新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/3/31-2008/4/13 第64期

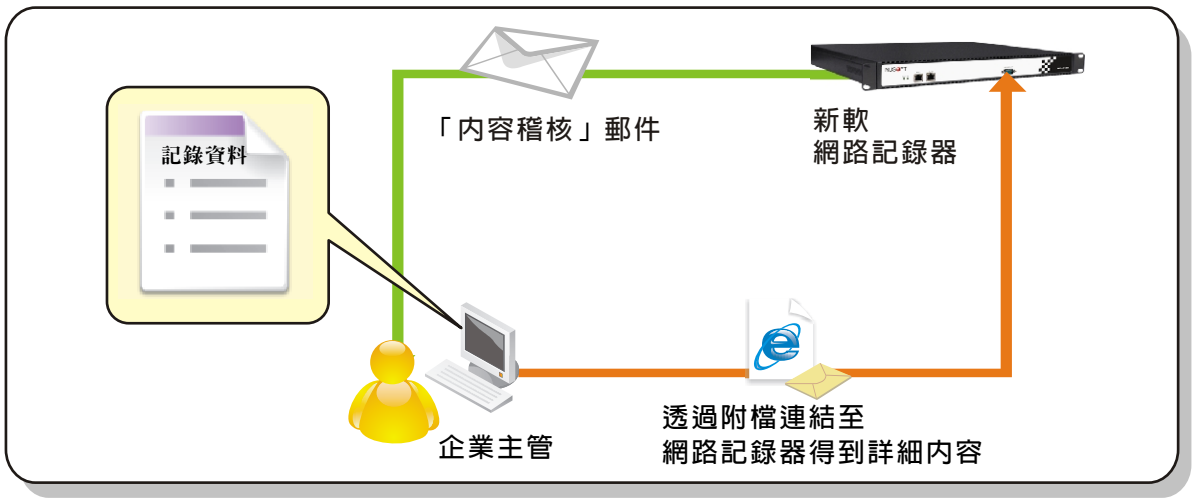
網路記錄器 / IR 系列報導

技術淺談與應用 - 記錄資料不必找，「內容稽核」自動呈上來

目前有越來愈多的企業在內部架設網路記錄器，不論是為了監督員工網路行為、防止企業機密外洩或者備份企業往來郵件…等目的，最終都是為了所需要的那幾筆記錄資料，但是網路記錄器所記錄的是全公司的網路行為呀，在記錄器裡找尋需要的記錄資料就有如大海撈針一般十分困難，雖然可利用搜尋功能找出記錄資料，不過這還得進入系統耗費一些時間呢，而且若之後有相關的記錄需要查核，就必須再做一次相同的搜尋動作，然而每天都做相同的動作何不讓系統自行來做呢。

為此新軟網路記錄器在最新的韌體版本中新增「內容稽核」功能，可按需求在稽核條例中設定搜尋的服務種類、使用者名稱、傳輸方向…等參數（關鍵字／字串），系統將根據稽核條例中的設定，自動於每天凌晨 0 點 30 分搜尋前一天的記錄資料，並將這些符合稽核規則的資料以附檔郵件的方式寄送給特定的收件者，收件者收到附有 HTML 檔案的郵件後，便可從郵件附檔中所提供的連結查看詳細的記錄內容。簡單的說，「內容稽核」就是代替使用者每天搜尋特定記錄資料的功能，這對於忙碌的主管來說，每天例行性的記錄篩檢也就輕鬆了許多。

舉例來說，假使目前公司正準備進行一場獲利可觀的標案，為了防範內神通外鬼將投標金額洩漏給競爭對手，專案主管可在「內容稽核」中設定稽核規則，使網路記錄器自動於每天凌晨，把含有與標案相關的文字或投標金額的記錄資料皆篩選出來，以郵件的方式寄送給主管查看，當主管收到此郵件時，再藉由郵件中所夾帶的 HTML 檔案瀏覽記錄，並進一步從檔案中的連結連線至網路記錄器而得到詳細的記錄內容，如此一來不需再花費多餘的精神進入系統中查尋記錄，只要每天接收郵件就能確保投標計劃是否遭到洩密，大大省去每天巡察記錄的時間。



