

## 網路記錄器 / IR 系列報導

### 技術淺談與應用 - 新軟網路記錄器新增「網站管制」機制

由於網際網路的開放與蓬勃發展，公司對於Internet的使用與依賴度越來越高，導致充斥各種不當的網路行為；例如：員工利用上班時間在公司盯股票、逛部落格、社群網站、看拍賣…等等上網行為。而且上網的同時一不小心就會使電腦遭病毒入侵，情況輕的導致個人使用的電腦出問題，嚴重的甚至影響到整個公司的營運，降低產能，影響收益。

為了能幫助公司有效管制內部網路資源，提升員工工作效益，新軟系統『網路記錄器IDR-1000』系列以上新增的「網站管制」功能；讓管理人員自行輸入欲管制的網站網址讓網路環境架構底下的使用者無法濫用網路資源進而達到有效管制。「網站管制」內容分為「網站白名單」、「網站黑名單」、「網站類別資料庫」三種；利用此管制功能，不但能降低中毒的機率，同時控管內部員工上班時利用網路來打混摸魚的情況！並且提供詳細的管制報告，鉅細靡遺的呈現所有員工上網記錄，協助管理人員後續的監控管理與資料存查。

#### 網站白名單：

管理人員欲開放特定網站讓內部員工進入瀏覽，只需將開放網站的「關鍵字」或「完整網域名稱」在『Whitelist』直接輸入即可。

#### 網站黑名單：

管理人員若是完全不想讓公司內部員工瀏覽特定網站，則可直接輸入「關鍵字」或「完整網域名稱」在『Blacklist』。

#### 網站類別資料庫(此為付費功能，需申請金鑰啟用)：

採用獨特的“雲端儲存”網站過濾技術；將網際網路的所有網頁分為八大類別(非法網站、情色網站、賭博與遊戲、社會與經濟、互動與服務、休閒嗜好、教育新知、其他類型)共計65個子項目。管理人員可依照公司網路政策，自行設定欲阻擋之『網站類型』，以輕鬆達到管制員工上網種類之目的，無須再逐一輸入網域名稱、關鍵字來阻擋。(若需申請及試用『網站類別資料庫』，詳情請參閱“新軟週報—第100期”)

此外，『網站管制』機制特別需注意的是存取規則比對順序：「白名單」>「黑名單」>「網站類別」只要網站符合某一比對條件，本功能將不再繼續向下比對！

如何運用「網站管制」機制，方能達到企業最大利益？舉下列情況為說明：  
管理人員依公司營運政策開放特定部門(如：行銷部門、業務部門…等等)進入facebook進行商業行為外；但是，限制其他部門連入facebook，而且限制特定部門使用facebook來進行遊戲與心理測驗相關功能，以及進入其他社交網站(如：推特、噗浪…等社群網站)。先在『Whitelist』功能將“www.facebook.com”之完整網域名稱新增即可。

| 名稱       | URL              | 變更    |
|----------|------------------|-------|
| facebook | www.facebook.com | 修改 刪除 |

1 / 1

新增

圖一 將“www.facebook.com”新增於『Whitelist』中

再至『Blacklist』功能輸入“app.facebook.com”及“apps.facebook.com”兩組關鍵字阻擋facebook的遊戲與心理測驗相關功能；

| Name           | URL               | Configuration |
|----------------|-------------------|---------------|
| facebook-game1 | app.facebook.com  | Modify Remove |
| facebook-game2 | apps.facebook.com | Modify Remove |

