新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/3/12 - 2007/3/18 第19期

多功能 UTM、負載平衡器 / MS、MH 系列報導

技術淺談與應用 - By Destination IP 與 By Source IP 的差異

隨著資訊安全意識崛起，多數公用伺服器已紛紛導入各種安全連線判斷機制。最常見的莫過於來源使用者（IP）的單一性判斷，舉凡網路遊戲、證券交易、網路銀行等伺服器皆廣泛使用。而利用“多 WAN 路由設備”上網之使用者會因為設備的“負載平衡功能”有機會同時使用兩條以上之 WAN 連線至目標伺服器，造成目標伺服器判斷連線異常而終止提供服務。

上述情況在一般企業裡，只要利用“策略路由”的方式，指定特定伺服器之連線僅由固定的 WAN 埠傳送即可。但是，網咖、學生宿舍、社區網路...這些網路環境則因為網路用途不固定，而導致一一以“策略路由”方式指定連線路徑成為不可能的任務。

為讓網咖、學生宿舍、社區網路...的使用者能暢通無阻的使用各種網路服務與更多元化及穩定的網路平衡機制，新軟公司在 MS 系列（多功能 UTM）與 MH 系列（負載平衡器）這些多 WAN 埠的產品中，增加了By Source IP（線上遊戲模式）與 By Destination IP（依照目的位置分配）兩種負載平衡模式來達到各種網路環境的需求。

	By Source IP Mode	By Destination IP Mode
適用對象	網咖、學生宿舍、社區網路...	網咖、學生宿舍、社區網路...
可達到效果	有效避免因伺服器的 IP 判斷機制，導致伺服器服務中斷的問題。	有效避免因伺服器的 IP 判斷機制，導致伺服器服務中斷的問題。 使用者可充分利用到每一條 WAN 埠的頻寬。
可能遇到問題	可能導致網路線路流量分配不均。	若同一線上遊戲需要同時連線至兩台以上伺服器（遊戲伺服器、遊戲認證伺服器...），則使用者的連線有可能經由兩個以上的 WAN 埠傳送，而導致伺服器服務中斷。

表 一 By Destination IP 與 By Source IP 模式差異比較表

- 以網咖採用 NUS-MH1000 並負載平衡設定為 By Source IP（線上遊戲模式）模式為例：

在 By Source IP 模式下，使用者的對外連線是根據來源位址（使用者 IP）來決定透過哪一個 WAN 埠連接網際網路。所以在圖一中，User 1 玩線上遊戲時所產生的連線（遊戲登入、腳色選擇、練功聊天...連線）會皆透過 WAN 1 來傳遞。倘若 User 1 想再使用其他的網路服務（至遊戲官網瀏覽網頁、收取信件），則也僅會透過 WAN 1 來遞送。直到 User 1 中斷了所有網路連線後，NUS-MH1000 才會開始對其新要求的連線封包重新導向。藉由此一負載平衡模式（By Source IP）將單一使用者的對外連線固定為同一WAN 埠發送，不但能有效防止無法取得服務的窒礙問題，更能提供使用者穩定的連線服務。

但因為 By Source IP 模式會強迫 User 1 的所有網路連線皆由同一個 WAN 埠傳輸，所以 User 1 不管是玩線上遊戲、瀏覽網頁...甚至是點對點下載檔案，都僅能使用單一WAN 埠之頻寬傳遞，進可能導致整個網咖的線路流量分配不均（一個大流量用戶將單一WAN 埠的頻寬耗用殆盡，其他 WAN 埠卻流量不高）。因 NUS-MH1000 有自動分配流量至頻寬使用率不高的 WAN 埠設計，所以線路流量分配不均之情形在網咖客人人數越多時會漸漸不明顯。