這看似平凡的「內容稽核」卻是企業主管例行性查核記錄的一大利器，而這新功能所帶來的便利，只有等新版本的韌體發佈後，使用過的人才能體會的到。

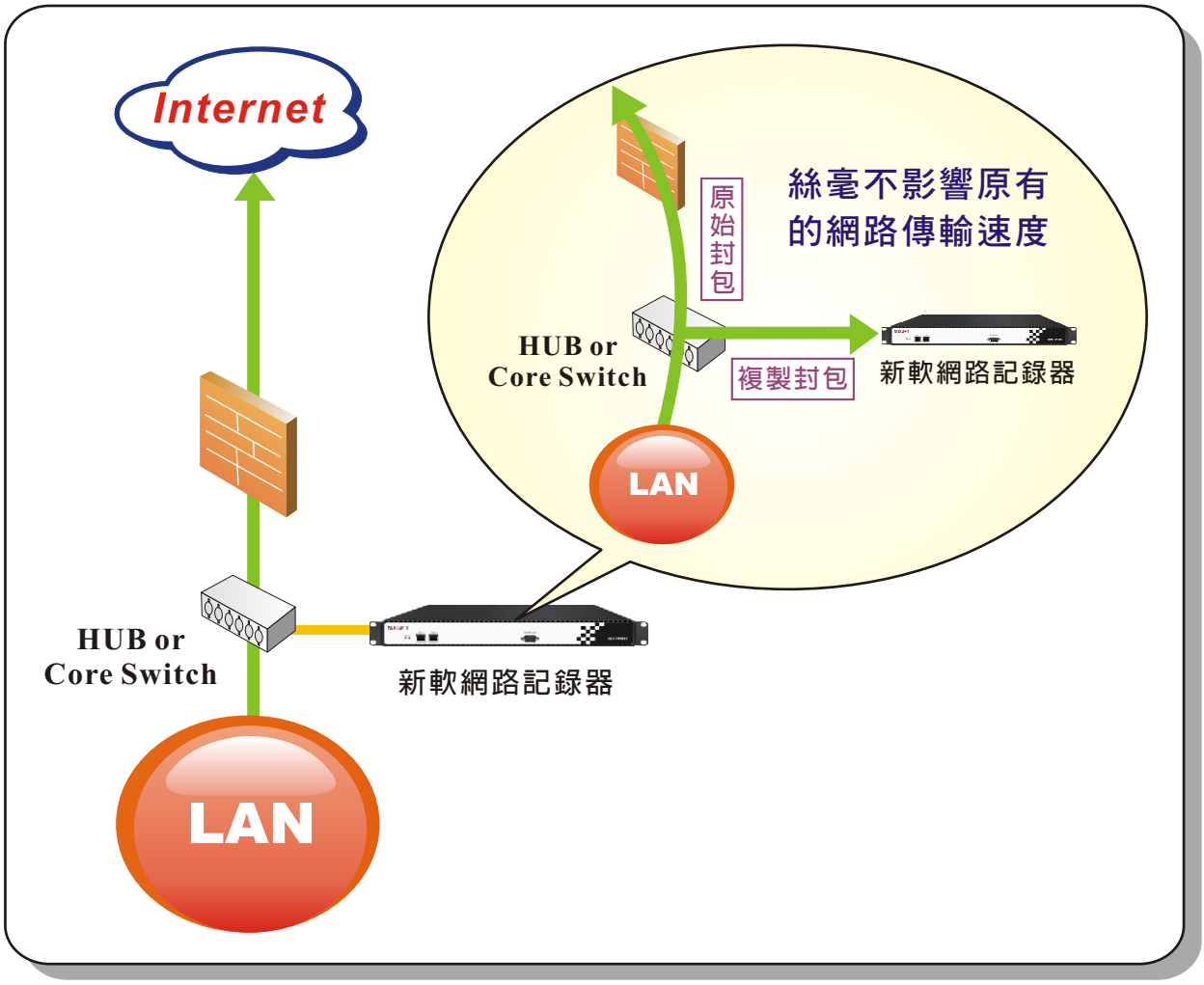
	舊有的記錄「搜尋」功能	新增的「內容稽核」功能
可分析的記錄種類	SMTP、POP3/IMAP、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET	SMTP、POP3/IMAP、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET
搜尋方式	使用者每日手動搜尋	系統根據稽核規則每日自動搜尋
顯示方式	立即顯示於操作介面	每天凌晨 0 點 30 分以附檔郵件寄出
顯示內容	依照所選擇的日期	前一天的記錄資料
方便性	對於立即需要查閱記錄資料的使用者較為方便	對於每天需例行性查閱資料的使用者較為方便

