行碼。 (2) 通行碼應以非明文方式儲存。	Π	Π
		16. 可信賴之時戳	待測物應具備可信賴之時戳，正確記錄稽核資料的日期及時間。	Π	Π
		17. 可信賴更新	待測物應具備以下韌體更新功能： (1) 可查詢待測物當前的韌體版本以及目前原廠提供可更新之最新韌體版本。 (2) 管理者可以啟動韌體更新程序。 (3) 需支援一機制，令管理者於韌體更新前，可辨別欲更新韌體之真偽。	Π	Π
		18. 安全功能自我測試	待測物應於啟動後進行安全功能自我測試，以確保其可提供正常服務。待測物必須通過安全功能自我測試才可提供服務。	Π	Π
		19. 最大資源配置	待測物應支援對以下資源上限配置的設定功能: (1) 可同時登入的管理者數量。 (2) 可同時連結 (Associate) 的無線用戶數。	Π	Π
		20. 登入連線之鎖定	若管理者登入後閒置時間超過待測物所允許的閒置時間值，待測物應： (1) 若為本地 (Local) 交談，待測物應鎖定或終止該連線；若為鎖定該連線，待測物應確保顯示資料不造成資訊外洩。同時，欲解除鎖定，待測物應重新進行使用者鑑別。 (2) 若為遠端連線，待測物應立即終止該遠端連線。	Π	Π
		21. 登入連線之終	待測物應允許管理者自行終止已登入之連線。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
		止			
		22. 待測物存取預設標語	待測物應支援管理者可設定之登入注意事項畫面，並於使用者欲登入時顯示此畫面。	Π	Π
		23. 金鑰保護	待測物應具備以下防護措施： (1) 防止共享金鑰、對稱金鑰 (Symmetric Keys) 以及私密金鑰 (Private Keys) 等各種金鑰被讀取。 (2) 不得提供讀取各種金鑰之指令	Π	Π
		24. 待測物交談建立	待測物應能依據地點、時間和日期拒絕無線用戶的交談建立請求。	Π	Π
		25. 可信賴通道	待測物與其他被授權的外部 IT 設備之連線應具備以下防護措施： (1) 應使用 802.11-2007、IPSec、SSH、TLS、TLS/HTTPS 或其他加密之通訊協定，在待測物與其他被授權的 IT 設備 (如，RADIUS Server) 之間提供可信賴通道。 (2) 允許待測物或其他被授權的 IT 設備使用可信賴通道發起連線。 (3) 請列出所有由待測物所發起與被授權的外部 IT 設備之連線。		Π
		26. 可信賴路徑	待測物與遠端管理者的連線應具備以下防護措施： (1) 應使用 IPsec、SSH、TLS、TLS/HTTPS 或其他加密之通訊協定與遠端管理者建立可信賴路徑進行連線，以保護通訊資料免遭修改或揭露。 (2) 管理者可用上述之可信賴路徑於遠端主動發起連線。 (3) 管理者所發起的遠端連線的鑑別與後續通訊，都必須透過可信賴路徑進行。		Π

6.2.2. 安全功能設計

申請者應提供待測物安全功能規格、設計安全性、安全架構及安全指引等文件，以確保安全功能 (TSF) 能正確執行。

6.2.2.1. 安全功能規格

本項書面審查內容依申請者提供之附件一、安全功能規格表，檢視安全功能規格之內容是否符合附表 1-3 安全功能規格之書面審查內容。

附表 1-3 安全功能規格之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全功能規格	安全功能介面應實現安全功能需求，應說明安全功能介面 (TSFI) 以下規格： (1) 安全功能介面名稱。 (2) 目的。 (3) 可實現的安全功能需求。 (4) 操作方式。 (5) 參數。 (6) 執行的動作。 (7) 錯誤訊息。	Π	Π

6.2.2.2. 設計安全性

本項書面審查內容依申請者提供之附件二、設計安全性表，檢視設計安全性之內容是否符合附表 1-4 設計安全性之書面審查內容。

本項書面審查內容與判定標準說明如附表 1-4：

附表 1-4 設計安全性之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能	設計安全	應說明如何以子系統組成安全功能規格之安全功能介面，並說明安全功能子系統以下規格：		Π

類別	項目	審查標準	基礎型	進階型
設計	性	(1) 子系統名稱。 (2) 目的。 (3) 子系統隸屬之安全功能介面。 (4) 子系統行為說明。		

6.2.2.3. 安全架構

本項書面審查內容依申請者提供之附件三、安全架構表，檢視安全架構之內容是否符合附表 1-5 安全架構之書面審查內容。

本項書面審查內容與判定標準說明如附表 1-5：

附表 1-5 安全架構之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全架構	應依據 6.2.2.1. 安全功能規格及 6.2.2.2. 設計安全性之檢附文件，說明待測物安全架構如何滿足安全功能需求 (SFR)，並作為實機測試項目設計的參考。針對安全功能介面及子系統，提出安全架構的設計概念與操作安全建議，也需符合後續提供的指引文件。安全架構應說明下列項目： (1) 待測物因執行安全功能所區隔的安全領域。 (2) 安全功能的安全初始程序。 (3) 安全功能的自我保護機制。 (4) 安全功能執行如何避免被繞道。		Π