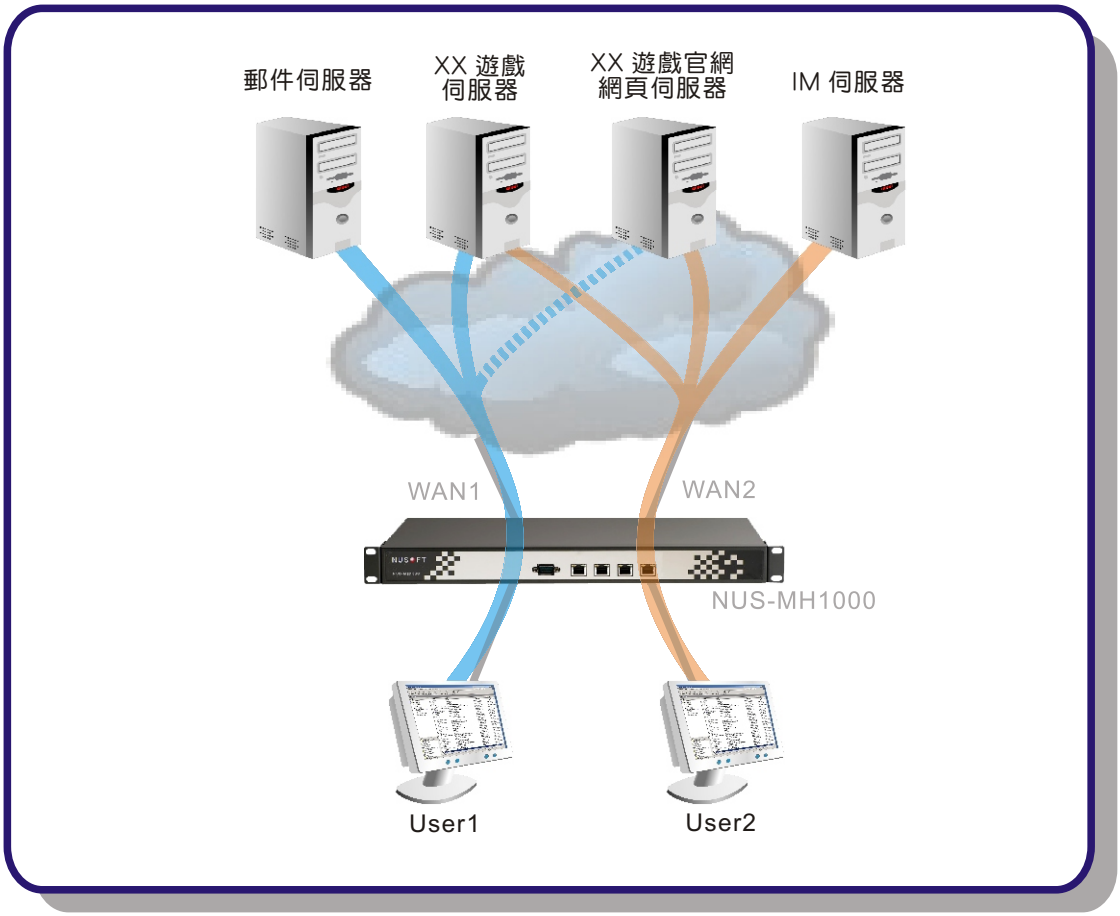

圖 一 By Source Mode 網路示意圖

● 以 NUS-MH1000 設置為 By Destination IP（依照目的位置分配） 模式為例：

在 By Destination IP 模式下，使用者的對外連線是根據目的位址（伺服器 IP）來決定透過哪一個 WAN 埠連接網際網路。所以在圖二中，所有連線至 “XX 遊戲伺服器” 的使用者（User 1、User 2）皆會透過 WAN 1來傳遞封包（遊戲登入、腳色選擇、練功聊天. . . 連線）。倘若 User 1 想從 “XX 遊戲官網” 找尋資料時，因 User 2 目前正經由WAN 2 瀏覽該網站，所以 NUS-MH1000 也會安排 User 1 透 過WAN 2 連線至此網站。直至所有使用者中斷了對 “XX 遊戲官網” 之連線，NUS-MH1000 才會對往後傳送至 “XX 遊戲官網” 的服務連線重新導向。藉由此一負載平衡模式（By Destination IP）將傳送至同一伺服器之連線固定為相同 WAN 埠發送，一樣也可以防止因伺服器來源 IP 判斷的機制，導致連線無法成功的窘境。

與 By Source IP 不同的是，使用者可充分利用到每一條 WAN 埠的頻寬，而不會侷限於單一WAN 埠。但有一點要特別注意：如果線上遊戲需要同時連線至兩台以上的伺服器（遊戲伺服器、遊戲認證伺服器. . .）時，使用者的連線有可能經由兩個以上的 WAN 埠傳送，導致線上遊戲連線失敗。

