新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/2/27 - 2007/3/4 第17期

負載平衡器 / MH 系列報導

技術淺談與應用 - VPN 負載平衡和備援

落實資訊安全已經成為目前企業使用網際網路連線時最基本的認知與政策。VPN 連線機制的導入更是為企業資訊安全注入一劑強心針。而在以往 VPN 的連線都是採用單一線路的連線方式建置，因此當線路中斷時，VPN 連線也隨之斷線。有鑑於此，新軟公司利用負載平衡器多個 WAN 埠的優勢，開發出 VPN 備援機制，不僅可整合多條 VPN 連線之頻寬，更能使 VPN 連線具有備援及負載平衡的效果，以達成 VPN 永不斷線的企業需求。

- 以 NUS-MH1500 為例：

總公司與子公司分別使用多 WAN 埠的 NUS-MH1500 建置網路閘道器，且均使用不同的兩條寬頻線路連上網際網路。首先，分別利用總公司之 WAN1 與 WAN2 介面位址建置至子公司之 VPN 連線，並命名為 VPN1 及 VPN2，同時於兩設備中 GRE/IPSec 功能選項填入相對應之 IP（如圖 一）。

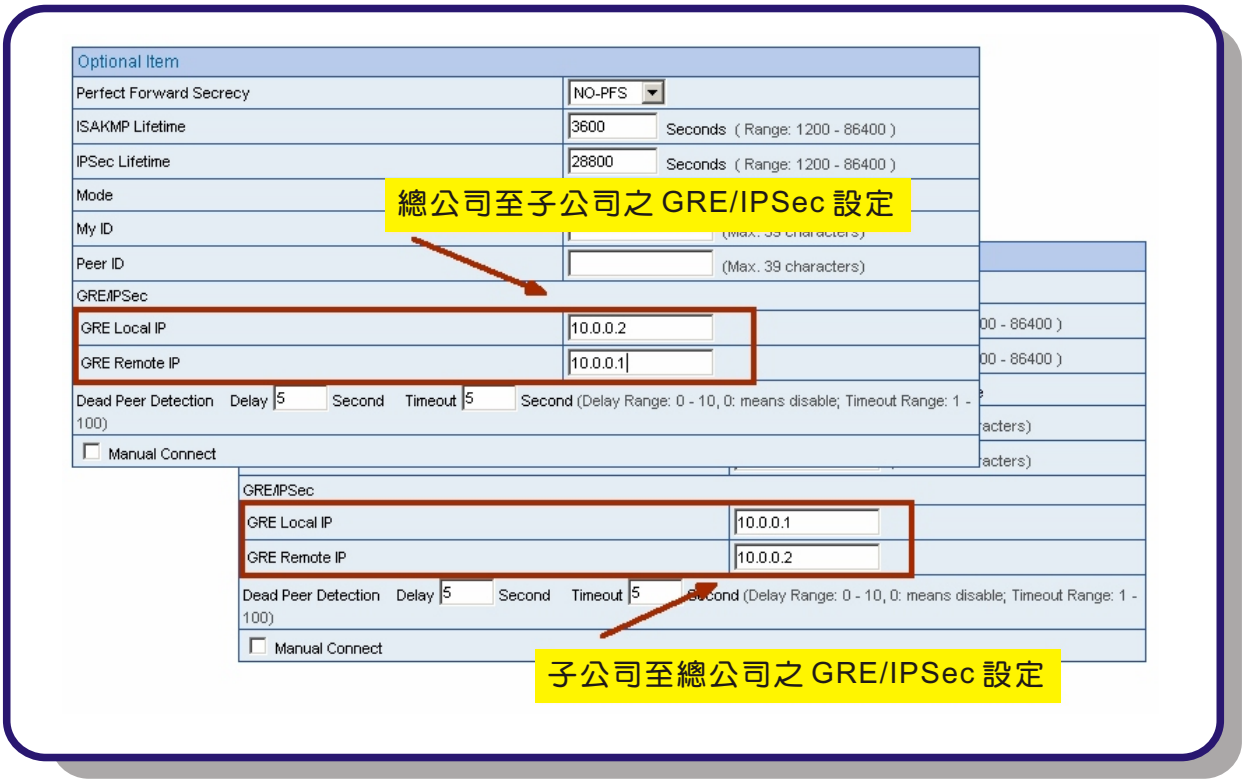

圖 一 GRE/IPSec 設置畫面

透過兩端點之子網域設定及管制條例的啟用，即可完成總公司至子公司之 VPN Trunk（如圖 二）。而子公司至總公司之 VPN Trunk 設定方式，亦採用上述之設定方式，藉此完成兩公司 VPN 連線備援機制。當 VPN1 或 VPN2 任一線路斷線時，NUS-MH1500 將會自動偵測並避開斷線的通道（ Tunnel ）傳輸資料，以避免單一 VPN 連線中斷造成相關作業停擺，並確保企業間 VPN 連線能夠暢通無阻。

