新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2010/2/8- 2010/2/28 第111期

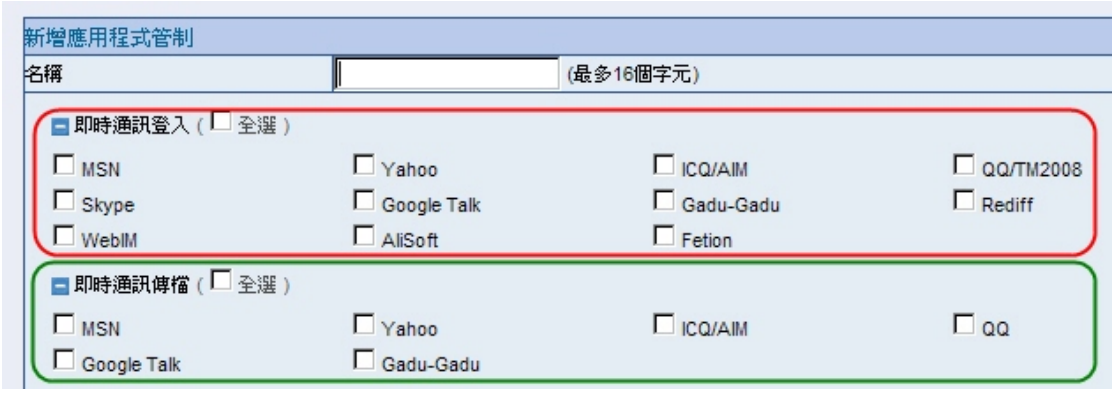
多功能 UTM / MS 系列報導

技術淺談與應用 - 即時通訊軟體的彈性管制及防護

即時通訊軟體目前已成為最為受歡迎的溝通工具，是繼電子郵件之後另一項最受公司所廣範使用的訊息溝通管道。透過即時通訊軟體使用者可立即相互的傳達文字、語音、影像、繪圖與檔案，卻也因為如此的方便性，漸漸讓各公司機關不得不重視相對而來的安全問題，而最近所爆發利用即時通訊軟體來洩露公司機密的事件，讓關於即時通訊軟體的安全議題不斷在持續發燒，也明白顯現出即時通訊軟體近年來對於各公司的重要性。

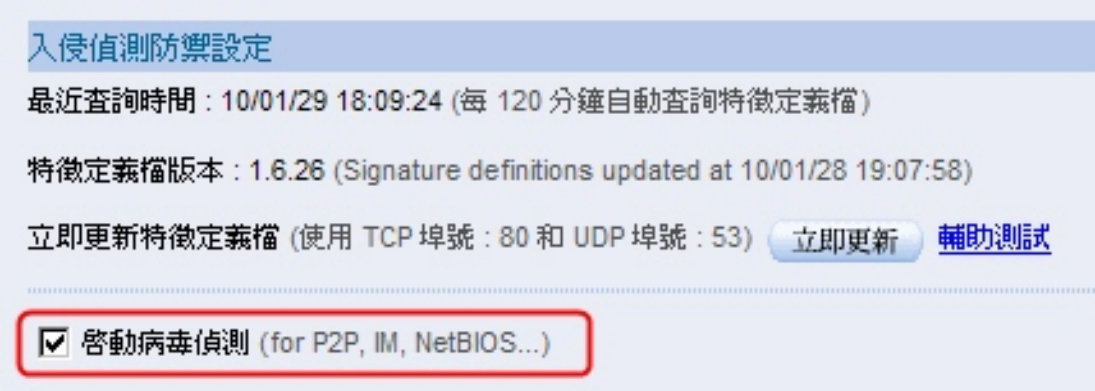
目前公司對於使用即時通訊軟體所存在的顧慮不外乎是『病毒的流入』、『檔案的交換』兩大方向，其次才是員工利用即時通訊軟體來進行私人用途，影響工作效率，傳送大容量影音檔案浪費公司頻寬資源…等。面對上述安全問題，公司網路安全管理人員又該如何去適當管制及防範即時通訊軟體來捍衛公司資訊安全呢？其實管理人員只需要利用新軟系統多功能 UTM 所內建的『應用程式管制』與『入侵偵測防禦』兩大功能，即可滿足公司針對即時通訊軟體 1.有效管制(阻擋、開放) 2.允許使用但限制傳送檔案 3.允許使用且同時搭配 Anti-Virus 防護，的三項資訊安全防護需求。

