新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/1/12- 2009/2/8 第84期

多功能 UTM / MS 系列報導

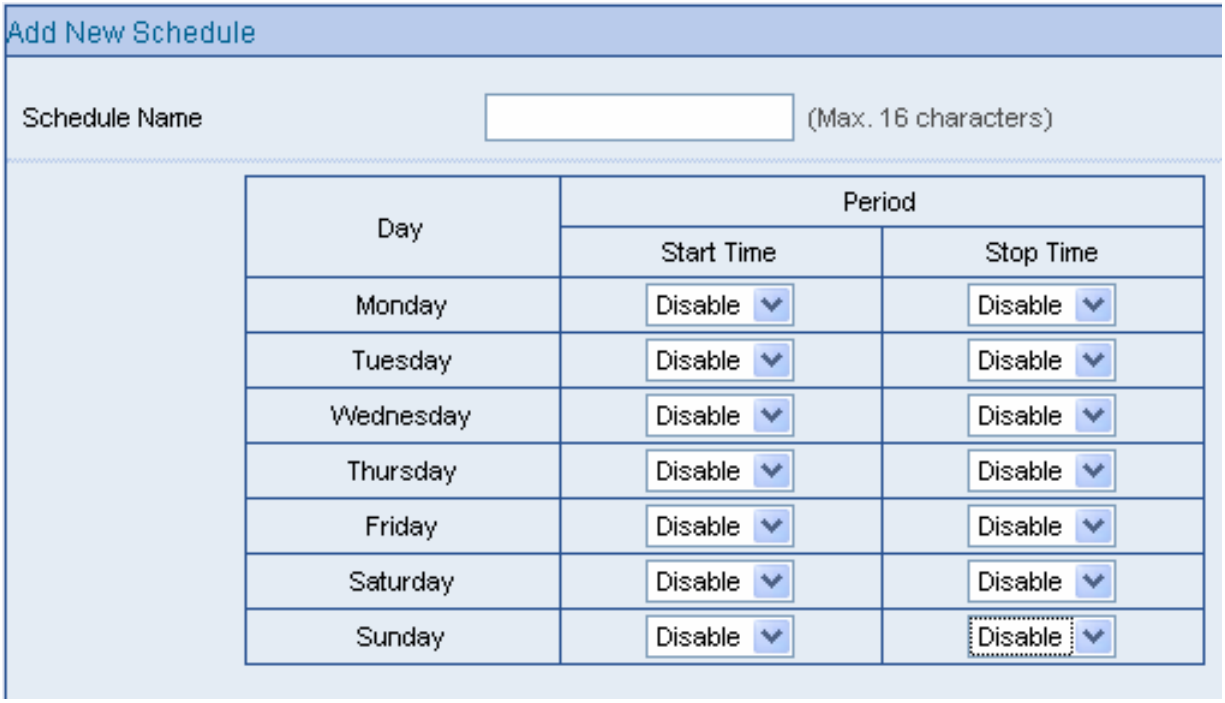
技術淺談與應用 - 妥善使用排程表，幫公司打造優質的工作環境

網際網路的方便，造就了企業不少的商機，網際網路不但縮短了公司與客戶間的距離，也同樣的縮短了公司與公司間互相交流的距離，在現階段的生活中一切的事物也大都與網路脫離不了關係，它的方便不但帶來了不可否認的利益，也漸漸的促使現代人對它的依賴，但越是方便的東西就越容易遭人濫用。

根據調查分析，75% 的員工都曾使用過公司的網路來處理私人事情，舉凡瀏覽網路拍賣、新聞及收發私人信件 or 使用網路通訊軟體進行聊天…等，如此一來員工的工作效率相對降低而相繼影響到的則是為公司所帶來的收益減少，在這種惡性循環下，時間越久對公司的影響就越大。

身為公司的網管人員，為了要幫公司打造出一個優質的網路環境，除了要維持內部網路的穩定及安全之外，同樣的也要兼顧到公司裡網路資源所使用的情況，在做網路管理限制的同時還必須考慮到各部門或特定人事（部門主管、老闆…）的網路資源，需求不同要給予不同的限制條件，在種種不同的需求情況下網管人員要如何去把多餘的時間空出來處理這類煩雜的事情？而管理人員除了去限制內部使用應用程式、各式軟體之外，還可利用什麼方式加以輔助及管理內部人員的上網權限呢？