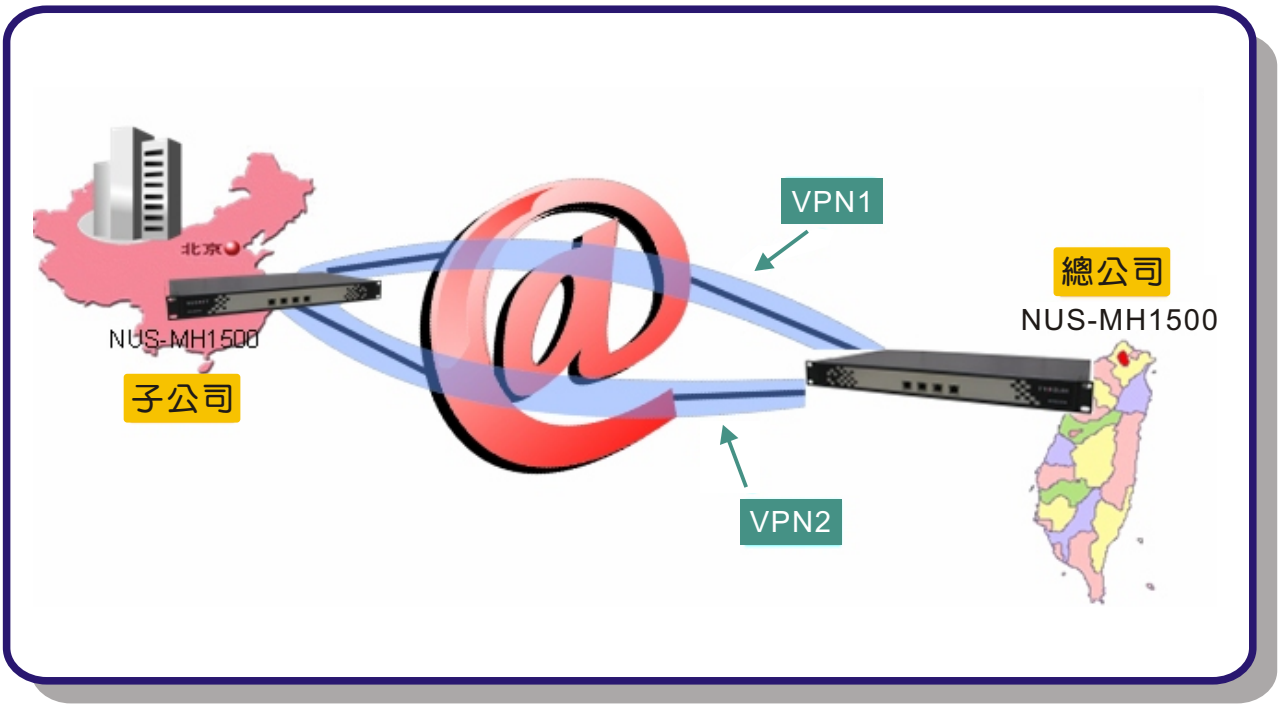

圖 二 VPN 連線網路示意圖

此外，當兩 VPN 連線皆處於正常連線之狀態下，而使用者欲透過 VPN 傳輸資料時，NUS-MH1500 將會根據管理人員事先所設定之負載平衡模式（如：自動分配模式、By Source IP、By Destination IP…等），分配至不同的 VPN 線路，使兩 VPN 線路之頻寬能夠得到完整的利用，藉此達到頻寬整合與負載平衡之企業需求。

