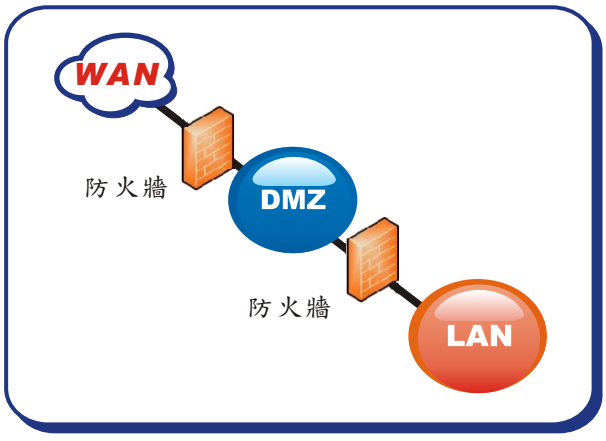
新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/9/3-2007/9/9 第41期

## 負載平衡器 / MH 系列報導

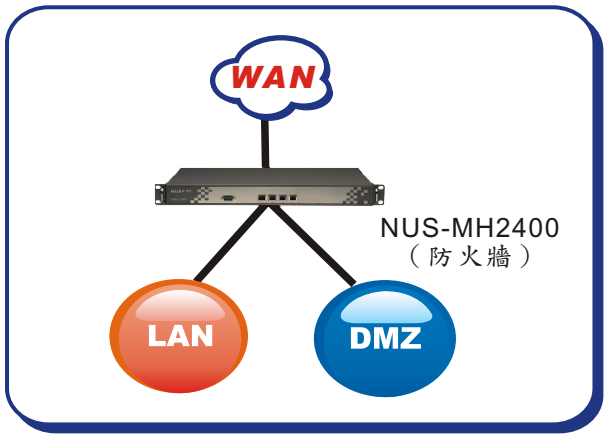
### 技術淺談與應用 - 什麼是 DMZ? 使用 DMZ 有何好處?

當您在架設新軟系統產品－多功能 UTM、負載平衡器時，是否在其外觀上發現其網路介面中除了擁有銜接內部網路的 LAN 埠、連接至網際網路的 WAN 埠外，還有一個使用者較不常接觸過的 DMZ 埠。甚麼是 DMZ 埠呢？

DMZ 為英文 De-Militarized Zone 的縮寫，一般稱之為“非軍事區”，本來是指軍事上禁止戰鬥的區域，而在網路方面在過去是指內部網路和外部網路之間的一小段網路（如圖一），常被用來架設伺服器之用。此種 DMZ 的架設方式可使伺服器的網路傳輸可受防火牆的監控，或受其它安全機制檢測，安全性高。但因為企業需要採購兩台防火牆，使得在架構與管理企業網路之成本大幅增加，令一般企業難以接受，所以絕大多數的企業已改採用另一種 DMZ 架構方式來建構企業網路（如圖二，新軟多功能 UTM 與負載平衡器皆是這種 DMZ 架構）。此種方式僅需要架設一台防火牆即可保護內部網路與 DMZ 區，兼具安全性與成本效益，故廣受企業喜愛。




圖一 傳統 DMZ




圖二 新式 DMZ

| | 安全性 | 成本 | 難度 | 便利性 |
|---|---|---|---|---|
| 傳統 DMZ | 高 | 高 | 高 | 低 |
| 新式 DMZ | 高 | 低 | 低 | 高 |

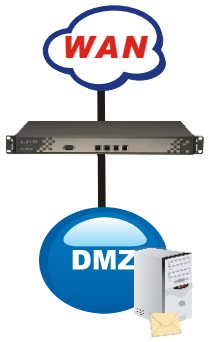
表一 兩種 DMZ 架構比較

為何伺服器放置於 DMZ 中會較為安全呢？放在內部網路不好嗎？一樣也可以受到防火牆的保護啊？實際上，伺服器所受到的網路威脅不一定來自於外部網路，亦有可能來自於內部網路－內部網路的電腦中毒是很有可能會拖累架設在內部網路之伺服器。將伺服器架設於 DMZ 時，任何通往 DMZ 的連線皆需要受到管制條例之控管，甚至是受到 IDP 與病毒偵測的保護（多功能 UTM），大大提昇了企業網路的安全性。

