新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2006/12/11 - 2006/12/17 第7期

網路記錄器 / IR 系列報導

技術淺談與應用 - 記錄資料檢索

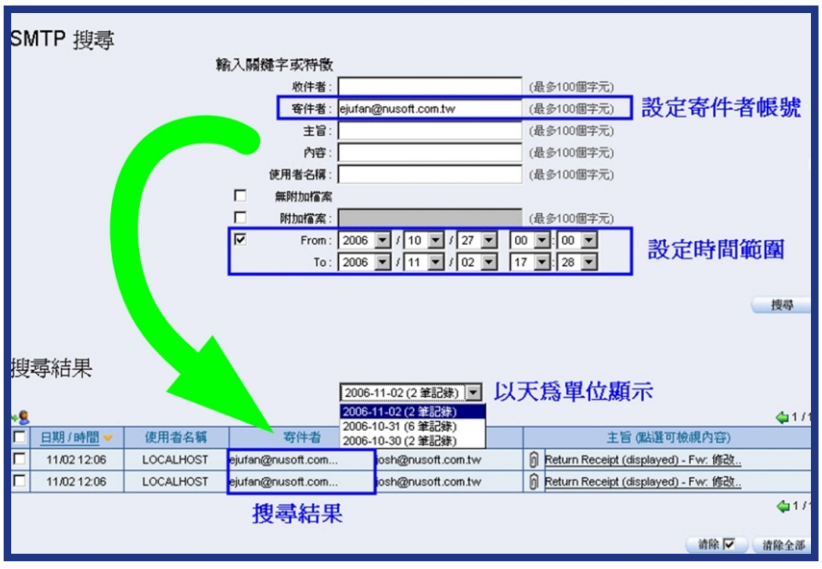
在做事愈來愈講求效率的趨勢中，拜科技之賜，許多方便的通訊和資料傳輸方式，以網路為媒介蓬勃發展。但，伴隨而來的是，有心人士的濫用，導致耗費工時、機密外洩…，眾多危害企業利益的行為。

因此，了解員工上網行為，嚴然成為企業管理上的一個新興課題。為了提供所需的資料，新軟公司研發了有別於市售行為管理防火牆的網路記錄器（NUS-IR2000、NUS-IR1500、NUS-IR1000），著重於內部上網行為的側錄。

以 NUS-IR2000 來說，對於上網封包的擷取和還原，皆以詳盡、深入為原則。於記錄資料之初，即依其性質，將可供檢閱的特徵提取出來，發展出方便調閱記錄內容的使用介面。獨特的 **全方位搜尋** 和 **內容檢索** 技術，由此應運而生：

1.全方位搜尋：

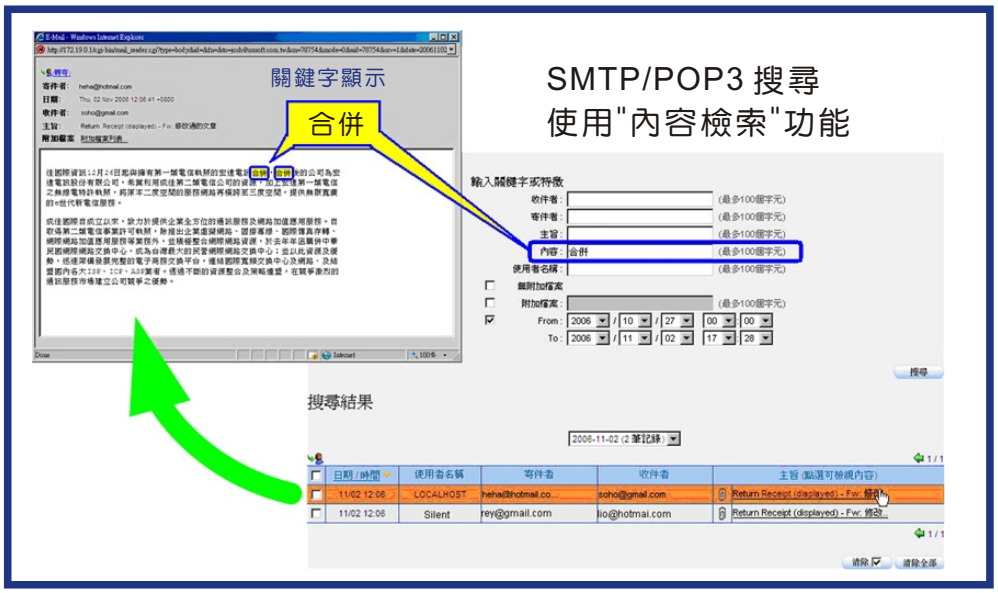
由於 NUS-IR2000 將常用的網路行為（例如：HTTP、SMTP、POP3、Web Mail『Web SMTP & Web POP3』、IM、FTP 和 TELNET）詳細記錄，必須運用龐大的資料庫做為儲存媒介。為了在大量的資料中做重點搜尋，NUS-IR2000 提供管理人員輸入關鍵字和特徵的搜尋介面，深入廣大的資料庫中一一比對資料庫內容，快速且正確找到所需的記錄。