管理人員可於多功能 UTM “管制條例選項 > 應用程式管制 > 設定” 下進行即時通訊軟體限制的相關設定，而且沒有麻煩的設定手續，只須針對所欲管制的選項進行勾選即可完成設定，但管理人員還要注意到的地方則是，對於設定完成的限制條件，一定要套入 “管制條例” 中才會有實際的作用。同時還可針對不同的來源(部門)來搭配不同的限制條件，如此一來能更靈活運用的做適當管制。



應用程式管理設定畫面

此外，在開放使用即時通訊軟體的情況下，為防止病毒藉此管道流入，管理人員還可於系統“入侵偵測防禦 > 組態 > 設定”下，進一步的啟動病毒偵測功能，來做到更完善的保護。同時管理人員須於管制條例中勾選啟用 IDP 選項才能有實際作用。



可針對即時通訊軟體啟動入侵偵測防禦

除了使用新軟系統多功能 UTM 來進行有效的控管及防護之外，公司還可搭配利用教育訓練的方式來傳達及教導員工該如正確運用即時通訊軟體等相關知識，讓員工養成良好的使用習慣，以達到更加優化的使用環境。以下將分別提出簡略的使用注意事項，以供公司教育參考使用。

1.使用即時通訊軟體要以處理公事為使用之目的

於上班時間不以即時通訊軟體與他人過度閒聊，或許與客戶間的情感交流對公司有莫大的幫助，但過度的濫用即時通訊軟體來進行與公司無關的私人聊天，不但有可能會於無意間洩露重要資訊，也會影響到公司使用即時通訊軟體的正面義意。

（管理人員除了可使用多功能 UTM 來做分別管理，同時也可搭配網路記錄器 -IR 來做到更進一步的監視與管制）

2.不使用『自動儲存密碼』來當作即時通訊軟體平時登入的方式

因為無法確定公司電腦一定不會遭他人所使用，若是員工使用即時通訊軟體中的『自動儲存密碼』來當作平時登入方式，就容易讓有心人事藉此發送病毒、木馬或其他有害程式至其他聯絡人電腦中，甚至假冒其身份來傳送公司或個人的重要檔案及內容。

3.不隨意傳遞公司資訊、檔案或其他軟體

若使用者任意傳遞與分享公司文件，很容易發生洩密疑慮，而使用者若是透過即時通訊軟體於公司傳遞非法軟體，還可能會因此而觸犯法律同時也影響到公司商譽。

4.不明的檔案別任意接收

即使是認識的人所傳送的檔案，也要在詢問確認之後才進行收取的動作，因為當下並無法得知對方是否是在被植入有害程式的情況所發送出的檔案，若任意接收來路不明的檔案，使用者電腦可能會因此也感染病毒或被植入有害程式，除了危害到自身電腦，還可能會經由通訊軟體管道來散佈至公司內其他使用者電腦造成更嚴重的損害，甚至是因有害程式而讓使用者電腦裡的公司重要資訊外洩。

（利用多功能 UTM 雖可做到檔案傳遞與接收的限制以及病毒的防護，但若能搭配員工的良好使用習慣，才可以更有效的提升公司網路品質）

5.定期更改使用者登入密碼

定期更改使用者登入密碼，可有效降低被有心人士破解的情況發生。

只要作好適當的防護設定並搭配完善的管理政策，便可讓公司有個安全、穩定的通訊環境，特別是現今以速度決勝的商場上，善用即時通訊軟體還能夠協助公司追求更多更大的商機。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新軟多功能UTM「聯合防禦系統」協助網管人員快速找出企業內部資安危機源