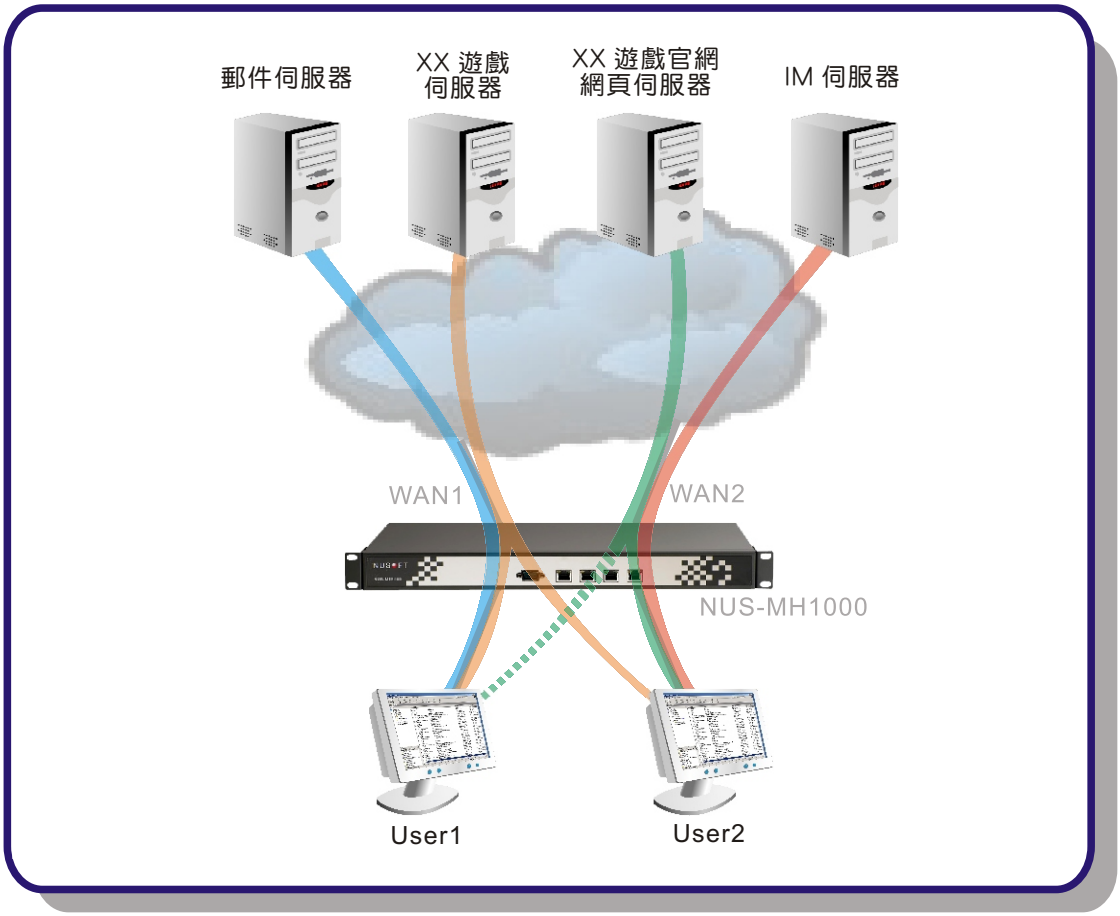

圖 二 By Destination IP Mode 網路示意圖

文 程智偉 rayearth@nusoft.com.tw

市場行銷報導 - 透過 DMZ 與 WAN 切換，擴充企業對外的線路支持

在這網際網路蓬勃發展的時代裡，頻寬連線的質（連線品質）與量（頻寬大小）一直是企業網路管理人員所熱切關注的話題。而如何在網路質、量與經濟利益之間，快速找尋到平衡點，更是企業網路管理人員終生搏鬥的使命。新軟公司所推之多功能 UTM 及負載平衡器等系列產品中，均採用多 WAN 埠的系統設計，提供企業最佳的解決方案。藉由多條便宜的外線取代單一且昂貴的專線費用，不但成就企業對於網路兼顧質與量的迫切需求，更節省了日後可觀的維護成本。

然而，在企業紛紛採用多 WAN 設備之際，卻往往僅針對現有的網路架構作規劃建置，或因設備價格落差大而被迫選擇較少外線之設備，忽視了企業成長之後對於網路外線的擴增需求。因此，當企業增加單一外線時，在以往似乎只能另外購買更多 WAN 埠的網路設備，對於企業組織來說，為增加單一外線而換購設備實在是勞民傷財的不智之舉。為此新軟公司特別研發出外線擴充功能，利用未使用的介面（DMZ）切換為第三個外部介面（如 圖一），提供企業增加單一外線時最適切的解決方案（如 圖二）。

圖 一 DMZ 埠與 WAN 埠介面轉換設定畫面

圖 二 透過 DMZ 與 WAN 切換，擴充企業對外的線路支援

反觀，一般市售網路設備則無此功能，在面對企業外線擴充需求時僅能選擇換購設備方式，與新軟公司之外線擴充功能有著明顯差異（如表 一）。

	方案一： 使用外線擴充功能擴充外線	方案二： 換購其他多 WAN 設備擴充外線
額外支出成本	無須額外支出成本	高成本支出
系統設定	無須重新設定	需重新編輯所有設定
所需時間	3 分鐘（重新開機即可）	一個工作天

表 一 擴增外線方案比較表

文 賴鴻文 tony@nusoft.com.tw