如上圖所示，以 NUS-IR2000 的 SMTP 搜尋為例，搜尋出來的資料是以天為單位呈現，並利用一目了然的表單方式呈現搜尋結果。

2.內容檢索：

NUS-IR2000 不僅能依標題、使用者、時間等條件搜尋，更可以針對記錄的網路行為內容進一步搜索，不必一筆一筆的比對查閱，就能使管理人員快速查詢相關資料，有效的為企業機密資訊嚴密把關，以降低資訊外流的危機，並提高管理效能。



如上圖所示，在 NUS-IR2000 的 SMTP 搜尋功能中，以“合併”為關鍵字，做郵件「內容」搜尋，符合條件的部份，便會以黃色方塊清楚標示出來，讓查閱者一目了然。

就「搜尋機制」來說，新軟 IR 系列產品和市售產品的比較（如下表）：

產品 / 查閱能力技術	新軟公司 NUS-IR2000	一般市售網路側錄設備
搜尋功能	能依指定的條件和特徵，於龐大的資料中搜尋，迅捷的找到所需的記錄。	1. Mail：無法針對信件的內容，附加檔案的檔名檢索。 2. Web Mail：常用網頁快照方式記錄 Web Mail，導致無法利用收件者、寄件者、主旨、信件內容…方式搜尋。 3. IM：大多僅能對聊天的帳號搜尋。無法針對聊天的內容、傳遞的檔案加以搜尋。 4. HTTP：通常只能針對 URL 搜尋，而不能搜尋網頁內容與網頁標題。
內容檢索	可深入搜尋各項資料的「內容」，對往來的資料嚴密把關，並有效管理。	

文 陳昱昇 josh@nusoft.com.tw

市場行銷報導 - 行為管理功能

隨著近年來網際網路的快速發展，企業 e 化提昇了整體的競爭力；但也因為過於便利的網路傳輸，而容易發生企業網路資源遭到濫用、員工上網摸魚等問題，造成無形的損失。因此，各家業者紛紛推出網路側錄設備來因應這個企業 e 化的後遺症。

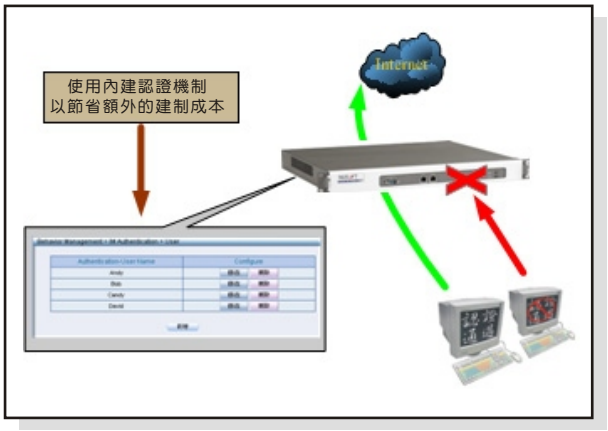
而部份廠商所推出的設備是以**閘道器**再加上**記錄資料功能**的方式濫竽充數，並稱之為“行為管理器”。宣稱可以記錄、管控員工之上網情況，甚至擁有防火牆功能與負載平衡機制！！殊不知，其往往呈現的是一團亂的記錄資料、簡單的管控功能、陽春的防火牆機制、不堪使用的負載平衡功能…，完全模糊了網路側錄設備之產品定位。