6.2.2.4. 安全指引

本項書面審查內容依申請者提供之指引文件，檢視文件內容是否符合

附表 1-6 安全指引之書面審查內容。

本項書面審查內容與判定標準說明如附表 1-6：

附表 1-6 安全指引之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全指引	(1) 應定義每個使用者角色。 (2) 應提供每個使用者角色於執行安全功能 (TSF) 時之相關說明，包括： A. 週邊設備及安全設定。 B. 允許使用的介面。 C. 安全參數定義。 D. 可能產生的安全事件。 E. 應遵循的安全措施。 (3) 應說明於特殊權限操作時的安全環境要求，並提供適當的警告。 (4) 應列舉待測物操作時的所有運作模式。 (5) 應列舉待測物作業失敗 (Failure) 或人員操作錯誤產生的各種情況及處理方式。 (6) 應說明待測物運作前的安全準備作業，包含待測物安裝及啟動方式。 (7) 應說明待測物操作的安全環境設置，應包括以下項目： A. 待測物使用目的 (如：針對伺服器進行網路協定管制作業等)。 B. 實體環境安全 (如：待測物置於具備門禁管制的環境等)。 C. 人員安全 (如：僅有授權人員可存取待測物	Π	Π

類別	項目	審查標準	基礎型	進階型
		等)。 D. 連接安全 (如：待測物與其他網路伺服器之連線安全等)。 (8) 指引文件將做為實機測試的依據。		

6.3. **實機測試類別**

實機測試包含安全功能測試、壓力測試、堅實測試及穩定測試。

6.3.1. 安全功能測試 (Security Functionality Test)

測試待測物所具有安全防護相關功能

6.3.2. 壓力測試 (Stress Test)

測試待測物面臨大量網路封包或連線時，安全功能是否能保持正常運作。

6.3.3. 堅實測試 (Robustness Test)

測試待測物本身開啟服務或協定時，面臨針對待測物本身而來的不正常連線行為，是否能保持正常運作。

6.3.4. 穩定測試 (Stability Test)

將待測物置於真實網路流量下運作測試，是否有不穩定的狀況發生。

6.4. **實機測試類別之項目及判定標準**

實機測試分為基礎型與進階型，皆包含安全功能測試、壓力測試、堅實測試及穩定測試四個類別。實機測試項目及標準如表 2。

表 2　實機測試之類別、項目及判定標準

類別	項目	判定標準	基礎型	進階型
安全功能測試	稽核資料產出	依 6.4.1.1.2. (1) 進行測試，待測物產出之稽核資訊應具備： (1) 是否成功啟動稽核功能，包含未被明確定義/指定等級稽核。 (2) 所有可稽核之事件。 (3) 所有可管理之行為。 (4) 將發生的稽核事件與使用者之間進行關聯性連結。 (5) 紀錄事件的日期、時間、類別、主題識別碼及結果（成功或失敗）。 依 6.4.1.1.2. (2) 進行測試，待測物的安全功能應支援選擇性的稽核的事件集。	Π	Π
	外部稽核伺服器失去連線的應變措施	依 6.4.1.2.2. 進行測試，如外部稽核伺服器失去連線時，待測物應進行一些處置行為或新任務指派。	Π	Π
	重送攻擊偵測	依 6.4.1.3.2. 進行測試，待測物應支援： (1) 偵測出重送至待測物的網路封包。 (2) 應拒絕重送封包的連線要求。	Π	Π
	可信賴更新	依 6.4.1.4.2. 進行測試，待測物應具備下列韌體更新功能： (1) 允許被授權的管理者查詢待測物目前韌體版本。 (2) 允許被授權的管理者更新韌體版本。 (3) 在安裝更新前使用電子簽章機制，於韌體更新前，可辨別欲更新韌體之真偽。	Π	Π

類別	項目	判定標準	基礎型	進階型
	待測物安全功能自我測試	依 6.4.1.5.2. 進行測試，待測物應於啟動後進行安全功能自我測試。	Π	Π
	鑑別失敗控制功能	依 6.4.1.6.2. 進行測試，待測物應具備下列功能： (1) 使用正確之通行碼應可正常登入。 (2) 當輸入錯誤通行碼超過最大錯誤次數且封鎖管理介面後，使用正確通行碼亦無法登入待測物。	Π	Π
	使用者識別及授權功能	依 6.4.1.7.2. 進行測試，待測物應具備下列功能： (1) 輸入正確的帳號及通行碼方能登入。 (2) 使用錯誤帳號或通行碼時，應提示使用者無法登入的訊息。 (3) 需要驗證使用者帳號及通行碼的網路服務，應輸入正確的帳號及通行碼，方能存取這些服務。	Π	Π
	檢查通行碼逾期功能	依 6.4.1.8.2. 進行測試，如通行碼逾期時，應強迫登入者更換通行碼，方能進行後續操作。	Π	Π
	通行碼重新鑑別功能	依 6.4.1.9.2. 進行測試，變更通行碼後，待測物應要求使用者重新登入方能進行後續操作。	Π	Π
	登入畫面保密功能	依 6.4.1.10.2. 進行測試，登入過程中，待測物之顯示畫面應以特殊號 (如： “*”) 遮蔽輸入之明文通行碼字元。	Π	Π
	802.1X 使用者識別及鑑別功	依 6.4.1.11.2. 進行測試，通過 RADIUS Server 鑑別後，應可經由待測物連上網際	Π	Π

