無線區域網路接取設備及路由設備

資通安全檢測技術指引

中華民國 107 年 10 月 16 日

目　次

1. 前言 1

2. 適用範圍 1

3. 引用標準 1

4. 用語釋義 3

5. 檢測方式及安全等級 7

6. 書面審查合格標準 9

7. 實機測試合格標準 17

表　次

表一、書面審查之檢測項目及對應之安全等級與適用設備 7
表二、實機測試之檢測項目及對應之安全等級與適用設備 8
表三、設備概述說明 32
表四、安全功能說明 33
表五、安全架構描述表 36
表六、安全功能介面表 38
表七、安全指引文件 39
表八、子系統描述與分類表 44

圖　次

圖一、待測物示意圖（精簡型 Wi-Fi AP） 4
圖二、待測物示意圖（多功能智慧型 Wi-Fi AP、路由器） 4
圖三、事件紀錄測試測試環境示意圖 17
圖四、管理者預設密碼安全測試環境示意圖 18
圖五、使用者鑑別與管控功能測試測試環境示意圖 20
圖六、網際網路流量管制功能測試測試環境示意圖 24
圖七、區域網路流量管制功能測試測試環境示意圖 25
圖八、吞吐量測試測試環境示意圖 26
圖九、共通弱點評估測試測試環境示意圖 29
圖十、動態分析測試測試環境示意圖 31

無線區域網路接取設備及路由設備資通安全檢測技術指引

1. 前言

為確保無線區域網路接取設備（Wireless Local Area Network Access Point）及無線區域網路路由設備(Wireless Local Area Network Router, WLAN Router）之連網資安品質，爰訂定本指引。

2. 適用範圍

本指引適用於嵌入式韌體之無線區域網路接取設備（以下簡稱 Wi-Fi AP）及無線區域網路路由設備（以下簡稱路由器），且支援開放系統互連參考模型（Open System Interconnection Reference Model，OSI）網路架構。

3. 引用標準

本指引參考標準如下，測試項目與相關國際標準對照詳附錄一及附錄二。

3.1. Collaborative Protection Profile forNetwork Devices，Version 2.0，2017/05，NIAP。

3.2. ISO/IEC 15408（Common Criteria for Information Technology Security Evaluation， CC），Version 3.1. Revision 5，2017/04，CCRA。

3.3. LABS Test Methodology - Wireless Networking，Version 1，2016/12，NSS。

3.4. Network Device Collaborative Protection Profile （NDcPP） Extended Package-Wireless Local Area Network（WLAN）Access Systems，Version 1.0，2015/05，NIAP。

3.5. Protection Profile for Wireless Local Area Network （WLAN） Access Systems，Version 1.0，2011/12，NIAP。

3.6. Recommended cryptographic measures - Securing personal data，2013/09，ENISA。

3.7. Special Publication 800-53Security and PrivacyControls forFederal Information Systemsand Organizations，Revision 4，2013/04，NIST。

3.8. Special Publication 800-63B Digital Identity Guidelines-Authentication and Lifecycle Management，2017/06，NIST。

3.9. Special Publication 800-92 Guide to Computer Security Log Management，

2006/04，NIST。

3.10. Special Publication 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i，2007/02，NIST。

3.11. Special Publication 800-193（DRAFT） Platform Firmware Resiliency Guidelines，2017/05，NIST。

3.12. Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements，Version 1.0，2017/07，UL 2900-1。

3.13. 行動應用 APP 基本資安規範，Version 1.1，2017/03，經濟部工業局。

3.14. 影像監控系統資安標準—第一部：一般要求（TAICS TS-0014-1, v1.0），2018/06，台灣資通產業標準協會。

4. 用語釋義

4.1. 開放系統互連參考模型（Open System Interconnection Reference Model，OSI）

指國際標準組織於 1983 年制定之開放式系統互連參考規定，依通訊協定屬性，分為實體層（Physical Layer）、資料連接層（Data Link Layer）、網路層（Network Layer）、傳輸層（Transport Layer）、會議層（Session Layer）、展示層（Presentation Layer）及應用層（Application Layer）等七層架構。

4.2. 韌體 （Firmware）

指嵌入在硬體裝置中的軟體。主要是將程式碼或資料寫入在唯讀記憶體內。

4.3. 共同準則（Common Criteria，CC）

指國際資通安全產品評估及驗證之標準（ISO/IEC 15408），用以評估及驗證資通安全產品之安全等級與功能性，其評估保證等級（Evaluation Assurance Level，下稱 EAL）分為 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7。

4.4. 安全標的（Security Target, ST）

指待測物符合保護剖繪或特定安全功能需求之規格文件。

4.5. 保護剖繪（Protection Profile, PP）

指待測物應具備之安全基本需求文件。

4.6. 安全功能（TOE Security Functions, TSF）

指待測物實現安全標的（ST）所列安全規格之功能。

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

指依「共同準則第二部：安全功能需求」所列 TSF 相關規定，陳述評估標的應具備之安全功能。

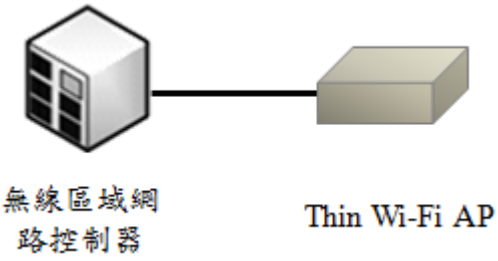
4.8. 評估標的（Target of Evaluation，TOE）

指待測物。即下列任一型態之設備（示意圖如圖一及圖二）：

（1）精簡型 Wi-Fi AP（Thin Wi-Fi AP）與無線區域網路控制器的組合，或

（2）多功能智慧型 Wi-Fi AP（Fat Wi-Fi AP），或

（3）路由器。



圖一、待測物示意圖（精簡型 Wi-Fi AP）

圖二、待測物示意圖（多功能智慧型 Wi-Fi AP、路由器）

4.9. 精簡型 Wi-Fi AP（Thin Wi-Fi AP）

指待測物的設定組態並非存在於設備本身，而是透過網路連接的方式向無線區域網路控制器索取設定組態。

4.10. 無線區域網路控制器（Wi-Fi Controller）

指作為核心管理之網路設備，以集中化方式控制無線區域網路內同廠牌之可控制 Thin Wi-Fi AP。

4.11. 多功能智慧型 Wi-Fi AP（Fat Wi-Fi AP）

指待測物的設定組態由設備本身自行控制，通過身分認證許可的使用者可直接存取無線區域網路並瀏覽網路上資料。

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

指待測物實現安全功能需求對外溝通之介面。

4.13. 稽核伺服器

提供遠端存放記錄稽核事件記錄功能的伺服器。

4.14. 動態分析（Dynamic Analysis）

指觀察啟動之設備是否有任何已知惡意程式或透過網路來傳送資料到未知的 IP 位址。

4.15. IPSec（InternetProtocolSecurity）

指 OSI 網路層之端對端相互鑑別及交換金鑰安全所設計之加密通訊協定。

4.16. SSH（Secure Shell）

指在應用層上，為提供遠程登入安全性所設計之加密通訊協定。

4.17. TLS（TransportLayerSecurity）

指在傳輸層上，為提升 SSL 數據安全性及完整性防護所設計之加密通訊協定。

4.18. HTTPS（Hypertext Transfer Protocol Secure）

指利用 SSL/TLS 加密方式，提供網頁瀏覽器安全及使用者身分鑑別之加密通訊協定。

4.19. SSL（Secure Sockets Layer）

指為確保 OSI 應用層之應用程式保密性及可靠性所設計之加密通訊協定。

4.20. IEEE 802.1x

指在資料連接層上，鑑別使用者身分之網路安全標準。

4.21. RFC（Request For Comments）

指網際網路工程任務編組（IETF）為發展網際網路所公布之一系列文件。

4.22. ITU X.509（以下簡稱 X.509）

指使用公開金鑰密碼系統之數位憑證標準，提供通訊鑑別機制，並規範鑑別過程中適用之憑證語法及資料介面。

4.23. 安全領域（Security Domain）

指待測物為實現安全功能需求，分配不同權限使用者之資源。

4.24. 自我保護（Self-Protection）

指防護安全功能不被無關之程式碼或外力破壞之機制。

4.25. 吞吐量（Throughput）

指待測物處理網路流量之速度，通常以 Mbps 或 Gbps 表示。

4.26. 最大同時連線數

指待測物能同時維持並處理之 TCP 最大連線數。

4.27. 常見弱點與漏洞 （Common Vulnerabilities and Exposures, CVE）

指美國國土安全部贊助之弱點管理計畫中，針對每一弱點項目所賦予其全球認可唯一共通編號。

4.28. 漏洞評鑑系統 （Common Vulnerability Scoring System, CVSS）

指包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度等判定標準之評鑑系統。評比從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險。

