入侵偵測防禦系統資通安全檢測技術規範

第 6 點修正總說明

為使本技術規範對目前市場上產品有更精確之技術要求，及參酌本會 101 年「資通設備之安全檢測規範增修訂及推廣計畫」委託研究案期末報告書，爰修訂入侵偵測防禦系統資通安全檢測技術規範第 6 點技術要求部分規定，修正對照表如下：

入侵偵測防禦系統資通安全檢測技術規範

第 6 點修正對照表

現行規定	修正規定	說明
6.4.1.1.2 (1) 基礎型測試樣本自 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 大於或等於 7.0 分且與 IDP 相關弱點數量的 5% 為依據。由測試儀器或攻擊程式產生至少等於該數量之攻擊測試樣本。 (2) 進階型測試樣本自 NVD (美國國家弱點資料庫) 篩選待測物送測前一個月起三年內、CVSS 大於或等於 7.0 分且與 IDP 相關弱點數量的 10% (一年內之弱點數量必須佔半數以上) 為依	(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。	6.4.1.1.2 測試樣本部份，進階型之測試樣本鑑別度不足，故將樣本部分調整為必測樣本與加測樣本，提高進階型設備之鑑別度。

現行規定	修正規定	說明
據。由測試平台產生至少等於該數量之攻擊測試樣本。		
6.4.1.1.3. (1)設定待測物對異常及攻擊流量進行阻擋，使用測試平台將攻擊測試樣本自A埠送至待測物，B埠無法收到異常及攻擊流量之封包，並可記錄此異常及攻擊事件。基礎型及進階型待測物，對於攻擊測試樣本之漏判率皆須小於或等於10%。 (2)使用測試平台自A埠產生無異常或攻擊行為之樣本至少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%。	(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%。	除測試樣本外，增加考量漏判通過率提升，不同弱點測試樣本set、涵蓋度等，提高進階型設備更嚴謹之鑑別度設計。
6.4.2.1.1. (9)測試平台產生大小為64、570、594及1518位元組之網路封包，將其依IMIX之比例57%、7%、16%及20%混合，時間至少60秒。	(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。	測試時間至少60秒的描述過於模糊，不同實驗室間可能使用60秒、120秒或300秒進行測試造成測試標準不一。壓力測試之測項對待測物加壓之時間應有一致的標準，故於技術規範中將加壓之時間“至少60秒”改為定值“60秒”

現行規定	修正規定	說明
		進行壓力測試。
6.4.3.1.2. 測試平台送出大量的網路流量，持續 600 秒攻擊待測物開啟的連接埠，並阻斷其服務。當攻擊流量低於或等於待測物規格說明之吞吐量最大值時，安全功能應正常運作。	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。	未清楚定義何謂阻斷式攻擊流量之內容與流量大小，將造成測試標準不一。建議指定待測物規格說明最大吞吐量 300% 的 HTTP 封包為阻斷式攻擊流量。
6.4.3.2.2. 以測試平台產生之服務或協定異常流量至少 10 種作為測試樣本。	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。	通常待測物會提供至少 1 種以上之服務，但規範原文可能造成(1)每項服務需要至少 10 個測試樣本或(2)全部服務至少有 10 個測試樣本等兩種不同解讀。如為後者之知況，若 10 個測試樣本都只針對其中一種服務進行測試，將無法驗證其他服務的安全狀態。
6.4.3.3.2. 待測物運作期間不正常關閉電源時，經重新啟動後，待測物應可復原到非正常關閉電源前的最後狀態。	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。	恢復到關閉電源前的最後狀態描述過於模糊，建議修正為待測物斷電後需回復至以下要求：(1)最後設定的系統組態、(2)保留斷電時間點前最後 5 分鐘的日誌檔案以及(3)可使用最後設定的系統組態正常開機。
6.4.4.1.2. (4) 流量最大速度在	(4)流量之平均速率在測試期間應維持待測	原文將造成用來測試待測物的流量介於

現行規定	修正規定	說明
測試期間需達待測物規格說明處理能力最大值之50%以上。	物規格說明處理能力最大值之50%。	50%～∞範圍，當標準訂為50%時，對待測物而言相對容易通過，但標準超過100%時，則待測物形同處於阻斷式攻擊的狀況下。此外，真實環境的網路流量呈現非固定數值，為保留真實流量測試的精神與意義，穩定測試不應採用固定百分比的方式進行流量重播。為取得一致的測試標準，重播之網路流量須以線性放大或縮小之原則使其維持待測物規格說明處理能力最大值之50%。