類別	項目	判定標準	基礎型	進階型
	能	網路。		
	安全功能行為管理	依 6.4.1.12.2. 進行測試，待測物應允許管理者正確輸入通行碼後登入進行設定。	Π	Π
	資源最大配額	依 6.4.1.13.2. 進行測試，待測物應支援： (1) IP 位址個數未達到最大值，輸入正確的無線連線帳號及通行碼時可以與待測物建立連線。 (2) IP 位址個數達到最大值，即使輸入正確的無線連線帳號及通行碼時亦不可與待測物建立連線。 (3) 登出後，待測物應可以收回原先指派之 IP 位址供下次使用。	Π	Π
	登入連線之鎖定	依 6.4.1.14.2. 進行測試，當鎖定計時之時間到達期限時，使用者應無法讀取待測物任何資訊。當終止計時之時間到達期限，應立即終止本次會談 (Session)。	Π	Π
	登入連線之終止	依 6.4.1.15.2. 進行測試，當使用者登出後，與待測物建立的連線應立即中斷。	Π	Π
壓力測試	吞吐量	依 6.4.2.1.2. 進行測試，當待測物所負荷的吞吐量達到其規格說明之最大值時，不能發生封包遺失且安全功能應正常運作。		Π
堅實測試	異常流量測試	依 6.4.3.1.2. 進行測試，待測物遠端管理介面對異常之協定或攻擊流量應保持正常運作。	Π	Π
	非正常關機恢復	依 6.4.3.2.2. 進行測試，待測物應可重新開機復原到斷電前的最後正常狀態。		Π
穩定	真實流量	依 6.4.4.1.3. 進行測試，待測物應持續 168	Π	