5. 檢測方式及安全等級

5.1. 檢測方式分為書面審查及實機測試。

5.1.1. 書面審查之檢測項目包括設備概述、安全功能需求、安全架構、安全功能規格、安全指引及設計安全性。

5.1.2. 實機測試之檢測項目包括安全功能測試、壓力測試、堅實測試、穩定性測試及弱點測試。

5.2. 安全等級依書面審查及實機測試之檢測項目之差異，分為初階、中階與高階三級。

5.3. 檢測項目、檢測細項所對應之安全等級與適用設備如表一至表二，申請者應依待測物申請之安全等級檢附表一所列文件。

5.4. 申請中階與高階安全等級之待測物，應併同檢附未加密韌體檔案。

表一、書面審查之檢測項目及對應之安全等級與適用設備

檢測項目	應檢附文件	安全等級			適用設備	
		初階	中階	高階	Wi-Fi AP	路由器
設備概述	設備概述說明 （如表三）	6.1	6.1	6.1	✓	✓
安全功能需求	安全功能說明 （如表四）	--	--	6.2	✓	✓
安全架構	安全架構描述表 （如表五）	--	--	6.3	✓	✓
安全功能規格	安全功能介面表 （如表六）	--	--	6.4	✓	✓
安全指引	安全指引文件 （如表七）	--	--	6.5	✓	✓
設計安全性	子系統描述與分類表（如表八）	--	--	6.6	✓	✓

表二、實機測試之檢測項目及對應之安全等級與適用設備

檢測項目	檢測細項	安全等級			適用設備	
		初階	中階	高階	Wi-Fi AP	路由器
安全功能測試	事件紀錄產出	7.1.1	7.1.1	7.1.1	✓	✓
	管理者預設密碼安全	7.1.2	7.1.2	7.1.2	✓	✓
	管理者鑑別及權限	7.1.3	7.1.3	7.1.3	✓	✓
	管理者遠端鑑別失敗控制功能	--	7.1.4	7.1.4	✓	✓
	使用者鑑別與管控功能測試	7.1.5	7.1.5	7.1.5	✓	✓
	登入畫面保密功能	7.1.6	7.1.6	7.1.6	✓	✓
	管理者權限有效時間	--	7.1.7	7.1.7	✓	✓
	登入連線之終止	--	7.1.8	7.1.8	✓	✓
	韌體更新	7.1.9	7.1.9	7.1.9	✓	✓
	網路通訊埠安全	--	7.1.10	7.1.10	✓	✓
	安全角色	--	7.1.11	7.1.11	--	✓
	資源最大配額	--	7.1.12	7.1.12	--	✓
	網際網路流量管制功能	7.1.13	7.1.13	7.1.13	--	✓
	區域網路流量管制功能	--	7.1.14	7.1.14	--	✓
壓力測試	吞吐量	--	--	7.2.1	✓	✓
堅實測試	異常流量測試	--	7.3.1	7.3.1	✓	✓
	非正常關機恢復	--	--	7.3.2	✓	✓
穩定性測試	真實流量	7.4.1	7.4.2	7.4.3	✓	✓
弱點測試	共通弱點評估	7.5.1	7.5.1	7.5.2	✓	✓
	惡意程式測試	--	7.5.3	7.5.3	✓	✓
	模糊測試	7.5.4	7.5.5	7.5.6	✓	✓
	動態分析	--	7.5.7	7.5.7	✓	✓
	WPS 測試	7.5.8	7.5.8	7.5.8	✓	✓

