新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/11/12- 2007/11/18 第50期

多功能 UTM / MS 系列報導

技術淺談與應用 - 如何簡單運用 SSL VPN

拜網路科技進步所賜，大部分企業皆將其各種業務放置於網路上，以增加企業競爭力。這些業務除了網站、電子郵件...企業常用之對外服務外，與子公司、海外/外地營運據點、駐外/外勤業務人員...之訊息溝通、檔案傳遞也都常透過網路達到目的。而為了確保網路安全，這些訊息溝通、檔案傳遞大多都是仰賴各種 VPN 連線作為橋樑，以確保企業機密不外洩。

由於各種 VPN 的特性不同，其適用之環境、場景亦有所差異；IPSec VPN 適用在“地點固定的公司間連線傳輸”、PPTP VPN 適用在“固定電腦的個人與公司之間的網路傳輸”...而相較於其他 VPN 連線，SSL VPN 的連線方式最為簡單、易用、安全性高，而且可用在任何有提供網路連線的地點（家中、網咖、客戶公司...），因此是最適合經常在外奔波的業務人員使用。

雖然說 SSL VPN 在使用上相當簡單，很適合在外洽公之業務人員使用。但很可惜的是「相當簡單」這形容詞也只針對“有些了解電腦常識的人”而言，而一般「會用電腦」的業務人員頂多也只是會瀏覽網頁、收發信件、使用即時通訊軟體、編寫文件...，超出這範圍的電腦常識則一概不知。即使特地為此開班授課也是有聽沒有懂，想要他們了解 SSL VPN 如何使用變成一種奢求。因此，要如何讓 SSL VPN 的操作變的更加簡單上手，已成為讓業務人員使用 SSL VPN 的首要條件。

其實這方法也不難，只要讓 SSL VPN 的使用方式貼近使用者的電腦使用習慣，即可減輕其使用 SSL VPN 之困擾。需要注意的地方有三個：「如何讓使用者記住 SSL VPN 的網址」、「如何讓使用者記住 SSL VPN 的帳號密碼」、「如何讓使用者記住所要連線之伺服器的 IP 位址」。

如何讓使用者記住 SSL VPN 的網址？

新軟 UTM 的 SSL VPN 連線網址是“http://新軟 UTM 之 IP/sslvpn”，看起是來很簡單，但誰會去背這個 IP 啊！就算將「新軟 UTM 之 IP」更改為企業的 Domain Name，時間一久使用者也很有可能把“/sslvpn”這一段字串都忘的一乾二淨。因此，讓使用者記住 SSL VPN 的連線方式是件困難的事。那要如何讓使用者輕鬆連線至 SSL VPN 的網址呢？

其實，要使用者記住 SSL VPN 之網址，還不如使用下列方式供其點選，省事又便利：

- 利用「捷徑」記錄 SSL VPN 之網址

  SSL VPN 的網址以「捷徑」方式提供給使用者，使用者只要點選該「捷徑」，即可進入 SSL VPN 的登入網頁。

- 利用我的最愛記錄 SSL VPN 的網址

  您在瀏覽網頁時，是否會將常去的網站加入「我的最愛」呢？SSL VPN 的登入網頁也可將它加入「我的最愛」中，使用者只要點選「我的最愛」，即可進入 SSL VPN 的登入網頁中。

- 於企業網站，員工網頁上刊載 SSL VPN 的連結網址

  這方法可能有點麻煩，管理人員需要變更企業網站的設計，將 SSL VPN 的登入網址放到員工專用的網頁中。使用者如有需要使用 SSL VPN，只要到此網頁，點選該連結即可進入登入網頁。

如何讓使用者記住 SSL VPN 的帳號密碼？

讓使用者記住 SSL VPN 的帳號密碼可能是件最困難的事。根據統計，一個人通常需要記憶的帳號密碼有 6、7 組之多（MSN、網路銀行、E-Mail...），而且為了安全考量，這些密碼又必須「長的奇形怪狀」，如再加上一組 SSL VPN 的帳號密碼豈不是亂上加亂。因此，能把業務所會用到的帳號密碼加以整合，將會讓使用者輕鬆許

