電信技術規範
檢驗規範

資通安全 0009 (IS0009-1)
修訂日期 102 年 3 月 13 日
通傳資技字第 10243008560 號

入侵偵測防禦系統
資通安全檢測技術規範

國家通訊傳播委員會

目　次

1. 概說　　5

2. 適用範圍5

3. 安全等級5

4. 參考標準5

5. 用語釋義6

6. 技術要求8

6.1. 書面審查類別 8

6.1.1. 安全標的.....8

6.1.2. 安全功能設計.....8

6.2. 書面審查類別之項目及判定標準　　8

6.2.1. 安全標的.....8

6.2.2. 安全功能設計.....15

6.3. 實機測試類別 18

6.3.1. 安全功能測試 (Security Functionality Test).....18

6.3.2. 壓力測試 (Stress Test).....18

6.3.3. 堅實測試 (Robustness Test).....19

6.3.4. 穩定測試 (Stability Test).....19

6.4. 實機測試類別之項目及判定標準　　19

6.4.1. 安全功能測試.....21

6.4.2. 壓力測試.....26

6.4.3. 堅實測試.....27

6.4.4. 穩定測試.....29

圖　次

圖 1　異常/攻擊偵測接續示意圖.....22
圖 2　安全管理功能測試接續示意圖.....24
圖 3　線上更新測試環境接續示意圖.....25
圖 4　吞吐量測試接續示意圖.....27
圖 5　阻斷式攻擊測試接續示意圖.....28
圖 6　流量錄製接續示意圖.....30
圖 7　流量重播接續示意圖.....30

表　次

表 1　書面審查之類別、項目及審查內容.....8
表 2　實機測試之類別、項目及判定標準.....19

附　錄

附錄一、安全功能介面表.....33
附錄二、子系統描述與分類表.....34
附錄三、安全架構描述表.....35

入侵偵測防禦設備資通安全檢測技術規範

1. 概說

入侵偵測防禦系統 (Intrusion Detection and Prevention system，以下簡稱 IDP) 能夠監視網路或網路設備的網路資料傳輸行為，當偵測到不正常或具有傷害性的網路資料傳輸行為時，能夠採取適當的防禦措施，免受惡意攻擊之影響。

2. 適用範圍

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網路型入侵偵測防禦系統，可檢測封包傳輸及阻擋網路應用層通訊協定之攻擊流量。

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)。

基礎型入侵偵測防禦系統

基礎型設備安全功能測試項目包括異常/攻擊偵測、安全管理、異常/攻擊事件紀錄及線上更新；壓力測試項目包括吞吐量；堅實測試項目包括阻斷式攻擊、躲避攻擊及非正常關機復原；穩定測試項目包括真實流量長時間測試。

進階型入侵偵測防禦系統

進階型設備除基礎型設備之測試項目外，另增加安全功能測試項目包括異常/攻擊偵測、使用者自訂安全規則及 IPv6 封包檢測；壓力測試項目包括最大同時連線數與最大建立連線速率；堅實測試項目包括異常流量；穩定測試項目包括真實流量長時間測試。

4. 參考標準

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

ICSA Network IPS Enterprise Certification Testing Criteria Version -1.4

5. 用語釋義

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，簡稱 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

入侵偵測防禦系統保護剖繪 (U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments)

指美國政府機關採購入侵偵測防禦系統之設備技術參考指引。

評估標的 (Target Of Evaluation, TOE)

指申請資通安全評估及驗證之產品及其相關使用手冊。

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彙(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 (Security Functional Requirement, SFR) 之相關功能。

安全屬性 (Security Attribute)

指定義主體、使用者 (包括設備外部資訊產品)、受體、資訊、對談 (Session)或資源的一種特性，並根據其定義的特性 (值) 來執行安全功能。

可信賴通道 (Trusted Channel)

指安全功能與一個外部可信賴的資訊產品達到安全通訊的方法。

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安全功能 (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)

指為評估標的 (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)

指安全功能本身無法被無關的程式碼或設施破壞，為安全架構的屬性之一。

繞道 (Bypass)