6. 書面審查合格標準

6.1. 設備概述

設備概述說明（如表三）應載明下列事項：

（1）設備識別

A.設備名稱、廠牌、型號。

B.申請者名稱（製造商或代理商）。

C.製造商名稱。

D.韌體版本（含雜湊資訊）。

E.預設開啟之網路通訊埠。

F.允許主動連接之網站或 IP 位址。

G.吞吐量額定值。

H.可分配區域網路使用之 IP 位址數量或範圍。（僅適用路由器）。

（2）範圍

A.待測物及其運作時所需之實體範圍：包含待測物之外觀、尺寸、主要零組件及相關周邊設施。

B.待測物之邏輯範圍：包含待測物安全功能及各功能間之相互關係。

6.2. 安全功能需求

安全功能說明（如表四）應載明下列事項，並符合相關要求。

6.2.1. 稽核紀錄

（1）待測物應就下列事件產生相關稽核紀錄，並存於其資料庫中：

A.管理介面之操作行為。

B.使用者身分之登入、登出、設定。

C.韌體更新。

D.可信任通道連接之建立、終止，及建立失敗、終止失敗。

（2）每筆稽核紀錄至少包含下列資訊：

A.事件發生日期及時間。

B.事件觸發者。

C.嚴重等級。

6.2.2. 稽核紀錄之查詢

待測物至少應提供下列類別之稽核紀錄查詢：

（1）事件發生日期及時間。

（2）事件觸發者。

（3）嚴重等級。

6.2.3. 稽核紀錄可用性之保證

安全功能應具備以下稽核紀錄可用性之保證：

（1）應確保已儲存的稽核紀錄不被非授權使用者刪除。

（2）當非授權使用者嘗試竄改已儲存的稽核紀錄時，應偵測並記錄之。

（3）當發生稽核紀錄儲存設備之空間用盡、故障或遭受攻擊時，應維持儲存稽核紀錄之功能。其中空間即將用盡時，除提供系統警告外，並應至少提供下列一種處置方式：

A.另存稽核紀錄：將需要保存的稽核紀錄另存至其他儲存設備。

B.刪除稽核紀錄：將不需要保存之稽核紀錄予以刪除。

C.覆蓋稽核紀錄：新增之稽核紀錄覆蓋最舊的稽核紀錄。

6.2.4. 加解密金鑰管理

待測物應具備下列加解密金鑰管理機制：

（1）以 128 位元以上（含）之金鑰強度加解密演算法（Cryptographic Algorithm）產生、分配、儲存及銷毀金鑰。

（2）連線終止或帳號移除後應刪除不需使用之明文或金鑰。

6.2.5. 加解密演算法操作

待測物應具備下列加解密演算法操作功能：

（1）以加解密演算法提供連線服務。

（2）應提供 WPA2 等級以上（含）之保密機制，並採用使用 128 位元以上（含）之 AES-CBC 或 AES-CCMP 演算法。

（3）與稽核伺服器之間的連線應以 IPSec 或其他相同等級之安全協定加密保護。（僅適用 Wi-Fi AP）

6.2.6. 殘餘資訊保護

應確保待測物之系統資源(如:資料暫存區)於前次使用歸還後清除，或於本次使用前清除。

6.2.7. 登入失敗處理

待測物應具備以下登入失敗處理能力：

（1）偵測同一帳號連續登入失敗次數。

（2）同一帳號連續登入失敗次數達到指定值時，待測物應拒絕該帳號後續之任何登入要求，但經管理者解除鎖定者，不在此限。

6.2.8. 帳號之密碼管理

待測物應提供下列帳號之密碼管理功能：

（1）密碼由英文大小寫、數字或特殊字元所組成。

（2）支援 15 字元以上之密碼；密碼長度由管理人員設定。

6.2.9. 鑑別機制

待測物應具備以下鑑別機制：

（1）使用者通過身分鑑別前後，可分別執行的安全功能。

（2）應提供本地密碼（Local Password）鑑別機制。

（3）管理者可以透過遠端或本機登入系統，但預設禁止遠端登入。

（4）密碼逾更換週期時，待使用者成功登入後，待測物應要求使用者立即更新密碼，經使用者更換密碼重新登入後，始得提供被授權的安全功能。

（5）鑑別過程中應避免顯示相關鑑別資訊（如輸入的密碼等）。

（6）以無線方式接取待測物之使用者，身分鑑別前，無法透過待測物接取網路。

（7）待測物應支援預共享金鑰(Pre-shared Key)，且符合以下要求：

A. 金鑰長度為 22 字元（可由數字、大小寫英文字母及“!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、和“)”等特殊字元所組成）。

B. 由安全雜湊演算法（Secure Hash Algorithm, SHA）轉換字元的

共享金鑰。

C.有接受或產生亂數位元的共享金鑰功能。

（8）應支援 RFC 5280 所規範之 X.509 v3 數位憑證功能。

（9）應具備儲存及保護憑證之機制。

（10）應支援授權之管理者匯入 X.509 v3 數位憑證功能。

（11）與稽核伺服器溝通、執行相關鑑別工作時，應符合 IEEE 802.1x 標準、RFC 2865 及 RFC 3579 規範。（僅適用 Wi-Fi AP）

6.2.10. 安全功能行為管理

只有被授權者方可管理安全功能相關資料，以及對任何安全功能進行異動與設定。

6.2.11. 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）賦予使用者具備管理者之權限。

6.2.12. 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。

6.2.13. 失效保全

待測物啟動後，執行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。

6.2.14. 管理者密碼保護

待測物應具備以下管理者密碼保護功能：

（1）不得以明文（Plaintext）方式呈現密碼。

（2）以密文方式儲存密碼。

6.2.15. 可信賴之時戳

待測物應正確記錄稽核資料的日期及時間。

6.2.16. 韌體更新

待測物應具備以下韌體更新功能：

（1）可查詢待測物使用中之韌體版本，及目前原廠提供之最新韌體版本。

（2）管理者可手動或設定自動啟動韌體更新程序。

（3）提供管理者於韌體更新前，可辨別欲更新韌體真偽之機制。

（4）待測物應自動通知管理者新版韌體釋出之資訊。（僅適用路由器）

6.2.17. 管理者權限有效時間

若管理者登入後閒置時間超過待測物所設定之閒置時間：

（1）採本地（Local）連線登入者：待測物應鎖定或終止該連線；經鎖定連線者，待測物應避免資訊外洩。欲解除鎖定時，待測物應重新進行使用者鑑別。

（2）採遠端（Remote）連線登入者：待測物應立即終止該遠端連線。

6.2.18. 管理設定連線之終止

待測物應允許管理者終止已登入之管理者連線。

6.2.19. 待測物存取預設標語

管理者可設定登入注意事項畫面，並於使用者登入時顯示該畫面。

6.2.20. 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）及私密金鑰（Private Keys）等金鑰被讀取。

（2）不得提供讀取金鑰之指令。

6.2.21. 可信賴通道

待測物提供連線服務或連接外部伺服器時，應具備以下防護措施：

（1）使用 802.11-2012（WPA2）、IEEE 802.1x、IPSec、SSH、TLS、TLS/HTTPS 或其他加密之通訊協定。

（2）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。

6.2.22. 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。

6.2.23. 資源最大配額（僅適用路由器）

待測物應提供可同時分配區域網路 IP 位址數量之設定功能。

6.2.24. 資料流控制（僅適用路由器）

待測物應根據以下 OSI 第三層（網路層）之封包資料屬性，提供資料流控制及過濾等管理能力：

（1）來源端位址及其他自行指定之來源格式。

（2）目的端位址及其他自行指定之目的格式。

（3）通訊協定。

（4）網路卡介面。

（5）服務型態。

（6）其他（自行指定）。

6.2.25. 安全屬性初始值（僅適用路由器）

當待測物之資料流控制功能開啟時，應具備以下功能：

（1）預設拒絕外部網路的設備發起進到內部網路的連線。

（2）允許被授權的管理者變更預設值。

6.3. 安全架構

應依據檢附之表六至表八，說明待測物安全架構之設計概念與操作安全建議，及如何滿足安全功能需求。安全架構描述表（如表五）應載明下列事項：

（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。

6.4. 安全功能規格

安全功能介面表（如表六）應載明下列事項：

（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。

6.5. 安全指引

安全指引（如表七）應載明下列事項：

（1）每個使用者角色之定義。

（2）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）於特殊權限操作時之安全環境要求，並提供適當的警告。

（4）待測物操作時的所有運作模式。

（5）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）待測物運作前之安全準備作業，包含待測物安裝及啟動方式。

（7）待測物操作之安全環境設置，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）安全指引文件將做為實機測試之依據。

6.6. 設計安全性

子系統描述與分類表（如表八）應說明如何以子系統組成安全功能規格之安全功能介面，並載明下列事項：

（1）子系統名稱。

（2）目的。

（3）子系統隸屬之安全功能介面。

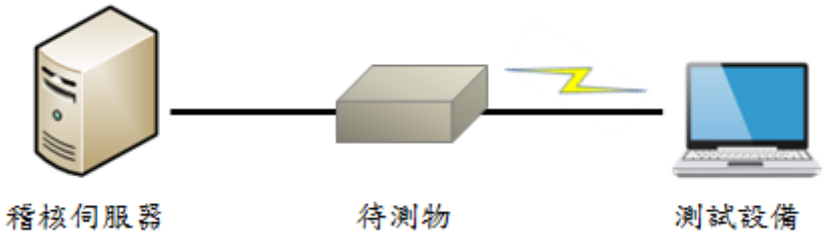
（4）子系統行為說明。

7. 實機測試合格標準

7.1. 安全功能測試

7.1.1. 事件紀錄產出

（1）測試環境



圖三、事件紀錄測試測試環境示意圖

A. 測試設備：以無線（如 Wi-Fi 或藍芽等）或有線（如乙太網路線或光纖等）方式連接待測物之設備。

B. 測試設備、待測物及稽核伺服器連接方式如圖三。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物。

B. 設定並開啟待測物之事件紀錄功能。

C. 對待測物進行分別進行下列行為：

a. 變更系統設定值並套用。

b. 清除事件紀錄。

c. 登出及登入。

（3）判定標準

A. 待測物應產生下列事件紀錄：

a. 事件發生日期及時間。

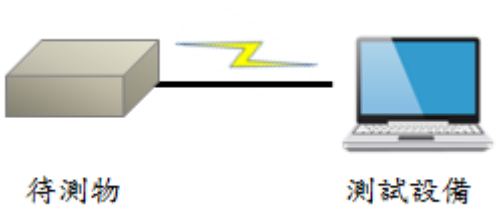
b. 事件觸發者。

c. 嚴重等級。

B. 待測物應同步傳送事件紀錄至外部稽核伺服器（通訊協定應支援 RFC 5424）並儲存。（僅適用申請高階安全等級之待測物）

7.1.2. 管理者預設密碼安全

（1）測試環境



圖四、管理者預設密碼安全測試環境示意圖

A. 測試設備：以無線（如 Wi-Fi 或藍芽等）或有線方式（如乙太網路線或光纖等）連接待測物之設備。

B. 測試設備及待測物連接方式如圖四。

（2）測試方法

A. 檢查二待測物於原廠設定狀態下之管理者密碼是否相同。

B. 二待測物之預設密碼相同者，於測試設備上以管理者身份登入任一待測物。

（3）判定標準

待測物應符合下列情形之一：

A. 二待測物於原廠設定狀態下之管理者密碼相異。

B. 首次以管理者身份登入待測物後，待測物應要求管理者變更密碼。經以變更後之密碼登入，始得使用管理者權限。

7.1.3. 管理者鑑別及權限

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 經由 console 埠或經加密保護之無線介面通訊協定連接待測物。

B. 使用一管理者帳號並連續輸入 3 次（含）以上錯誤之密碼登入待測物之管理介面。

C. 使用正確管理者帳號與密碼登入待測物之管理介面。

（3）判定標準

A. 輸入錯誤密碼時無法登入待測物。

B. 輸入正確的帳號及密碼始可登入待測物之管理介面，並具完整安全功能設定權限。

7.1.4. 管理者遠端鑑別失敗控制功能

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物之管理介面，開啟待測物之安全管理功能，設定待測物可允許之同一帳號連續輸入錯誤密碼次數上限為 3 次後登出。