## 新軟系統所提供的 DMZ

新軟系統所推出的多功能 UTM（MS 系列）、負載平衡器（MH 系列）產品，擁有實體的 DMZ 埠（可以物理方式區隔內部網路與 DMZ）。並且支援兩種 DMZ 模式－NAT 模式 & Transparent 模式供企業選擇。

圖三 DMZ 採用 NAT 模式



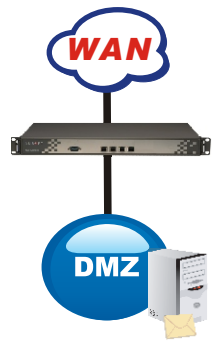

NUS-MH2400
WAN:61.134.36.168
DMZ:192.168.100.1

Mail Server
IP:192.168.100.100
採用虛擬 IP

### 1.NAT 模式

在此模式中 DMZ 為一獨立虛擬網域，其下伺服器採用虛擬 IP 架設，常用於真實 IP 不敷使用的企業。倘若欲開放伺服器供外部使用者連線時，需設定 IP 對應或虛擬伺服器，將外部尋求服務的連線透過實體 IP 導到內部伺服器的虛擬 IP。

圖四 DMZ 採用 Transparent 模式




NUS-MH2400
WAN:61.134.36.168

Mail Server
IP:61.134.36.169
採用實體 IP

### 2.Transparent 模式

又稱為透通模式，其下伺服器採用實體 IP 架設。因使用上較為方便，所以企業真實 IP 假如足夠，多使用此模式建構網路。倘若欲開放伺服器供外部使用者連線時，僅需要開放管制條例。

## 常見於市面上的“偽”DMZ

除了上述 DMZ 之外，市面上還有些產品因硬體設計關係（無實體 DMZ 埠），導致無法實際提供 DMZ 功能，因此將可新增網段的 Multiple-Subnet 功能宣稱為“軟體 DMZ”。“軟體 DMZ”並無法以物理方式區隔 DMZ 與內部網路，因此並無法確實保護架設於 DMZ 區域的伺服器。

另外，部分 IP 分享器也宣稱擁有 DMZ，但其與真正的 DMZ 功能天差地遠－設定於這種“DMZ”下的電腦將失去任何保護，面臨種種的安全風險。

文 周政達 zhengda@nusoft.com.tw

## 市場行銷報導 - 任意 IP 路由-解決開放式網路環境的有效方案

在網路運用日益普及的趨勢下，日常生活中所需之資訊來源，也漸漸被此管道取代。然而，一但離開了所熟悉的環境，您是否會為了要使用網路而遇到許多窘境？

由於行動設備（例如：筆記型電腦）的廣泛使用，所以無論在咖啡廳、餐廳、飯店、機場、休閒廣場…中，皆開始提供有線或無線的上網環境。但在一個陌生的網路環境中，常常需要依循一堆繁雜的程序、設定後方能使用。而絕大部分的使用者只懂得如何瀏覽網頁，如何收發信件，對於網路連線相關設定則是一竅不通，到最後還需要求助於相關服務單位來解決其問題。

在外洽公、旅遊、…的網路使用者，基於上述的原因，在急於取得、傳遞所需的訊息時，只能耐著性子找出連通網路的方法，這種迫於無奈造成的時間延誤，常常影響著這些使用者的利益。最明顯的例子就是，一份急需審核的授權文件遲遲無法傳輸、欲獲得資訊隨時調整行程…，無不因為這些因素導致許多無法彌補的後果。

有鑒於此，任意 IP 路由技術，就成為解決諸多問題的關鍵。不論使用者筆記型電腦的網路設定為何（IP 是否隸屬於既定的內部網段、預設閘道是否設定為既定的 IP），只要能在支援此技術的網路環境中獲得存取點，就可立即上網。以往在異地使用網路的不便和困擾從此成為歷史。（如下表）