指避開待測物安全功能檢查之技巧。(如：未經過身分鑑別，直接進入稽核功能介面)。

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。

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	附錄一、安全功能介面表	Π	Π
	設計安全性	附表 1-4	附錄二、子系統描述與分類表		Π
	安全架構	附表 1-5	附錄三、 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	安全	1. 安全角色	安全功能應具備及設定以下安全角色： (1) 經授權的管理者 (2) 其他 (自行列舉)	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
標的	功能需求	2. 使用者屬性定義	安全功能應具備以下使用者屬性定義： (1) 使用者身分識別 (Identity) (2) 使用者被設定的角色屬性 (3) 其他 (自行列舉)	Π	Π
		3. 認證時序	安全功能應具備以下認證時序： (1) 列舉使用者身分認證前，可執行的安全功能(如 DHCP, Show Status 等)。 (2) 完成使用者身分認證後，始可執行被授權的安全功能。	Π	Π
		4. 認證失敗處理	安全功能應具備以下認證失敗處理： (1) 可偵測出認證連續失敗次數。 (2) 當使用者進行登入，連續認證失敗次數達到指定值時，應拒絕該使用者再次登入，經採取特殊處置後，始可重新登入。	Π	Π
		5. 安全功能行為管理	安全功能應具備以下安全功能行為管理： (1) 待測物數據蒐集功能之設定。 (2) 待測物數據分析與反應之設定。	Π	Π
		6. 安全功能資料管理	安全功能應具備以下安全功能資料管理： (1) 查詢/新增系統與稽核資料。 (2) 查詢/修改其他安全屬性資料。	Π	Π
		7. 安全功能之可用性	待測物在提供遠端可信賴資訊產品有關系統與稽核資料時，應確保資料的可用性。	Π	Π
		8. 安全功能相互傳輸時之機密性	待測物應具備在系統資料傳送給遠端可信賴資訊產品時 (如：下載特徵值(Signature)或遠端管理認證等機制)，保護資料免於被揭露。	Π	Π
		9. 安全功	安全功能應具備以下傳輸資料遭到修改時之偵測	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
		能間修改之偵測	能力： (1) 待測物在與遠端可信賴資訊產品間傳送或接收資料之間 (如：下載特徵值) 遭受非法竄改時，應予以偵測。 (2) 待測物應確認在與遠端可信賴資訊產品間所傳送或接收資料之完整性，當偵測資料遭修改時，定義所應採取的動作。		
		10. 可信賴之時戳	待測物應具備可信賴之時戳 (Reliable Timestamp)，正確記錄稽核資料的日期及時間。	Π	Π
		11. 稽核紀錄	安全功能應具備以下稽核紀錄： (1) 待測物應依下列事件類型產生其稽核紀錄，並存於資料庫中： A. 啟閉稽核功能。 B. 存取稽核資料。 C. 使用者登錄成功或失敗、登錄權限變更及恢復。 D. 變更安全屬性。 E. 變更系統時間。 (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	Π	Π
		12. 稽核紀錄之查詢	安全功能應具備以下稽核紀錄之查詢： (1) 可由被授權的管理者查詢各種稽核紀錄（含事件之稽核紀錄）。 (2) 稽核紀錄應以適合管理者理解之方式呈現。 (3) 可依設定條件查詢稽核紀錄。	Π	Π
		13. 稽核紀錄可用性之保	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。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
		證	(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。		
		14. 系統資料蒐集	安全功能應具備以下系統資料： (1) 待測物應從特定的資訊系統蒐集以下資訊(自行挑選)： A. 設備起始/關機 B. 系統登入記錄 C. 資料存取 D. 服務請求 E. 網路流量 F. 安全組態變更 G. 資料轉送 H. 已被偵測之惡意碼 I. 存取控制組態 J. 服務組態 K. 授權組態 L. 可靠之規則組態 M. 已被偵測之弱點 N. 其他 (自行列舉) (2) 待測物至少應可蒐集與記錄以下資訊之能力： A. 事件發生日期/時間 B. 事件類型 C. 識別發生來源 D. 事件發生的結果	Π	Π
		15. 系統資料分	安全功能應具備以下系統資料分析功能： (1) 待測物應對接收之資料執行以下分析工作： A. 接收資料之統計、特性及完整性	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
		析功能	B. 其他分析動作 (自行列舉) (2) 待測物應就資料分析結果記錄以下訊息： A. 日期與時間 B. 結果類型 C. 資料來源 D. 其他 (自行列舉)		
		16. 系統資料回應功能	待測物偵測到入侵行為時應發出警示，並採取回應措施 (自行列舉)。	Π	Π
		17. 受限制的系統資料審查	安全功能應具備以下限制系統資料審查之能力： (1) 待測物應可設定被授權使用者讀取特定系統資料。 (2) 系統資料應以適合管理者理解之方式呈現。 (3) 待測物應禁止未經授權使用者讀取系統資料。	Π	Π
		18. 系統資料可用性之保證	安全功能應具備以下系統資料可用性之保證： (1) 待測物應防止儲存的系統資料被非授權使用者刪除或竄改。 (2) 當發生系統資料保存機制失效時 (如：儲存空間已滿、設備故障或遭受攻擊)，設備安全功能應提供機制以維護已經儲存系統資料之可用性。	Π	Π
		19. 系統資料漏失之預防	當系統資料儲存空間耗盡時，除提供系統告警外，安全功能應執行下列動作之一，以維持儲存系統資料之功能： (1) 忽略新增之系統資料 (2) 保護被授權使用者所選擇的系統資料 (3) 每筆最新的系統資料必須從最舊的系統資料開始覆蓋	Π	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錄一、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錄二、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	設計	應說明如何以子系統組成安全功能規格之安全功能介		Π