類別	項目	判定標準	基礎型	進階型
測試		小時穩定運作。		
		依 6.4.4.1.3. 進行測試，待測物應持續 336 小時穩定運作。		Π

6.4.1. 安全功能測試

檢視待測物之安全功能需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.4.1.1. 稽核資料產出

6.4.1.1.1. 測試環境

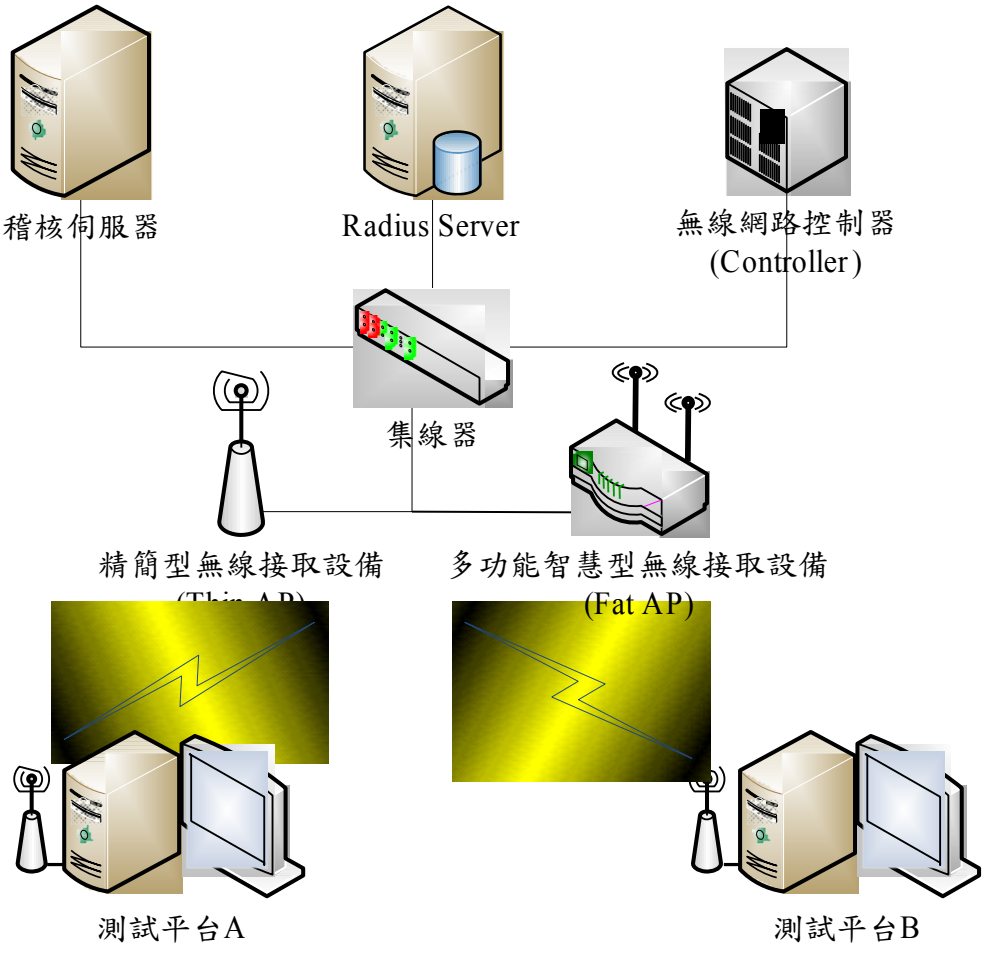

圖 1　稽核測試接續示意圖

(1) 測試平台 A：模擬被授權存取的無線用戶 A。

(2) 測試平台 B：模擬被授權存取的無線用戶 B。

(3) 待測物：精簡型無線接取設備 + 無線網路控制器的組合，或是多功能智慧型無線接取設備。

(4) RADIUS Server：提供 RADIUS 功能的伺服器。

(5) 稽核伺服器：提供記錄稽核事件功能的伺服器。

(6) 集線器：匯集多條通訊纜線之裝置。

(7) 網路連接線：乙太網路線或光纖纜線。

(8) 連接測試平台 A、測試平台 B、待測物、無線網路控制器、稽核伺服器及 Radius Server 如圖 1。

(9) 開啟待測物稽核功能及外部稽核伺服器的相關設定。

6.4.1.1.1. 測試方法及標準

(1) 稽核伺服器上有關管理上的操作及相關資訊應被紀錄且須產出下列稽核資訊：

A. 稽核功能啟動成功與否。

B. 所有可稽核的事件，包含未被明確定義/指定等級稽核。

C. 所有管理行為。

D. 將發生的稽核事件與使用者進行關聯性連結。

E. 事件的日期、時間、類別、主題識別碼及結果（成功或失敗）。

(2) 應支援選擇性的稽核事件集並根據下列屬性，在所有可稽核事件的列表中進行稽核：

A. 管理者身分鑑別。

B. 事件類型。

C. 可稽核安全事件的成功通知。

D. 可稽核安全事件的成功與否。

E. 其它待測物規格說明書所列舉之事件。

6.4.1.1. 外部稽核伺服器失去連線的應變措施

6.4.1.1.1. 測試環境

同圖 1。

6.4.1.1.2. 測試方法及標準

如外部稽核伺服器失去連線時，待測物應進行一些處置行為或新任務指派。

6.4.1.2. 重送攻擊偵測

6.4.1.2.1. 測試環境

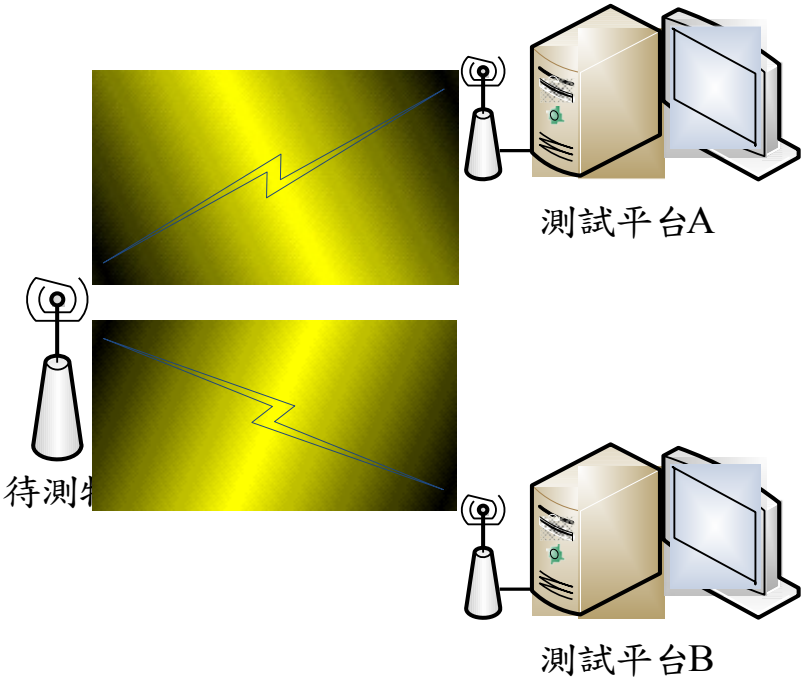

圖 2　重送攻擊偵測接續示意圖

(1) 測試平台 A 及測試平台 B：具備無線介面之測試儀器。

(2) 待測物：精簡型無線接取設備 + 無線網路控制器的組合，或是多功能智慧型無線接取設備。

(3) 透過無線方式連接測試平台與待測物如圖 2。

(4) 以測試平台 B 模擬一惡意使用者 B 在訊號範圍內開啟無線網卡監聽模式，並以測試平台 A 模擬同一頻段中另一使用者 A，當取得使用者 A 與待測物間傳送 的封包內容及相關資訊後，惡意使用者 B 偽裝成使用者 A 並注入偽造的 Deauth 的指令至待測物，企圖中斷使用者 A 與待測物間的連線。

6.4.1.1.1. 測試方法及標準

待測物的安全功能需滿足下列條件：

(1) 應偵測出惡意使用者重送至待測物的網路封包。

(2) 偵測出重送之網路封包後，應拒絕該封包的連線要求。

6.4.1.1. 可信賴更新

6.4.1.1.1. 測試環境

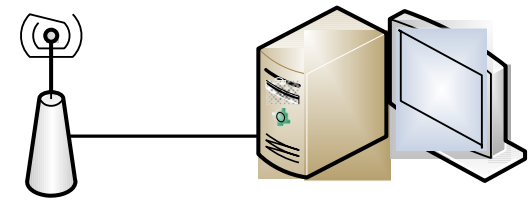

圖 3　可信賴更新測試接續示意圖

(1) 測試平台：可連線至待測物之測式儀器或程式。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接測試平台及待測物如圖 3。

(4) 開啟待測物安全管理功能。

6.4.1.1.1. 測試方法及標準

待測物的安全功能應滿足下列條件：

(1) 被授權的管理者登入後，可以查詢待測物內部韌體版本資訊及更新內部韌體版本。

(2) 在安裝更新前須通過待測物之電子簽章機制驗證，如驗證失敗，應拒絕執行該次更新操作。

6.4.1.1. 待測物安全功能自我測試

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 開啟待測物安全事件紀錄之功能。

(2) 將待測物重新啟動，應於開機前進行自我檢測，並於開機

後進行安全功能自我測試。

6.4.1.1. 鑑別失敗控制功能

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

開啟待測物之安全管理功能，並依其規格說明提供之功能，以下列方法擇一進行測試。

(1) 方法一 (待測物提供 Quiet Period 功能)：

A. 應輸入正確通行碼才能對待測物進行管理設定。

B. 輸入錯誤通行碼，待測物應檢查是否超過最大錯誤次數時，如超過最大錯誤次數，則應封鎖管理介面一段時間 (Quiet Period) 以避免遭受攻擊。於管理介面封鎖期間內即便使用正確的通行碼亦無法登入待測物之管理介面。

C. 靜置待測物一段時間，不對待測物進行任何操作，直到 Quiet Period 逾時，使用正確的通行碼應可正常登入管理介面。

(2) 方法二 (待測物永久鎖定登入管理介面)：

A. 應輸入正確通行碼才能對待測物進行管理設定。

B. 輸入錯誤通行碼，待測物應檢查是否超過最大錯誤次數時，如超過最大錯誤次數，則應封鎖管理介面以避免遭受攻擊。封鎖登入管理介面後，即便使用正確的通行碼亦無法登入待測物之管理介面。

C. 根據待測物使用手冊的說明步驟，解除管理介面之封鎖。解除後，輸入正確通行碼應能正常登入管理介面。

6.4.1.1. 使用者識別及授權功能

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 應輸入正確通行碼才能登入待測物，如使用錯誤帳號通行碼時，應提示使用者無法登入的訊息。