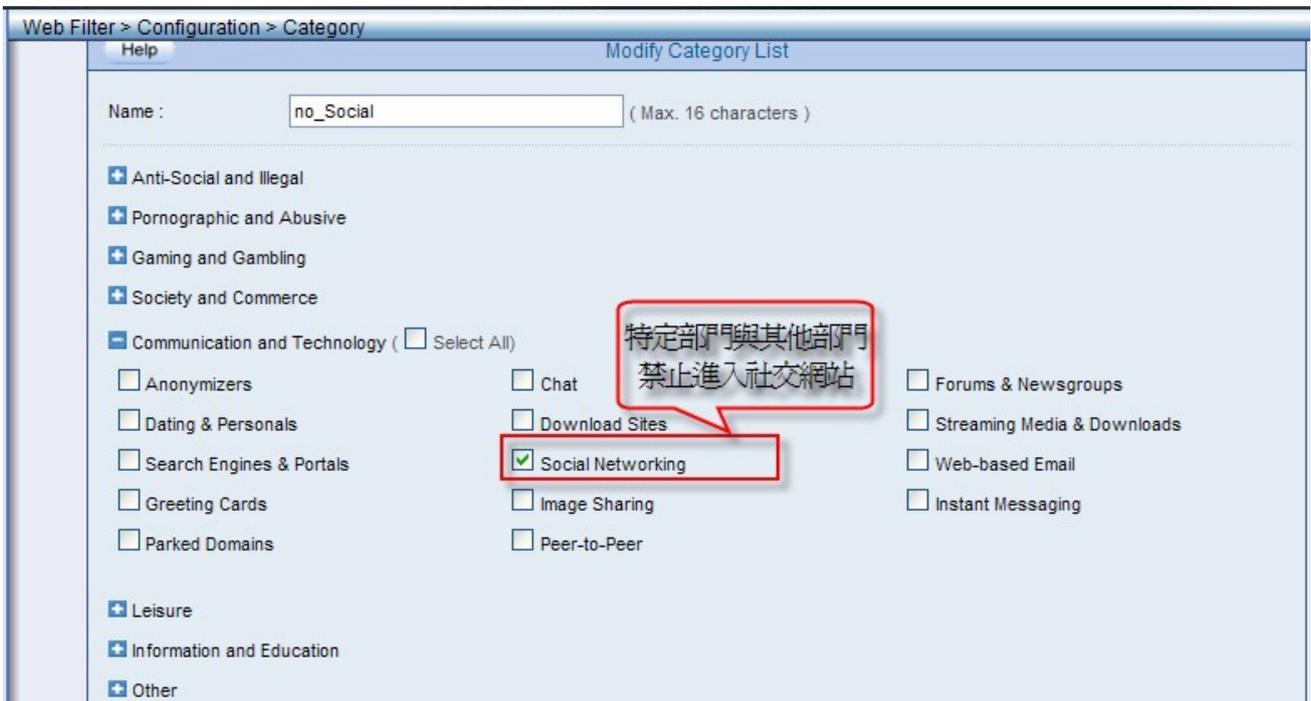
1 / 1

New Entry

特定部門(行銷部門、業務部門…等等)

圖二 限制特定部門使用facebook的遊戲與心理測驗相關功能

若是公司於系統中另外有申請金鑰啟用「網站類別資料庫」功能時，則可以更輕鬆的來進行阻擋。假使特定部門不能進入其他社交網站，及其他部門完全不能登入社群網站(如：推特、噗浪、facebook…等等)，管理人員則在『Web Filter > Configuration > Category』位置下，新增一條阻擋『Social Networking』選項即可。

