新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/2/5 - 2007/2/11 第15期

# 負載平衡器 / MH 系列報導

## 技術淺談與應用 - 永不斷線的商機

隨著世界網路潮流，電子商務系統的運用已是企業網路必備之勢。而如何提供永不中斷的商務服務更是企業當務之急。為此新軟公司積極投入各項平衡機制的研發，運用高可靠度的 DNS 技術與 Inbound 平衡技術，使得平衡效能凌駕於國內外其他競爭產品之上。

新軟公司所研發之 Inbound 負載平衡機制提供多種模式（包括：Round Robin / Weighted Round Robin / Auto Back Up），來因應企業網路平衡需求。而內建的 DNS 伺服器，更支援同時維護多個網域（domain），並藉由每個網域多種紀錄（A / CNAME / MX)的設置，來達到 Inbound Load Sharing 的功能，協助電子商務系統能提供更即時、快速與穩定不斷線的網際網路線上服務。

- 以 NUS-MH1500 設置 BackUp 模式為例：

為避免企業網路斷線錯失商機，系統管理人員可於 Inbound 負載平衡功能中設置備援功能（如圖 一）。當使用者於外部網路瀏覽網站時，將一律經由 WAN1 進入網頁伺服器。倘若 WAN1 線路斷線時，WNA2 將於第一時間啟用接任 WAN1 線路的工作，使企業線上服務永不中斷（如圖 二）。


圖 一 自動備援模式設定畫面

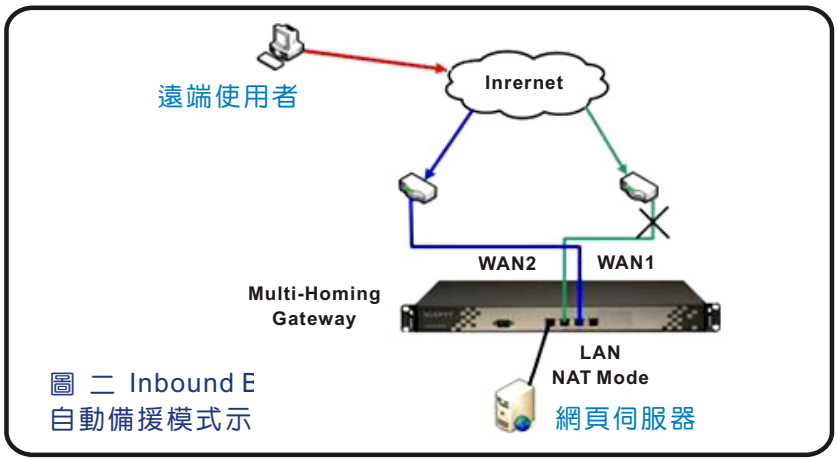


圖 二 Inbound E
自動備援模式示

● 以 NUS-MH1500 設置 Weighted Round Robin 模式為例：

系統管理人員可根據需求設計線路負載承受量，假設 WAN1 線路頻寬較 WAN2 低，因此設置權重循環分配（Weighted Round Robin）功能，將流量依 1:2 的比例導向至不同的外部介面（如圖 三）。使外部使用者與內部伺服器皆能享用到最充裕的頻寬，藉此提高企業電子商務之服務品質（如圖 四）。