(2) 開啟待測物需要驗證使用者帳號及通行碼的網路服務，應於輸入正確的帳號及通行碼後，方能存取這些服務並進行後續操作。

6.4.1.1. 檢查通行碼逾期功能

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 開啟待測物之檢查通行碼逾期功能。

(2) 輸入已逾期的通行碼進行登入程序。

(3) 待測物應提示通行碼已逾期，並強制更換新的通行碼，否則無法繼續對待測物進行任何操作。

6.4.1.1. 通行碼重新鑑別功能

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 開啟待測物之安全管理功能。

(2) 完成登入程序後立即更換通行碼。

(3) 待測物應要求以新通行碼重新登入後，方能進行後續操作。

6.4.1.1. 登入畫面保密功能

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 開啟待測物之安全管理功能。

(2) 輸入帳號及通行碼進行登入。

(3) 登入過程中，待測物之使用者介面應以特殊代號 (如：“*”) 遮蔽輸入的明文通行碼字元。

6.4.1.1. 802.1X 使用者識別及鑑別功能測試

6.4.1.1.1. 測試環境

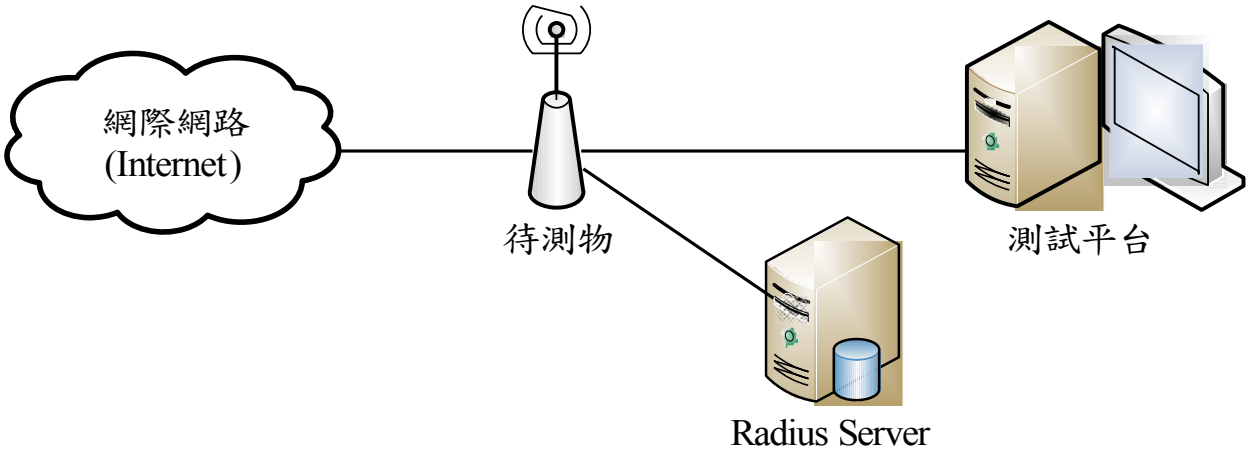

圖 4　802.1X 使用者識別及鑑別功能測試接續示意圖

(1) 測試平台：可供測試人員連線至待測物及網際網路之測試儀器。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) RADIUS Server：提供 RADIUS 功能的伺服器。

(4) 待測物：精簡型無線接取設備 + 無線網路控制器的組合，或是多功能智慧型無線接取設備。

(5) 連接測試平台及待測物如圖 4。

(6) 開啟待測物之 802.1X 存取鑑別功能。

6.4.1.1.1. 測試方法及標準

(1) 尚未 RADIUS Server 的鑑別前，應無法透過待測物連上 Internet。

(2) 通過 RADIUS Server 的鑑別後，應可透過待測物連上 Internet。

(3) 如使用錯誤的 Client 端數位憑證進行 EAP-TLS 鑑別，EAP-TLS 鑑別應無法順利進行且無法透過待測物連上 Internet。

(4) 如使用錯誤的 RADIUS 端數位憑證進行 EAP-TLS 鑑別，EAP-TLS 鑑別應無法順利進行且無法透過待測物連上 Internet。

6.4.1.1. 安全功能行為管理

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 以管理者身分透過 console 埠、IPsec、SSH、TLS/HTTPS 或無線介面登入待測物，管理者應輸入正確通行碼後方能進行後續操作。

