附件

關鍵電信基礎設施資通設備資通安全檢測技術規範

1. 法源依據

本規範依電信管理法（以下簡稱本法）第四十二條第八項規定訂定之。

2. 適用範圍

本規範適用於經國家通訊傳播委員會（以下簡稱本會）依本法第四十二條第一項規定，指定公眾電信網路之全部或一部為關鍵電信基礎設施，其設施內所設置具乙太網路介面之防火牆、交換器、路由器（以下統稱資通設備）。

3. 技術標準

本規範係參考資通安全責任等級分級辦法附表十之資通系統防護基準、美國 NIST SP 1800-14 及 Forum of Incident Response and Security Teams (FIRST) CVSS Based Patching Policy 等定之。

4. 用詞定義

4.1 防火牆(Firewall)

指放置在網路環境間的安全閘道或柵欄(包含專用的裝置或由多個組件與技術所結合之裝置)，所有從一個網路環境到另一個網路環境的訊務流經該裝置，只有經授權的訊務可以通過，反之亦然。

4.2 交換器(Switch)

指由內部交換機制提供網路裝置連接能力的裝置。

4.3 路由器(Router)

指依選路協定機制與演算法選擇路徑或選路，用來建立與控制不同網路間資料流的網路裝置，網路可能依據不同的網路協定。

4.4 傳送層安全協定(Transport Layer Security, TLS)

指於二個應用程式之間透過網路建立安全通道，定義於 RFC 5246，可防止交換資料時遭竊聽及篡改。

4.5 國家脆弱性資料庫(National Vulnerabilities Database, NVD)

指美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)提供的國家脆弱性資料庫，負責常見脆弱性與漏洞之資料的發布及更新。

4.6 共同脆弱性及曝露(Common Vulnerabilities and Exposures, CVE)

指美國國土安全部贊助之脆弱性管理計畫，該計畫針對每一脆弱性項目賦予其全球認可唯一共同編號。

4.7 共同脆弱性計分系統(Common Vulnerability Scoring System, CVSS)

指一套共同脆弱性計分系統的判定標準，包括威脅所造成損害的嚴重性、資通安全脆弱性的可利用程度與攻擊者不當運用該脆弱性的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，而 10 則代表最高風險。

4.8 通行碼(Password)

指一組字元串，能使系統辨識用戶身分，並可進一步控管用戶存取之權限。

4.9 安全事件日誌(Security Event Log)

指每個規則所定義之活動紀錄，用以發現及察覺威脅或攻擊事件的發生(例：用戶登入系統)。

4.10 安全通道(Security Tunnel)

指網際網路通訊端點與端點(End-to-End)間，兼顧資料隱密性及完整性所建立之通道，例：目前常見之實作通訊協定為安全接套層(Secure Sockets Layer, SSL)及傳送層安全協定(Transport Layer Security, TLS)。

4.11 加密(Encryption)

指明文資訊透過演算法進行轉換而達到保密的目的。

4.12 管理介面(Management Interface)

