分散式安全聯合防禦系統

游坤明,黃立明
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）是以被動方式過濾可疑封包，
檢驗網路傳輸中是否含有惡意攻擊之封包，若發現惡意攻擊封包則發出警訊通知管理者，此種方式僅能偵察與阻擋在網路應用層中可被識別的攻擊型態。因此，近幾年來有
學者提出入侵防禦系統(Intrusion Prevention System 簡稱IPS，亦稱IDP)來彌補 IDS 功
能之不足，IDP 可以主動偵測入侵行為並且主動防禦，但IDS 和IDP 有一共同的特點--
一般皆應用於網路骨幹上，因此相對的硬體支出和軟體搭配皆須達到企業級以上水準，
而且集中式控管也容易造成管理和成本的代價過高，目前網路攻擊型藉由檔案分享、郵
件傳送和軟體漏洞彼此散播感染，IDP 裝置除了必須抵擋外部的網路攻擊行為外，也要
抵擋內部區域網路彼此感染所發起的網路攻擊，而內部區域網路的攻擊也是往往造成區
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，當底部使用者眾多，網路攻擊在內部
區域網路彼此交叉感染後，最後衝擊的將是金字塔端的網路骨幹出口，傳統的解決辦法
為不斷更換成本更高、硬體等級更高之IDP/防火牆(Firewall)等防禦設備。針對以上缺
點，本研究提出一個模組化的分散式IDP 安全聯合防禦系統，架構出網路控管分散式架
構、模組化控管、高效能網路傳輸等功能，有效徹底解決一般IDP 高成本、高負載、

複
雜化設定等問題，在網路攻擊發起第一時間內有效阻絕於內部區域網路，降低其餘使用
者遭受網路攻擊感染可能性。

關鍵字：IDS、IDP、 Snort、網路安全、嵌入式系統