新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2011/5/1-2011/5/31 第127期

UTM / UTM 系列報導

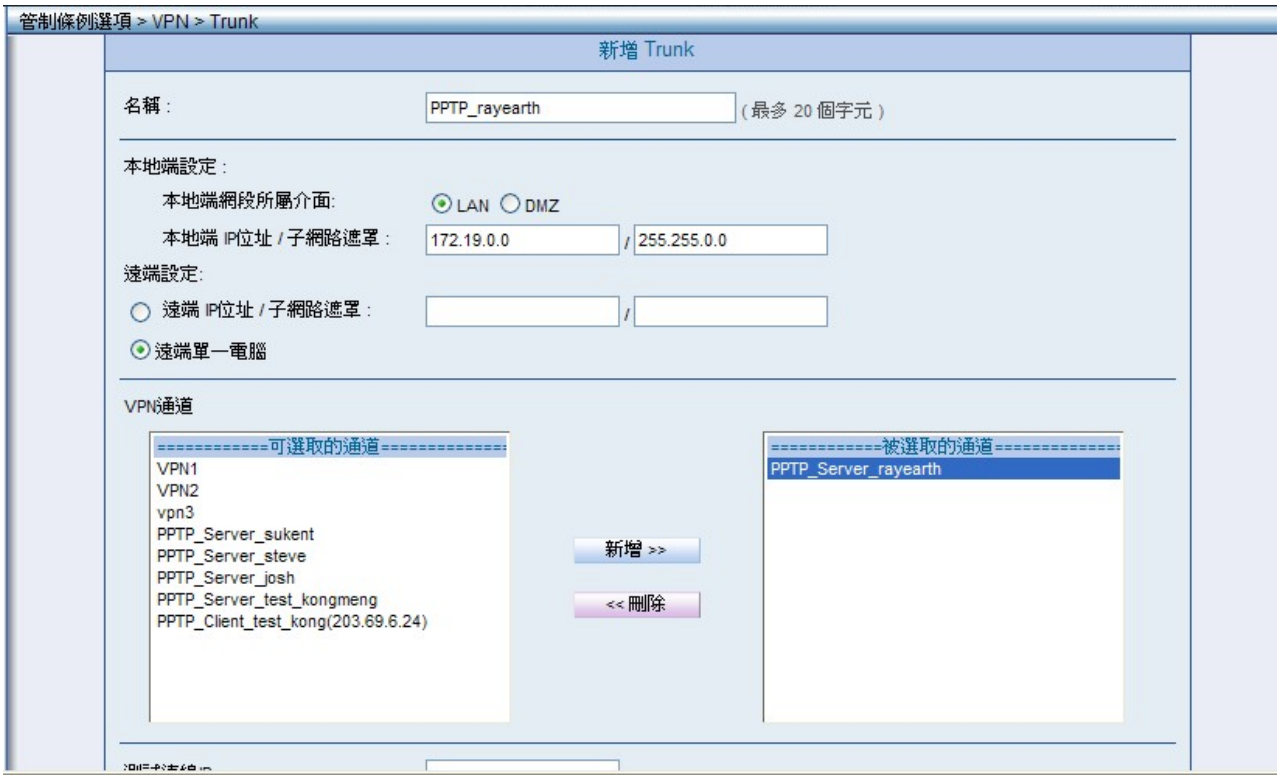
技術淺談與應用 - 如何用智慧型手機連線至公司內部網路

隨著企業化與網路發展之演變，有越來越多在外奔波的商業人士、業務人員及行動通訊使用者，希望能隨時在任何地方處理企業內部狀況。以便能及時完成主管所交待的工作事項或立即回應客戶之需求。但是，以往在外的管理人員，主要是透過筆記型電腦處理工作項目；然而，就像你在外地的旅遊景點休假，也會發生沒有隨身攜帶筆電，卻接到公司內部突發狀況，需要你處理。此時，必須放下手邊的行程，趕回飯店的房間開啟電腦上線解決。所幸，有了智慧型手機這樣的行動裝置，在外的管理人員可以隨時隨地拿出口袋裡的手機連線至公司，完成各項需要即時進行的工作。

由於智慧型手機的風行，有許多企業 IT 廠商也把腦筋動到這個平臺上(大致以 iSO 及 Android 平臺為主)，推出不少該平臺專用的應用程式，應用性質包括 VPN 遠端連線、設備的遠端登入等。其中，VPN 遠端連線為最熱門的整合運用。因此，新軟系統 UTM / MHG 系列之 “VPN” 功能，提供建立安全與私密的網路通訊服務，並讓管理人員透過智慧型手機連至公司網路，簡單易懂的操作畫面，讓管理人員在設定輕鬆許多。

首先，管理人員於系統「管制條例選項 →VPN→PPTP 伺服器」新增 PPTP 伺服器，輸入使用名稱與密碼即可。並且在「管制條例選項 →VPN→Trunk」新增 Trunk，輸入名稱、本地端設定、遠端設定，且可選取的通道新增至被選取的通道。設定好後，套入管制條例，便可設定智慧型手機上 VPN，連至公司網路。因此，不論是管理人員、業務人員、外勤人員只要擁有一組帳號密碼，便可連線至公司內部網路，完成各項需要即時進行的工作。