類別	項目	審查標準	基礎型	進階型
功能設計	安全性	面，並說明安全功能子系統以下規格： (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錄三、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。		Π

類別	項目	審查標準	基礎型	進階型
		(4) 安全功能執行如何避免被繞道。		

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	Π	Π

類別	項目	審查標準	基礎型	進階型
		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 (如待測物需置於有門禁管制的環境等) C. 人員安全 (如僅有授權人員能存取待測物等) D. 連接安全 (如待測物與其他網路伺服器之連線安全等) (8) 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)

測試待測物於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	異常/攻擊偵測	1. 漏判測試： 依 6.4.1.1.3. (1) 進行測試，對於必測樣本之漏判率須小於或等於 10%。 2. 誤判測試: 依 6.4.1.1.3. (3) 進行測試，誤判率須小於或等於 5%。	Π	
		1. 漏判測試： 依 6.4.1.1.3. (2) 進行測試，對於必測樣本之漏判率須小於或等於 7%，對於加測樣本之漏判率須小於或等於 10%。 2. 誤判測試: 依 6.4.1.1.3. (3) 進行測試，誤判率須小於或等於 5%。		Π
	躲避攻擊	依 6.4.1.2.2. 進行測試，可阻擋惡意躲避偵測之攻擊行為。	Π	Π
	安全管理	依 6.4.1.3.2. 進行測試，應具備下列	Π	Π

類別	項目	判定標準	基礎型	進階型
		管理功能： 1. 具備通行碼 (Password) 管理。 2. 具備通行碼輸入錯誤次數之上限設定，錯誤輸入超過上限次數後須封鎖管理介面一段時間。		
	異常/攻擊事件紀錄	依 6.4.1.4.2. 進行測試，應正確記錄違反安全規則之事件名稱、時間、來源 IP、目的 IP 及內容。	Π	Π
	線上更新	依 6.4.1.5.2. 進行測試，應可透過網路進行線上更新特徵碼資料。	Π	Π
	IPv6 封包檢測	1. 依 6.4.1.6.2. (1) 進行測試，應可偵測 IPv6 之異常/攻擊網路封包。 2. 依 6.4.1.6.2. (2) 進行測試，應可偵測 IPv4 及 IPv6 混合之異常/攻擊網路封包。		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待測物安全功能應正常運作。	Π	Π
	最大同時連線數	依 6.4.2.2.2. 進行測試，當達到待測物規格說明之最大連線數時，不能發生斷線且待測物安全功能應正常運作。		Π
	最大連線建立速率	依 6.4.2.3.2. 進行測試，當達到待測物規格說明之最大連線建立速率時，不能發生斷線且待測物安全功能應		Π