文 賴鴻文 tony@nusoft.com.tw

市場行銷報導 - 網咖老闆的夢魘：ARP 病毒的偽裝與預防

一般網咖業者所採用的網路結構是屬於常見的區域網路型態。而在區域網路環境中存在著許多安全性危機。目前最常見的就是 ARP 欺騙了，很多駭客工具甚至是病毒都是透過區域內網中的 ARP 欺騙手法，來實現對電腦進行攻擊和阻止電腦存取網路資訊的目的。由於網咖業者並不能對來店消費的使用者進行過多的行為管制，因此造成部分不肖使用者將病毒工具帶入區域內網中，藉由 ARP 欺騙手法使其他電腦的對外連線皆透過特定電腦，完成其竊取他人機密資訊的目的，如：遊戲帳號、網路銀行帳號及身份證號碼…等（如圖 一）。不僅使正常使用網路資源的消費者權益受損，網咖業者對於隨之而來的網路效能降低更是難以根絕。

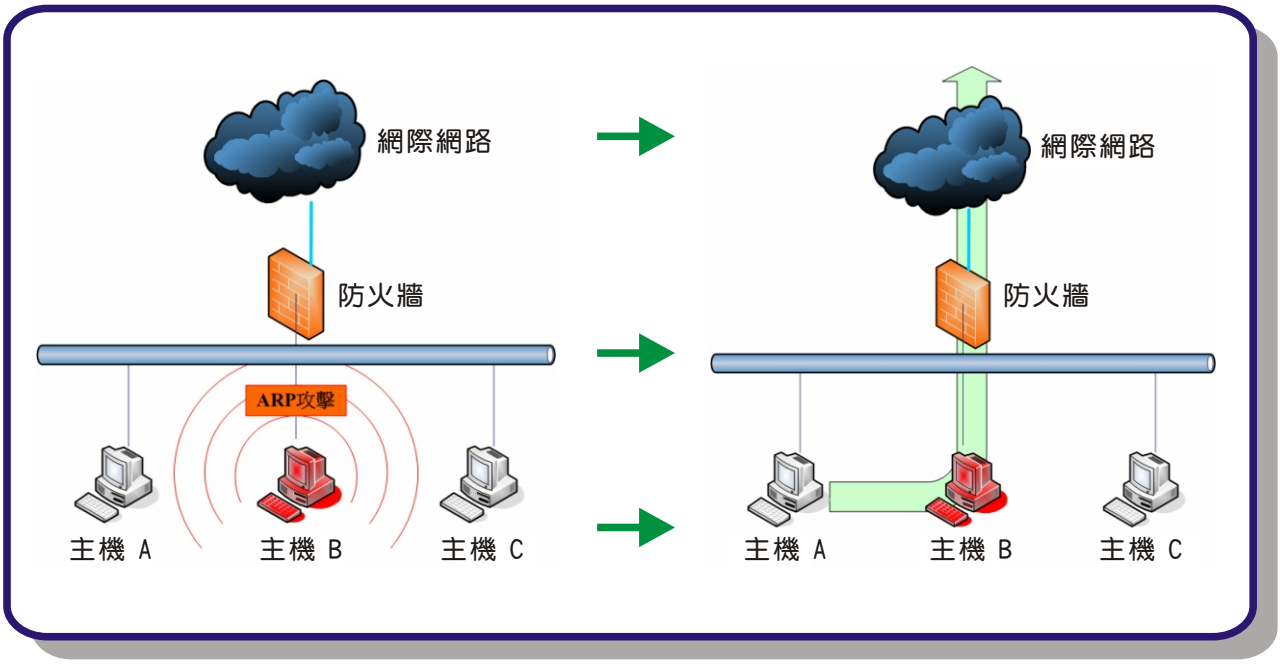

圖 一 利用 ARP 欺騙手法竊取他人機密資訊

由於它的攻擊手法不需高階的網路技術，隨便一個人都可以透過攻擊軟體來完成 ARP 欺騙攻擊，而內部網路一旦遭受此一類型攻擊，內部電腦可以說是無一倖免且難以追查攻擊來源。因此，目前為止坊間大多出現的大多只是消極的事後處理方案而非主動防護（如表 一）。

	使用方式	缺點
sniffer 檢測法	利用封包擷取程式檢測內網間所有傳輸封包。	1.消極的事後處理辦法而非主動防護。 2.需由專業人員逐一比對所有封包詳細資訊，相當耗時。
網路閘道監測	在網路閘道上面使用 TCPDUMP 程式截取每個 ARP 協議，且利用分析軟體分析這些ARP協議。	1.消極的事後處理辦法而非主動防護。 2.需借重專業網管技術，建置擷取及分析軟體。

