新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/11/19- 2007/11/25 第51期

負載平衡器 / MH 系列報導

技術淺談與應用 - IP 對映與虛擬伺服器有何分別

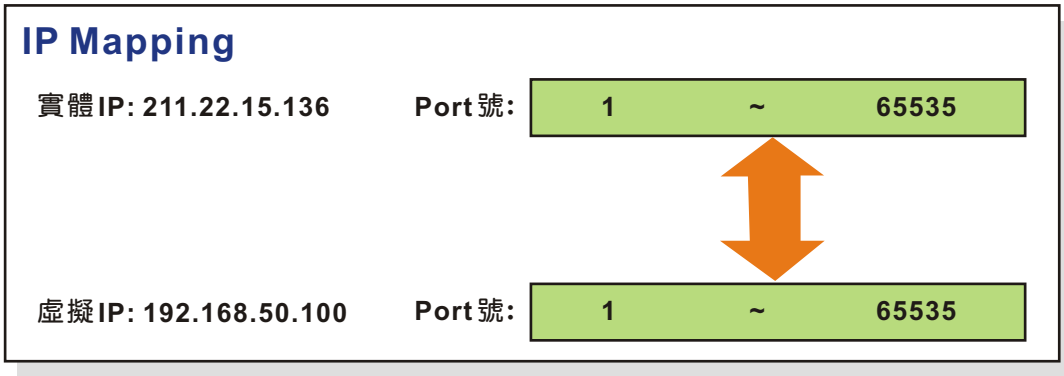
拜申請實體 IP 所費不貲的影響，絕大部分之企業都沒有足夠的實體 IP 供所有電腦上網使用。在實體 IP 僧多粥少的情況下，NAT（Network Address Translation）技術以虛擬 IP 的方式為企業解決了實體 IP 不夠使用之問題。而且使用此方式亦可避免企業內部電腦之 IP 直接暴露在網際網路之上被有心人士利用，間接提升企業網路之安全。但是，若企業需要架設網站、FTP Server. . .等對外服務時，NAT 技術反而會造成客戶無法與伺服器連線的問題！

要知道在 NAT 底下架設伺服器，伺服器也必需要使用虛擬 IP 來連接企業網路，所以位於企業網路外部的客戶根本無法透過伺服器之 IP 與其連線。如要解決這個問題，必須讓伺服器之虛擬 IP 有個可以對映的實體 IP 才行；讓客戶可以透過真實 IP 與伺服器連線。

因此，新軟系統的負載平衡器（MH 系列產品）、多功能 UTM（MS 系列產品）這兩款有 NAT 機制的產品，也擁有著可將實體 IP 對映至虛擬 IP 之功能－「IP 對映（IP Mapping）」、「虛擬伺服器（Virtual Server）」。這兩種功能皆可達到上述之目的，但其本質上又有些許的不同。

IP 對映

「IP 對映」就如字面上所示，其功能就是將外部的實體 IP 直接對映至企業網路內部的虛擬 IP，客戶可藉此功能從實體 IP 連線至伺服器。因「IP 對映」是將實體 IP 的服務埠“100% 全數對映”至“單一”虛擬 IP，所以比較適用於擁有充足實體 IP 的企業或是只須架設單一伺服器的 SoHo 使用。倘若將「IP 對映」使用在僅有單一功能之伺服器時，則算一種是比較奢侈的運用方法。畢竟一個實體 IP 所擁有的服務埠有 65535 個，伺服器如僅用到一個服務埠不是太浪費了嗎？（圖一）