指透過本地端或遠端網路取得裝置系統之操控權的介面，例：

(1)於操控程式、網頁管理介面或指令介面執行產品維護、存取裝置資源。

(2)於操控程式、網頁管理介面或指令介面進行系統設定，例：網際網路協定(Internet Protocol, IP)位址。

5. 測試項目

5.1 關鍵電信基礎設施設置之資通設備，除本規範另有規定外，應符合有關機關國家安全考量及5.3與5.4規定。

5.2 資通設備功能含括5.4所列其他設備功能者，亦須符合含括設備之規定。

5.3 共通測試項目及合格標準

5.3.1 存取控制

5.3.1.1 帳戶閒置逾時管理

待測物應具備帳戶閒置逾時管理機制，即閒置超過設定時間時，待測物應將帳戶鎖定或登出，經重新輸入帳戶名稱與通行碼始可持續操作。

5.3.1.2 帳戶登入鑑別失敗管理

待測物應具備帳戶登入鑑別失敗管理機制；帳戶鑑別失敗超過設定次數時，待測物應在設定時間內限制該帳戶登入或限制使用權限。

5.3.1.3 帳戶角色權限管理

待測物應具備設定二組以上及授權相異帳戶角色之功能。

5.3.1.4 遠端登入存取管理

待測物具備遠端登入存取功能者，資料傳輸應符合5.3.3.1遠端存取傳送加密規定。登入、存取及管理介面操作行為之紀錄保存應符合5.3.2.1安全事件日誌紀錄規定。

5.3.1.5 通行碼輸入遮蔽保護

待測物以通行碼進行鑑別者，輸入之通行碼應以特殊符號遮蔽。

5.3.1.6 通行碼儲存安全

待測物以通行碼進行鑑別者，該通行碼應加密或經雜湊處理後儲存。

5.3.2 稽核與可歸責性

5.3.2.1 安全事件日誌紀錄

待測物應具備以日誌方式記錄包括帳戶登入及登出、組態設定、韌體更新等管理介面操作行為，以及可信任通道連接之建立、終止及建立失敗、終止失

敗等事件，與事件發生之時間戳記等。

5.3.2.2 安全事件日誌紀錄保護

安全事件日誌紀錄不得被未經授權之帳戶存取、刪除或修改。

5.3.2.3 時戳及校時

待測物內部時鐘每二十四小時應至少與世界協調時間(Coordinated Universal Time)或格林威治平均時間(Greenwich Mean Time)同步校時一次，以確保時間戳記(Timestamp)之正確性。

5.3.3 系統與通訊保護

5.3.3.1 遠端存取傳送加密

待測物具備遠端登入存取功能者，其資料傳輸應採用 TLS 1.2 以上之安全通道，並使用進階加密標準(Advanced Encryption Standard)128 位元或同等加密強度以上之加密演算法。

5.3.4 系統弱點及漏洞

5.3.4.1 已知弱點及漏洞

待測物之作業系統與網路服務無 CVSS 評分 7.0 分以上之 CVE。

5.3.5 持續性測試

5.3.5.1 非正常電源中斷

待測物經非正常電源中斷，再重新啟用後，待測物之安全政策、安全事件日誌、登入鑑別資料、遠端管理組態，應與電源中斷前一致。

5.3.5.2 組態備份及還原

待測物應具備組態備份及還原功能。

5.4 個別設備測試項目及合格標準

5.4.1 防火牆

5.4.1.1 封包過濾規則

待測物應可阻擋特定過濾條件之封包，過濾條件至少包括封包來源端與目的端之 IP 位址、連接埠號碼(Port number)及所採用之通訊協定(如：TCP、UDP 及 ICMP)等。