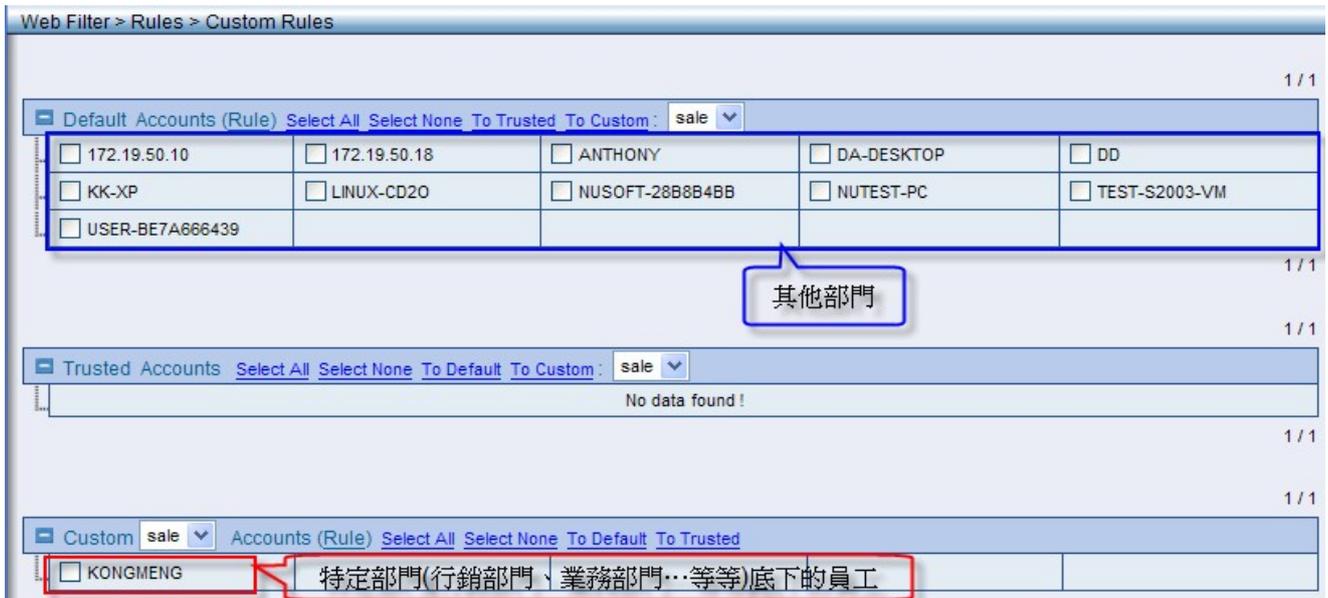


圖三 勾選欲管制之網站類別之子項目

上述所設定完成的值，套用於不同群組中，再將群組設定於『使用者規則』的「預設規則」、「不管制規則」及「自訂規則」三種之一，以達到管制員工上網種類之目的。



圖四 套用於預設群組或新增自訂群組



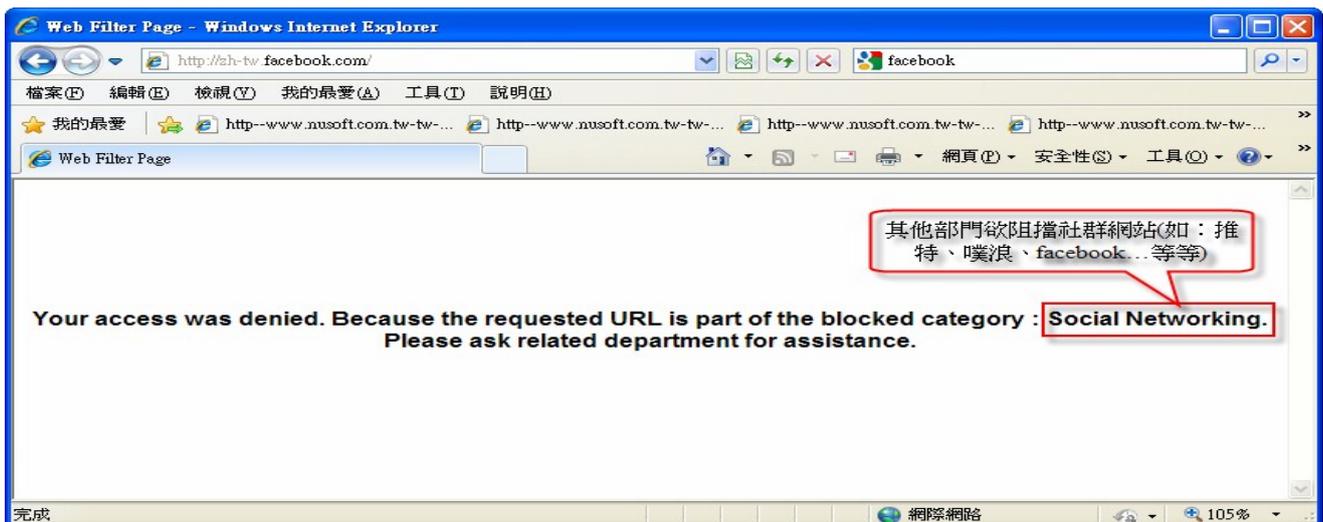
圖五 套用於使用規則種類(預設規則、不管制規則、自訂規則)

如此一來，管理人員可從Log記錄中查閱開放或阻擋的列表及其他相關訊息，以供管理人員後續的存查與備份使用，並藉以調整公司網路政策。

| 時間       | 使用者名稱    | 網址               | 類別  | 處置方式 |
|----------|----------|------------------|-----|------|
| 17:05:27 | KONGMENG | www.facebook.com | 白名單 | ✓    |