類別	項目	判定標準	基礎型	進階型
		正常運作。		
堅實測試	阻斷式攻擊	依 6.4.3.1.2. 進行測試，不能發生當機、重開或斷線之情況。當攻擊結束後，安全功能應正常運作。	Π	Π
	遠端管理異常流量	依 6.4.3.2.2. 進行測試，待測物遠端管理介面對服務/協定異常流量應保持正常運作。		Π
	非正常關機復原	依 6.4.3.3.2. 進行測試，待測物應復原到非正常關閉電源前的狀態： (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。	Π	Π
穩定測試	真實流量測試	依 6.4.4.1.3. 進行測試，待測物應可持續 168 小時穩定運作。	Π	
		依 6.4.4.1.3. 進行測試，待測物應可持續 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. 異常/攻擊偵測

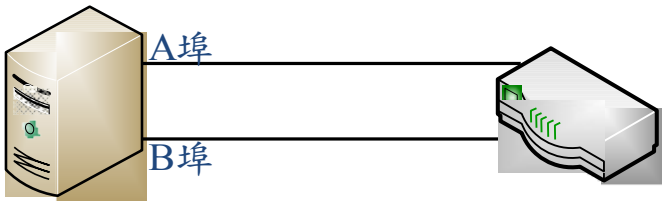


圖 1　異常/攻擊偵測接續示意圖

6.4.1.1.1. 測試環境

(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：模擬用戶端送收網路封包。
(3) 測試平台 B 埠：模擬伺服器端送收網路封包。
(4) 網路連接線：乙太網路線或光纖纜線。
(5) 連接測試平台及待測物如圖 1，其中乙太網路線或光纖線路連接數量依待測物運作模式 (如 Proxy 或 Transparent Mode) 決定。
(6) 代理模式 (Proxy Mode)：乙太網路線或光纖線路連接數量為一條，測試平台 A 埠及 B 埠為同一連接埠。
(7) 通透模式 (Transparent Mode)：乙太網路線或光纖線路連接數量為兩條，測試平台 A 埠及 B 埠為獨立的兩個連接埠。
(8) 開啟待測物之異常或攻擊偵測功能。

6.4.1.1.2. 測試樣本

(1) 必測樣本：自 NVD (美國國家弱點資料庫) 篩選待測物送測前一個月起一年內、CVSS ≧7.0 且與 IDP 設備相關之弱點，以此數量的 5% 為依據，由測試平台或儀器產生大於或等於該數量之測試樣本。

(2) 加測樣本：除上述必測樣本外，自 NVD (美國國家弱點資料庫) 篩選待測物送測前二至三年內、CVSS ≧7.0 且與 IDP 設備相關之弱點，以此數量的 5% 為依據，由測試平台或儀器產生大於或等於該數量之測試樣本。

6.4.1.1.3. 測試方法及標準

(1) 基礎型測試：使用測試平台將攻擊測試樣本之必測樣本自 A 埠送至基礎型待測物，B 埠無法收到異常或攻擊流量之封包，

並可記錄此異常或攻擊事件。基礎型待測物對於攻擊測試樣本之漏判率須小於或等於 10%。

(2) 進階型測試：使用測試平台將攻擊測試樣本之必測樣本及加測樣本分別自 A 埠送至進階型待測物，B 埠無法收到異常或攻擊流量之封包，並可記錄此異常或攻擊事件。待測物對於必測樣本之漏判率須小於或等於 7%，對於加測樣本之漏判率須小於或等於 10%。

(3) 誤判測試：使用測試平台自 A 埠產生無異常行為之樣本至少 5000 筆，B 埠可正常接收到封包且不會產生異常及攻擊事件之紀錄。基礎型及進階型待測物之誤判率皆須小於或等於 5%。

6.4.1.2. 躲避攻擊偵測

6.4.1.2.1. 測試環境 同 6.4.1.1.1.。

6.4.1.2.2. 測試方法及標準

開啟待測物預設之安全規則，使用測試平台自 A 埠各式躲避攻擊 (Evasion Attacks) 之流量，如：IP Packet Fragmentation、TCP Stream Segmentation 、URL Obfuscation 、FTP Evasion 及 RPC Fragmentation 等躲避攻擊之流量，確認無法從 B 埠收到躲避攻擊之封包。