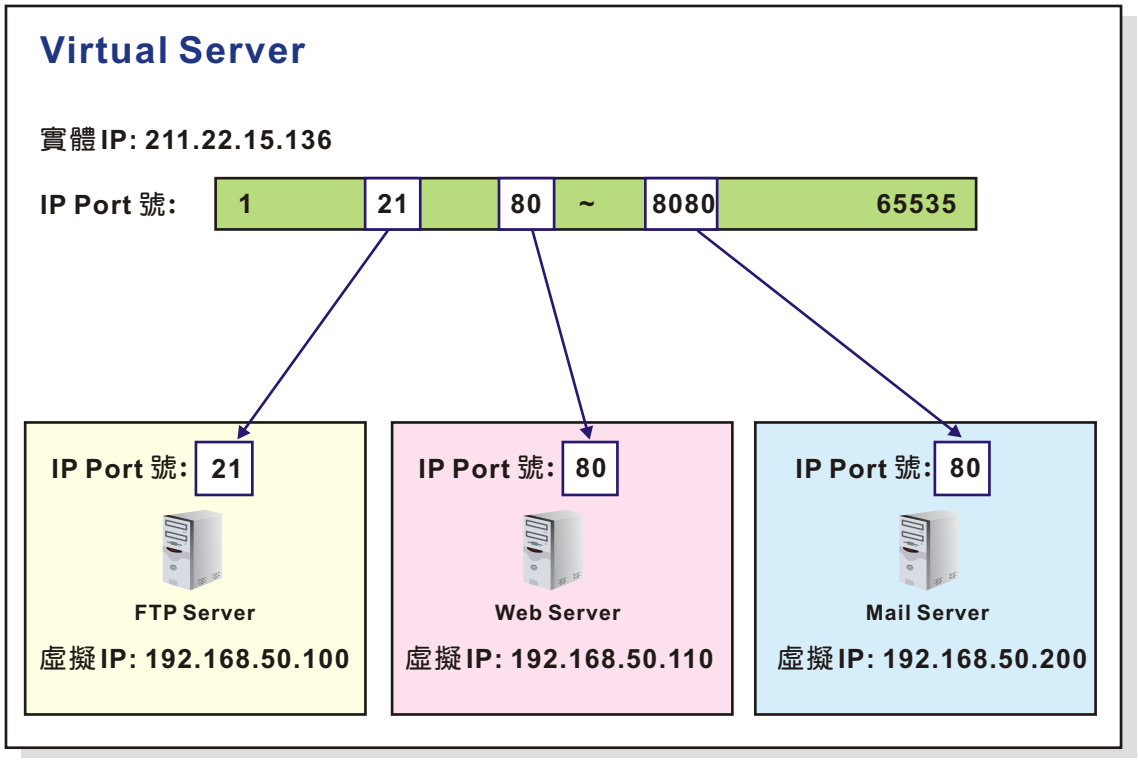
圖一 IP 對映會將實體 IP 的服務埠“全數”對映至“單一”虛擬 IP

虛擬伺服器

倘若「IP 對映」是實體 IP 與虛擬 IP 之間的對映，則「虛擬伺服器」就是屬與“埠的對映（Port Mapping）”；它可以將一個實體 IP 的服務埠分配給多個伺服器所使用。因此適合用於實體 IP 有限的公司，企業只需用單一實體 IP 就可架設多種伺服器（例如：把實體 IP 的 80 port 對映至 Web Server；21 port 對映至 FTP Server...），可將實體 IP 的利用價值運用的淋漓盡致。

而且，新軟系統所提供的「虛擬伺服器」亦擁有“伺服器負載平衡”機制－每個實體 IP 的服務埠可以循環分配方式對映至四個內容相同的伺服器。有效分散各伺服器的負載量，以維持這些伺服器的運作效能，讓客戶連線至伺服器時能更加順暢、更加穩定。

另外，假如企業需要架設兩個網站（企業網站、Web Mail），卻只有一個實體 IP 要怎麼辦呢？一個實體 IP 只有一個 80 埠啊！「虛擬伺服器」提供的“埠號變換”機制－可將實體 IP 的其中一個服務埠對映至虛擬 IP 的另一個服務埠。以上面的例子來說：企業可用實體 IP 的 80 埠對映至企業網站伺服器的 80 埠，再將實體 IP 的 8080 埠對映至 Web Mail 伺服器的 80 埠。如此一來，客戶只要從實體 IP 的 80 埠就可進入企業網站；而員工只要從實體 IP 的 8080 埠及可進入 Web Mail 中。（圖二）