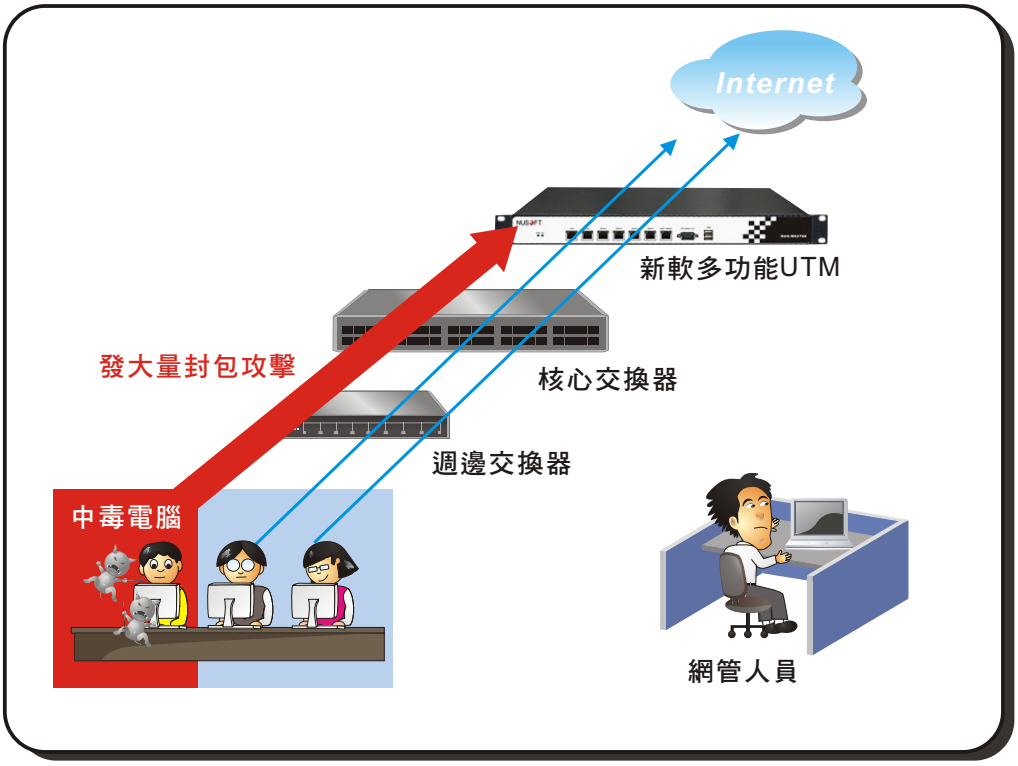
網路科技隨著時間增長而快速進步，並為人類帶來大幅度的文明進化，就連現代的公司企業也得依靠網路 e 化藉此提升企業本身的競爭力進而創造更高的企業營收。然而企業 e 化雖然能使企業獲取更高的利潤，但是這在駭客眼中將是他們「賺錢」好機會，因此許多網路駭客相繼研究出令企業聞風喪膽的電腦病毒進而在網路上散播，想藉此賺取他們所想要的金錢利益。因此危害企業資訊財產安全的電腦病毒問題一直存在於各大企業中且令許多企業十分頭痛；所以企業本身的資訊安全必然得做到最好、最完善，才能安安全全的保護企業資訊財產。

因為如此許多企業便斥資採購相關防火牆設備，想藉此安全保護自家企業資訊安全。不過現在市場上許多防火牆設備僅單純做到網路防護的功能，簡單來說：只是單純用來阻擋外部網路攻擊的網路前端防護設備；但是現在電腦病毒攻擊方式千變萬化，只靠單純的前端防護設備是不足以安全保護企業的。假使企業內部電腦的使用者誤下載含有電腦病毒之檔案的話，那麼電腦病毒便是從內部擴散出來，此時該使用者的電腦便在不自覺的情況下「中毒」了。目前最常見的攻擊方式便是採用發出大量封包（阻斷式攻擊）來癱瘓企業網路的手法，此時即便是裝設有一般防火牆的企業遇到此狀況的話，也是完全束手無策而任人宰割。

有鑑於此，新軟系統在多功能 UTM 中建置「聯合防禦系統」此智慧型防禦機制，有別於其他市售產品，此功能著重於“內部安全防護”重點上，機制啟動後將會主動檢查網路架構內所有電腦之網路流量，假設發現內部有台電腦會不斷發送大量封包企圖攻擊其他電腦藉此癱瘓企業網路，此時新軟多功能 UTM 經過規則分析比對後，判斷此部電腦為「中毒電腦」，便會依照規則控制「核心交換器 (Core Switch)」立即阻斷該電腦所傳送的連接埠，接著發送通知給網管人員並發送警告予該電腦用戶。如此一來，便可以在第一時間內防止該部電腦繼續發送攻擊，也可避免其他電腦遭到中毒電腦的病毒感染。