B. 使用一管理者帳號並連續輸入 4 次錯誤之密碼遠端登入待測物之管理介面（若待測物因錯誤次數達設定上限而主動中斷連線者，不在此限）。

C. 待測物具 Quiet Period 功能者：經過 Quiet Period 設定時間後，再以同一帳號及正確密碼進行遠端登入。

D. 待測物具永久鎖定特定管理帳號遠端登入功能者：以管理者身分於本地端解除測試方法 B 之帳號登入鎖定，再以該帳號及正確密碼進行遠端登入。

（3）判定標準

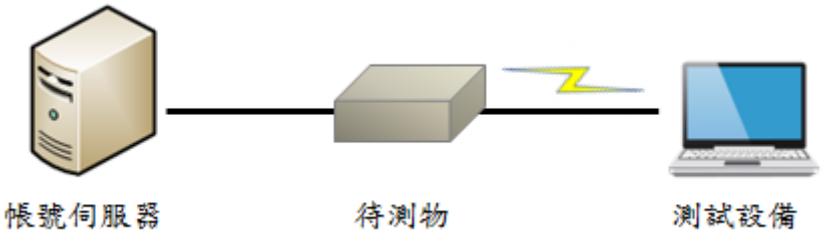
連續登入失敗次數超過允許上限後，待測物應拒絕該帳號後續之任何登入請求，但有下列情形者不在此限。

A. 待測物具 Quiet Period 功能者：經過 Quiet Period 設定時間後，同一帳號始得以正確密碼進行登入。

B. 待測物具永久鎖定特定管理帳號遠端登入功能者：經解除帳號登入鎖定後，該帳號始得以正確密碼進行登入。

7.1.5. 使用者鑑別與管控功能測試

（1）測試環境



圖五、使用者鑑別與管控功能測試測試環境示意圖

A.測試設備：以無線（如 Wi-Fi 或藍芽等）或有線（如乙太網路線或光纖等）方式連接待測物之設備。

B.測試設備、待測物及帳號伺服器連接方式如圖五。但待測物具備本地帳號資料庫功能者，得不連接帳號伺服器。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物之管理介面，設定並啟用使用者鑑別與管控功能後登出。

B. 測試設備 A 模擬無線使用者，選擇待測物之無線上網服務名稱（SSID），並以下列方式嘗試通過待測物之驗證。

a. 待測物使用 IEEE 802.11i （含）以上之無線網路安全標準進行使用者鑑別管控功能者，並依待測物之設計，輸入錯誤及正確之共享金鑰、憑證或帳號密碼。

b. 待測物使用加密保護之通訊協定標準之驗證網頁進行使用者鑑別管控功能者，並輸入錯誤及正確之帳號密碼。

（3）判定標準

輸入正確資訊，始得通過驗證。

7.1.6. 登入畫面保密功能

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

開啟待測物之使用者登入介面，並輸入帳號及密碼進行登入。

（3）判定標準

登入過程中，待測物之使用者登入介面應以特殊符號（如：＊）遮蔽輸入之明文密碼字元。

7.1.7. 管理者權限有效時間

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物之管理介面，開啟待測物之登入連線鎖定功能，並設定待測物自動鎖定或自動登出之時間。

B. 測試設備經由加密保護之無線介面通訊協定連接待測物，並閒置超過自動鎖定或自動登出之設定時間。

（3）判定標準

A. 閒置超過自動鎖定或自動登出設定時間後，待測物應自動顯示鎖定或重新登入畫面，且任何人無法讀取其管理畫面資訊或進行操作。

B. 待測物具自動鎖定功能者，經重新輸入正確密碼，始得登入使用。

C. 待測物具重新登入功能者，經重新輸入正確帳號及密碼，始得登入使用。

7.1.8. 登入連線之終止

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以使用者身份登入待測物。

B. 使用者完成正常登出作業。

（3）判定標準

使用者完成正常登出作業後，與待測物間該次之通訊協定交握及相關驗證授權應立即失效。

7.1.9. 韌體更新

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物之管理介面。

B. 檢視待測物目前韌體版本，並備份待測物設定檔。

C. 更新韌體並檢視更新後之版本。

D. 回復 B 備份之設定檔及重新開機。

（3）判定標準

A. 測試方法 C 執行後，待測物之韌體應為更新後之版本。

B. 測試方法 D 執行後，待測物之安全功能應與韌體更新前相符。

7.1.10. 網路通訊埠安全

（1）測試環境

A. 測試設備應具網路通訊埠掃描功能。

B. 測試設備及待測物連接方式如圖四。

（2）測試方法

掃描待測物於原廠設定狀態下開啟之網路通訊埠。

（3）判定標準

A. 待測物開啟之網路通訊埠，應與申請者檢附之表三相符。

B. 待測物應關閉 FTP 及 Telnet 使用之網路通訊埠，但以明確之方式宣告（如載明於說明書）前述網路通訊埠開啟者，不在此限。

7.1.11. 安全角色（僅適用路由器）

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以管理者身分登入待測物之管理介面，並建立 2 組（含）以上，具相異功能及授權之角色，如管理者、維護者等。

B. 分別以 A 建立之角色進行授權及非授權功能操作。

（3）判定標準

不同角色登入後，待測物僅得提供符合其權限之功能。

7.1.12. 資源最大配額（僅適用路由器）

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物之管理介面，並依申請者檢附之表三所列可分配區域網路 IP 位址數量或範圍，設定同時分配 IP 位址數量（X）。

B. 測試設備向待測物請求 X 個 IP 位址分配，並以管理介面確認 IP 位址分配狀況。

C. 測試設備請求增加 IP 位址分配數量至 X+1，並以管理介面確認 IP 位址分配狀況。

D. 測試設備請求釋出 1 個 IP 位址，並以管理介面確認 IP 位址分配狀況。

（3）判定標準

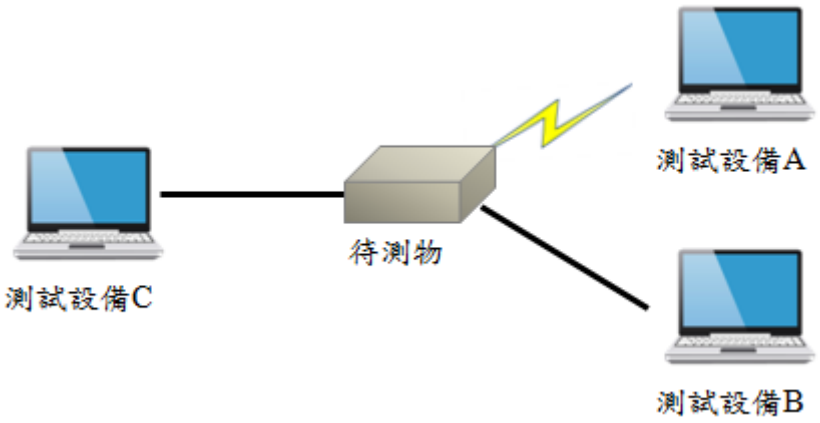
A. 測試方法 B 執行後，待測物之管理介面應顯示已分配 X 個 IP 位址，並與測試設備獲分配之 IP 位址相符。

B. 測試方法 C 執行後，待測物之管理介面應顯示已分配 X 個 IP 位址，並與測試設備獲分配之 IP 位址相符，另測試設備提出之 1 個請求未獲待測物分配 IP 位址。

C. 測試方法 D 執行後，待測物之管理介面應顯示已分配 X-1 個 IP 位址，並與測試設備獲分配之 IP 位址相符。

7.1.13. 網際網路流量管制功能（僅適用路由器）

（1）測試環境



圖六、網際網路流量管制功能測試測試環境示意圖

A. 測試設備 A：以 Wi-Fi 連接待測物之設備，其網路遮罩設定應與待測物之無線區域網路設定相同。

B. 測試設備 B：以有線（乙太網路線或光纖等）方式連接待測物有線區域網路介面之設備，其網路遮罩設定應與待測物之有線區域網路設定相同。

C. 測試設備 C：以有線（乙太網路線或光纖等）方式連接待測物網際網路介面之設備，其網路遮罩設定應與待測物之網際網路設定相同。

D. 測試設備 A、測試設備 B、測試設備 C 及待測物連接方式如圖六。

（2）測試方法

A. 確認測試設備 A、測試設備 B、測試設備 C 與待測物間之連線已建立。

B. 於測試設備上以管理者身份登入待測物之管理介面，開啟待測物之流量管制功能，並分別以下述設定進行測試：

a. 測試設備 A 不得連線至測試設備 C。

b. 測試設備 B 不得連線至測試設備 C。

c. 測試設備 A 及 B 不得連線至測試設備 C。

（3）判定標準

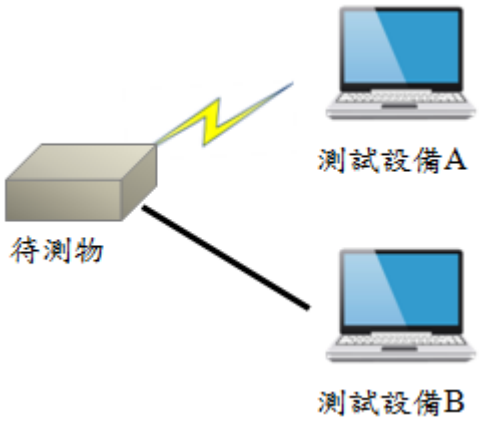
A. 測試方法 B.a 執行後，測試設備 C 無法收到測試設備 A 傳送之流量，但測試設備 C 仍可收到測試設備 B 傳送之流量。

