設計與建構一個高效率且高可靠的安全聯合防禦系統

游坤明,黃立明,何日緯
資訊工程學系
資訊學院
yu@chu.edu.tw

摘要

傳統入侵偵測系統（IDS，Intrusion Detection System）是過濾可疑封包，檢驗網路傳輸中是否含有惡意的攻擊封包，並發出警訊通
知管理者，僅能偵察與阻擋在網路應用層中可被識別的攻擊型態。但是隨著網路應用的蓬勃發展，為了因應網路安全的需求，近幾年有學者提出入侵防
禦系統(IPS，Intrusion Prevention System，亦稱IDP)來彌補IDS功能之不足
，IPS可以偵測入侵行為並且主動防禦，但IDS和IPS有一共同的特點--
一般皆應用於公司企業連外的網路骨幹上，因此相對在硬體支出和軟體搭配上皆須達到企業級以上的水準，而且集中式控管也容易造成建構和管理上付出的成本過高
，IPS裝置除了必須抵擋外部的網路攻擊行為外，也要抵擋區域網路內部彼此感染所引起的網路攻擊，而來自區域網路內部的攻擊也往往是造成區域網路崩潰的主要原因，一般網路環境有如金字塔，對外出口集中於金字塔頂端，內部區域網路依照各部門單位產生階層式架構向下延伸，當底層使用者眾多，網路攻擊在區域網路內部彼此交叉感染後，最後衝擊的將是金字塔頂端的網路骨幹出口，傳統的解決辦法是不斷更換成本更高、硬體等級更高的IPS或防火牆(Firewall)等網路防禦設備。

關鍵字：網路安全、分散式聯合防禦系統、Snort、嵌入式系統、網路攻擊