6.4.1.3. 安全管理功能

6.4.1.3.1. 測試環境

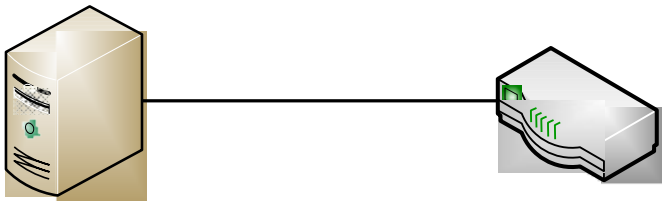


圖 2　安全管理功能測試接續示意圖

(1) 測試平台：可供測試人員連線至待測物之終端設備。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接待測物及測試平台如圖 2。

6.4.1.3.2. 測試方法及標準

(1) 由測試平台連線至待測物，確認待測物是否需要通行碼才可進行設定，待測物應須輸入正確通行碼才可進行管理設定。

(2) 嘗試輸入錯誤通行碼，待測物是否檢查當超過最大錯誤次數時，會封鎖管理介面一段時間，避免遭受攻擊。

6.4.1.4. 異常/攻擊事件紀錄

6.4.1.4.1. 測試環境

(1) 測試平台：可供測試人員連線至待測物之終端設備。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接待測物及測試平台如圖 2。

(4) 開啟待測物之異常/攻擊偵測功能。

6.4.1.4.2. 測試方法及標準

當違反安全事件紀錄的網路流量通過待測物，待測物的流量統計資訊應正確紀錄違反安全規則之事件名稱、時間、來源 IP、目的 IP 及內容。

6.4.1.5. 線上更新

6.4.1.5.1. 測試環境

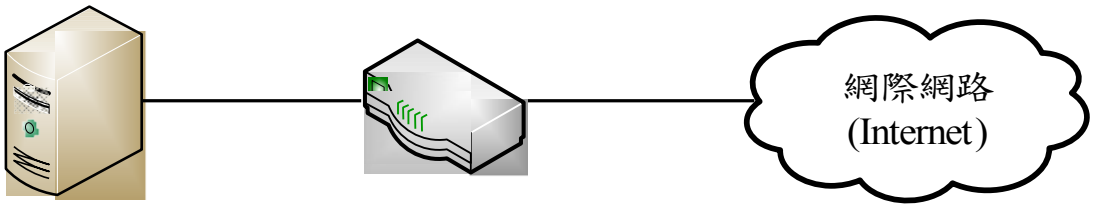


圖 3　線上更新測試環境接續示意圖

(1) 測試平台：可供測試人員連線至待測物之終端設備。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接待測物、測試平台與網際網路如圖 3。

(4) 開啟待測物之自動線上更新功能。

6.4.1.5.2. 測試方法及標準

待測物應至少每天一次自動進行線上入侵攻擊特徵碼之更新。

6.4.1.6. IPv6 封包檢測 (適用進階型)

6.4.1.6.1. 測試環境

(1) 測試平台：可產生 IPv4 及 IPv6 網路封包之測試儀器或程式。
(2) 測試平台 A 埠：模擬用戶端送收網路封包。
(3) 測試平台 B 埠：模擬伺服器端送收網路封包。
(4) 網路連接線：乙太網路線或光纖纜線。
(5) 連接測試平台及待測物如圖 1，其中乙太網路線或光纖線路連接數量依待測物運作模式 (如 Proxy 或 Transparent Mode) 決定。
(6) 代理模式 (Proxy Mode)：乙太網路線或光纖線路連接數量為一條，測試平台 A 埠及 B 埠為同一連接埠。
(7) 通透模式 (Transparent Mode)：乙太網路線或光纖線路連接數量為兩條，測試平台 A 埠及 B 埠為獨立的兩個連接埠。
(8) 開啟待測物之異常/攻擊偵測功能。

6.4.1.6.2. 測試方法及標準

(1) 以測試平台自 A 埠產生異常/攻擊之 IPv6 網路流量通過待測物，待測物應偵測異常/攻擊之網路封包，並可正確紀錄此異常/攻擊事件。
(2) 設定待測物對異常/攻擊流量進行阻擋，以測試平台自 A 埠產生異常/攻擊之 IPv4 及 IPv6 混合網路流量通過待測物，待測物應偵測異常/攻擊之網路封包，並正確紀錄此異常/攻擊事件。