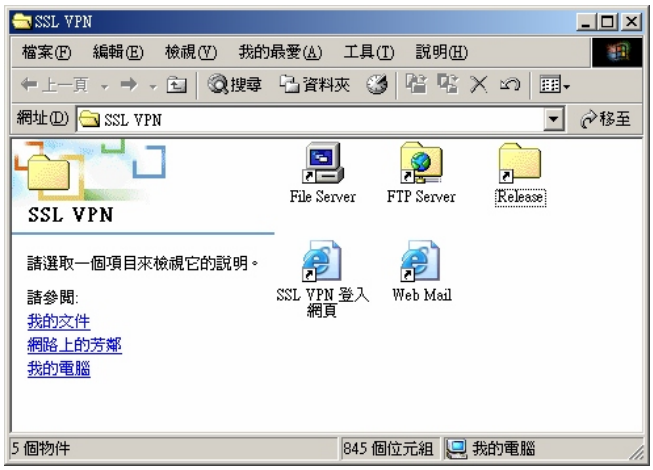
有鑑於此，新軟系統產品中所內建的各種認證功能都有支援外部 RADIUS、LDAP、POP3 之機制，當然 SSL VPN 也不例外。管理人員可透過此機制，將業務所會用到的帳號密碼加以整合（E-Mail、SSL VPN、FTP...）。如此一來使用者只需要一組密碼即可在企業網路中“趴趴走”。

如何讓使用者記住所要連線之伺服器的 IP 位址？

這是使用 SSL VPN 連線的最後一步，也是最重要的一步。倘若使用者 SSL VPN 成功連線，但不知如何進入各大伺服器中（FTP Server、File Server...），豈不是前功盡棄？其實，可以套用先前提到的「捷徑」、「我的最愛」、「員工網頁」這三種方式讓使用者直接用點選的方式連線至伺服器：

1. 以「捷徑」方式完成 SSL VPN 之連線

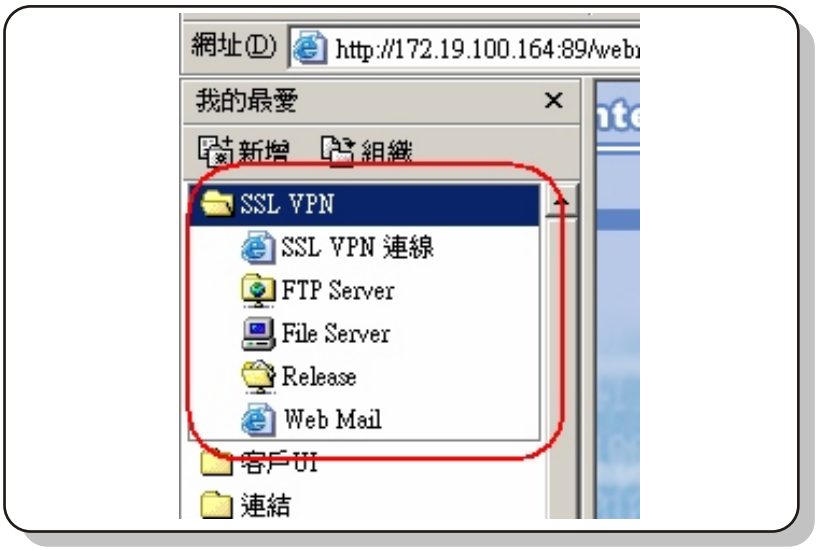
   管理人員可將「SSL VPN 之登入網頁捷徑」、「各大伺服器的連線捷徑」存放在相同一個資料夾中，再發佈給每一個使用者。使用者可將這資料夾放在桌面上或者是放在隨身碟中隨處攜帶，需要 SSL VPN 連線時點選其連線「捷徑」即可。



圖一 將 SSL VPN 相關之「捷徑」存放在同一資料夾中

2. 採用「我的最愛」來連線 SSL VPN

管理人員可預先將「SSL VPN 之登入網址」、「各大伺服器的連線 IP」加入至自己電腦的「我的最愛」中，再將它匯出。往後在教育使用者如何使用 SSL VPN 時，僅需幫使用者匯入先前所匯出的「我的最愛」檔案於其電腦中，即可完成 SSL VPN 相關連接建置工作。往後使用者只要點選瀏覽器之「我的最愛」中的 SSL VPN 連結，即可完成 SSL VPN 連線之相關工作。



圖二 利用「我的最愛」存放 SSL VPN 的相關聯結

3. 使用者透過「員工網頁」使用 SSL VPN

將「SSL VPN 登入網址」、「各大伺服器的連線 IP」以超連結的方式放在企業網站的員工網頁中。使用者只要需要進入員工網頁點選該超連結，即可完成 SSL VPN 連線之相關工作。

