新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/3/12 - 2007/3/18 第19期

多功能UTM、负载均衡器 / MS、MH系列报导

技术浅谈与应用 - By Destination IP 与 By Source IP 的差异

随着信息安全意识崛起，多数公用服务器已纷纷导入各种安全联机判断机制。最常见的莫过于来源使用者（IP）的单一性判断，举凡网络游戏、证券交易、网络银行等服务器皆广泛使用。而利用“多 WAN 路由设备”上网之使用者会因为设备的“负载平衡功能”有机会同时使用两条以上之 WAN 联机至目标服务器，造成目标服务器判断联机异常而终止提供服务。

上述情况在一般企业里，只要利用“策略路由”的方式，指定特定服务器之联机仅由固定的 WAN 埠传送即可。但是，网吧、学生宿舍、小区网络...这些网络环境则因为网络用途不固定，而导致一一以“策略路由”方式指定联机路径成为不可能的任务。

为让网吧、学生宿舍、小区网络...的使用者能畅通无阻的使用各种网络服务与更多元化及稳定的网络平衡机制，新软公司在 MS 系列（多功能 UTM）与 MH 系列（负载平衡器）这些多 WAN 端口的产品中，增加了 By Source IP（在线游戏模式）与 By Destination IP（依照目的位置分配）两种负载平衡模式来达到各种网络环境的需求。

	By Source IP Mode	By Destination IP Mode
适用对象	网吧、学生宿舍、小区网络...	网吧、学生宿舍、小区网络...
可达到效果	有效避免因服务器的 IP 判断机制，导致服务器服务中断的问题。	有效避免因服务器的 IP 判断机制，导致服务器服务中断的问题。 使用者可充分利用到每一条 WAN 埠的带宽。
可能遇到问题	可能导致网络线路流量分配不均。	若同一在线游戏需要同时联机至两台以上服务器（游戏服务器、游戏认证服务器...），则使用者的联机有可能经由两个以上的 WAN 埠传送，而导致服务器服务中断。

表 — By Destination IP 与 By Source IP 模式差异比较表

● 以网吧采用 NUS-MH1000 并负载平衡设定为 By Source IP（在线游戏模式）模式为例：

在 By Source IP 模式下，使用者的对外联机是根据来源地址（使用者 IP）来决定透过哪一个 WAN 埠连接因特网。所以在图一中，User 1 玩在线游戏时所产生的联机（游戏登入、脚色选择、练功聊天...联机）会皆透过 WAN 1 来传递。倘若 User 1 想再使用其它的网络服务（至游戏官网浏览网页、收取信件），则也仅会透过 WAN 1 来递送。直到 User 1 中断了所有网络联机后，NUS-MH1000 才会开始对其新要求的联机封包重新导向。藉由此一负载平衡模式（By Source IP）将单一使用者的对外联机固定为同一 WAN 埠发送，不但能有效防止无法取得服务的窒碍问题，更能提供使用者稳定的联机服务。

但因为 By Source IP 模式会强迫 User 1 的所有网络联机皆由同一个 WAN 埠传输，所以 User 1 不管是玩在线游戏、浏览网页...甚至是点对点下载档案，都仅能使用单一 WAN 埠之带宽传递，进可能导致整个网吧的线路流量分配不均（一个大流量用户将单一 WAN 端口的带宽耗用殆尽，其它 WAN 埠却流量不高）。因 NUS-MH1000 有自动分配流量至带宽使用率不高的 WAN 埠设计，所以线路流量分配不均之情形在网吧客人人数越多时会渐渐不明显。