5.4.1.2 靜態網路位址轉換

待測物應具備將內部 IP 位址與外部 IP 位址相互轉換之功能。

5.4.1.3 動態網路位址轉換

待測物應具備將多個內部 IP 位址以動態隨機方式，對應到多個外部 IP 位址之功能。

5.4.1.4 異常流量測試

待測物在連續接收異常流量（即違反安全政策規則之流量）八小時期間，應依設定之安全政策正確過濾封包，並就異常流量提出警示。

5.4.1.5 流量限制功能

待測物應具備流量限制功能，以限制接收或轉送網路介面之傳輸流量。

5.4.1.6 防火牆通訊協定安全測試

待測物在連續接收混合下列協定之變異封包八小時期間，應正常運作：

(1)網際網路協定第四版(Internet Protocol Version 4, IPv4)(RFC 791)。

(2)網際網路協定第六版(Internet Protocol Version 6, IPv6)(RFC 8200)。

(3)網際網路控制訊息協定第四版(Internet Control Message Protocol Version 4, ICMPv4)(RFC 792)。

(4)網際網路控制訊息協定第六版(Internet Control Message Protocol Version 6, ICMPv6)(RFC 4443)。

5.4.2 交換器

5.4.2.1 位址解析協定(Address Resolution Protocol, ARP)安全機制

待測物應具備ARP欺騙攻擊之防護機制。

5.4.2.2 虛擬區域網路(Virtual Local Area Network, VLAN)安全機制

待測物應具備雙層封裝802.1Q(Double Encapsulated 802.1Q) VLAN跳躍攻擊之防護機制。

5.4.2.3 內容可定址記憶體(Content Addressable Memory, CAM)表格安全機制

待測物應具備媒介接取控制(Media Access Control, MAC)流量攻擊之防護機制。

5.4.2.4 交換器通訊協定安全測試

待測物在連續接收混合下列協定之變異封包八小時期間，應正常運作：

(1)ARP(RFC 826)。

(2)乙太網路媒體存取控制訊框(Ethernet MAC Frame)(IEEE 802.3)。

(3)乙太網路控制訊框(Ethernet Control Frame)(IEEE 802.3)。

(4)VLAN標記(Tag)(IEEE 802.1Q)。

(5)鏈結層發現協定(Link Layer Discovery Protocol, LLDP)(IEEE 802.1AB)。

5.4.3 路由器

5.4.3.1 路由資訊保護機制

待測物應具備路由資訊保護或資源公鑰基礎建設(Resource Public Key Infrastructure, RPKI)機制，僅接受可信來源之路由資訊。

5.4.3.2 路由器通訊協定安全測試

待測物在連續接收混合下列協定之變異封包八小時期間，應正常運作：

(1)路由資訊協定(Routing Information Protocol,RIP)(RFC 2453)。

(2)開放式最短路徑優先協定(Open Shortest Path First, OSPF)(RFC 2328)。

(3)邊界閘道器協定(Border Gateway Protocol, BGP)(RFC 4271)。

(4)IPv4(RFC 791)。

(5)IPv6(RFC 8200)。

6. 設備認證規定

6.1 申請程序

6.1.1 關鍵電信基礎設施設置者、資通設備製造商、進口商、經銷商或代理商，申請資通設備資安審驗（即認證）時，應填具關鍵電信基礎設施資通設備資通安全審驗申請書，並檢附下列文件之紙本或電子檔向本會或本會委託之關鍵電信基礎設施資通設備驗證機構（以下簡稱驗證機關（構））提出申請。經審驗合格者，由驗證機關（構）核發印有審驗合格標籤式樣之審驗合格證明：

(1)正體中文或英文之設備使用手冊或說明書（包括軟體更新支援週期、年限，及不再提供更新時之設備更換計畫）。

(2)依第5點所為之資通設備資通安全測試報告（以下簡稱測試報告）。

(3)正體中文或英文之原廠設備性能規格資料、型錄、軟韌體版本號編碼原則，與設備功能、安全功能、管理功能之架構圖或方塊圖，及安全功能摘要表。設備性能規格資料至少應包括：

I. 防火牆：吞吐量（Throughput）、每秒最大建立連線數、最大同時連線數量、效能穩定度及效能可靠度。

II. 交換器：吞吐量／頻寬、生成樹（Spanning Tree）防護、效能穩定度及效能可靠度。

III. 路由器：吞吐量／頻寬、最大路由設定數、效能穩定度及效能可靠度。

(4)軟韌體開發供應鏈安全聲明。

(5)申請者為本國自然人應檢附身分證明文件，本國法人、非法人團體或外國製造商應檢附設立相關證明文件。

(6)其他經主管機關要求提供之審驗相關資料。

(7)包括(1)至(6)之資料電子檔（以電子檔申請者免附）。

6.1.2 申請審驗檢附之文件，除電子檔由驗證機關（構）留存外，其餘文件於核發審驗合格證明時一併發還。

6.1.3 測試報告應由經財團法人全國認證基金會（以下簡稱認證組織）認證，且經本會認可，具執行本技術規範測試內容之測試機構出具。無測試機構可提供測試服務時，申請者應依下列順序洽相關機構提供測試報告：

(1)他國取得國際實驗認證聯盟(International Laboratory Accreditation Cooperation, ILAC)會員資格之認證組織認可之測試實驗室。

(2)設備製造商。

6.1.4 測試報告內容應包括下列各項：

(1)申請者名稱及地址。

(2)測試機構之名稱及地址。

(3)測試報告之唯一識別及每一頁上之識別。

(4)設備製造商名稱及地址。

(5)設備名稱、廠牌、型號、軟韌體版本及4×6吋以上正面清晰可辨之彩色照片或圖片，其廠牌、型號須清晰可辨讀，並包含樣品之頂視圖、底視圖、左視圖、右視圖、正視圖及背視圖。

(6)測試項目及合格標準。

(7)測試紀錄及判定結果。

(8)測試設備之名稱、廠牌、型號、軟韌體版本及參考之NVD版本。

(9)測試受理及完成日期。

(10)執行測試人員及報告簽署人之姓名、職稱及簽名。

6.1.5 應檢附之文件或物品誤漏或不全時，驗證機關（構）應通知申請者於一個月內補正；屆期未補正或補正仍不完備者，駁回其申請。

6.1.6 驗證機關（構）依第5點審驗。經審驗不合格者，驗證機關（構）得列舉不合格事項，通知申請者於二個月內改善；屆期未改善或改善後再次審驗仍不合格者，駁回申請。