B. 測試方法 B.b 執行後，測試設備 C 無法收到測試設備 B 傳送之流量，但測試設備 C 仍可收到測試設備 A 傳送之流量。

C. 測試方法 B.c 執行後，測試設備 C 無法收到測試設備 A 及 B 傳送之流量。

7.1.14. 區域網路流量管制功能（僅適用路由器）

（1）測試環境



圖七、區域網路流量管制功能測試測試環境示意圖

A. 測試設備 A：以 Wi-Fi 連接待測物之設備，其網路遮罩設定應與待測物之無線區域網路設定相同。

B. 測試設備 B：以有線（乙太網路線或光纖等）連接待測物有線區域網路介面之設備，其網路遮罩設定應與待測物之有線區域網路設定相同。

C. 測試設備 A、測試設備 B 及待測物連接方式如圖七。

（2）測試方法

A. 確認測試設備 A、測試設備 B 與待測物間之連線已建立。

B. 於測試設備上以管理者身份登入待測物之管理介面，開啟待測物之流量管制功能，設定測試設備 B 不得連線至測試設備 A。

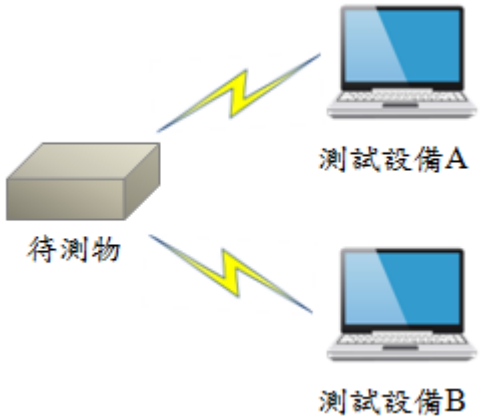
（3）判定標準

測試設備 A 及 B 應無法相互收到對方傳送之流量。

7.2. 壓力測試

7.2.1. 吞吐量測試

（1）測試環境



圖八、吞吐量測試測試環境示意圖

A. 測試設備 A：具備無線介面並可產生網路封包之設備。

B. 測試設備 B：具備無線介面，並可透過待測物接收從測試設備 A 所傳送之網路封包。

C. 透過無線方式連接測試設備 A、測試設備 B 及待測物如圖八。

（2）測試方法

A. 開啟待測物之安全功能。

B. 建立測試設備 A 經待測物至測試設備 B 之連線後，測試設備 A 開始傳送依 57%、7%、16%及 20%之比例混合之 64、570、594 及 1,518 位元組網路封包，並持續傳送混合後之網路封包 60 秒。

（3）判定標準

當待測物所負荷的吞吐量達申請者檢附之表三所列吞吐量額定值時，待測物應能正常運作，且測試過程中不得發生下列情況：

A. 2 分鐘內待測物無任何反應。

B. 重新開機。

7.3. 堅實測試

7.3.1. 異常流量測試

（1）測試環境

A. 測試設備：具 Wi-Fi 收發功能，且可產生異常或攻擊流量。

B. 測試設備以無線方式連接待測物如圖四，並以其所產生之各種異常或攻擊流量進行測試。

（2）測試方法

測試設備持續傳送以下類型之封包至待測物。

A. 802.11 鑑別氾濫式攻擊（802.11 Authenticate Flood）。

B. 802.1x EAP-Start 氾濫式攻擊（802.1x EAP-Start Flood）。

C. 802.1x EAP-of-Death 攻擊（802.1x EAP-of-Death）。

D. 802.1x EAP 長度攻擊（802.1x EAP Length Attacks）。

E. 異常 Frame-Assoc 請求（Malformed Frame Associates Request）。

F. 異常 Frame-Auth（Malformed Frame Authentication）。

G. 阻斷式攻擊（Denial-of-service attack）。（僅適用路由器）

（3）判定標準

當待測物所負荷的吞吐量達申請者檢附之表三所列吞吐量額定值時，待測物應能正常運作，且測試過程中不得發生下列情況：

A. 2 分鐘內待測物無任何反應。

B. 重新開機。

7.3.2. 非正常關機恢復

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

A. 於測試設備上以管理者身份登入待測物之管理介面，查詢並記錄待測物之安全功能設定。

B. 待測物連線時將電源中斷，並於 1 分鐘後接上電源，重新啟動待測物。

（3）判定標準

A. 待測物應保留斷電前的系統設定。

B. 待測物應保留斷電前 5 分鐘內之日誌檔案（含系統日誌及安全事件日誌）。

C. 待測物應復原至斷電前之正常狀態。

7.4. 穩定性測試

7.4.1. 真實流量初階測試

（1）測試環境

A. 測試設備：以 Wi-Fi 及有線（如乙太網路線或光纖等）方式連接待測物之設備，且可產生或播放真實流量測試樣本。

B. 測試設備及待測物連接方式如圖四。

（2）測試方法

A. 由測試設備產生測試樣本，或重覆播放錄製之實際網路流量，網路流量樣本必須符合以下要求：

a. 至少 100 組 IP 位址同時接取網際網路服務之流量。

b. 建立測試設備 A 埠經待測物至測試設備 B 之連線後，測試設備 A 開始傳送，測試流量應達待測物最大吞吐量（throughput）50%以上。

c. 流量內容須涵蓋 Chat、E-Mail、File Transfer、Game、P2P、Remote Access、Streaming、Web、Network Infrastructure Services 等 9 種（含）以上類型，且每種類型應由 3 項（含）以上之應用程式或服務所組成。

