新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/2/18-2008/3/2 第61期

多功能 UTM / MS 系列報導

技術淺談與應用 - DMZ的透通路由模式(Transparent Routing)與透通橋接模式(Transparent Bridge)差異為何

新軟 Multi Security UTM 以往在 DMZ 的介面擁有 NAT 及 Transparent 兩種模式，可依照網路架構的需求做選擇。在 NAT 模式下的 DMZ 為一個獨立的虛擬網域，常用於實體 IP 不足的企業網路中，以 Port Mapping 或是 IP Mapping 的方式將連接在 DMZ 中伺服器的虛擬 IP 對映至實體 IP，以供其運作網路服務於 Internet，而 Transparent 模式又稱為透通模式，連接在 DMZ 中的伺服器須以實體 IP 架設，由於使用上較為方便，固常用於實體 IP 足夠的企業網路當中。

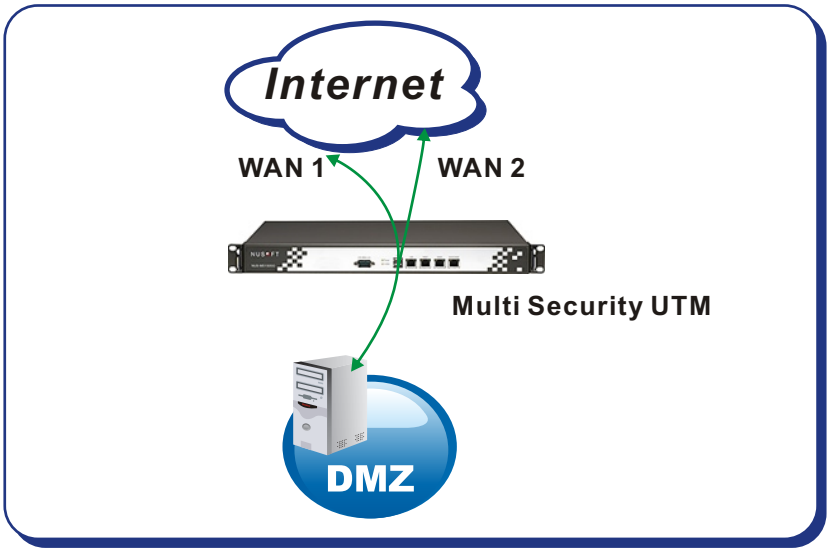
新軟 Multi Security UTM 的韌體開發至今不斷地新增、改善各項功能，其中 NUS-MS1000 以上型號在 V. 4. 01 的版本中，將 DMZ 細分為 NAT、Transparent Routing、Transparent Bridge 三種模式。在此之前我們已清楚了解 NAT 與 Transparent 模式的差異，那麼 Transparent Routing 和 Transparent Bridge 這兩種模式又有何區別呢？

Transparent Routing：

來自 DMZ 的封包經過新軟 Multi Security UTM 時，會根據系統內的路由表決定此封包由哪一個介面傳送。

適用環境：

當使用兩條以上外線，需要運行負載平衡的機制時，可用此模式。系統會將來自 DMZ 的封包依照負載平衡機制分配至各個 WAN Port。

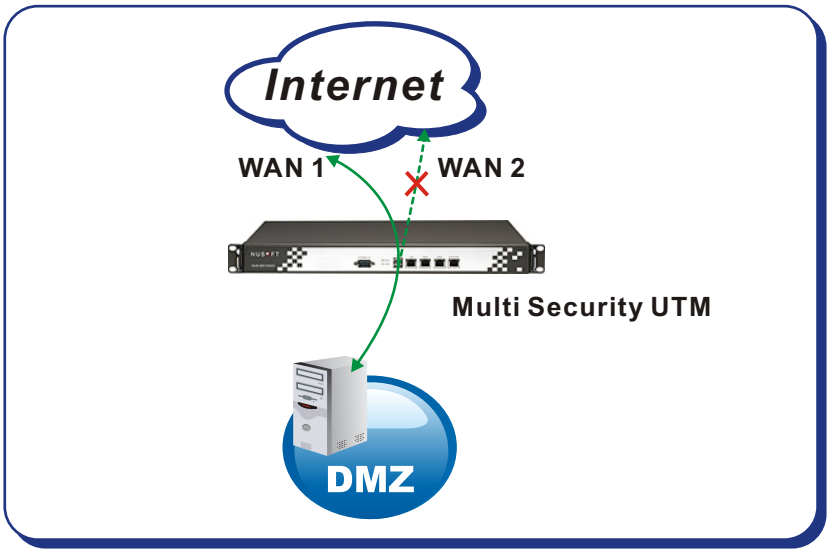


Transparent Bridge:

