# E-News

發行人：捷宇網安行銷部　發行日期：**2012.03.19**

## NetIRS 增加整合威播科技 NetKeeper，使整體網路聯合防禦更趨完善

NetIRS 系統是業界唯一針對內部網路包含「內網 L2-L7 安全偵測、防禦、與隔離」、「複合式使用者身份識別控管」、「內網關連性流量分析與報表管理」、「階層式多宮格流量地圖」、「歷史資料整合分析紀錄儲存」等等功能集結於一機的完整性研發產品。而且 NetIRS 會自動而快速地搜尋網路的主機與設備，並且立即產生關聯性 IP 與流量報表，其安裝與設定都極為簡易方便。

今年，NetIRS 更增加了搜集『威播科技 NetKeeper』等 IPS 設備與攻擊相關的 LOG，使 NetIRS 可以搭配聯合防禦的廠商更加堅強，更方便管理者以最少的經費，就能佈建完善的資安防護網。

| NetIRS 支援眾多 IPS/IDS 設備列表 | |
|---|---|
| Fortigate | Snort |
| GNatBox | Netscreen IDP |
| Tipping Point | Dragon |
| Cisco IDS | ISS |
| Watch Guard | SonicWall |
| BroadWeb | |

## 何謂聯合防禦？

NetIRS 是如何與其他資安設備整合組成聯合防禦呢？

### 阻擋外部攻擊：防火牆、IPS

一般企業為了阻擋外部 Internet 的外來攻擊，都會購買防火牆、IPS 等相關設備放置於網路骨幹上，這些設備會巨細靡遺地完整紀錄從外部進入內網時發生的事件，並同時回防阻擋外來攻擊，但是若攻擊事件是來自於企業內部的訪客或員工時，此攻擊事件根

本不會跑到網路骨幹上，其防火牆、IPS 等就無法偵測到了。

## 阻擋內部攻擊：NetIRS、NetAgent（Layer2）

因 NetIRS 主要針對企業內網做控管，當遇到來自內網的異常事件發生時，除了產生事件列表（EVEN LOG）之外，也會依據管理者所設定的事件嚴重等級進行回應與處理，處理的方式便如同前幾期所描述，便不再重述。

## NetIRS 的聯合防禦：

NetIRS 可與其它資安設備共同整合，不論使用者是由何種途徑進入內部網路 (由遠端、無線、或有線；持 iPad、iPhone、或筆電)，NetIRS 可幫助企業建立一個完善的聯合資安防護網，其聯合防禦的方式如下：

### 與路由器或交換器整合下 ACL 指令

若使用者是從遠端外網進入內部網路，在防火牆、IPS 判定其為合法的使用者時，就會讓他順利進入內部網路，但是若這合法的使用者在內網做異常的網路存取時，防火牆、IPS 等設備便束手無策；由於該使用者是從遠端進入的，亦無法用 Switch Port Shutdown 去終結他，此時，NetIRS 可與支援 ACL 功能的路由器或交換器互相配合，由 NetIRS 針對異常 IP 下 ACL 指令到路由器或交換器端使其斷線，以阻止合法的使用者在內網帶來的潛在資安危機。

| NetIRS 支援 IP ACL 的設備 |
| --- |
| Alcatel |
| Cisco |
| Extreme |
| Foundry |
| Juniper |
| HP |
| D-Link |

### 與防火牆或 IPS/IDS 整合讀取 LOG 加以判讀分析

NetIRS 可以搜集防火牆、IPS/IDS 等設備所產生與攻擊相關的 LOG（在其它資安設備所產生數萬筆的 LOG 之中，NetIRS 會自動過濾排除非必要的資訊，只會留取與攻擊相關的 LOG，以避免耗盡資源），並針對這些 LOG 加以分析、歸類事件輕重程度，然後做適當的處理，如同 NetIRS 偵測到內網的異常事件一樣，發出警訊、主動斷線等等。

## 多重告警系統

相信大部份的網管人員最大的夢魘就是一打開郵件信箱，就看見等待著讀取的大量告警郵件，甚至無法辨別何者才是真正需要立即處理的事件，等到管理者好不容易找到之後想處理，卻已經來不及了！所以一個沒有經過整理的告警系統，在資安的防護上完全起不了作用。

以 NetIRS 為例，在事件發生的時後，就已經按管理者所設定的輕重程度加以歸類，然後亦按管理者所設定的方式散佈告警。

| NetIRS 的多重告警系統 | |
|---|---|
| SMS | Syslog |
| Web | E-Mail |
| MSN | Trap |

舉例來說，NetIRS 支援的告警方式多達 6 種，管理者可以自行設定嚴重等級的事件以 SMS 簡訊發送至管理者手機、中等程度的事件顯示在 E-Mail 或是 MSN、而輕微事件者則直接紀錄在 Syslog 或 Trap 裡以備不時之需，如此經過歸類後的告警便可大大幫助管理者得到最迅速的資訊並做正確的處置。

### NetIRS 的 SMS 告警支援中文與雙向回應

特別值得一提的是，NetIRS 的 SMS 簡訊告警不但支援中文顯示，還可雙向溝通。例如，NetIRS 因故將高階主管斷線，同時也發送簡訊通知管理者〝高階主管被斷線〞(屬單向告知)，同時問管理者〝是否釋放？〞，此時管理者可以立即回撥手機通知 NetIRS 釋放，此回撥動作便屬雙向回應，讓管理者即使不在電腦旁也能立即處理緊急事件，甚為便利！