B. 測試設備應以 Wi-Fi 方式連續 72 小時傳送測試樣本至待測物，待測物並以有線方式將所接收之測試樣本回傳至測試設備。

（3）判定標準

測試過程中不可發生下列情況：

A. 重新開機。

B. 傳輸中斷。

7.4.2. 真實流量中階測試

除測試方法之傳送測試樣本時間應連續 144 小時之外，測試環境、測試方法及判定標準依 7.4.1 規定為之。

7.4.3. 真實流量高階測試

除測試方法之傳送測試樣本時間應連續 240 小時之外，測試環境、測試方法及判定標準依 7.4.1 之規定為之。

7.5. 弱點測試

7.5.1. 共通弱點評估初階測試與中階測試

（1）測試環境

圖九、共通弱點評估測試測試環境示意圖

A. 測試設備：以 Wi-F 方式連接待測物之設備。

B. 測試設備及待測物連接方式如圖九。

（2）測試方法

A. 更新測試設備弱點偵測功能之 CVE 弱點資料庫，該資料庫應包含 NIST 發布之 CVE 弱點，及採用 NIST 發布之弱點評估方式。

B. 掃描待測物通訊或管理介面之 CVE 弱點。

（3）判定標準

待測物不得檢出弱點評鑑系統（CVSS）嚴重性等級評比為重大（Critical，即 9 分以上）之弱點。

7.5.2. 共通弱點評估高階測試

待測物不得檢出弱點評鑑系統(CVSS)嚴重性等級評比為高(High，即 7 分以上）之弱點；測試環境、測試方法依 7.5.1 規定為之。

7.5.3. 惡意程式測試

（1）測試環境

無。

（2）測試方法

A. 使用韌體分析工具還原申請者檢附之未加密韌體檔案。

B. 以 1 套（含）以上防毒軟體完整掃描前述檔案，掃描前應先更新最新之病毒碼。防毒軟體必須符合以下要求：

a. 資安測試機構 AV-Test 最近一年測試結果，防護分數（Protection Score）達 5.5 分以上。

b. 資安測試機構 AV-Comparatives 最近一年測試結果，Malware Protection Tests 取得 Advanced+(三星)等級。

（3）判定標準

不得檢驗出惡意程式(如：病毒、蠕蟲、特洛依木馬、邏輯炸彈、間諜軟體、廣告程式及後門程式等)。

7.5.4. 模糊初階測試

（1）測試環境

同 7.5.1 之測試環境。

（2）測試方法

使用模糊測試工具(參考附錄三)進行 5,000 筆隨機樣本之測試，並將結果儲存在測試設備。前述隨機樣本至少應包含 IEEE 802.11i 標準下產生變異樣本。

（3）判定標準

測試過程中待測物應正常運作，且不得重新開機。

7.5.5. 模糊測試中階測試

除測試方法之測試樣本筆數增加至 7,000 筆之外，測試環境、測試方法及判定標準依 7.5.4 之規定為之。

7.5.6. 模糊測試高階測試

除測試方法之測試樣本筆數增加至 10,000 筆之外，測試環境、測試方法及判定標準依 7.5.4 之規定為之。

7.5.7. 動態分析

（1）測試環境

圖十、動態分析測試測試環境示意圖

A. 測試設備：以有線（如乙太網路線或光纖等）方式連接待測物及網際網路之設備。

B. 連接測試設備及待測物如圖十。

（2）測試方法

持續分析待測物收發之網路封包 144 小時，並分析該網路封包連接之網站或 IP 位址。

（3）判定標準

除申請者檢附之表三所列允許主動連接之網站或 IP 位址，待測物不可主動對其他網站或 IP 位址發起連線或傳輸任何資料。

7.5.8. WPS 測試

（1）測試環境

同 7.1.2 之測試環境。

（2）測試方法

開啟並檢視待測物之管理介面。

（3）判定標準

具備 WPS PIN 功能之待測物，該功能應預設關閉。

表三、設備概述說明

設 備 識 別		
設備名稱		
廠牌		
型號		
申請者 （公司、商號名稱）	□製造商 □進口商 □經銷商	
製造商		
韌體版本 （含雜湊資訊）		
預設開啟之 網路通訊埠		
允許主動連接之 網站或 IP 位址		
吞吐量額定值 （註 1）		
可分配區域網路使用之 IP 位址數量或範圍 （註 2）		
範　圍		
實體範圍		
邏輯範圍		

註 1：應參照 IEEE 802.11 相關標準之調變與編碼架構索引。

註 2：「可分配區域網路使用之 IP 位址數量或範圍」僅適用路由器。

表四、安全功能說明

檢測細項	審查要求	申請者填寫內容
1.稽核紀錄	本指引 6.2.1.	
2.稽核紀錄之查詢	本指引 6.2.2.	
3.稽核紀錄可用性之保證	本指引 6.2.3.	
4.加解密金鑰管理	本指引 6.2.4.	
5.加解密演算法操作	本指引 6.2.5.	
6.殘餘資訊保護	本指引 6.2.6.	
7.登入失敗處理	本指引 6.2.7.	
8.帳號之密碼管理	本指引 6.2.8.	
9.鑑別機制	本指引 6.2.9.	
10.安全功能行為管理	本指引 6.2.10.	
11.安全角色	本指引 6.2.11.	

檢測細項	審查要求	申請者填寫內容
12.安全功能自我測試	本指引 6.2.12.	
13.失效保全	本指引 6.2.13.	
14.管理者密碼保護	本指引 6.2.14.	
15.可信賴之時戳	本指引 6.2.15.	
16.韌體更新	本指引 6.2.16.	
17.管理者權限有效時間	本指引 6.2.17.	
18.管理設定連線之終止	本指引 6.2.18.	
19.待測物存取預設標語	本指引 6.2.19.	
20.金鑰保護	本指引 6.2.20.	
21.可信賴通道	本指引 6.2.21.	
22.可信賴路徑	本指引 6.2.22.	

檢測細項	審查要求	申請者填寫內容
23.資源最大配額	本指引 6.2.23 （僅適用路由器）	
24.資料流控制	本指引 6.2.24 （僅適用路由器）	
25.安全屬性初始值	本指引 6.2.25 （僅適用路由器）	

表五、安全架構描述表

項目	說明	申請者填寫內容
1.安全領域	列出各安全功能介面對應之安全領域名稱，並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：TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection* *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	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.自我保護機制	1.自我保護功能 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* 2. 與外部設備之關係 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* 3.自我保護機制說明 安全功能介面提供實體上或邏輯上的	

項目	說明	申請者填寫內容
	自我保護機制 *範例：* *（1）應輸入密碼才能進入介面。* *（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	1. 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* 2.列舉可能繞道之手法 *範例：可能直接以維護介面不經身分鑑別操控待測物。* 3.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：防範作法為以實體封鎖方式，防止利用維護介面繞道身分鑑別程序。*	

表六、安全功能介面表

項目	項目說明	申請者填寫內容
1.安全功能介面名稱	列出所有安全功能介面。 *範例：TSFI_CLI*	
2.目的	說明各安全功能介面之安全功能目的。 *範例：提供命令列模式操作介面*	
3.可實現的安全功能需求	說明各安全功能介面如何實現表二所列之實機測試檢測項目。 *範例：SFR_安全管理：提供安全管理功能*	
4.操作方式	說明如何使用各安全功能介面。 *範例：以 ssh 連接待測物，即提供命令列模式操作介面*	
5.參數	說明各安全功能介面所有參數及其意義。 *範例：ID & password*	
6.執行動作	說明各安全功能介面如何運作及其執行細節。 *範例：可下達管理命令操作待測物*	
7.錯誤訊息	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：連接失敗、鑑別失敗*	

表七、安全指引文件

項目	說明	申請者填寫內容
1.每個使用者角色之定義	列出待測物應具備及設定所有安全角色，並對所有安全角色說明。 *範例：* ● *一般管理者：指具備基礎管理者權限，僅包含監視待測物運作及網路運作狀態，不可對安全功能進行任何設定(一般管理者角色之權限說明參照本表第 2 項目)。* ● *完整權限管理者：除具備一般管理者安全功能外，具備完整待測物安全功能設定及使用功能(完整權限管理者角色之權限說明參照本表第 2 項目)。*	
2.每個使用者角色於執行安全功能時之相關說明	1.週邊設備及安全設定。 列出待測物應具備及設定所有安全角色，並對所有安全角色之可使用安全功能。 *範例：* ● *一般管理者具備以下安全功能：* ■ *查看待測物管理主畫面* ■ *查看待測物告警訊息* ■ *查看待測物網路流量* ■ .... ● *完整權限管理者具備以下安全功能：* ■ *查看待測物管理主畫面* ■ *開啟及關閉日誌稽核功能* ■ *系統時間變更* ■ *軟、韌體更新* ■ ... 2.允許使用的介面 列出待測物應具備及設定所有安全角色及相對所有允許使用的介面。 *範例：* ● *一般管理者允許使用的介面：* ■ *TSFI_CLI*	

項目	說明	申請者填寫內容
	■ …. ● *完整權限管理者允許使用的介面：* ■ *TSFI_CLI* ■ … 3.安全參數定義 列出待測物應具備及設定所有安全角色及相對所有允許設定安全參數之定義。 *範例：* ● *一般管理者無法設定任何安全參數。* ● *完整權限管理者可設定安全參數如下：* ■ *Admin_count:同時登入的管理者數量。* ■ … 4.可能產生的安全事件 列出待測物應具備及設定所有安全角色及相對所有允許設定安全參數之可能產生的安全事件。 *範例：* ● *一般管理者無法設定任何安全參數。* ● *完整權限管理者可設定安全參數如下：* ■ *當設定「Admin_count」安全參數時會有以下安全事件：「成功」表示同時登入的管理者數量設定成功。* ■ … 5.應遵循的安全措施 列出待測物應具備及設定所有安全角色及相對應遵循的安全措施。 *範例：* ● *一般管理者應遵循安全措施，包含如下：* ■ *一般管理者在進行帳號之*	