利用新軟系統『多功能 UTM - MS』中所內建的 Schedule（排程表）功能即可輕鬆的為管理人員來達成上述的要求，排程表可以針對特定的群組、人員來依網路的需求性不同而言，進一步的自由調整、設定每天的哪段時間是否開放使用網路的權限，規劃內部使用者一週中每天透過管制條例，存取網路資料的有效時段，例如：面對平時正常工作時間不需要用到網路的部門人員來說（倉庫、基層做業員…），就可以只設定每日的下班時間才開放此群組、部門或是特定人員的網路使用權限，也可設定成每日的中午休息用餐時間才開放網路使用或是設定成只有正常上班的時間才開放網路使用權限，來以防止部分員工利用下班回家時，使用公司網路來下載私人程式、軟體…等，如此一來則可以有效的減少網路資源遭到濫用。而該如何做到適當的搭配則可視公司內部的狀況而定。



產品功能 Schedule 畫面

妥善利用排程表的自動執行功能，同時再配合上前端防火牆阻擋及限制，系統管理員可以節省更多的管理時間，同時讓網路系統發揮最大的效能。適時的開放網路使用權限，可讓公司內部更有制度化，而對於一個有制度的公司，相繼影響到的就是有效的提升內部的工作效率，如此一來不但可幫公司創造更大的收益，也能為公司帶來更多的商機。

最後要注意到的則是排程表必須配合『管制條例？』來使用，管理人員在設定完排程表後必須套用到『管制條例？』裡，才能實際的運作。

排程表套入管制條例圖示

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新增管理帳號密碼容錯次數限制

在現今資訊安全事件不斷發生的環境下，不論是家用電腦、公司電腦、資訊設備…等等，只要能跟網路有相關的設備、機器，都免不了網路上不斷湧出的入侵攻擊事件，而對於這類型的事件發生，也已經演變成多到讓人覺得即使發生也見怪不怪了。

然而，為了防止同樣的事情發生在自身家裡或公司的機器設備上，除了於設備前端加裝防火牆及安裝防毒軟體來防止機器設備遭入侵破壞，同時也要注意如何防範病毒入侵、駭客入侵，但往往會忽略了最基本的利用破解設備上帳號密碼來達到入侵目的，尤其是近期最常見的情況就是不少人為了探討別人隱私而不擇手段的去破解使用者放在網路上任何需要帳號、密碼的網路日誌、相簿、信箱、設備…等，甚至在破解進入後將其資料內容加以破壞竄改來達到滿足感及成就感。而誰又敢保證哪天公司裡的機器設備IP能不被有心人士掃到而加以入侵及破壞呢？

面對如此最基礎的入侵方式，為了能有效預防使用者利用帳號密碼破解的方式來進行入侵，近期也於功能內新增了帳號密碼容錯次數的限制，不論對內或是對外皆可有效的防止有心人事暴力式的破解帳號密碼來達到入侵。管理人員可自行設定登入之帳號及密碼可容許的錯誤次數，及達到錯誤上限後所要將該登入之IP加以阻擋封鎖的時間，相較於一般市售的前端防護設備只以單純的登入系統方式來說，新軟系統多功能UTM目前所擁有的帳號密碼容錯限制絕對是優勢許多。

同時於系統Event Log中也會記錄所登入且帳號、密碼輸入錯誤的IP訊息及遭阻擋之訊息，以供管理人員查看，讓管理人員可以清楚的瞭解是內部使用者或是外來的IP在對系統做帳號、密碼的破解，則可有效率的做防範。

Time	Event
Dec 30 15:21:47	admin user admin (192.168.10.78) Login Block (exceeded the bad logon attempt limit)
Dec 30 15:21:47	admin user admin (192.168.10.78) [Login failed]
Dec 30 15:21:43	admin user admin (192.168.10.78) [Login failed]

Event Log登入遭阻擋畫面

除此之外為了有效的防止駭客的入侵，新軟系統所推出的多功能UTM中不僅是只單單內建管理帳號密碼容錯次數限制的功能，同時還擁有強大的入侵防禦偵測系統（IDP）可抵擋駭客的攻擊，並且支援網頁掃毒的功能，可補足防毒軟體無法防護的項目，多方面的保護下讓企業的網路安全防護更加有保障，相信多功能UTM一定是企業防護最好的幫手，也是最好的選擇。

文 陳殿鴻 kim@nusoft.com.tw