入侵偵測防禦系統資通安全檢測技術規範

逐點說明

條文	說明
1.概說 入侵偵測防禦系統(Intrusion Detection and Prevention system，以下簡稱 IDP)是補充防毒軟體和防火牆功能的網路安全設備。IDP 能夠監視網路或網路設備的網路資料傳輸行為，當偵測到一些不正常或是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，如即時中斷、調整或隔離。	說明入侵偵測防禦系統之基本功用
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，可支援開放系統介面(OSI, Open System Interface)至第七層應用層(Layer 7)，支援預設安全策略或自訂安全策略，用以檢測封包傳輸及阻擋異常或攻擊流量。	明定本技術規範之適用範圍
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)之入侵偵測防禦系統(IDP)，對於進階型入侵偵測防禦系統比基礎型有更嚴格的技術要求。* 3.1.基礎型入侵偵測防禦系統 指具有安全稽核、身分認驗證、資料安全管理、功能自我保護、入侵偵測等功能之防禦系統。 3.2.進階型入侵偵測防禦系統 指具有基礎型入侵偵測防禦功能外，還須具備資料加密、資源配置等功能之防禦系統。	明定設備安全等級區分為基礎型(Basic)與進階型(Advanced)。
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* *NSS IPS Group Test Methodology Version-6.1*	明定本技術規範之參考依據。
5.用語釋義 *5.1.共同準則* 為資通安全產品評估及驗證之標準之一，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、測試實驗室	定義及解釋本技術規範所使用之專業用語。

條文	說明
與驗證機關(構)評估及驗證資通安全產品安全性與功能性之依據。參考網址 http://www.commoncriteriaportal.org *5.2.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。 *5.3.評估標的(Target Of Evaluation, TOE)* 指申請評估及驗證之產品及其相關使用手冊。 *5.4.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。 *5.5.安全標的(Security Target, ST)* 指產品能符合保護剖彙(PP)或特定安全需求製作之規格文件 *5.6.安全功能(TOE Security Functions, TSF)* 指該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。 *5.7.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。 *5.8.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。 *5.9.安全功能需求(Security Functional Requirement, SFR)* 指為定義於共同準則第二部(Common Criteria, Part 2)的安全相關需求條文，用以描述一產品之安全功能(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。 *5.10.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。 *5.11.安全領域(Security Domain)* 指一個主動式個體(包括人、機器)被授權存取的資源集合，為安全架構的屬性之一。 *5.12.自我保護(Self-Protection)*	

條文	說明
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。 *5.13.繞道(Bypass)* 指以非安全功能之方式去執行設備安全功能需求(SFR)的動作。(例如：未經過身分鑑別，直接進入稽核功能介面) *5.14.角色(Role)* 指一組預先定義的規則，用來建立操作者與送驗設備使用權限的關係。	
6.技術要求 *(詳如附件一)*	1.明定書面審查及實機測試之類別。 2.明定書面審查項目及標準。 3.明定實機測試項目及標準。