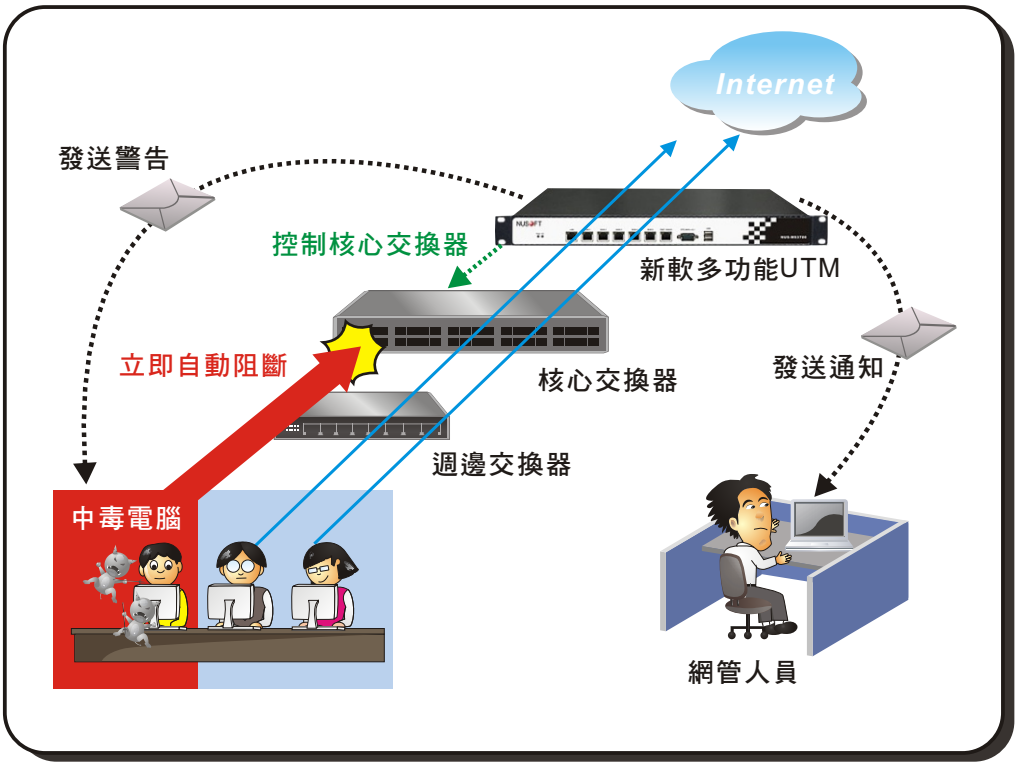
假設企業內部核心交換器 (Core Switch) 後端另接有周邊交換器 (Edge Switch) 的話，為了避免該核心交換器 (Core Switch) 後端其他無辜沒中毒的電腦用戶遭到網路封鎖，那麼收到通知的網管人員可以依照「交換器 MAC 表」所顯示的資訊，快速找出核心交換器後端“哪個周邊交換器在發送封包攻擊？”，接著單獨阻斷此周邊交換器並快速查出此周邊交換器“哪個通訊埠後端的哪部電腦在發送攻擊？”，藉此避免其他無辜電腦用戶遭到無妄之災而影響原本的工作進度。

新軟系統多功能 UTM 產品設計理念不單單只是「網路前端防護設備」而是以「全面性企業網路安全防護設備」為主；即使遇到資安危機發生源位於企業網路內部的話，新軟多功能 UTM 也能有效率地快速處理狀況，以避免資安危機的擴散，讓企業資訊財產能獲得更妥善的保護。



當企業內部有中毒電腦發動大量封包企圖癱瘓企業網路時

招財進寶



新軟多功能 UTM 會控制核心交換器阻擋發送攻擊的通訊埠，
並發送通知給管理員和該電腦用戶

文 黃政銘 ming@nusoft.com.tw