特定部門(行銷部門、業務部門...等等)底下員工

圖六 「網站管制」之Log記錄查閱相關訊息



圖七 其他部門進入facebook網站，系統阻擋畫面

所以，不論「網站白名單、黑名單」或「網站類別資料庫」完成設定後，必須得套用到『規則』中才會有實際的用途。

文 余光明 kongmeng@nusoft.com.tw

## 市場行銷報導 - 擁有新軟『網路記錄器』，企業不再擔心打混摸魚的員工

在今日企業普遍 e 化的型態下，網際網路帶給企業相當便捷的商業工具；但同時也提供了企業內部員工摸魚的最佳管道，進而影響工作效率，占據企業網路頻寬並導致網路阻塞，甚至嚴重則不慎洩漏商業機密損失慘重。為杜絕此網路摸魚歪風盛行，除了透過企業的網路使用政策來宣導警告外，最根本的辦法就是透過安裝網路側錄設備來監督員工的網路使用情況。

一般來說，企業員工在上班時間常見的網路摸魚行為，為下列幾項：

### 1. IM 即時通訊：

IM 即時通訊方便快捷與不需付費的特性使它成為企業與顧客商業往來的主要溝通工具。但是，也因為 IM 即時通訊的便利，導致企業員工利用它聊天摸魚，造成降低員工工作效率，使企業競爭力下降。

### 2. 網路應用程式：

由於網際網路的便利，網路充斥著免費的網路應用程式，如：點對點軟體(eMule、Foxy、BT…)、影音串流(PPLive、PPStream…)、VPN通道、遠端控制…等軟體，亦成為企業員工於上班時間打混摸魚的工具，甚至為了避開企業內部的防火牆與網路記錄器，員工就利用VPN通道軟體以穿牆方式從事私人事件，或者用遠端控制軟體上家中網路避免上網記錄。

### 3. 網頁瀏覽(HTTP服務)：

企業普遍 e 化的型態，網際網路已為企業商業的工具，利用它搜尋資料，或者與客戶往來溝通等商業行為。但是，也容易成為員工消磨時間的工具，如瀏覽不明網站(色情網站、下載網站)，間接造成電腦中毒，甚至嚴重導致公司機密資料外洩。

為了解決上述問題，並能協助企業完全掌握其網路使用情形，新軟系統『網路記錄器-IDR』系列產品除了擁有完整之「事前管制」外，還有「事後記錄」。如此一來，鉅細靡遺的呈現所有員工上網記錄，到時誰還敢利用企業網路打混摸魚。

## 事前管制：

如何遏止員工網路摸魚，最佳方法就是妥善做好「事前管制」，可管制員工使用非公務上的應用程式軟體，以及瀏覽不明網站；因此新軟系統『網路記錄器-IDR』提供多款網路上常用的「應用程式」、「IM 即時通訊軟體」及「網站管制」之相對應管制機制予用戶，讓管理人員可依公司政策自行訂定相關使用規則。管理人員因公司業務上的需求欲開放或限制員工使用「IM 即時通訊」，假使有不肖員工利用通道軟體躲開防火牆，或者用遠端控制軟體避開網路記錄器的記錄，管理人員亦可用「應用程式管制機制」功能中勾選VPN 通道軟體與遠端控制軟體選項作阻擋。甚至可利用「網站管制」機制欲開放或限制員工瀏覽網頁。如此一來，使員工無法於上班時間使用非公務上的應用程式軟體，或瀏覽不明網站，遏止員工網路摸魚行為，藉此提高企業資安防護的安全性。

