

IDP 入侵偵測防禦

隨著網際網路日益發達，大多數的企業透過網路傳遞積極提昇競爭力。也因此網路的安全對企業來說日益重要，為了保護自身網路安全，企業建構了許多相關安全設備。目前一般企業大多以防火牆保護本身網路門戶安全，但是防火牆只是一種被動的防禦機制，它的主要目的是在建一道堅固的防護牆，拒絕某些的網路連線。但是有時候，我們並不能完全阻隔網路的連線，這時候就需要入侵偵測的系統。

因此，市面上推出了 **IDS 入侵偵測系統(Intrusion detection system)**，它是一種監測封包進出、比對入侵型態、預防入侵攻擊，可在偵測到問題時做相關的紀錄並及時發出警告的防禦系統。但是 IDS 屬於被動式的防禦，只能偵測到已經發生的事件，對於入侵的駭客或病毒卻無法有效管控。IDS 無法針對主動攻擊的事件做反制行為，只能透過電子郵件或手機簡訊通知管理人員，減少其他系統的損害。

舉例子來說，一般的住宅，都會建置鐵門防止陌生人進入。但是如果這是一家百貨公司，當然你不能阻擋所有的陌生人進入，不然生意怎麼做呢？這時候，當然就只能開放所有人員進場，萬一遇到客人鬧場，只能做事後防範處理或通報。

為了徹底解決企業網路安全問題，眾至在 UTM 設備中提供了最新的防禦利器 IDP 入侵偵測防禦系統，它結合了入侵偵測與入侵防禦的功能，可以檢查出包藏在應用層裡的惡意攻擊碼並加以攔阻與警告。以剛剛百貨公司例子來說：

百貨公司營業的時候，對於入場消費的客戶就靠保全人員去幫忙判斷，如果進來的客人是拿開山刀或武器入場，當然要將他擋在門外阻止其進入，並報警處理。IDP 就是這樣的東西，我們沒有辦法一開始拒絕所有的網路連線，但是可以透過分析其網路行為，判斷是否為惡意使用者後來決定是否放行，保障企業網路的安全。

眾至 IDP 入侵偵測防禦方法步驟：

眾至 UTM 設備可即時針對異常流量與封包內容檢驗與示警(圖一)，並加以阻絕、隔離、干擾或發出警訊通知(圖二)管理者的處置，以預防可疑程式碼入侵目標主機。所以當 UTM 偵測到來自內部或外部的攻擊行為時，可即時提供保護網路與阻絕攻擊行為的措施，使企業網路依然可運行暢通，並提高資訊傳輸的安全性。



【圖一：
入侵偵測防禦設定功能畫面】

【圖二：
發送至管理員 PC 之 NetBIOS 警訊通知】