圖二 虛擬伺服器將實體 IP 的服務埠分給多個伺服器所使用

從上面的文章看起來「虛擬伺服器」好像比「IP 對映」好用的多啊？那為甚麼新軟系統還要兩種功能都提供呢？這是因為「虛擬伺服器」的功能雖然強大，不過卻有使用數量的限制（新軟系統產品提供四組「虛擬伺服器」），而且設定上也比「IP 對映」繁瑣。所以當內建的四組「虛擬伺服器」不敷使用時企業即可應用「IP 對映」，而對於擁有足夠實體 IP 架設伺服器的企業，也較偏好使用「IP 對映」這種設定較為簡便的功能。

	IP 對映	虛擬伺服器
設定流程	簡便	需設定項目較多
可對應實體 IP 數量	64 組	4 組
一個 IP 可對映的伺服器數	一個	多個
伺服器負載平衡機制	無	有
是否支援埠號變換	否	是
適用時機	當四組虛擬伺服器不敷使用時	當所需架設的伺服器多於實體 IP 時
適用對象	擁有足夠實體 IP 架設伺服器的企業	實體 IP 不足的企業

表一 IP 對映與虛擬伺服器之差別（以 NUS-MH2400G 為例）

文 黃智傑 alex@nusoft.com.tw

市場行銷報導 - 新軟系統推出「One-Step IPSec」機制，讓您 IPSec VPN 一個步驟就建置完成

在以往，企業如需與其分公司、海外駐點... 透過網路傳遞重要資訊時，為了安全起見，會架設專線做為溝通管道。唯專線之價格不斐，並非一般企業可負擔的起，因此大部分之企業會採用 VPN（Virtual Private Network）的方式來取代專線。

在各種 VPN 連線當中，IPSec VPN 因適用在“地點固定的公司間傳輸”，所以企業常用在總公司與分公司的重要資訊傳遞上。但 IPSec VPN 在架設上素來複雜，且在近年來新軟系統為了提升其產品內建的 IPSec VPN 之傳輸安全性、管控靈活度...特別加入了「VPN Trunk」機制，將 IPSec VPN 列入「管制條例」控管。但也卻使得其設定上更加複雜，讓部分不常接觸 IPSec VPN 的管理人員不知該如何設定。難道，魚（安全、靈活管控...）與熊掌（設定簡單）不可兼得嗎？

為了讓管理人員能夠輕鬆使用架設 IPSec VPN 之環境，新軟系統特別在其負載平衡器（MH 系列產品）、多功能 UTM（MS 系列產品）加入了「One-Step IPSec（IPSec一步設定）」功能，來協助管理人員架設 IPSec VPN。什麼是「One-Step IPSec」呢？簡單的來講，「One-Step IPSec」將大部分在 IPSec VPN 架設時所要設定之資料以預設值替代，管理人員僅需要填入少數幾個必需自訂的設定值，其他像是「VPN Trunk」、「管制條例」...的設定則由系統代勞完成；管理人員只要一個步驟，即可完成 IPSec VPN 之建置工作，大幅降低其困難度。

	以往 IPSec VPN 所需設定步驟	One-Step IPSec VPN 所需設定步驟
1	IPSec 自動加密設定 名稱、外部網路介面、到目的位置、認證方法、加密金鑰、加密或認證方式、進階加密、ISAKMP 更新週期、加密金鑰更新週期、GRE / IPSec...	One-Step IPSec 設定 名稱、來源位置、目的位址、加密金鑰
2	VPN Trunk 設定 名稱、來源位址、目的位址、通道、保持連線IP...	系統自動完成 VPN Trunk 相關設定
3	管制條例設定 建立由內至外管制條例 建立由外至內管制條例	系統自動完成管制條例相關設定

表一 以往 IPSec 與 One-Step IPSec 設定上之差別

文 程智偉 rayearth@nusoft.com.tw