項目	說明	申請者填寫內容
	密碼設定時，密碼應由英文大小寫、數字或特殊字元所組成，並且應至少 15 字元以上。 ● *完整權限管理者應遵循安全措施，包含如下：* ■ … ■ …	
3.於特殊權限操作時之安全環境要求，並提供適當的警告	1.安全環境要求 列出於特權限操作時之安全環境要求 *範例：當 3.5G 網卡接上後無法進行待測物連線，請到 XXXX 官網查詢產品支援清單檢閱待測物所使用網卡有無支援。若有支援，請到官網下載服務將韌體更新至最新版本。* 2. 提供適切警語 利用提示警語方式讓待測物使用者優先注意及採用。 *範例：* *[注意]* *官網產品支援清單請參閱:https://www.product.com.tw/support/，並且韌體更新請參閱:https://www.product.com.tw/update/*	
4.待測物操作時的所有運作模式	列出待測物操作時所有運作模式 *範例：* ● *正常運作模式：管理者透過管理畫面登入及對各安全功能監視及設定。* ● *維修運作模式：待測物之製造商為進行設備軟體或硬體維修，透過維修管理畫面或硬體介面(如：特定埠)以進行維修作業。* 2.說明防範作法，包含進入各運作模式安全功能介面如何被保護及執行階段的資料處理如何保護等。	

項目	說明	申請者填寫內容
5.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	1.說明常見作業失敗或人員操作錯誤產生情境 *範例：待測物連線使用者搜尋不到該設備 SSID。* 2. 提供該作業失敗情境之處理方式 *範例：* *可依照以下項目檢查 SSID 設定正確性：* *1.待測物可能將 SSID 設定為關閉。...*	
6.待測物運作前之安全準備作業	說明待測物管理者在開放待測物提供服務前，應具備安全準備作業，包含待測物安裝及啟動方式。 *範例：* *1. 待測物包裝完整性：為確保待測物從製造商到顧客運送過程中，無有心人士調包並安裝後門在待測物中，請確保待測物包裝完整性及對照型號及序號確保一致。* *2. 待測物安裝步驟...*	
7.待測物操作之安全環境設置	說明待測物管理者開放待測物提供服務前，應確保安全功能可正常運作之安全環境設置。 1.待測物使用目的 為確保待測物之安全功能可正常運作，應針對使用面之安全環境設置作說明。 *範例：* *1.為確保待測物可正常運作，應對網路協定管制作業。* 2.實體環境安全 為確保待測物之安全功能可正常運作，應針對實體環境安全要求作說明。 *範例：* *1.為確保待測物可正常運作，應將待測物置於具備門禁管制的環境，以確保無有心人士對待測物作破壞。*	

項目	說明	申請者填寫內容
	3.人員安全 *為確保待測物之安全功能可正常運作，應針對人員控管安全要求作說明。* *範例：* *1.僅有授權人員可存取待測物。* 4.連接安全 *為確保待測物之安全功能可正常運作，應針對連接控管安全要求作說明。* *範例：* *1.待測物與其他網路伺服器之連線安全。*	

表八、子系統描述與分類表

項目	項目說明	申請者填寫內容
1.子系統名稱	列出各安全功能介面之子系統。 *範例：Subsystem_ssh*	
2.目的	說明各子系統之安全功能目的。 *範例：提供 ssh 服務*	
3.子系統隸屬之安全功能介面	說明各子系統隸屬於表五所列之安全功能介面。 *範例：TSFI_CLI*	
4.子系統行為說明	說明各子系統行為如下： 1.如何實現安全功能介面的功能。 *範例:提供 TSFI_CLI 命令列模式操作介面* 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：與其他子系統之互動：* *（1）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* *（2）Subsystem_terminal: ...*	

附錄一、書面審查安全功能需求檢測細項與國際標準對照表

檢測細項	審查標準	參考來源	參考內容
稽核紀錄	本指引 6.2.1	Collaborative Protection Profile for Network Devices	FAU_GEN.1 Audit data generation
		UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	11. Product Management
		Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	● AU-3 CONTENT OF AUDIT RECORDS ● AU-8 TIME STAMPS
		Special Publication 800-92 Guide to Computer Security Log Management	2.1.1 Security Software
稽核紀錄之查詢	本指引 6.2.2	Protection Profile for Wireless Local Area Network(WLAN) Access Systems	FAU_SEL.1Selective Audit
		Special Publication 800-92 Guide to Computer Security Log Management	5.2.2 Prioritizing Log Entries
稽核紀錄可用性之保證	本指引 6.2.3	Collaborative Protection Profile for Network Devices	6.3.2.1 FAU_STG_EXT.1 Protected Audit Event Storage
加解密金鑰管理	本指引 6.2.4	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	● FCS_CKM.1(2) Cryptographic Key Generation (Symmetric Keys for WPA2 Connections） ● FCS_CKM.2(2) Cryptographic Key Distribution (PMK)
		Collaborative Protection Profile for Network Devices	FCS_CKM.4 Cryptographic Key Destruction
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	10 Sensitive Data
		ENISA Recommended cryptographic measures - Securing personal data	5.4. Key management
加解密演算法操作	本指引 6.2.5	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area	● FCS_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)

檢測細項	審查標準	參考來源	參考內容
		Network (WLAN) Access Systems	● FCS_CKM.2(2) Cryptographic Key Distribution (PMK)
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	10 Sensitive Data
殘餘資訊保護	本指引 6.2.6	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	Residual Information Protection (FDP_RIP)
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	11 Product Management
登入失敗處理	本指引 6.2.7	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	FIA_AFL.1 Authentication Failure Handling
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8 Access Control, User Authentication and User Authorization
		Special Publication 800-92 Guide to Computer Security Log Management	5.2 General Authenticator Requirements
帳號之密碼管理	本指引 6.2.8	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	Password Management (Extended – FIA_PMG_EXT)
		Protection Profile for Wireless Local Area Network (WLAN) Access Systems	FIA_PMG_EXT.1 Password Management
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8 Access Control, User Authentication and User Authorization
鑑別機制	本指引 6.2.9	Collaborative Protection Profile for Network Devices	● FIA_UIA_EXT.1 User Identification and Authentication

檢測細項	審查標準	參考來源	參考內容
			● FIA_UAU_EXT.2 Password-based Authentication Mechanism ● FIA_UAU.7 Protected Authentication Feedback
		Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	● FIA_UAU.6 Re-authenticating ● FIA_8021X_EXT.1 Extended: 802.1x Port Access Entity (Authenticator) Authentication
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8 Access Control, User Authentication and User Authorization
		NIST Special Publication 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11I	3 Overview of IEEE 802.11 Security
安全功能行為管理	本指引 6.2.10	Collaborative Protection Profile for Network Devices	● FMT_MOF.1/ManualUpdate Management of security functions behaviour ● FMT_MTD.1/CoreData Management of TSF Data
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8 Access Control, User Authentication and User Authorization
安全角色	本指引 6.2.11	Collaborative Protection Profile for Network Devices	FMT_SMR.2 Restrictions on Security Roles
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8 Access Control, User Authentication and User Authorization
安全功能自我測試	本指引 6.2.12	Collaborative Protection Profile for Network Devices	FPT_TST_EXT.1 TSF Testing (Extended)
失效保全	本指引 6.2.13	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	FPT_FLS.1 Failure with preservation of secure state

檢測細項	審查標準	參考來源	參考內容
管理者密碼保護	本指引 6.2.14	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	FPT_APW_EXT.1 Protection of Administrator Passwords
可信賴之時戳	本指引 6.2.15	Collaborative Protection Profile for Network Devices	FPT_STM.EXT.1 Reliable Time Stamps
		Special Publication 800-92 Guide to Computer Security Log Management	5 Log Management Operational Processes
韌體更新	本指引 6.2.16	Collaborative Protection Profile for Network Devices	FPT_TUD_EXT.1 Trusted Update
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	11 Product Management
		Special Publication 800-193(DRAFT)Platform Firmware Resiliency Guidelines	3.5 Firmware Update Mechanisms
管理者權限有效時間	本指引 6.2.17	Collaborative Protection Profile for Network Devices	FTA_SSL_EXT.1 TSF-initiated Session Locking
管理設定連線之終止	本指引 6.2.18	Collaborative Protection Profile for Network Devices	FTA_SSL.3 TSF-initiated Termination (Refinement) FTA_SSL.4 User-initiated Termination (Refinement)
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8 Access Control, User Authentication and User Authorization
待測物存取預設標語	本指引 6.2.19	Collaborative Protection Profile for Network Devices	FTA_TAB.1 Default TOE Access Banners (Refinement)
金鑰保護	本指引 6.2.20	Collaborative Protection Profile for Network Devices	FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared,symmetric and private keys)
可信賴通道	本指引 6.2.21	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	FTP_ITC.1 Inter-TSF Trusted Channel
		Collaborative Protection Profile for Network Devices	FTP_ITC.1 Inter-TSF trusted channel
		UL 2900-1	8 Access Control, User Authentication and User