目前提供的『應用程式管制機制』有：

點對點分享軟體、影音串流軟體、線上遊戲、VPN 通道軟體、遠端控制軟體。

目前提供的『IM 即時通訊程式機制』有：

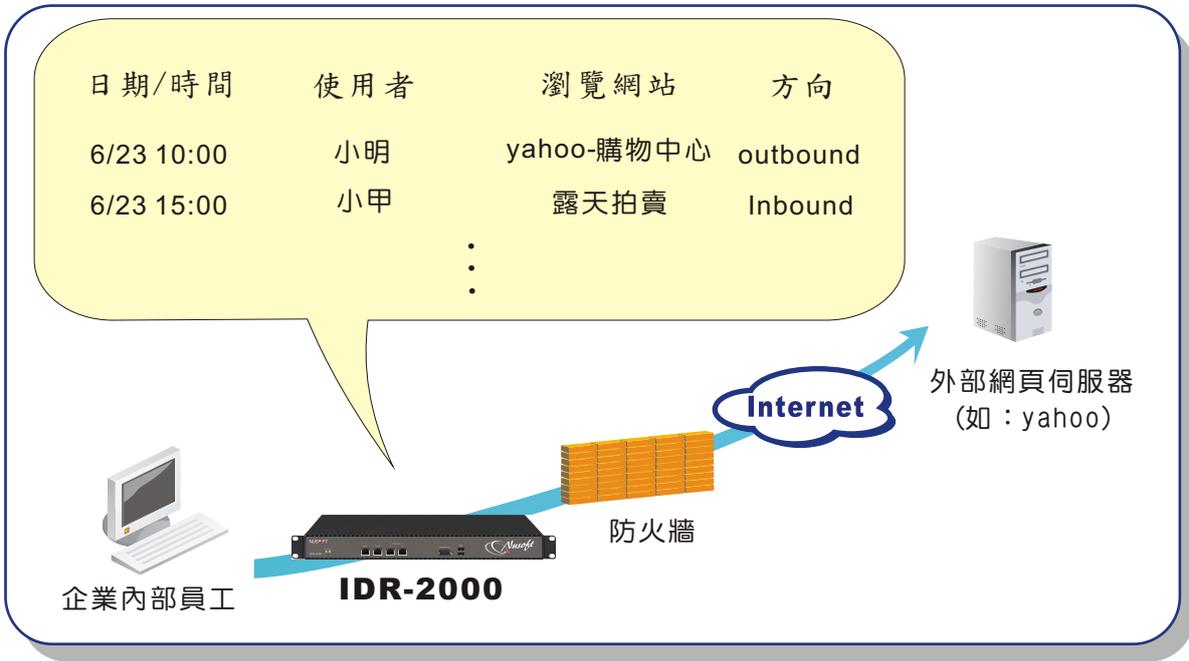
MSN、Yahoo、Skype、QQ、GoogleTalk、ICQ、AIM、Gadu-Gadu。

目前提供的『網站管制』有：

網站白名單、黑名單、網站類別資料庫(此為付費功能，將全球的所有網頁分為非法網站、情色網站、賭博與遊戲、社會與經濟、互動與服務、休閒嗜好、教育新知…八大類別之共計65個子項目；管理人員可依照公司網路政策，指定非公務相關的類別網站並讓內部員工禁止瀏覽所指定之類別網站)。

## 事後記錄：

企業除了做好「事前管制」外，最主要的就是「事後記錄」。若因應企業內部員工公務需求，管理人員必須開放使用其他網路服務的話，新軟『網路記錄器-IDR』提供完整的Outbound(內部至外部連線)記錄及Inbound(外部至內部連線)記錄，讓企業可全面掌握網頁瀏覽(HTTP/HTTPS)、收發電子郵件(SMTP、POP3/IMAP、Web SMTP、Web POP3)、即時通訊(MSN、Yahoo、ICQ、QQ…)、檔案傳輸(FTP)、遠端登入(Telnet)…這八大項常用網路服務之使用情況。不論是內部員工上網，還是外部使用者連線進入，將會在新軟『網路記錄器-IDR』底下一五一十的完整呈現。讓管理人員不僅可隨時查閱記錄，透過管理介面也清楚顯示流量來源去向之IP位址、網頁連結網址、聊天訊息字串…，使得企業在網路管理上更能得心應手，掌握所有員工上網資訊，企業不再擔心員工於上班時間混水摸魚。此外，倘若有發生內部員工使用其他服務而洩漏企業商業機密資料，就可依據『網路記錄器』所記錄的資料做為事後法律告訴的舉證資料。



圖一 外部使用者瀏覽企業網頁時，新軟網路記錄器可詳細記錄其點選之網頁

另外，新軟系統建議企業雇主在設置『網路記錄器』前務必對該安全機制訂定施行規章並告知全體同仁，甚至以書面與員工簽屬同意書，來保障該安全機制的合法性；並將『網路記錄器』設定管理權限，僅供特定管理人員進入系統察看，且對管理人員實行法律教育規範，如此一來便可兼備企業機密資料及員工隱私權的保障。

文  余光明 kongmeng@nusoft.com.tw