# E-News

發行人：捷宇網安行銷部　發行日期：**2011.11.8**

## ●行動裝置正夯，資安危機飆增

在行動裝置開放的同時，不管是使用微軟、蘋果、或是谷歌(Goole)的系統，企業必須要准許更多的人員持各式設備進入內部網路，自然就增加面臨資安危機的風險！這類的企業如大專院校、壽險公司、線上遊戲、跨國公司…等等必須開放網路供來自各地學生、教職人員，持個人行動裝置請求使用內部資源；又如政府機關推動網路無障礙服務的部門、或者醫院病房…等等必須開放民眾持行動裝置上網服務者。所以此時，強化企業資安的重點便落在控管眾多已知或未知人員與其設備上網的偵測與防禦工作，也就是「使用者控管機制」的應用，此機制須要能幫助 IT 管理員解決二大最頭痛的問題：

一、如何分辯合法使用者與非法使用者

二、如何找出合法使用者潛藏的危機

## ●認識使用者控管機制

使用者控管機制主要分為二種層面來控管：

一、彈性的使用者身份識別與管理認證

二、對異常使用者的偵測防禦

上期已針對第二項做過說明與探討，今日就第一項：彈性的使用者身份識別與管理認證，搭配持行動裝置的使用者網路管理，以本公司產品 NetIRS 做應用來逐一說明其方法。

## ●彈性的使用者身份識別與管理認證
## (分辯合法使用者與非法使用者)

### ◆ IP＋MAC 鎖定功能

一個 MAC 地址固定分配一個 IP 地址；只要不存在配對表上面的 IP 與 MAC 都無法使用網路，就算只有 IP 或 MAC 其中一種符合都無法通行。

範例一：如某電視台員工人數 500 人，節點數約 800 個，不歡迎也不開放網路給非員工以

外的人使用。所以，在企業要求網路環境相對嚴謹時，IP-MAC 鎖定是較為安全且容易管理的管控機制。

應用範圍： 限制上網設備固定不變動的企業。優點是使用者可以不需每次上網都要輸入使用者 ID 與密碼，就連無法輸入 ID 及密碼的設備如 PDA、IP Phone 等都能進入安全管控表列！

## ◆ MAC Authentication

此方式適用於以 DHCP 來配發 IP 者。當使用者發出上網請求時，會先透過 DHCP Snooping 檢測其 MAC 地址是否合法，若合法，則 DHCP Server 便配發其專屬或臨時的 IP 供其上網。

範例二：某電信公司因員工人數眾多，無法每人配給一個固定 IP；同時其網路環境在各樓層裡又劃分不同的 VLAN，當員工帶著行動裝置從 3 樓到 8 樓跨 VLAN 存取網路時，NetIRS 可與具備 MAC Based 的 Switch 搭配，提供網路實體層的存取認證，依據合法使用者的 MAC 配發所屬 VLAN 的 IP 地址。

應用範圍：無法提供固定 IP 的環境，適用目前流行的行動裝置（如 iPad、iPhone、Notebook…），可跨 VLAN 上網的彈性，亦兼俱防止顧駭客假冒員工的可能。

## ◆ Web Authentication

對不受地理限制，不固定 IP 與 MAC 設備的上網用戶，就使用 Web 認證。當使用者發出請求時，會開啟 Browser，要求使用者輸入帳號及密碼，達到過濾使用網路權限的效果。

範例三：某縣市網路中心必須要開放給各區的行政管理者或老師可以跨鄉鎮學校申請有線或無線上網服務；此時，NetIRS 系統會對申請者先在隔離區配發暫時的 IP 供其使用，若認證成功則另外配給真正的合法 IP 給申請者，不成功者就繼續待在隔離區囉！