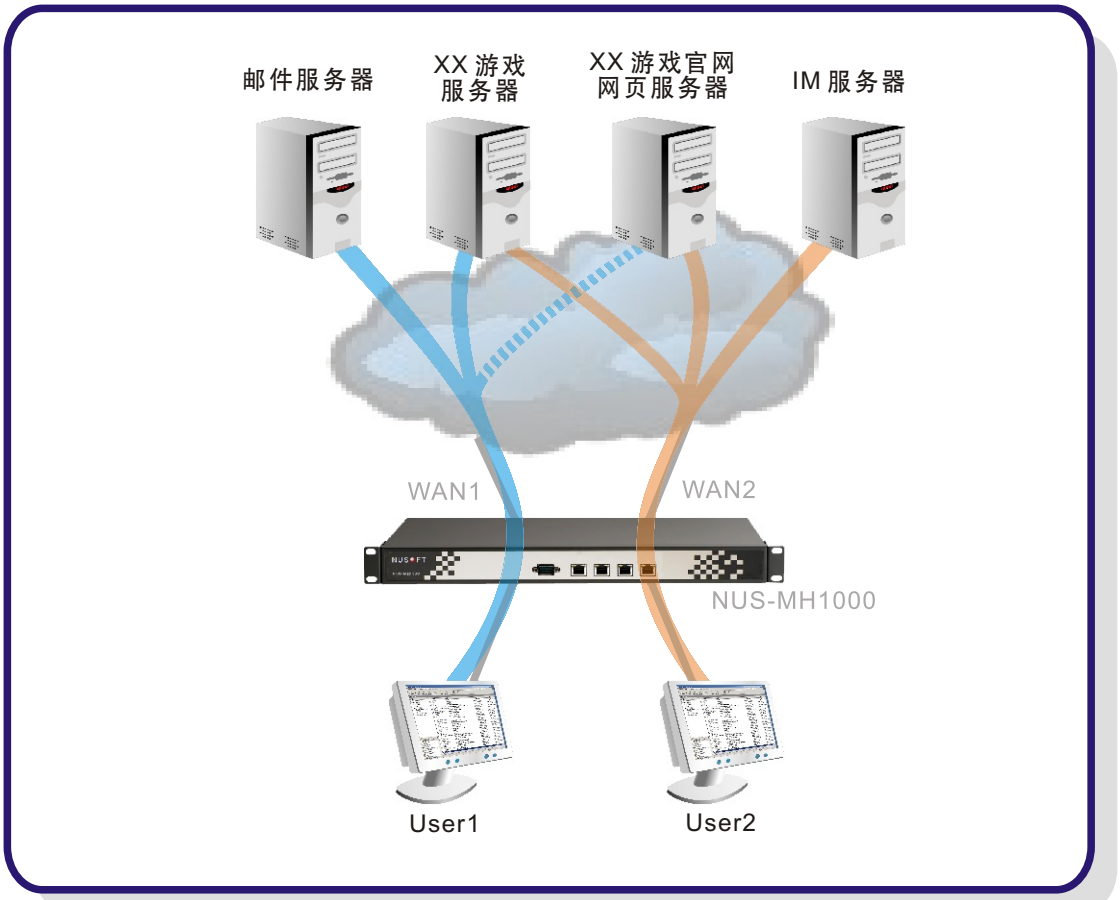

图 — By Source Mode 网络示意图

● 以 NUS-MH1000 设置为 By Destination IP（依照目的位置分配） 模式为例：

在 By Destination IP 模式下，使用者的对外联机是根据目的地址（服务器 IP）来决定透过哪一个 WAN 埠连接因特网。所以在图二中，所有联机至“XX 游戏服务器”的使用者（User 1、User 2）皆会透过 WAN 1 来传递封包（游戏登入、脚色选择、练功聊天...联机）。倘若 User 1 想从“XX 游戏官网”找寻资料时，因 User 2 目前正经由 WAN 2 浏览该网站，所以 NUS-MH1000 也会安排 User 1 透过 WAN 2 联机至此网站。直至所有使用者中断了对“XX 游戏官网”之联机，NUS-MH1000 才会对往后传送至“XX 游戏官网”的服务联机重新导向。藉由此一负载平衡模式（By Destination IP）将传送至同一服务器之联机固定为相同 WAN 埠发送，一样也可以防止因服务器来源 IP 判断的机制，导致联机无法成功的窘境。

与 By Source IP 不同的是，使用者可充分利用到每一条 WAN 埠的带宽，而不会局限于单一 WAN 埠。但有一点要特别注意：如果在线游戏需要同时联机至两台以上的服务器（游戏服务器、游戏认证服务器...）时，使用者的联机有可能经由两个以上的 WAN 埠传送，导致在线游戏联机失败。