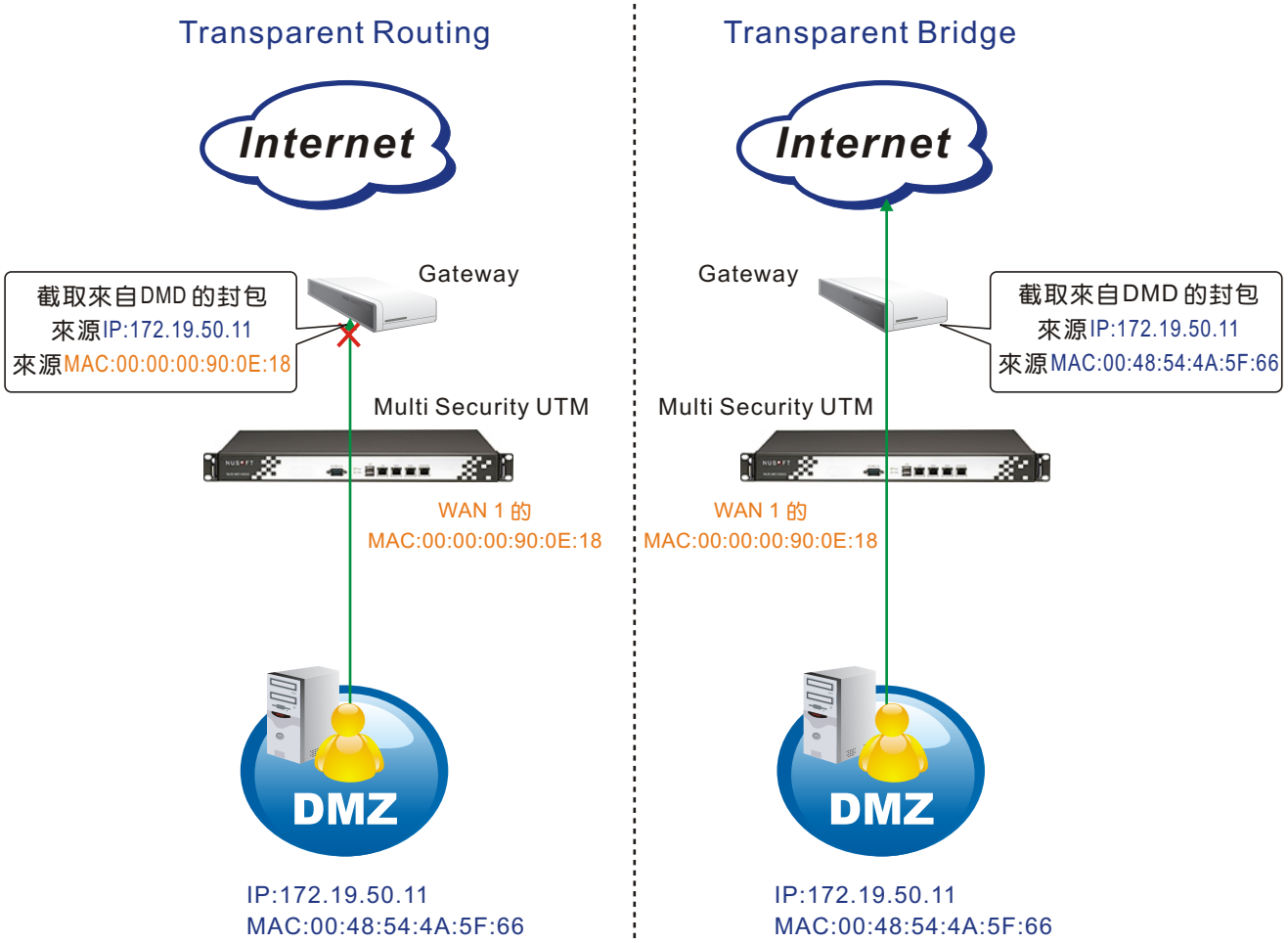
來自 DMZ 的封包並不經由系統內的路由表決定封包的傳送介面，而是根據封包裡目地端的 MAC 來決定由哪一個介面傳送，運作方式如同一般的交換器（Switch）。

適用環境：

當只有一條外線或是只允許 DMZ 的封包固定通過一個 WAN Port，便可使用此模式。系統會將來自 DMZ 的封包全都導向固定的一個 WAN Port，這使得其他的 WAN Port 對 DMZ 來說變得無用武之地。



雖然此模式對 DMZ 無法提供負載平衡，但是在某些網路架構中此模式卻是十分實用。如下圖所示，若在 Multi Security UTM 前端的 Gateway 綁定底下的 PC 及伺服器的 IP 及 MAC，只允許 IP 及 MAC 都符合的封包才能通過，那麼在 Multi Security UTM 底下的 PC 及伺服器就必須以出口端 Gateway 所允許通過的 IP 及 MAC 連至網際網路。然而使用 Transparent Routing 模式，在出口端的 Gateway 將會看到 DMZ 下的每一個 IP 都搭配著 Multi Security UTM WAN1 Port 的 MAC 而無法通過，若選擇 Transparent Bridge 模式則在出口端將會看到所有 DMZ 下的 PC 及伺服器均以自己的 IP 及 MAC 通過 Gateway 連至 Internet。



