IDS 運作原理解析

/台灣思科系統提供

隨著網路應用的普及，企業對於網路的依賴程度也與日俱增，電子商務 e 化早已是現代企業提升競爭力、增加生產力的不二法門。然而隨著企業對網路 e 化的依賴加深，病毒式駭客攻擊、非法入侵的事件層出不窮，入侵攻擊的難度與手法也比以往提昇許多，其所造成的財產與商譽損失，更是許多企業面對的難題與挑戰。對此，思科系統(Cisco Systems)提出 SAFE 架構，針對客戶如何建構安全的網路環境提供完整而詳盡的規劃建議，其中提到的監控與及時回應階段，更是企業面對入侵攻擊時不可或缺的防禦要素。

網路安全防禦傳統上均著重在網際網路的防火牆及 VPN 的建置，然而對於符合防火牆及 VPN 存取規則的封包，則無法提供進一步的防禦動作，此時入侵偵測系統可補防火牆之不足，做動態的非法封包偵測與提供即時的防禦。

入侵偵測系統主要可偵測三種網路攻擊行為：

1. 網路探測偵察：例如未經授權的探測系統及服務上的漏洞與弱點，如 SATAN，NMAP，NESSUS 等軟體工具 。
2. 非法存取：例如系統入侵使得竊取權限提昇等，工具如 Brate force 或利用系統管理者缺失及 Protocol 弱點。
3. 阻斷服務攻擊：使得系統服務或者網路無法正常提供服務或遭受破壞，例如 ping floods、 SYN flood 、 UDP bombs 等。

入侵偵測系統依其防禦重點不同，可分為主機型(Host based)與網路型(Network-based)入侵偵測系統。顧名思義主機型入侵偵測系統，在提供個別主機偵測與防禦偵測系統，將系統安裝於每一主機上，阻絕外來網路攻擊(如 HTTP port 80)或中斷系統內部非法程序之存取，以免主機遭受破壞；另有管理中控台，以提供監視與控制設定，報表與事件通知服務。而網路型入侵偵測系統之功能，在於監控一個或多個網段內之網路活動，提供較大的監控範圍，通常與主機型互補使用，形成深度而有效地防禦措施。

入侵偵測的原理可分為 Profile-Based 或 Signature-Based。Profile-Based 需先建立用戶網路環境之正常活動模式，再據以判別異於常態之活動，技術難度較高且用戶環境差異大，較難定義何謂”正常模式 ”；而 Signature-based 則是建立一套規則(signature) ，用於形容遭惡意利用的網路封包行為，原理如同病毒碼一般。以網路型入侵偵測系統為例，在防禦角色上可分為偵測器(sensor)與中控台(console)，其中偵測器通常佈置於重要網段，例如 Internet Server Farms、VPN 通道出口等。

偵測器在監控網段上若發現有符合規則形容之違法封包出現，可依環境及管理者事先之定義而有下列不同的反應動作：

1. 即時中斷 Session：例如 CODE RED/NIMDA 病毒攻擊時，偵測器可針對攻擊者發起之來源位置做 TCP RESET，降低病毒攻擊及防止擴散對內部伺服器之影響。
2. 阻隔攻擊者 IP：偵測器可通知路由器、交換器或防火牆機動地產生存取控制列(ACL)阻隔攻擊者。
3. Session 記錄：管理者可選擇是否將入侵者之 IP session 整個活動記錄下來，傳至中控台供日後進一步分析使用。

中控台之功能，在於事先設定並告知偵側器所指揮協防之路由器/交換器/防火牆為何，以及規則(Signature)之更新調整及相應攻擊處理方式(阻斷/阻隔或者捕捉記錄)，並可接受由偵側器所傳來之警告訊息記錄事件，並發出 e-mail 或 pager 通知管理者，而管理者可藉由中控台設定當偵側器遇到攻擊時通知另一協防之偵側器。例如某一企業同時有兩個 ISP 線路連線 Internet，若駭客由 ISP1 入侵攻擊在 ISP1 網段，防禦之偵側器除了在路由器上產生一個存取控制列(ACL)阻隔駭客位置外，並可通知在 ISP2 網段上防禦之偵側器，在連線 ISP2 之路由器亦產生對應之存取控制列(ACL) ，以達整體防禦效果。

若欲進一步瞭解 Cisco SAFE 架構，可連結至 www.cisco.com/go/safe 。