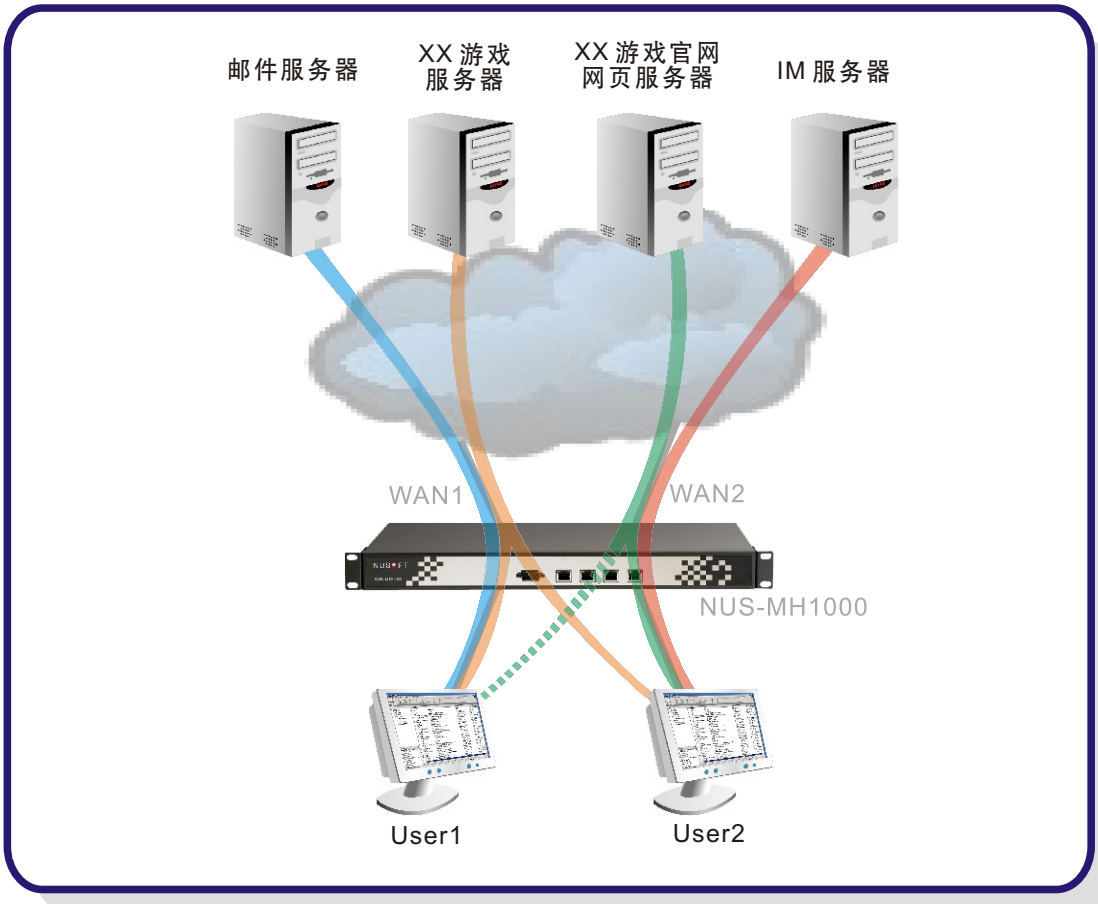

图 二 By Destination IP Mode 网络示意图

文 程智伟 rayearth@nusoft.com.tw

市场营销报导 - 透过 DMZ 与 WAN 切换，扩充企业对外的线路支持

在这因特网蓬勃发展的时代里，带宽联机的质（联机质量）与量（带宽大小）一直是企业网络管理人员所热切关注的话题。而如何在网络质、量与经济利益之间，快速找寻到平衡点，更是企业网络管理人员终生搏斗的使命。新软公司所推之多功能 UTM 及负载平衡器等系列产品中，均采用多 WAN 端口的系统设计，提供企业最佳的解决方案。藉由多条便宜的外线取代单一且昂贵的专线费用，不但成就企业对于网络兼顾质与量的迫切需求，更节省了日后可观的维护成本。

然而，在企业纷纷采用多 WAN 设备之际，却往往仅针对现有的网络架构作规划建置，或因设备价格落差大而被迫选择较少外线之设备，忽视了企业成长之后对于网络外线的扩增需求。因此，当企业增加单一外线时，在以往似乎只能另外购买更多 WAN 端口的网络设备，对于企业组织来说，为增加单一外线而换购设备实在是劳民伤财的不智之举。为此新软公司特别研发出外线扩充功能，利用未使用的接口（DMZ）切换为第三个外部接口（如 图一），提供企业增加单一外线时最适切的解决方案（如 图二）。

图 一 DMZ 與 WAN 端口接口转换设定画面

图 二 透过 DMZ 与 WAN 切换，扩充企业对外的线路支援

反观，一般市售网络设备则无此功能，在面对企业外线扩充需求时仅能选择换购设备方式，与新软公司之外线扩充功能有着明显差异（如表 一）。

	方案一： 使用外线扩充功能扩充外线	方案二： 换购其他多 WAN 设备扩充外线
额外支出成本	无须额外支出成本	高成本支出
系统设定	无须重新设定	需重新编辑所有设定
所需时间	3 分钟（重新开机即可）	一个工作天

表 一 扩增外线方案比较表

文 赖鸿文 tony@nusoft.com.tw