(2) 正確登入後，管理者應可正確設定各項安全功能設定。

6.4.1.1. 資源最大配額

6.4.1.1.1. 測試環境

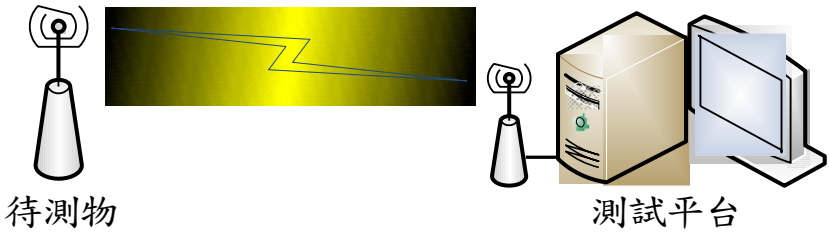

圖 5　安全管理測試接續示意圖

(1) 測試平台：可模擬無線用戶之測式儀器或程式。

(2) 待測物：Thin AP + Controller 的組合或 Fat AP。

(3) 透過無線之方式連接測試平台及待測物如圖 5。

6.4.1.13.2. 測試方法及標準

(1) 開啟待測物指派 IP 位址之功能並設定固定時間內可以指派的 IP 位址個數。

(2) 當指派之 IP 位址個數尚未達到規格說明所列之最大值時，輸入正確的連線帳號及通行碼應可建立無線傳輸之連線。此時，待測物應指派一個新 IP 位址給用戶端且可用的 IP 位址個數應自動減少一個。

(3) 測試平台模擬用戶經無線介面使用 IPSec、SSH、TLS 或 HTTPS 連至待測物，如指派之 IP 位址個數達到最大值，即使輸入正確的連線帳號及號通行碼應無法與待測物建立連線。

(4) 當無線用戶登出後或離線後，待測物應收回原先指派之 IP 位址，且可用之 IP 位址個數應自動加一。

6.4.1.1. 登入連線之鎖定

6.4.1.1.1. 測試環境

同圖 3。

6.4.1.1.2. 測試方法及標準

(1) 開啟待測物之登入連線鎖定功能。

(2) 指定待測物自動鎖定 (Lock) 之計時時間值或自動終止 (Terminate) 之計時時間值。

(3) 由測試平台以 IPSec、SSH、TLS 或 HTTPS 方式連至待測物，並輸入正確之帳號及通行碼。

(4) 成功登入後如無任何操作，鎖定之計時應自動啟動。當時間到達設定之期限應無法讀取待測物任何資訊，除非重新登入成功，否則無法繼續對待測物進行任何操作。

(5) 成功登入後如無任何操作，終止之計時應開始啟動，當時間到達設定之期限，此次會談應立即終止。

6.4.1.1. 登入連線之終止

6.4.1.1.1. 測試環境

同圖 5。

6.4.1.1.2. 測試方法及標準

(1) 輸入正確之使用者帳號及通行碼後應可登入待測物。

(2) 當使用者登出後，與待測物建立的連線應立即中斷。

6.4.1. 壓力測試

6.4.1.1. 吞吐量測試

6.4.1.1.1. 測試環境

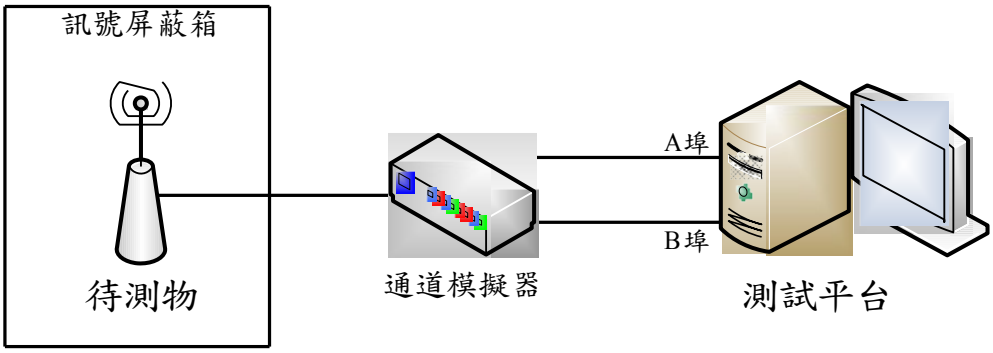

圖 6　吞吐量測試接續示意圖

(1) 測試平台：可產生網路封包之測試儀器或程式。

(2) 測試平台 A 埠：模擬用戶端收送網路封包。

(3) 測試平台 B 埠：模擬伺服器端收送網路封包。

(4) 通道模擬器：模擬無線通訊環境可將有線訊號轉換成無線訊號。

(5) 訊號遮蔽箱：可遮蔽無線訊號之裝置。

(6) 網路連接線：乙太網路線或光纖纜線。

(7) 連接測試平台、通道模擬器及待測物如圖 6。

(8) 開啟待測物之安全功能。

(9) 測試平台產生大小為 64、570、594 及 1518 位元組之網路封包， 並依 IMIX 之比例 57%、7%、16%及 20%混合，時間為 60 秒。