圖一



圖一

以 Android 平臺為主的智慧型之 3G 手機為例：

1. 進入 VPN 設定畫面(路徑：【無線與網路】>【VPN 設定】)，“新增 VPN 設定”。(圖二，由步驟 1~ 步驟 3)

圖二

2. 新增 VPN 後，選擇“新增 PPTP VPN”，在 PPTP 設定上，輸入“VPN 名稱”、“VPN 伺服器”、“DNS 網域”（伺服器可輸入 Domain 或伺服器 IP），連至網路。此時需輸入“帳號”與“密碼”，輸入正確，狀態呈顯已連線。（圖三，由步驟 1~ 步驟 8）

圖三

以 iOS 平臺為主的蘋果 iPhone 之 3G 手機為例：

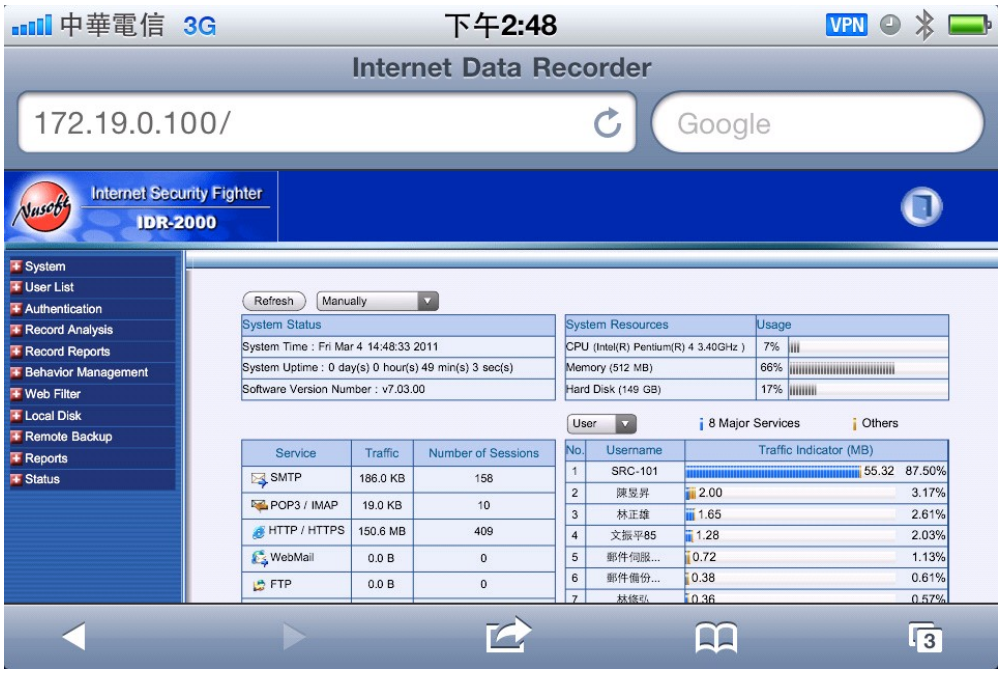
1. 進入 VPN 設定畫面（路徑：【設定】>【一般】>【網路】>【VPN】），新增 VPN 設定，選擇 PPTP 選項。（圖四，由步驟 1~ 步驟 2）

圖四

2. 在 PPTP 設定上，輸入“VPN 名稱”、“伺服器”、“帳號”與“密碼”(伺服器可輸入 Domain 或伺服器 IP)。帳號與密碼輸入正確，狀態呈顯已連線。(圖五，由步驟 1~步驟 4)

圖五

另外，VPN 連線成功後可直接連線設備的 Web 控制介面，可透過圖形介面的 RDP、VNC 這類的遠端控制軟體直接操控 PC、或是透過網管 APP 管控公司內部伺服器…。(圖六，連線設備的 Web 控制介面)



圖六

文 余光明 kongmeng@nusoft.com.tw

市場行銷報導 - UTM、MLS與MAF系列產品在於郵件安全防護功能的差異性

近幾年電子郵件的普及帶給人們許多便利，卻也潛藏著許多陷阱與危機，網際網路上到處充斥著垃圾郵件與病毒郵件的傳播，不時有駭客利用電子郵件讓企業成為轉送垃圾郵件的跳板，進而對企業機密資料和業務管理造成相當的危害。因此，一個好的電子郵件安全防護就是需要面面俱到，不但要能夠符合企業IT架構及穩定，並且同時兼具資訊安全的議題。當然，在實務上能做到確實的電子郵件控管，才是最為重要的。

新軟系統為了協助企業保護其電子郵件安全，一共推出了三款擁有郵件安全防護性質的產品—『MLS系列』、『MAF系列』、『UTM系列』供企業選擇。『MLS』、『MAF』與『UTM』皆提供多重垃圾郵件過濾機制，與病毒郵件防護（內建ClamAV與Sophos雙掃毒引擎）功能完美結合，可直接將垃圾、病毒郵件擋在企業網路之外。

