網路型防火牆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5月29日召開「防火牆及入侵偵測防禦系統資通安全檢測技術規範」實機測試紀錄研討會議之檢測報告，爰修訂網路型防火牆資通安全檢測技術規範第6點技術要求部分規定，主要修正重點分述如下：

1. 6.4.1.1封包過濾-刪除測試平台產生之網路封包須符合IMIX之規定。
2. 6.4.1.3安全事件紀錄-防火牆未必支援病毒防護，故修正測試平台產生測試樣本之樣式。
3. 6.4.2壓力測試-刪除進行壓力測試時，不能發生封包遺失之要求。

網路型防火牆資通安全檢測技術規範

第6點修正對照表

| 修正規定 | 現行條文 | 說明 |
| --- | --- | --- |
| 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) 開啟待測物之封包過濾功能。 | 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) 開啟待測物之封包過濾功能。  (9) 測試平台產生大小為64、570、594及1518 位元組之網路封包，將其依IMIX之比例57%、7%、16%及20%混合，時間至少 60 秒。 | 封包過濾測試所用之測試封包，不須符合IMIX 之要求，故刪除之。 |
| 6.4.1.1.2. 測試方法及標準  (3) 使用測試平台自A埠產生一來源IP位址為特定IP的封包，並關閉待測物封包過濾功能，B埠應可接收該封包。 | 6.4.1.1.2. 測試方法及標準  (3) 使用測試平台自A埠產生一目的IP位址為特定IP的封包，待測物關閉封包過濾功能，B埠收到測試封包。 | 自A埠產生之封包應為來源IP位址為特定IP之封包。 |
| 6.4.1.3.1. 測試環境  (1) 測試平台A：可模擬終端使用者之測試儀器或程式。  (2) 測試平台B：可模擬伺服器之測試儀器或程式。  (3) 連接待測物、測試平台A及測試平台B如圖3。  (4) 開啟待測物之安全防護及事件記錄功能。  (5) 由測試平台A產生違反安全事件之網路流量經待測物連線至測試平台B。 | 6.4.1.3.1. 測試環境  (1) 測試平台A：可模擬終端使用者之測試儀器或程式。  (2) 測試平台B：可產生病毒測試樣本並提供網路服務之測試儀器或程式。  (3) 連接待測物、測試平台A及測試平台B如圖3。  (4) 開啟待測物之病毒防護及安全記錄功能。  (5) 由測試平台A連線至測試程式平台B並下載病毒檔案。 | 防火牆未必支援病毒防護，故改以產生違反安全事件之網路流量，來觸發待測物產生安全事件紀錄。 |
| 6.4.1.4.2. 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。 | 6.4.1.4.2. 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密碼才可進行設定，待測物應須輸入正確密碼才可進行管理設定。  (2) 嘗試輸入錯誤密碼，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。 | 將密碼用語統一改為通行碼，避免混淆。 |
| 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。 | 6.4.2.1.2. 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，不能發生封包遺失且待測物安全功能應正常運作。 | 進行壓力測試時，待測物丟棄部分封包屬正常功能，故刪除此要求。 |