6.4.2. 壓力測試

6.4.2.1. 吞吐量測試

6.4.2.1.1. 測試環境

(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：模擬用戶端送收網路封包。
(3) 測試平台 B 埠：模擬伺服器端送收網路封包。

(4) 網路連接線：乙太網路線或光纖纜線。
(5) 連接測試平台及待測物如圖 4，其中乙太網路線或光纖線路連接數量依待測物運作模式 (如 Proxy 或 Transparent Mode) 決定。
(6) 代理模式 (Proxy Mode)：乙太網路線或光纖線路連接數量為一條，測試平台 A 埠及 B 埠為同一連接埠。
(7) 通透模式 (Transparent Mode)：乙太網路線或光纖線路連接數量為兩條，測試平台 A 埠及 B 埠為獨立的兩個連接埠。
(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。

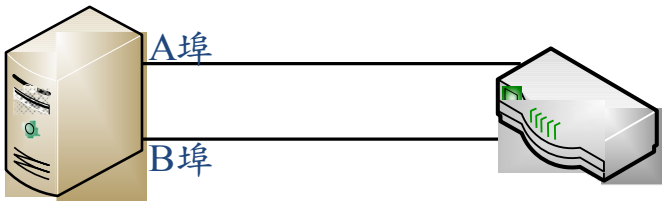


圖 4　吞吐量測試接續示意圖

6.4.2.1.2. 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，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。

6.4.2.2. 最大連線數 (適用進階型)

6.4.2.2.1. 測試環境 同 6.4.2.1.1.。

6.4.2.2.2. 測試方法及標準

測試平台每秒建立一條自 A 埠經待測物至 B 埠之連線。當達到待測物規格說明之最大連線數時，不能發生斷線且待測物安全功能應正常運作。

6.4.2.3. 最大連線建立速率 (適用進階型)

6.4.2.3.1. 測試環境 同 6.4.2.1.1.。

6.4.2.3.2. 測試方法及標準

測試平台建立自 A 埠經待測物至 B 埠之連線，並逐漸提高連線建立速率，當達到待測物規格說明之最大連線建立速率時，不能發生斷線且待測物安全功能應正常運作。

6.4.3. 堅實測試

6.4.3.1. 阻斷式攻擊

6.4.3.1.1. 測試環境

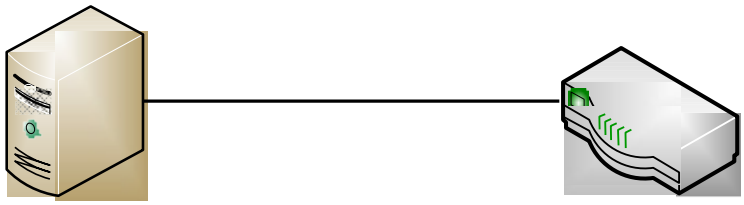


圖 5　阻斷式攻擊測試接續示意圖

(1) 測試平台：可產生大量網路流量之測試儀器或程式。
(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 5。
(4) 開啟待測物之安全功能。
(5) 測試平台針對待測物的服務連接埠，發動阻斷式攻擊。

6.4.3.1.2. 測試方法及標準

測試平台產生待測物規格說明之最大吞吐量 300%的 HTTP 封包，持續 600 秒攻擊待測物開啟的連接埠以阻斷其服務，待測物不能發生當機、重開或斷線之情況。當攻擊結束後，安全功能應正常運作。

6.4.3.2. 遠端管理異常流量

6.4.3.2.1. 測試環境

(1) 測試平台：可產生大量網路流量之測試儀器或程式。
(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 5。
(4) 開啟待測物之安全功能。