同時導入「郵件稽核 / 歸檔」功能，來達到郵件管制的目的，以便提供主管稽核與郵件事後存檔調閱，作為全方位的郵件備份功能以及完整的佐證需求。這些基本機制是MLS、MAF、UTM系列所共有的郵件安全防護。但是，三者功能不盡相同。因此，當客戶有垃圾郵件過濾、病毒過濾、郵件稽核歸檔需求時，如何選擇產品，須先瞭解MLS系列、MAF系列、UTM系列的差異性：

1. 產品類型之差異：

   『MLS』－為Mail Server產品，內建完整Mail Server相關機制，需架設於企業內部網路中。

   『MAF』－為Mail Gateway類型產品，架設於企業Mail Server前端，以協助企業之Mail Server稽核、歸檔信件與排除垃圾、病毒郵件侵擾。

   『UTM』－為Gateway類型產品，架設於企業網路的最前端以保護企業網路。

2. 在“郵件安全（垃圾、病毒郵件過濾）”、“郵件稽核過濾”運作範圍上的差異：

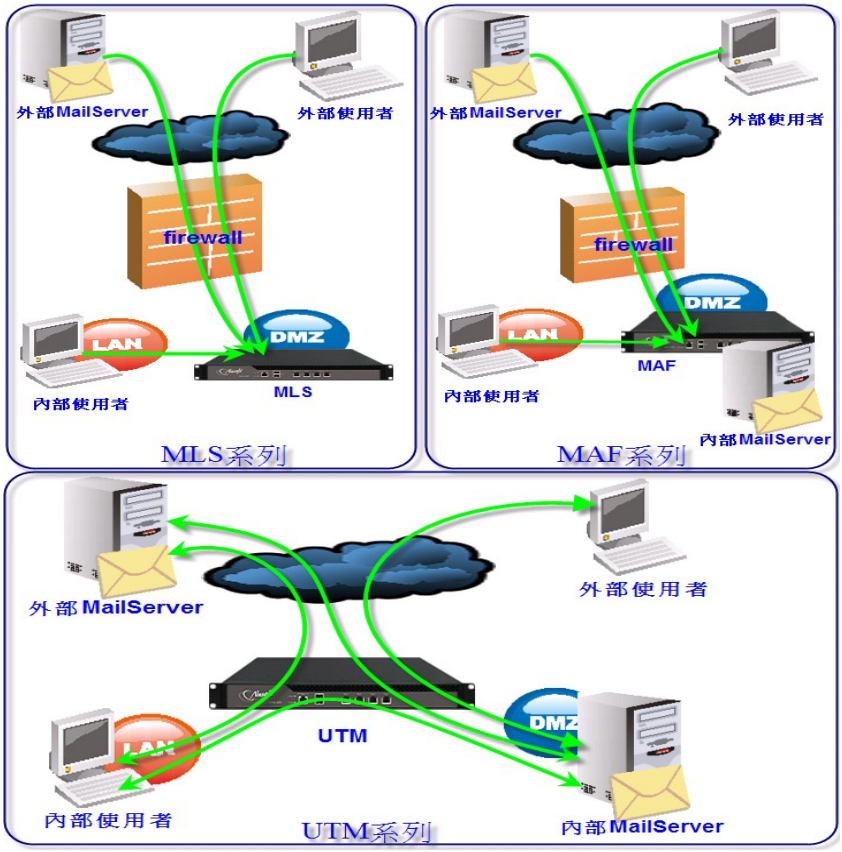
   『MLS』、『MAF』－其郵件相關機制最主要是針對企業信箱運作，企業往來信件皆可受到保護、管理與備份。

   『UTM』－所有經過UTM之郵件（企業信箱與外部信箱）皆可受到保護、管理與備份。

3. 郵件備份的差異：

   『MLS』、『MAF』－除了可主動備份企業往來之信件（企業信箱）外，亦可以將信件額外備份至外部備份伺服器（NAS、File Server. . .有提供網路芳鄰機制的設備皆可）。

   『UTM』－所有經過UTM之郵件（企業信箱與外部信箱）皆可備份。



註明：綠色代表郵件安全(垃圾、病毒郵件過濾)機制的方向

UTM、MAF、MLS 的垃圾及病毒郵件過濾圖

新軟系統產品	UTM	MAF	MLS
產品類型	Gateway	Mail Gateway	Mail Server
郵件安全、稽核、歸檔功能運作範圍	所有往來信件（含企業信箱、外部信箱）	企業信箱	企業信箱
郵件歸檔	歸檔於設備內部	歸檔於設備內部 ＋ 遠端備份	歸檔於設備內部 ＋ 遠端備份
使用時機	欲保護整個企業網路。	想要稽核、歸檔往來信件與排除垃圾、病毒郵件侵擾，卻因故無法替換於郵件伺服器。	欲替換郵件伺服器。

表-UTM、MAF、MLS 在郵件安全（垃圾、病毒過濾）、郵件稽核歸檔的差異性

文 余光明 kongmeng@nusoft.com.tw