文 黃智傑 alex@nusoft.com.tw

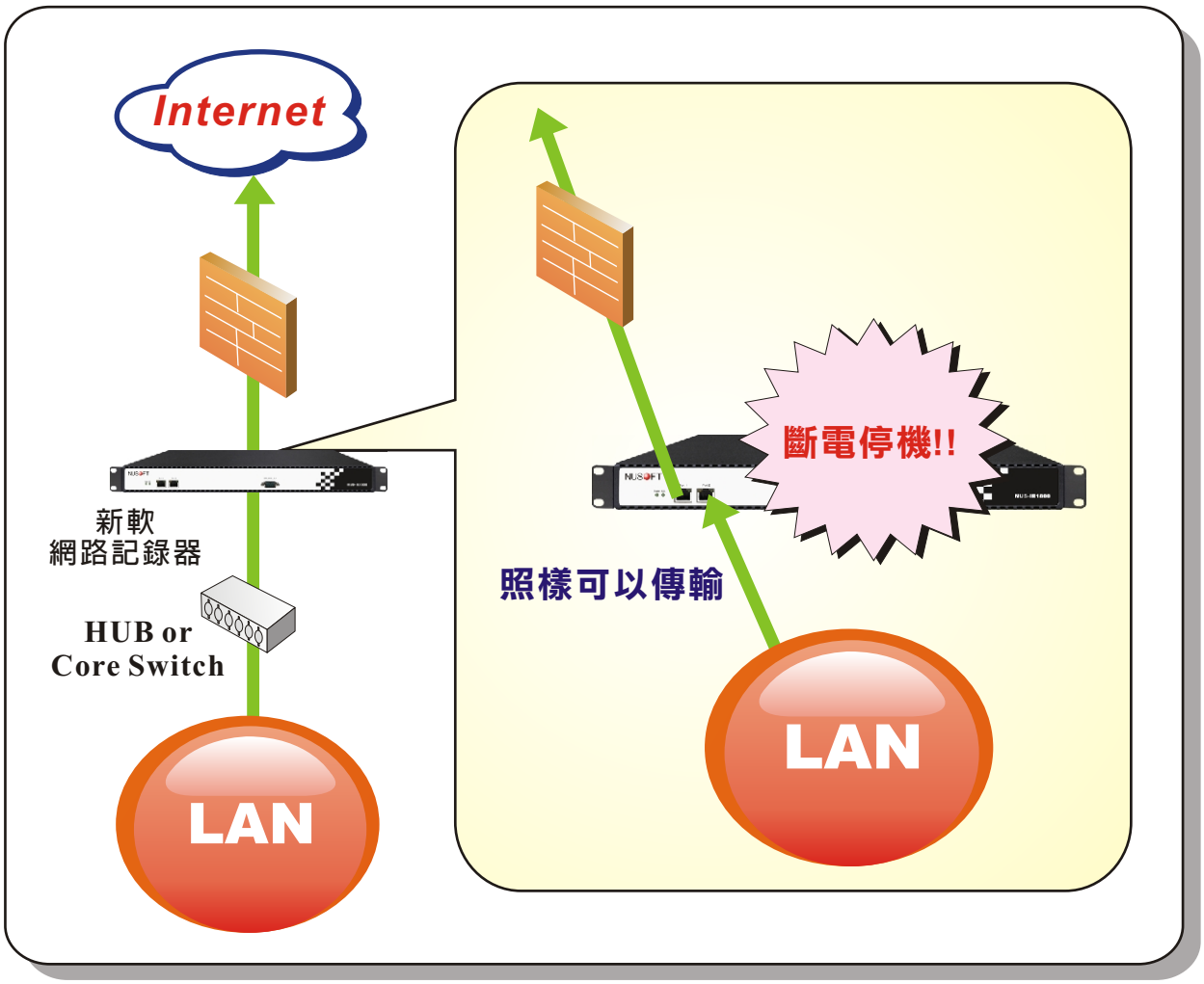
市場行銷報導 - 網路記錄器會影響企業網路的運作嗎

許多企業為了記錄企業內部網路活動情況，以確保資訊安全並遏止員工濫用網路資源，通常會考慮在企業網路裡架設網路記錄器，但在購買網路記錄器之前，往往心中都有一個疑慮，擔憂一旦架設網路記錄器便會影響網路的傳輸速度。

其實不然，以旁接方式架設網路記錄器，進出企業網路的封包皆會複製一份傳給網路記錄器做為記錄，而原來的封包在傳輸上並不會因網路記錄器有任何的影響或停頓，所以並不會因為在固有的網路架構中架設網路記錄器就造成線路壅塞，此外就算網路記錄器故障甚至埠孔鏽蝕損壞，也都絲毫不會影響企業網路原有的運作。



而另一方面企業更害怕的是萬一以橋接的方式架設網路記錄器，萬一設備當機或是故障斷電的時候，企業網路不就完全停擺了嗎？對此新軟網路記錄器不僅在設備當機時會自動重啟系統回復原來的運作，也因新軟網路記錄器支援 By Pass 機制，就算設備故障斷電也能讓往來頻繁的封包順利通過，維持企業網路正常運行。



文 黃智傑 alex@nusoft.com.tw