Transparent Routing & Transparent Bridge 差異表

	Transparent Routing	Transparent Bridge
負載平衡	可	否
最佳適用環境	擁有兩條外線以上	只有使用一條外線
來自 DMZ 封包中的 MAC	WAN1 Port 的 MAC	屬於 PC 及伺服器自己的 MAC

文 黃智傑 alex@nusoft.com.tw

市場行銷報導 - UTM應包含哪些基本功能

隨著網路科技不斷演進、資料傳輸也越來越發達，相對衍生出來的資訊安全問題也隨之增多，為因應此情形，各家網路設備廠商不斷推出解決方案及相關產品（ex：防火牆、防毒牆、入侵偵測防禦、VPN...）來滿足企業需求。但是，隨著企業網路架構日益複雜，所添購的網路設備也愈來愈多，導致企業 IT 人員不僅必須隨時熟悉不同網路設備繁雜的管理介面，同時因不斷添購設備，使得建置資金增加，造成企業預算負擔。

於是，近年出現了相當熱門的『整合式威脅管理（United Threat Management，UTM）』產品。UTM 產品的出現，不僅順利解決企業 IT 人員必須熟悉管理多台不同介面網路設備的問題；同時 UTM 產品將網路管理「簡單化」，透過單一設備及單一管理介面，即可滿足企業多方面的功能需求。

而『UTM』設備應該包含哪些基本功能？根據 IDC 於 2004 年的市場研究報告中所提出的定義，UTM 設備應包含的基本功能如下：

UTM 基本功能	說明
完整『防火牆』功能	在一道完善的防火牆機制下，其不僅能阻擋 99% 的網路外在攻擊，還兼備封包過濾及代理伺服器（proxy）的功能，有些甚至還提供友善的操作設定介面，讓使用者能依個人需求來開放管制相關網路安全功能。
具備『入侵防禦偵測（IDP）』防護機制	當企業受到外來的駭客網路入侵、阻斷服務/分散式阻斷服務（DoS / DDoS）、惡意病毒...等網路攻擊時，IDP 功能會發揮來源攻擊特徵偵防動作，將這些惡意攻擊有效攔截阻擋，並通知網管人員，使其能在關鍵時刻處理危機情形。
提供『VPN』安全連線解決方案	「IPSec VPN」：在總公司與分公司等兩固定地點間建立 VPN 安全連線，彼此存取內部網路檔案。 「PPTP VPN」：外勤工程師在客戶公司 or 家裡使用個人常用的筆記型電腦，透過網路與公司建立 VPN 安全連線，下載內部檔案伺服器的資料。 「SSL VPN」：無論任何地點，只要電腦可以上網，透過瀏覽器即可與公司建立 VPN 安全連線，存取公司內部檔案。
內建『閘道防毒』功能	企業最擔心網路傳輸的資料檔案含有病毒了！深怕其危害企業內部個人主機或重要伺服器資料，對於常用的 HTTP 與 FTP 上傳/下載檔案、即時通訊軟體聊天交流（MSN、Yahoo Message...）、Web Mail 收發信等網路行為更是步步為營！透過 UTM 內建的病毒過濾機制，可有效偵測攔截檔案的病毒，維護企業資訊安全。

隨著時間演進與企業成長，企業對於 UTM 功能的要求也不斷增加，於是各廠商無不卯足全力將更多更強大的功能加入 UTM 產品中，ex：網頁內容過濾、IM/P2P 軟體管制、郵件安全機制（垃圾郵件過濾、病毒郵件過濾）、多 WAN port 頻寬管理（負載平衡、頻寬分流、斷線備援）、QoS、認證服務、容易判讀的 Log. . .。

但，令人惋惜的是，市面上有太多廠商都僅僅是將軟體功能不斷地加入 UTM 產品中，卻從未考慮到硬體的執行相容性及是否能承受負荷，也沒有想過功能是否在硬體上能正常運作的可行性，這樣不僅使 UTM 產品無法發揮所長，嚴重的是造成客戶的不信任。

新軟系統觀察到市場此情形的嚴重性，謹慎評估企業的真實需求，將企業最常用的網路防護功能妥善規劃分配，並經由管制條例（Policy）依功能特性與硬體做適當搭配，充分發揮硬體效能，不再出現資源浪費的情形發生。新軟系統 UTM 產品不再只是號稱多合一功能的資安防護設備，其目的在於將企業網路資源做最適當的分配，同時有效減少網管人員的工作負擔，以「簡單管理」的方式來完成企業所交付的工作責任。

文 黃贊中 isaac@nusoft.com.tw