應用範圍：適用目前流行的行動裝置（如 iPad、iPhone、Notebook…），可跨 VLAN 上網的彈性，與使用無線網路上網的服務認證。

## ◆ 多重認證整合方式

面對複合式的網路環境，就必須採取多重認證的整合方式：

對訪客僅開放上 Internet，員工則無限制

範例四：某大型醫院各樓層的病房管理櫃檯為了查房與照顧住院病患，其各科主機都是用 Notebook 並使用無線上網，所以病房裡必須要開放上網以連線醫院的伺服器，然而病患與家屬每日往來變動相當大，因而使得病房成為內網管理的一大漏洞。

解決方案：針對院內 200 台重要主機採取 IP-MAC 鎖定，其他僅開放上 Internet。

應用範圍：舉凡政府機構、醫院、飯店等室內公眾場所，員工與民眾混合的網路環境下，都可以暢遊在無障礙無線上網的網際空間，而無後顧之憂。

使用 Web 認證，通過後並自動轉成 MAC 認證。

範例五：某大學因為要開放校園網路，又顧慮到內網使用者如教授或研究生與其個人行動設備都不是長期固定在校園內，機動性又強，所以採用 Web 認證；但教授或研究生可能一天出入內網很多次，每次 Web 認證都要做一次 ID 與密碼審核，非常麻煩。

解決方案：使用 Web 認證，通過後並自動轉成 MAC 認證。

這就是 NetIRS 在複合式的網路環境的身份控管最大的優勢。由於教授或學生至多每學期才會有一次變動，所以管理者可以設定要求在開學一開始時，讓教授或研究生先以 Web 認證確定身份，在此同時 NetIRS 便紀錄該師生 Notebook 的 MAC 地址，日後這一學期內，只要該師生持相同的 Notebook 上內部網路，直接採用 MAC 認證，就不須再經過 Web 認證了。

## ●合法使用者潛藏的危機：網路第二層攻擊

另外，最容易被 IT 管理者忽略的，是網路第二層的攻擊。發生原由可能來自合法使用者未知的中毒或有意的報復攻擊，這來自網路底層的攻擊會使得企業重金購買資安防護設備如防火牆或 IPS 設備在這場戰爭中毫無用武之地。第二層的網路攻擊只會出現在內部網路，如 ARP/IP Spoofing、DHCP Attack、Broadcast Storm 等，而這層攻擊一但發生，幾乎是全面性並且立即癱瘓內部網路，尤其在開放行動裝置的存取之餘，第二層的資安防護實是 IT 管理者不容小覷。

- 流量分析報表管理
- 歷史資料儲存紀錄
- 入侵偵測防禦隔離
- 使用者控管認證

# L2-L7智慧型內網安全控管

NetIRS

NetAgent

## NetIRS

自動搜尋網路設備並加以分類標示(如自動歸類為交換器、路由器等等)並顯示即時與歷史流量
可判讀智慧型交換器、路由器、防火牆、IPS、...多種網路設備之資料封包，方便集中控管
支援NetFlow/sFlow分析功能，可監看分析IPv4/IPv6網路服務
提供階層式流量地圖，可觀察每一層級的網路環境且資料相互關連，並以顏色區別流量狀態
自動利用節點定位功能將異常的節點封鎖隔離，此功能可同時支援IPv4/IPv6
多重告警機制如Syslog、Trap、Web、E-Mail、MSN、SMS等，可發中文簡訊至手機
提供DHCPv4/DHCPv6伺服器功能，可同時支援多網段DHCP服務
提供有線/無線網路使用者認證之安全防禦閘道功能，直接控管終端網路存取政策
可以Browser達成身份認證，並支援Single Sign-On應用，可整合Windows AD Domain

## NetAgent

提供Layer2安全偵測防禦，每個介面可獨立監控一VLAN，此VLAN可包含多個IP網段
異常封包包含IP衝突與盜用、IP/ARP Spoofing、ARP掃瞄、廣播風暴、非法DHCP伺服器偵測
支援MAC與IP地址定位功能，可找出單一MAC、單一IP、與網段中所有IP連接的交換器連接埠
提供日誌資料搜尋功能，可依時間、來源、目的、關鍵字、IP與服務埠進行搜尋
可與NetIRS整合納管NetAgent設備達成Layer2-Layer7中央控管機制，使防禦沒有漏洞