要知道，網路側錄設備應專注於網路資料的記錄與分析，至於行為管理部分則是與企業原有的專業防火牆搭配使用；旨在彌補專業防火牆的不足，而不是凡事都想插一腳，最後變成功能樣樣都有，樣樣不精的設備。有鑑於此，新軟公司在開發網路記錄器的行為管理功能時，即依循上述之原則，特別著重於一般企業防火牆無法掌控的地方，讓新軟網路記錄器與企業原有之防火牆能夠相輔相成，來為企業解決這企業 e 化的後遺症。

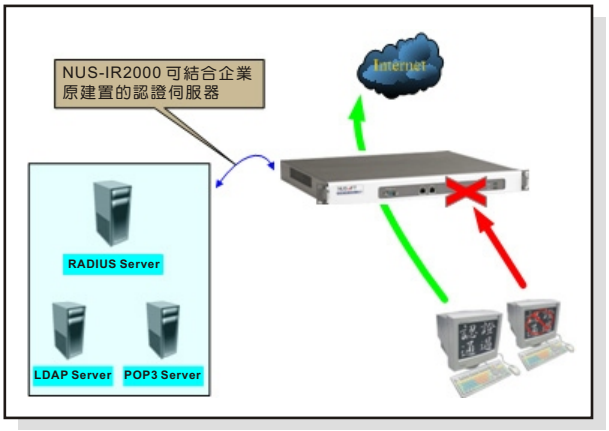
新軟網路記錄器的行為管理功能：

即時通訊認證

即時通訊認證機制可協助企業有效掌握旗下員工的即時通訊使用。管理人員可要求員工在使用即時通訊前，必須通過網路記錄器之認證否則將禁止使用。此外，網路記錄器支援了多種認證帳號資料。企業除了可使用其內建的認證用戶表（不須再額外架設認證伺服器，可節省建置之成本）之外，亦可結合企業原本已建置完成的現有認證伺服器（如：RADIUS、POP3、LDAP 等），以達到帳號整合的目標。



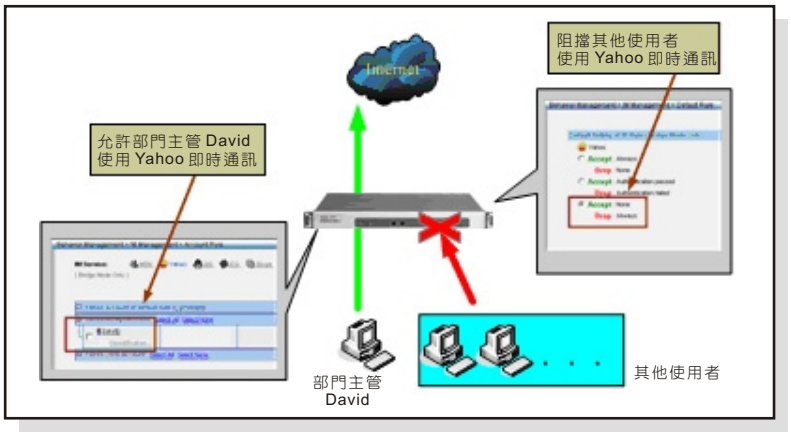
利用本機之認證表完成認證設置



利用外部伺服器完成認證設置

即時通訊管理

可使企業能有效管理企業內部即時通訊之使用，彌補一般防火牆無法阻擋員工使用即時通訊軟體之問題。它不僅可管控整個企業的即時通訊使用（如全部允許、僅有通過認證者允許或全部不允許等），更能針對個別帳號制訂規則，以符合企業的管理需求。



利用即時通訊管理掌控即時通訊之使用

P2P 管理

點對點軟體的傳輸可以使用任何的 Service Port 來進行，因此一般防火牆根本無法阻擋這個企業頻寬殺手。因此，新軟公司在網路記錄器裏添加了 P2P 管理功能。P2P 管理功能不僅可以管控整個企業的點對點軟體使用，也可針對個別使用者制訂規則，以符合企業對於點對點軟體的管理需求。