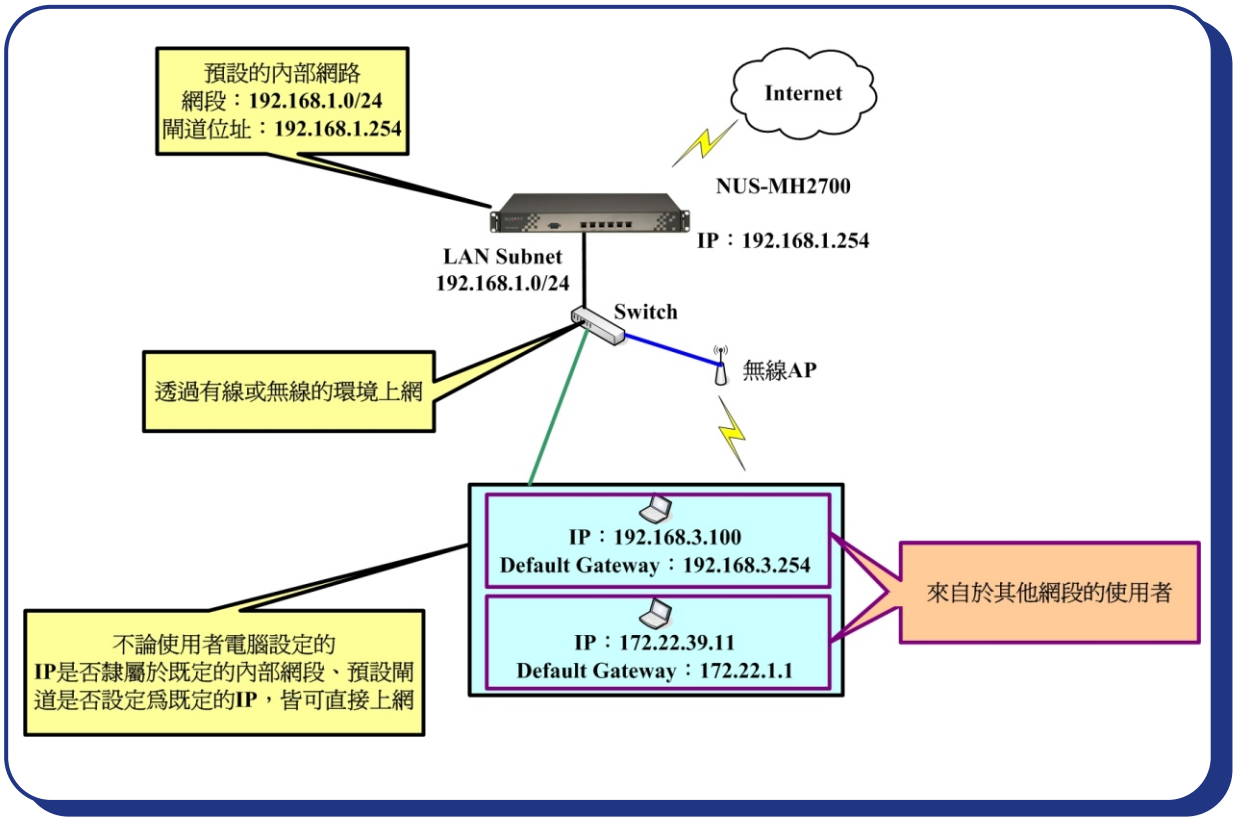
| | 任意 IP 路由器 | 傳統路由器 |
|---|---|---|
| 使用環境 | 開放式環境（例如：咖啡廳、餐廳、酒店、機場、休閒廣場…） | |
| 使用對象 | 持有行動設備（例如：筆記型電腦）在外洽公、旅遊…的人 | |
| 使用方式 | 獲得連線訊號直接上網 | 須依照指示說明，更改需多設備上的網路設定 |
| 便利性 | 可即時傳遞訊息 | 需耗費一定時間完成前置作業 |

任意 IP 路由和傳統網路在開放式環境中的差異

以飯店為例－

在傳統網路環境的情況下，房客如需上網，必須將其行動設備的 IP 位址、子網路遮罩、預設閘道位址...依飯店網路的需求設定。倘若房客對於網路連線方式不甚了解，則需花費大量時間嘗試連線，或是尋求飯店方面的協助。

而在任意 IP 路由的環境下，不管房客先前使用網路的連線設定為何，只要其行動設備可接上存取點（有線 or 無線網路）就可立即上網，不需要再變更行動設備的網路相關設定。（如下圖）




文 陳昱昇 josh@nusoft.com.tw