新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/2/5 - 2007/2/11 第15期

负载均衡器 / MH 系列报导

技术浅谈与应用 - 永不断线的商机

随着世界网络潮流，电子商务系统的运用已是企业网络必备之势。而如何提供永不中断的商务服务更是企业当务之急。为此新软公司积极投入各项平衡机制的研发，运用高可靠度的 DNS 技术与 Inbound 平衡技术，使得平衡效能凌驾于国内外其它竞争产品之上。

新软公司所研发之 Inbound 负载平衡机制提供多种模式（包括：Round Robin / Weighted Round Robin / Auto Back Up），来因应企业网络平衡需求。而内建的 DNS 服务器，更支持同时维护多个网域 (domain)，并藉由每个网域多种纪录 (A / CNAME / MX)的设置，来达到 Inbound Load Sharing 的功能，协助电子商务系统能提供更实时、快速与稳定不断线的因特网在线服务。

- 以 NUS-MH1500 设置 BackUp 模式为例：

为避免企业网络断线错失商机，系统管理人员可于 Inbound 负载平衡功能中设置备援功能（如图 一）。当使用者于外部网络浏览网站时，将一律经由 WAN1 进入网页服务器。倘若 WAN1 线路断线时，WNA2 将于第一时间启用接任 WAN1 线路的工作，使企业在线服务永不中断（如图 二）。

图 一 自动备援模式设定画面

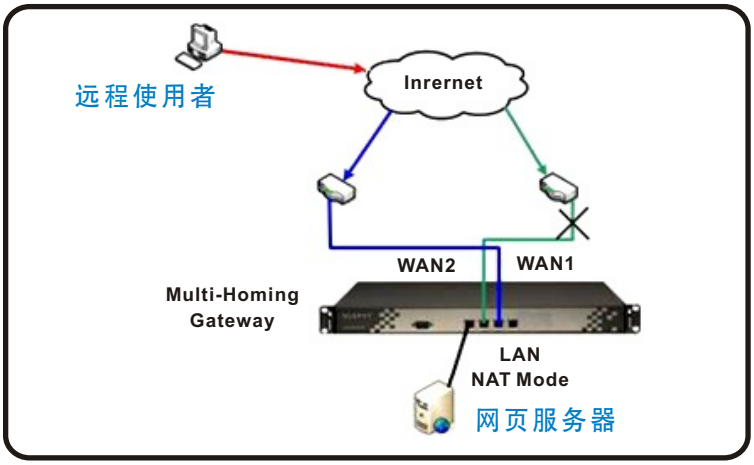

图 二：
Inbound Balance
自动备援模式示意图

以 NUS-MH1500 设置 Weighted Round Robin 模式为例：

系统管理人员可根据需求设计线路负载承受量，假设 WAN1 线路带宽较 WAN2 低，因此设置权重循环分配（Weighted Round Robin）功能，将流量依 1:2 的比例导向至不同的外部接口（如图三）。使外部使用者与内部服务器皆能享用到最充裕的带宽，藉此提高企业电子商务之服务质量（如图四）。