圖 三 權重循環模式設定畫面

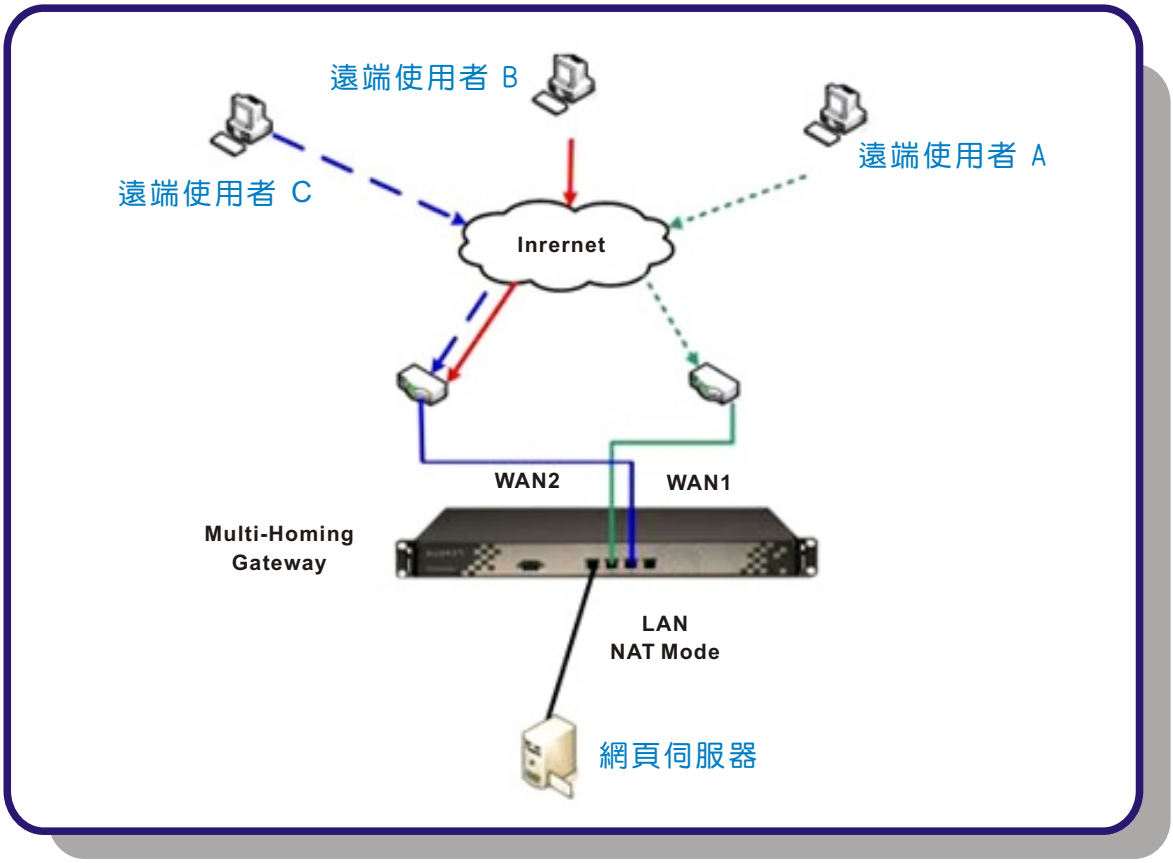


圖 四 Inbound Balance 權重循環模式環境示意圖

文 賴鴻文 tony@nusoft.com.tw

## 市場行銷報導 - 聯合防禦(Co-Defense)的重要性

企業作業流程大量 e 化與電子商務的興起，加重了企業管理階層對於資訊安全的需求與程度。為有效保護企業內部網路安全，大多數的企業都採用架設防火牆方式來保護來自 Internet 上的不明或惡意的存取行為；但是對於內部網路的攻擊行為（DoS、DDoS...）卻往往是心有餘而力不足，造成企業網路無法承受這樣的大量攻擊事件，進而導致整體網路使用效能降低，最後網路設備紛紛因無法承受大量的攻擊行為而導致網路癱瘓，甚至嚴重影響企業營運上的損失。

- **網路破壞程式對於企業網路往往造成以下情事發生：**

1.由於大部分的網路破壞程式，並不會對使用者造成嚴重的傷害及影響。因此，多數使用者往往身中其毒而不自知，但對於路由器、防火牆…等網路重要設備的執行效能而言，大量的封包傳輸加重了網路設備的負載量，往往使設備的 CPU 使用率高達 99% 甚至出現資安漏洞，使企業網路門戶大開嚴重影響資訊安全。

2.當異常封包開始暴增，網路效能出現異常時，其狀態已經是中毒電腦開始發作並開始已飽和式攻擊某特定目標。若管理人員無法即時處理，將使企業網路效能大為降低，嚴重影響各項電子商務系統的正常運作。

3.當異常流量發生時，管理人員通常無法快速、正確的找出使用者的身分與在哪個地方使用網路，而必須透過大量的人力去對可疑電腦進行逐一掃瞄，找出有問題的電腦。在長時間成本消耗之下，企業往往需付出可觀的損失。

- **雖是市面出現許多宣稱可防禦網路攻擊程式的替代方案，其可歸納成兩大類：**
  - 安裝於用戶電腦的防毒軟體：雖可以有效的偵測並阻絕各種已知病毒，但也僅只針對用戶電腦自身安全作出防禦。對於擁有眾多主機群的中、大型企業體系來說，需要所有的電腦都各安裝一套防毒軟體，無疑又是一筆可觀的開銷。不僅如此，企業一但被最新或變種病毒入侵對區域內網發動攻擊，企業網路總免不了再次癱瘓的命運。
  - 安裝於往閘道器的入侵偵測系統（IDS）：IDS 系統雖可以檢查網路使用者進出該閘道端口時是否有惡意的攻擊行為（如：DOS、DDOS…等），但為達成區域內網的病毒防制需求，企業需於各個網路閘道安裝 IDS 設備。因此，所支付之建置成本將非常龐大。

有鑑於此，由新軟公司所研發的聯合防禦機制，可提供企業杜絕上述問題的發生。透過管理人員的設定，主動察覺企業內部每位使用者的使用流量。當發現有大量不明連線（session）產生時，在第一時間內主動發出警訊給該用戶及網管人員知曉，並立即通知事先指定的交換器(Core Switch)組織聯合防禦連線，阻斷發生問題的使用者電腦對外連線，以最快速的時間確保網路安全，避免內部資安事件擴大。此外，系統內建的異常大流量 IP 功能，可協助管理者更快速的發現和找出問題電腦，而管理人員可以依據異常大流量記錄，針對這些有異常存取行為的電腦進行掃毒與清除的工作，避免網路異常行為持續發生在網路上，提供網路使用者一個更安全、穩定的網路使用環境。

聯合防禦系統與其他防禦方案比較如下：

| | 聯合防禦系統 | 入侵防禦偵測(IDS) | 防毒軟體 |
|---|---|---|---|
| 建置成本 | 低 | 高 | 高 |
| 即時阻斷異常連線 | 可 | 不可 | 不可 |
| 異常 IP/MAC 記錄 | 可 | 可 | 不可 |
| 即時通知管理人員 | 可 | 可 | 不可 |

文 賴鴻文 tony@nusoft.com.tw