圖三 將 SSL VPN 的相關超連結至放於「員工網頁」中

透過上面的文章可以知道其實使用 SSL VPN 的方法十分簡單，要讓使用者學會如何使用一點都不難。如要再更加省事，只要預先準備好相關設定檔案，在教育員工時提供給使用者，其學習成果一定可以事半功倍。

文 程智偉 rayearth@nusoft.com.tw

市場行銷報導 - 多功能UTM:有硬碟機種與無硬碟機種之差異

現今網路科技的發達，雖帶給企業無限商機，但也間接導致各種網路威脅的日益增多。在這企業網路安全備受威脅的時機，新軟系統為企業研發了各種網路安全設備來替企業分憂，其中最為企業所矚意的就是多功能 UTM（MS 系列產品）。其不僅整合了企業所需的各項網路安全防禦機制，一次滿足企業對於網路安全的所有需求。同時透過簡單明瞭的管理介面，讓管理者輕鬆完成設定，大大地減少管理者維護企業網路的工作量。

多功能 UTM 系列產品目前共有四個型號：NUS-MS3500、NUS-MS2800、NUS-MS1500G、NUS-MS700 可供企業選用。這四個型號最大差異在其效能方面（適用人數之差異），至於功能方面則雖大致相同，但也有所部分差異。其中最顯而易見的地方就是「有硬碟機種與無硬碟機種」之功能差別。

那到底有硬碟機種與無硬碟機種的差異何在呢？其主要的差別就在於：有硬碟機種多了「郵件通知（Mail Notice）」與「隔離區」這兩項功能。

	無硬碟機種（NUS-MS700）	有硬碟機種（NUS-MS1500G、NUS-MS2800、NUS-MS3500）
提供郵件通知功能（發送垃圾/病毒郵件通知信）	X	O
隔離區（提供垃圾/病毒郵件保存、查詢）	X	O

表一 有硬碟機種與無硬碟機種之主要功能差別

多功能 UTM 的內建硬碟最主要是作為「信件的隔離區」之用，凡是垃圾郵件、病毒郵件皆可隔離在「隔離區」中。倘若有信件被隔離至此，多功能 UTM 會主動發出「郵件通知」給收件者，告知使用者有哪些郵件因發現異常而被隔離。收件者亦可藉由此機制取回所需之郵件，完全不用麻煩管理人員。同時，儲存於隔離區內的郵件，可依管理者的需求，來隨時進行搜尋、查閱及取回的動作，方便管理者了解目前郵件安全系統運作情況。

至於在無硬碟機種方面，因沒有內建硬碟作為「隔離區」之用，因此當電子郵件經多功能 UTM 判斷為病毒或是垃圾郵件時，無法做到「隔離」這個動作；僅能對該郵件做「刪除」、「傳送給收件者」及「轉寄郵件」之處置。在一般情況下，病毒郵件通常是直接「刪除」沒有任何問題，但是對垃圾郵件來說，卻不是最好的選項。

要知道，現今再怎麼厲害的郵件過濾機制，也無法百分之百完全正確判別所收到的郵件是否為垃圾郵件；如果是垃圾郵件判斷錯誤還好，但正常郵件被誤判為垃圾郵件而被刪除，對於企業來說風險就相當高了，不可不慎。

那這些垃圾郵件該如何處置呢？難道就無法解決這難題了嗎？其實，是有折衷方案的，對於無硬碟的 MS 系列產品，強烈建議垃圾郵件的處理方式是將這些信件，「轉寄」至特定郵件信箱存放，往後只需要到這郵件信箱即可取回所需要的信件。

產品類別	郵件類別	直接 刪除郵件	轉寄至 特定郵件信箱	存放於 隔離區
『有硬碟』 之 MS 產品	垃圾郵件	✳	○	◎
	病毒郵件	○	○	◎
『無硬碟』 之 MS 產品	垃圾郵件	✳	◎	—
	病毒郵件	○	◎	—
圖形表示	○ 可以使用	◎ 建議使用	✳ 不建議使用	— 無此功能

表二 有硬碟、無硬碟新軟 MS 產品之垃圾／病毒郵件處置方式

文 黃贊中 isaac@nusoft.com.tw