图 三 权重循环模式设定画面

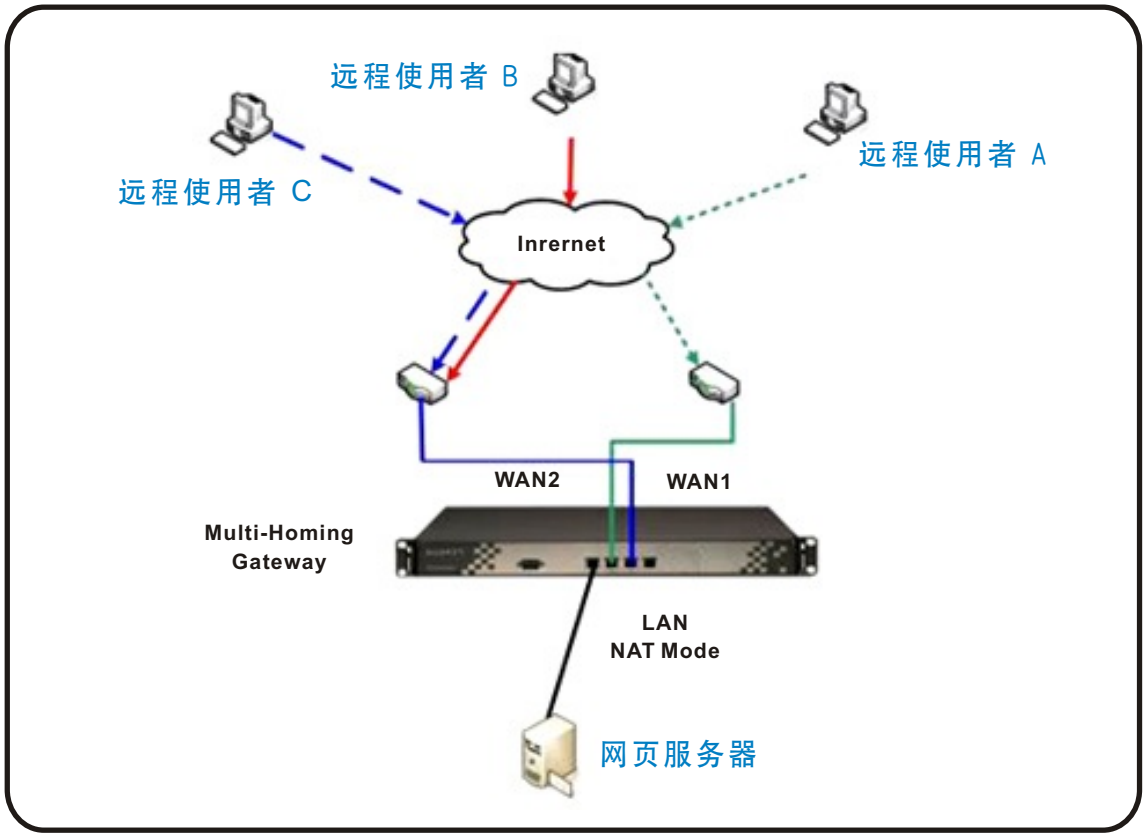

图 四 Inbound Balance 权重循环模式环境示意图

文 赖鸿文 tony@nusoft.com.tw

市场营销报导 - 联合防御(Co-Defense)的重要性

企业作业流程大量 e 化与电子商务的兴起，加重了企业管理阶层对于信息安全的需求与程度。为有效保护企业内部网络安全，大多数的企业都采用架设防火墙方式来保护来自 Internet 上的不明或恶意的存取行为；但是对于内部网络的攻击行为（DoS、DDoS...）却往往是心有余而力不足，造成企业网络无法承受这样的大量攻击事件，进而导致整体网络使用效能降低，最后网络设备纷纷因无法承受大量的攻击行为而导致网络瘫痪，甚至严重影响企业营运上的损失。

- 网络破坏程序对于企业网络往往造成以下情事发生：

1.由于大部分的网络破坏程序，并不会对使用者造成严重的伤害及影响。因此，多数使用者往往身中其毒而不自知，但对于路由器、防火墙…等网络重要设备的执行效能而言，大量的封包传输加重了网络设备的负载量，往往使设备的 CPU 使用率高达 99% 甚至出现信息漏洞，使企业网络门户大开严重影响信息安全。

2.当异常封包开始暴增，网络效能出现异常时，其状态已经是中毒计算机开始发作并开始已饱和式攻击某特定目标。若管理人员无法实时处理，将使企业网络效能大为降低，严重影响各项电子商务系统的正常运作。

3.当异常流量发生时，管理人员通常无法快速、正确的找出使用者的身分与在哪个地方使用网络，而必须透过大量的人力去对可疑计算机进行逐一扫瞄，找出有问题的计算机。在长时间成本消耗之下，企业往往需付出可观的损失。

- 虽是市面出现许多宣称可防御网络攻击程序的替代方案，其可归纳成两大类：
  - 安装于用户计算机的防毒软件：虽可以有效的侦测并阻绝各种已知病毒，但也仅只针对用户计算机自身安全作出防御。对于拥有众多主机群的中、大型企业体系来说，需要所有的计算机都各安装一套防毒软件，无疑又是一笔可观的开销。不仅如此，企业一但被最新或变种病毒入侵对区域内网发动攻击，企业网络总免不了再次瘫痪的命运。
  - 安装于往网关器的入侵侦测系统（IDS）：IDS 系统虽可以检查网络使用者进出该网关端口时是否有恶意的攻击行为（如：DOS、DDOS…等），但为达成区域内网的病毒防制需求，企业需于各个网络网关安装IDS设备。因此，所支付之建置成本将非常庞大。

有鉴于此，由新软公司所研发的联合防御机制，可提供企业杜绝上述问题的发生。透过管理人员的设定，主动察觉企业内部每位使用者的使用流量。当发现有大量不明联机（session）产生时，在第一时间内主动发出警讯给该用户及网管人员知晓，并立即通知事先指定的交换器(Core Switch)组织联合防御联机，阻断发生问题的使用者计算机对外联机，以最快速的时间确保网络安全，避免内部资安事件扩大。此外，系统内建的异常大流量 IP 功能，可协助管理者更快速的发现和找出问题计算机，而管理人员可以依据异常大流量记录，针对这些有异常存取行为的计算机进行扫毒与清除的工作，避免网络异常行为持续发生在网络上，提供网络使用者一个更安全、稳定的网络使用环境。

联合防御系统与其它防御方案比较如下：

	联合防御系统	入侵防御侦测(IDS)	防毒软件
建置成本	低	高	高
实时阻断异常联机	可	不可	不可
异常 IP/MAC 记录	可	可	不可
实时通知管理人员	可	可	不可

文 赖鸿文 tony@nusoft.com.tw