6.4.1.1.1. 測試方法及標準

測試平台建立自 A 埠經待測物至 B 埠之網路連線後，開始傳送不同大小之封包。當待測物所負荷的吞吐量達到其規格說明之最大值時，待測物安全功能應正常運作。

6.4.2. 堅實測試

6.4.2.1. 異常流量測試

6.4.2.1.1. 測試環境

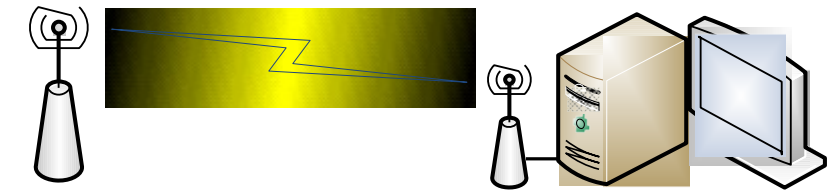

圖 7　異常流量測試接續示意圖

(1) 測試平台：可產生各種異常或攻擊流量之測試儀器或程式。

(2) 以無線方式連接測試平台及待測物如圖 7。

6.4.1.1.1. 測試樣本

以測試平台分別產生下列 8 種類型之異常或攻擊流量。

攻擊類型	行為描述
(1) 802.11 關聯/鑑別氾濫式攻擊 (802.11 Associate / Authenticate Flood)	從隨機產生的 MAC 表中大量傳送偽冒的鑑別或關聯資訊。
(2) 802.11 TKIP MIC 弱點攻擊(802.11 TKIP MIC Exploit)	產生不合法的 TKIP 資料造成目標物 AP 的 MIC 錯誤超過上限值，進而使其無法正常提供服務)。
(3) 802.1X EAP-Start 氾濫式攻擊 (802.1X EAP-Start Flood)	不斷傳送 EAP-Start 訊息來消耗目標的資源或使其癱瘓。
(4) 802.1X EAP-of-Death 攻擊 (802.1X EAP-of-Death)	傳送變形的 802.1X EAP 鑑別回應訊息，使得某些 AP 持續鑑別此資訊進而造成癱瘓。
(5) 802.1X EAP 長度攻擊 (802.1X EAP Length Attacks)	傳送符合 EAP 型態但長度不正確的訊息，進而利用此訊息癱瘓目標物 AP 或 RADIUS 伺服器。
(6) 變形的 Frame-Assoc 請求 (Malformed Frame-Assoc Request)	產生一個含有空白 SSID 的惡意關聯請求用以癱瘓目標物。
(7) 變形 Frame-Auth (Malformed Frame-Auth)	以變形的 802.11 鑑別框架試探目標物的弱點。
(8) 虛擬 Carrier-Sense 攻擊 (Virtual Carrier-Sense Attack)	利用長時間出現之 ACK, data, RTS 及 CTS 框架，阻礙合法使用者正常存取頻道。

6.4.1.1.2. 測試方法及標準

測試平台送出異常或攻擊流量至待測物，待測物之遠端管理功能應正常運作。

6.4.1.2. 非正常關機恢復

6.4.1.2.1. 測試環境無

6.4.1.2.2. 測試方法及標準

待測物運作期間不正常關閉電源時，經重新啟動後，應復原到非正常關閉電源前的狀態且須符合下列要求：

(1) 應保留最後設定的系統組態。

(2) 應保留斷電時間點前最後 5 分鐘的日誌檔案 (含系統日誌及安全事件日誌)。

(3) 能以最後設定的系統組態正常開機。

6.4.1. 穩定測試

6.4.1.1. 真實流量

在一般使用者上線的真實運作之網路，以場測方式進行測試，或將真實網路流量錄製後，再以重播之方式進行測試。

6.4.1.1.1. 測試環境

(1) 流量錄製平台：錄製網路封包。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接流量錄製平台、路由器、內部網路及網際網路如圖 8。