表 一 消極的事後處理方案

有鑑於此，新軟公司以主動防護機制取代消極事後處理，研發出ARP欺騙（攻擊）手法的防範機制 — 靜態ARP模式。並將此一安全機制導入網咖專用機NUS-MH1000，藉此協助網咖業者杜絕ARP不法情事發生。管理人員可根據實際網路環境對表單內容進行新增與修改，以達成ARP Table之正確性與不可變動性。而區域內網之電腦群則可於功能介面中下載內建之防偽軟體，使內網電腦不再對網路閘道之ARP表進行更新。當雙方完成設定，日後若區域內網中發生ARP欺騙（攻擊）時，由於網路閘道與電腦並不會再對其更新相關資訊，因此，ARP欺騙（攻擊）也就無法達成其目的了（如圖 二）。

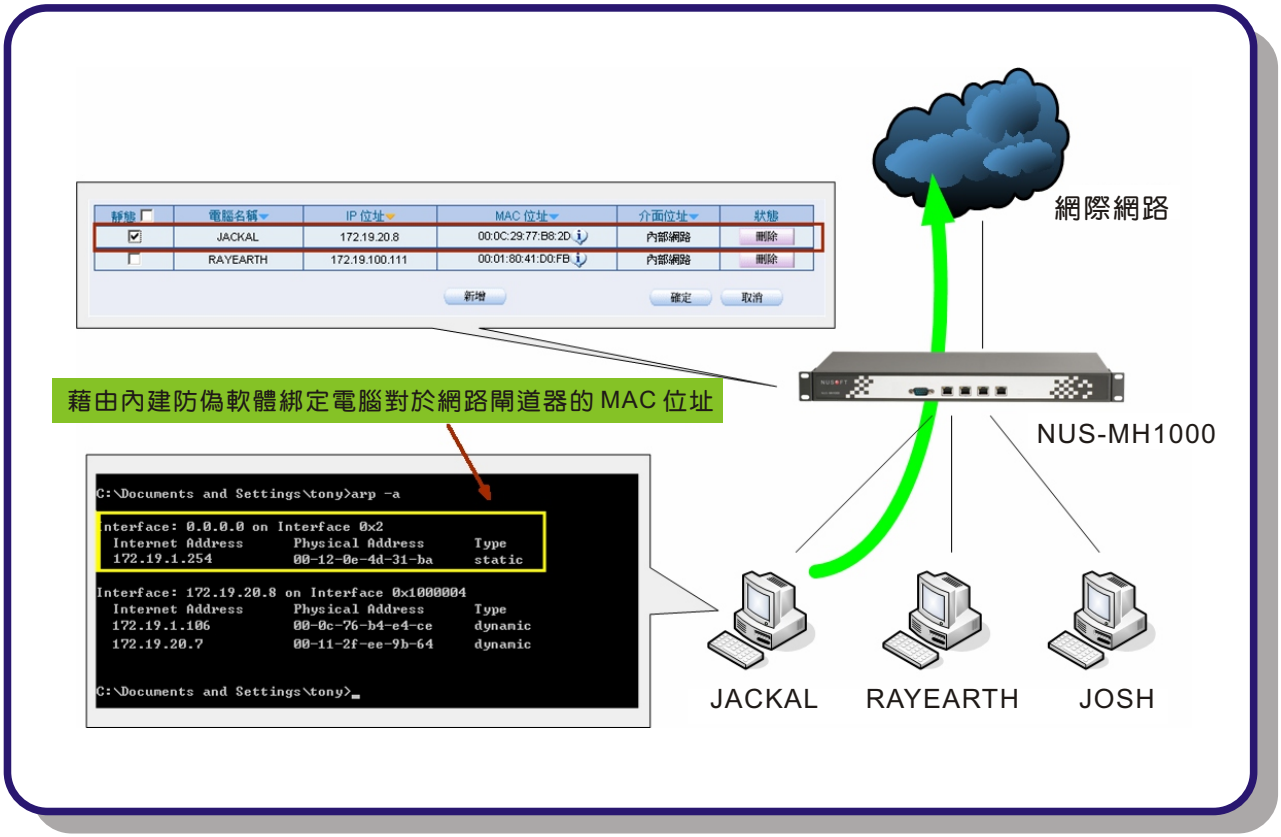

圖 二 NUS-MH1000 可有效杜絕ARP欺騙（攻擊）

文 賴鴻文 tony@nusoft.com.tw