(5) 透過待測物提供的終端管理介面進入待測物進行設定，開啟待測物之遠端管理功能。

6.4.3.2.2. 測試樣本

以測試平台針對待測物提供之每項服務皆產生 10 種異常流量作為測試樣本。

6.4.3.2.3. 測試方法及標準

測試平台送出測試樣本至待測物，待測物之遠端管理功能應正常運作。

6.4.3.3. 非正常關機

6.4.3.3.1. 測試環境 無

6.4.3.3.2. 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。

6.4.4. 穩定測試

6.4.4.1. 真實流量測試

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，測試環境同 6.4.4.1.1.。

6.4.4.1.1. 測試環境

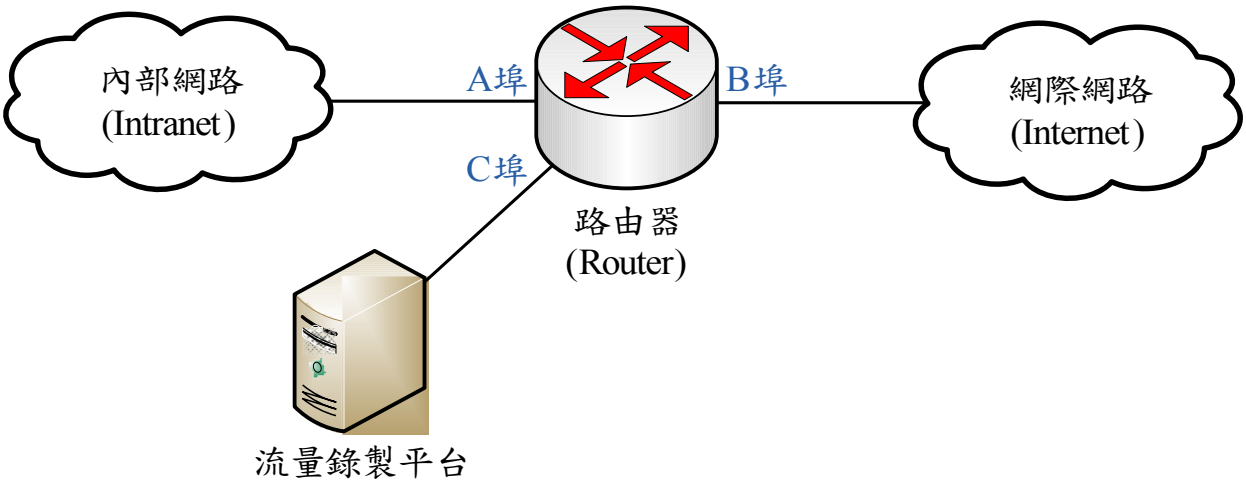


圖 6　流量錄製接續示意圖

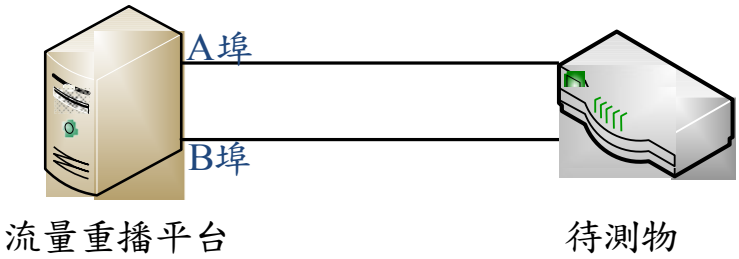


圖 7　流量重播接續示意圖

(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 6。

(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：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 7。

(7) 網路封包來源 IP 位址如屬內部網路，流量重播平台將網路封包經 A 埠送至待測物；反之，來源 IP 位址如屬網際網路，則網路封包經 B 埠送至待測物。

6.4.4.1.2. 測試樣本

測試樣本必須滿足以下要求：

(1) 具備至少 100 位使用者同時上線的網路流量。

(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、qqtv、pplive、ppstream、qvod、flashcom、itunes、rtp 及 shoutcast。

H. VoIP：skype 及 sip。

I. Web：http、https、http download、http video 及 http range get。

J. Others：hopster、softether、dns、snmp、oracle 及 ms-sql。

6.4.4.1.3. 測試方法及標準

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

(2) 測試過程待測物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。

附件

附件一、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* *認證失敗*

附件二、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錄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: 傳遞認證資訊給 Subsystem_auth，並由回覆訊息確認認證是否成功* *(B) Subsystem_terminal: ...*

附件三、安全架構描述表

項目	說明	
1.安全領域 Security Domain	**安全領域名稱**	**安全領域說明**
	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。*

項目	說明	
2.初始程序 Secure Initialization	**相關元件**	**初始程序說明**
	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。*

項目	說明		
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。*

項目	說明	
4.防止繞道 Non- Bypassibility	**防止繞道功能**	**防止繞道機制說明**
	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認證操控待測物。* *防範作法：以實體封鎖方式，防止利用維護介面繞道身分認證程序。*