(4) 路由器將往來 A、B 兩埠的網路封包複製一份後，經 C 埠送至流量錄製平台，流量錄製平台將網路封包錄製成為檔案儲存。

(5) 流量重播平台：具備無線介面之重播設備，能將預先錄製之真實流量檔案還原成網路封包送至待測物。

(6) 連接流量重播平台與待測物如圖 9。

(7) 流量重播平台將網路流量透過無線界面重播至待測物。

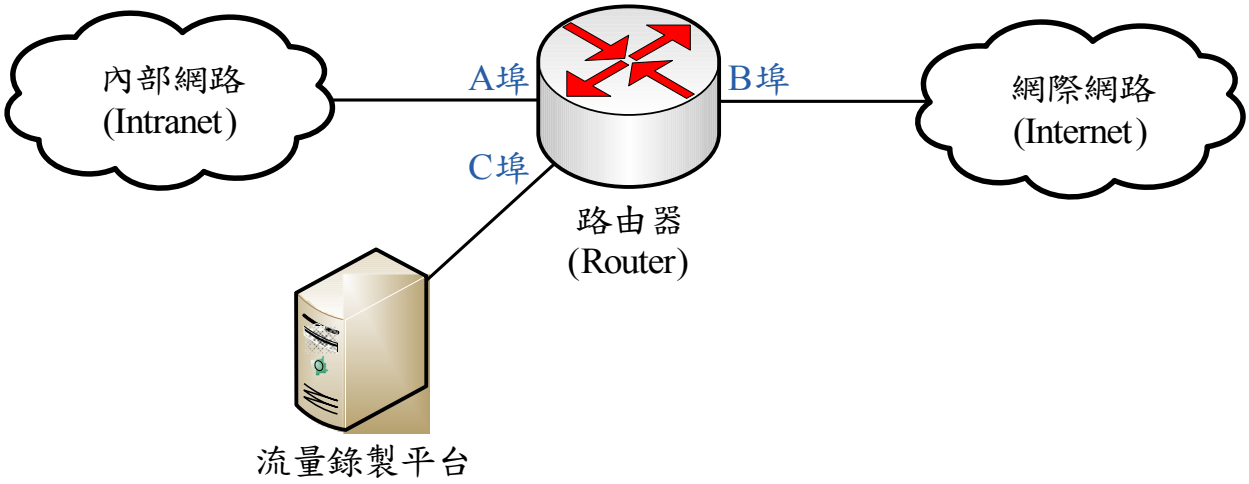

圖 8　流量錄製接續示意圖

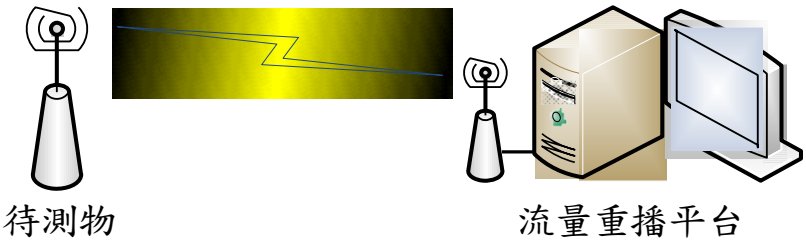

圖 9　流量重播接續示意圖

6.4.1.1.1. 測試樣本

測試樣本必須滿足以下要求：

(1) 具備至少 100 位使用者同時上線之網路環境。

(2) 若以重播方式進行測試，所使用之網路流量必須為送測日前 2 周內從真實網路環境所錄製之流量。

(3) 重播之網路流量其最大同時連線數於測試期間必須達待測物規格說明處理能力最大值之 50%以上。

(4) 重播之網路流量須以線性放大或縮小以維持波形，並使其平均流量為待測物規格說明處理能力最大值之 50%。

(5) 流量內容須涵蓋 10 種以上之應用類型並包含 smtp、pop3、imap、ftp、smb、http、https、dns 及 snmp 等應用項目，全部之應用項目須達 50 個以上。應用項目舉例如下:

A. Chat：　msn、yahoo messenger、qq、xmpp 及 aol-icq。

B. Email：gmail、smtp、pop3、imap 及 webmail。

C. File Transfer：ftp、flashget 及 smb。

D. Game：garena、facebook app 及 steam。

E. P2P：gnutella、edonkey、bt、xunlei、fasttrack、ares、kazaa 及 ed2k。

F. Remote Access：windows remote desktop、telnet、ssh 及 vnc。

G. Streaming：rtsp protocol, qqtv, pplive, qvod, flashcom, itunes, funshion

H. Web：http, http download, http video, http range get, https, http proxy

I. Others：sslvpn, nntp protocol, dns protocol, snmp protocol, dhcp protocol, mysql, ntp protocol

6.4.1.1.1. 測試方法及標準

(1) 基礎型待測物應進行連續 168 小時測試；進階型待測物應進行連續 336 小時測試。

(2) 測試過程不能發生下列不穩定之情況：

A. 當機。
B. 重新開機。
C. 連線不正常中斷。
D. 安全功能失效。

附錄

附錄一、安全功能介面表

安全功能介面名稱 **TSFI**	**目的** **Purpose**	**安全功能介面可實現之安全功能需求** **SFR**	**操作方式** **Method of Use**	**參數** **Parameter**	**執行動作** **Actions**	**錯誤訊息** **Error Message**
列出所有安全功能介面。	說明各安全功能介面之安全功能目的。	說明各安全功能介面如何實現附表 1-2 所列之安全功能需求。	說明如何使用各安全功能介面。	說明各安全功能介面所有參數及其意義。	說明各安全功能介面如何運作及其執行細節。	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。
範例： *TSFI_CLI*	*範例：* *提供命令列模式操作介面*	*範例：* *SFR_安全管理：提供安全管理功能*	*範例：* *以 ssh 連接待測物，即提供命令列模式操作介面*	*範例：* *ID & password*	*範例：* *可下達管理命令操作待測物*	*範例：* *連接失敗* *鑑別失敗*

附錄二、子系統描述與分類表

子系統名稱 Subsystem	目的 Purpose	子系統隸屬之安全功能介面 TSFI	子系統行為說明 Behavior Description
列出各安全功能介面之子系統。	說明各子系統之安全功能目的。	說明各子系統隸屬於附件一所列之安全功能介面。	說明各子系統行為如下： (1) 如何實現安全功能介面的功能。 (2) 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。
範例： *Subsystem_ssh*	*範例：* *提供 ssh 服務*	*範例：* *TSFI_CLI*	*範例：* *(1)提供 TSFI_CLI 命令列模式操作介面* *(2)與其他子系統之互動：* *(A) Subsystem_auth: 傳遞鑑別資訊給 Subsystem_auth，並由回覆訊息確認鑑別是否成功* *(B) Subsystem_terminal: ...*

附錄三、安全架構描述表

項目	說明	
1.安全領域	**安全領域名稱**	**安全領域說明**

項目	說明	
Security Domain	列出各安全功能介面對應之安全領域 *範例：* *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：* *透過 TSFI_GUI 來執行管理功能時，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*
2.初始程序	**相關元件**	**初始程序說明**

項目	說明		
Secure Initialization	操作待測物的相關元件/環境 *範例：* *待測物網路連接程序*	提供安全啟動待測物之相關元件起始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/0（ethernet0/0 接口）連接一個 RJ-45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/1（ethernet0/1 接口）連接一個 RJ-45 電纜到交換機或路由器中的 DMZ 安全區。*	
3.自我保護	**自我保護功能**	**與外部設備之關係**	**自我保護機制說明**

項目	說明		
Self-Protection	列出各安全功能介面對應之自我保護機制 *範例：* *TSFI_WEB:* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密*	說明安全功能及其介面與外部設備之資料交換動作 *範例：* *遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證*	需說明安全功能介面提供實體上或邏輯上的自我保護機制 *範例：* *1. 應輸入通行碼才能進入介面。* *2. 資料傳輸機制：TLS/SSL。* *3. 特殊執行方式：指紋辨識。* *4. 特殊設備需求：指紋辨識器。*
4.防止繞道	**防止繞道功能**	**防止繞道機制說明**	

項目	說明	
Non-Bypassibility	列出各安全功能對應之防止繞道機制 *範例：* *TSF_Authentication 身分驗證功能*	1. 列舉可能繞道之手法 2. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：* *可能直接以維護介面不經身分鑑別操控待測物。* *防範作法：以實體封鎖方式，防止利用維護介面繞道身分鑑別程序。*