及時流量分析（NUS-IR1000 無此功能）

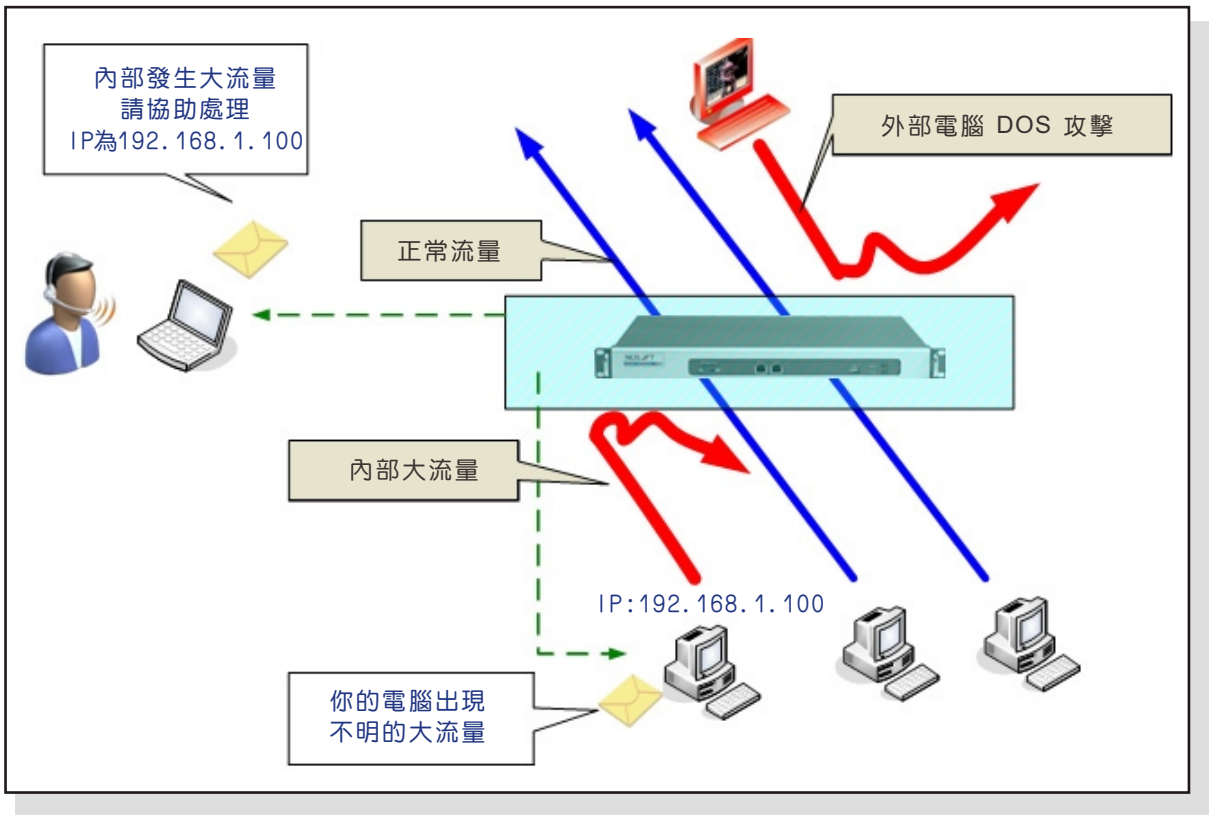
一般防火牆的流量記錄功能較於陽春，管理人員較難從中得知重要訊息。而網路記錄器的流量分析機制，可分析整個企業網路之流量，輕鬆得知目前企業網路的使用情況，是何人在何時使用何種服務佔據企業網路頻寬。再配合企業原有防火牆的阻擋功能、頻寬管理…，有效控管企業的頻寬利用。

流量分析機制分為三大功能：【流量統計】、【今日排行榜】、【歷史排行榜】

產品 / 流量分析功能	新軟網路記錄器	一般網路測路設備
流量統計	以圖表方式顯示當日企業網路的即時流量，管理人員可從此得知在何時段有反常之流量發生。	僅提供特定時間點內的分析記錄，且無法分析預設服務以外的各類型資訊。不僅無法符合企業多元化的網路服務需求，更不能藉此協助企業揪出濫用企業網路的使用者。
今日排行榜	可統計今日任何時段的流量排行，並列出前十名。有助於管理人員，對於企業頻寬之掌控。	
歷史排行榜	可統計任何時段的流量排行，並全部列出。讓管理人員，了解整個企業網路之運用情況。	

異常流量偵測

若企業網路內部之電腦發出異常之大流量時（DoS 攻擊），網路記錄器會先行阻擋此異常大流量之傳送，確保整個企業網路的流暢。並可與 Core Switch 協同防禦，將異常大流量封鎖在局部範圍。最後網路記錄器會向管理人員與該電腦的使用者提出異常警告，讓管理人員可迅速找到問題的所在。



文 程智偉 rayearth@nusoft.com.tw