檢測細項	審查標準	參考來源	參考內容
		Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	Authorization
可信賴路徑	本指引 6.2.22	Collaborative Protection Profile for Network Devices	FTP_TRP.1/Admin Trusted Path (Refinement)
資源最大配額	本指引 6.2.23	Collaborative Protection Profile for Network Devices	FRU_RSA.1.1
資料流控制	本指引 6.2.24	Collaborative Protection Profile for Network Devices	FDP_IFC.2.1 FDP_IFF.1.1
		NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations, Revision 5	AC-4 INFORMATION FLOW ENFORCEMENT
安全屬性初始值	本指引 6.2.25	Collaborative Protection Profile for Network Devices	FDP_IFF.1.2 FDP_IFF.1.3 FDP_IFF.1.4 FDP_IFF.1.5
		NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations, Revision 5	AC-4 INFORMATION FLOW ENFORCEMENT (3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL

附錄二、實機測試項目與國際標準對照表

檢測項目	檢測細項	判定標準	參考來源	參考內容
安全功能測試	事件紀錄產出	本指引 7.1.1	Collaborative Protection Profile for Network Devices	FAU_GEN.1 Audit data generation
	管理者預設密碼安全	本指引 7.1.2	NIST Special Publication 800-53Security and Privacy Controls forFederal Information Systemsand Organizations	SA-4 ACQUISITION PROCESS Control Enhancements: (5) ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS
			OWASP IoT Top Ten	I1：Insecure Web Interface
	管理者鑑別及權限	本指引 7.1.3	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	FIA_UAU_EXT.2 Password-based Authentication Mechanism
	管理者遠端鑑別失敗控制功能	本指引 7.1.4	Network Device Collaborative Protection Profile (NDcPP) Extended Package-Wireless Local Area Network (WLAN) Access Systems	FIA_AFL.1 Authentication Failure Management
	使用者鑑別與管控功能測試	本指引 7.1.5	Collaborative Protection Profile for Network Devices	FIA_UIA_EXT.1 User Identification and Authentication
	登入畫面保密功能	本指引 7.1.6	Collaborative Protection Profile for Network Devices	FIA_UAU.7 Protected Authentication Feedback
	管理者權限有效時間	本指引 7.1.7	Collaborative Protection Profile for Network Devices	FTA_SSL_EXT.1 TSF-initiated Session Locking
	登入連線之終止	本指引 7.1.8	Collaborative Protection Profile for Network Devices	● FTA_SSL.3 TSF-initiated Termination (Refinement) ● FTA_SSL.4 User-initiated Termination (Refinement)
	韌體更新	本指引 7.1.9	Collaborative Protection Profile for Network Devices	FPT_TUD_EXT.1 Trusted Update
	網路通訊埠安全	本指引 7.1.10	OWASP IoT Top Ten	I3：Insecure Network Services

檢測項目	檢測細項	判定標準	參考來源	參考內容
	安全角色	本指引 7.1.11	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMR.1.3
	資源最大配額	本指引 7.1.12	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	Resource Allocation (FRU_RSA) FRU_RSA.1 Maximum Quotas
	網際網路流量管制功能	本指引 7.1.13	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	FDP_IFC.2.1. FDP_IFC.2.2 FDP_IFF.1.1
	區域網路流量管制功能	本指引 7.1.1.4	Protection Profile for Wireless Local Area Network (WLAN) Access Systems	FDP_IFC.2.1. FDP_IFC.2.2 FDP_IFF.1.1
壓力測試	吞吐量測試	本指引 7.2.1	NSS LABS Test Methodology - Wireless Networking	4.2 Capacity and Throughput
堅實測試	異常流量測試	本指引 7.3.1	NSS LABS Test Methodology - Wireless Networking	3.4.1 Exploit Library
	非正常關機恢復	本指引 7.3.2	NSS LABS Test Methodology - Wireless Networking	5 Stability and Reliability
穩定性測試	真實流量測試	本指引 7.4.1、7.4.2、7.4.3	NSS LABS Test Methodology - Wireless Networking	5 Stability and Reliability
弱點測試	共通弱點評估	本指引 7.5.1、7.5.2	NIST Special Publication 800-53Security and Privacy Controls forFederal Information Systemsand Organizations	RA-5 VULNERABILITY SCANNING
			Collaborative Protection Profile for Network Devices	Vulnerability Survey (AVA_VAN.1)
	惡意程式測試	本指引 7.5.3	UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	14. Malware Testing
			NIST Special Publication 800-53Security and	SI-3 MALICIOUS CODE PROTECTION

檢測項目	檢測細項	判定標準	參考來源	參考內容
			Privacy Controls forFederal Information Systemsand Organizations	(10) MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS
	模糊測試	本指引 7.5.4、7.5.5、7.5.6	NIST Special Publication 800-53Security and Privacy Controls forFederal Information Systemsand Organizations	SA-11 DEVELOPER SECURITY TESTING AND EVALUATION (8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	15 Malformed Input Testing
	動態分析	本指引 7.5.7	NIST Special Publication 800-53Security and Privacy Controls forFederal Information Systemsand Organizations	PE-19 INFORMATION LEAKAGE
			經濟部工業局行動應用 APP 基本資安規範	動態分析（Dynamic Analysis）
	WPS 測試	本指引 7.5.8	影像監控系統資安標準—第一部：一般要求	5.3.3.1 產品須提供使用者得自行開/關「Wi-Fi 保護設置 (WPS)」之 WPS PIN 功能，而其預設值須為關閉狀態。

附錄三、測試工具應備功能及要求說明表

檢測項目	檢測細項	測試工具	
		工具名稱	具備功能
安全功能測試	事件紀錄產出	不適用。	不適用。
	管理者預設密碼安全	不適用。	不適用。
	管理者鑑別及權限	不適用。	不適用。
	管理者遠端鑑別失敗控制功能	不適用。	不適用。
	使用者鑑別與管控功能測試	不適用。	不適用。
	登入畫面保密功能	不適用。	不適用。
	管理者權限有效時間	不適用。	不適用。
	登入連線之終止	不適用。	不適用。
	韌體更新	不適用。	不適用。
	網路通訊埠安全	不適用。	不適用。
	安全角色	不適用。	不適用。
	資源最大配額	不適用。	不適用。
	網際網路流量管制功能	不適用。	不適用。
	區域網路流量管制功能	不適用。	不適用。
壓力測試	吞吐量	吞吐量測試工具	（1）產生大小分別為 64、570、594 及 1,518 位元組之網路封包。 （2）依 57%、7%、16%及 20%之比例混合，持續向待測物發送混合後之網路封包。
堅實測試	異常流量測試	異常流量測試工具	（1）產生大量封包以中斷待測物網路服務。 （2）修改 EAP 協定中封包欄位數值功能。 （3）修改信框內容功能。
	非正常關機恢復	不適用。	不適用。
穩定性測	真實流量	真實流量測試工具	（1）具備至少 100 組 IP 位址同時上線使用網際網路所產生的網

檢測項目	檢測細項	測試工具	
		工具名稱	具備功能
試			路流量例如瀏覽網頁，收發電子郵件或是網上交談等。 （2）流量內容須涵蓋 9 種以上之應用程式或服務類型(包含 Chat、E-Mail、File Transfer、Game、P2P、Remote Access、Streaming、Web、Network Infrastructure Services 等)，及每種類型應至少包含 3 項(含)以上之應用程式或服務所產生之流量。
弱點測試	共通弱點評估	共通弱點評估工具	至少包含 NIST 發布之 CVE 漏洞資料庫。
	惡意程式測試	防毒軟體	（1）資安測試機構 AV-Test 最近一年測試結果，防護分數 (Protection Score)達 5.5 分以上。 （2）資安測試機構 AV-Comparatives 最近一年測試結果，Malware Protection Tests 取得 Advanced+（三星）等級。 （3）病毒、蠕蟲、木馬偵測功能。 （4）間諜、廣告軟體偵測功能。
	模糊測試	模糊測試工具	IEEE 802.11i 標準下產生變異樣本。
	動態分析	動態分析測試工具	（1）擷取網路封包。 （2）讀取網路封包內容。 （3）確認網路封包並無傳送資料到可疑 IP 位址或網站。
	WPS 測試	不適用。	不適用。