6.1.7 申請者與申請測試報告者不同時，申請者應另行檢附公司或商業登記證明文件影本，及測試報告使用之授權書。

6.1.8 關鍵電信基礎設施設置者申請資通設備審驗者，其結果適用於所有同廠牌同型號同軟韌體版本之資通設備。資通設備製造商、進口商、經銷商或代理商申請審驗者，審驗結果適用其同廠牌同型號同軟韌體版本之資通設備。除本規範另有規定外，同軟韌體版本以資通設備之大修正版本（Major/Main release）為原則。

6.1.9 不同廠牌、型號之資通設備應分別申請審驗。經審驗合格之資通設備，如變更其廠牌、型號，應重新申請審驗；軟韌體版本變更者，應於十四日內以書面敘明版本及性能差異報請原驗證機構備查；必要時，驗證機構得要求重新審驗或就變更部分進行審驗。

6.2 審驗合格證明管理

6.2.1 審驗合格標籤專屬取得審驗合格證明者所有。取得審驗合格證明者檢具下列文件，報請驗證機關備查後，得同意他人於同廠牌、型號及韌體版本之關鍵資通設備使用該審驗合格標籤：

(1)審驗合格證明影本。

(2)使用人之公司或商業登記證明文件影本。

6.2.2 取得資通設備審驗合格證明之資通設備製造商、進口商、經銷商或代理商，其審驗合格之資通設備有下列情形之一時，核發其審驗合格證明之驗證機關（構）應於該設備審驗合格證明註記「安全漏洞待修補」字樣。經取得審驗合格證明者，檢附測試機構出具資通設備已修補相關CVE之測試報告予驗證機構，驗證機關（構）始予塗銷審驗合格證明「安全漏洞待修補」註記。

(1)資通設備之作業系統或網路服務，經披露具CVSS評分7.0分以上之CVE，未於披露之日起十四日內，檢附檢測機構出具足以佐證該CVE已修補完成之測試報告。

(2)資通設備之作業系統或網路服務，經披露具CVSS評分4.0-6.9分(含)之CVE，未於披露之日起四十五日內，檢附檢測機構出具足以佐證該CVE已修

補完成之測試報告。

(3)資通設備之作業系統或網路服務，經披露具CVSS評分0.1-3.9分(含)之CVE，未於披露之日起六個月內，檢附檢測機構出具足以佐證該CVE已修補完成之測試報告。

6.2.3 有下列情事之一者，得廢止或撤銷其審驗合格證明：

(1)申請審驗時提供不實資料。

(2)違反6.1.9規定。

(3)經抽驗未符合5.1及5.2規定。

(4)因代理權、專利權爭議，經法院判決敗訴確定或違反其他規定致不得販賣。

(5)經有關機關公告或通知有危害國家安全之虞。

6.2.4 審驗合格證明遺失或毀損時，得檢附換（補）發申請書，向原驗證機關（構）申請補發或換發。

6.2.5 審驗合格證明登載事項變更符合下列情形之一者，向原驗證機關（構）申請換發：

(1)製造商變更或新增。

(2)申請者變更名稱或地址。

(3)申請者因公司合併或分割，經報請主管機關同意由合併或分割後存續或新設之公司使用原審驗合格證明。

6.2.6 依前項規定申請換發，應檢附文件如下：

(1)屬6.2.5(1)者：換（補）發申請書、設備委託生產相關證明文件及設備符合技術規範之聲明書。

(2)屬6.2.5(2)者：換（補）發申請書、自然人應檢附身分證明文件（雙證件）影本，法人、非法人團體應檢附設立相關證明文件影本。

(3)屬6.2.5(3)者：換（補）發申請書、公司或商業登記證明文件、主管機關同意函。

6.3 附則

6.3.1 本規範所定之相關書表、作業流程及審驗合格證明格式，由本會訂定公告之。

6.3.2 申請審驗、審驗合格證明補發或換發者，應依本會所定收費標準向驗證機關(構)繳交審驗費或證照費。