新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/11/19- 2007/11/25 第51期

负载均衡器 / MH 系列报导

技术浅谈与应用 - IP 对映与虚拟服务器有何分别

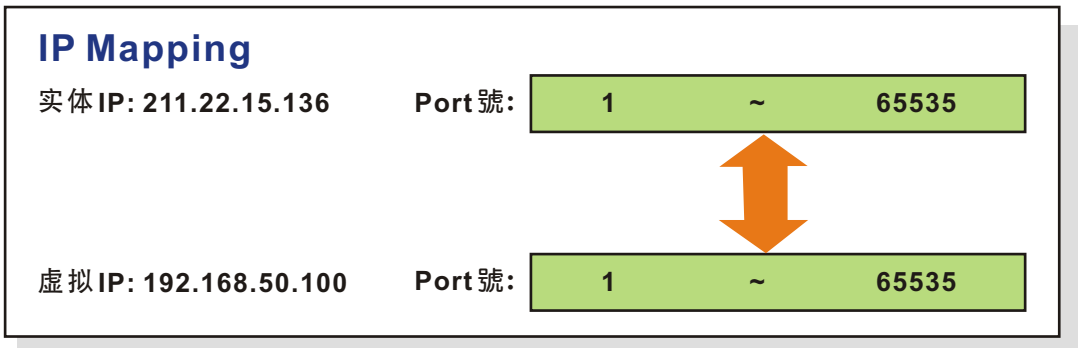
拜申请实体 IP 所费不赀的影响，绝大部分之企业都没有足够的实体 IP 供所有计算机上网使用。在实体 IP 僧多粥少的情况下，NAT（Network Address Translation）技术以虚拟 IP 的方式为企业解决了实体 IP 不够使用之问题。而且使用此方式亦可避免企业内部计算机之 IP 直接暴露在因特网之上被有心人士利用，间接提升企业网络之安全。但是，若企业需要架设网站、FTP Server...等对外服务时，NAT 技术反而会造成客户无法与服务器联机的问题！

要知道在 NAT 底下架设服务器，服务器也必需要使用虚拟 IP 来连接企业网络，所以位于企业网络外部的客户根本无法透过服务器之 IP 与其联机。如要解决这个问题，必须让服务器之虚拟 IP 有个可以对映的实体 IP 才行；让客户可以透过真实 IP 与服务器联机。

因此，新软系统的负载平衡器（MH 系列产品）、多功能 UTM（MS 系列产品）这两款有 NAT 机制的产品，也拥有着可将实体 IP 对映至虚拟 IP 之功能－「IP 对映（IP Mapping）」、「虚拟服务器（Virtual Server）」。这两种功能皆可达到上述之目的，但其本质上又有些许的不同。

IP 对映

「IP 对映」就如字面上所示，其功能就是将外部的实体 IP 直接对映至企业网络内部的虚拟 IP，客户可藉此功能从实体 IP 联机至服务器。因「IP 对映」是将实体 IP 的服务端口“100% 全数对映”至“单一”虚拟 IP，所以比较适用于拥有充足实体 IP 的企业或是只须架设单一服务器的 SoHo 使用。倘若将「IP 对映」使用在仅有单一功能之服务器时，则算一种是比较奢侈的运用方法。毕竟一个实体 IP 所拥有的服务端口有 65535 个，服务器如仅用到一个服务端口不是太浪费了吗？（图一）



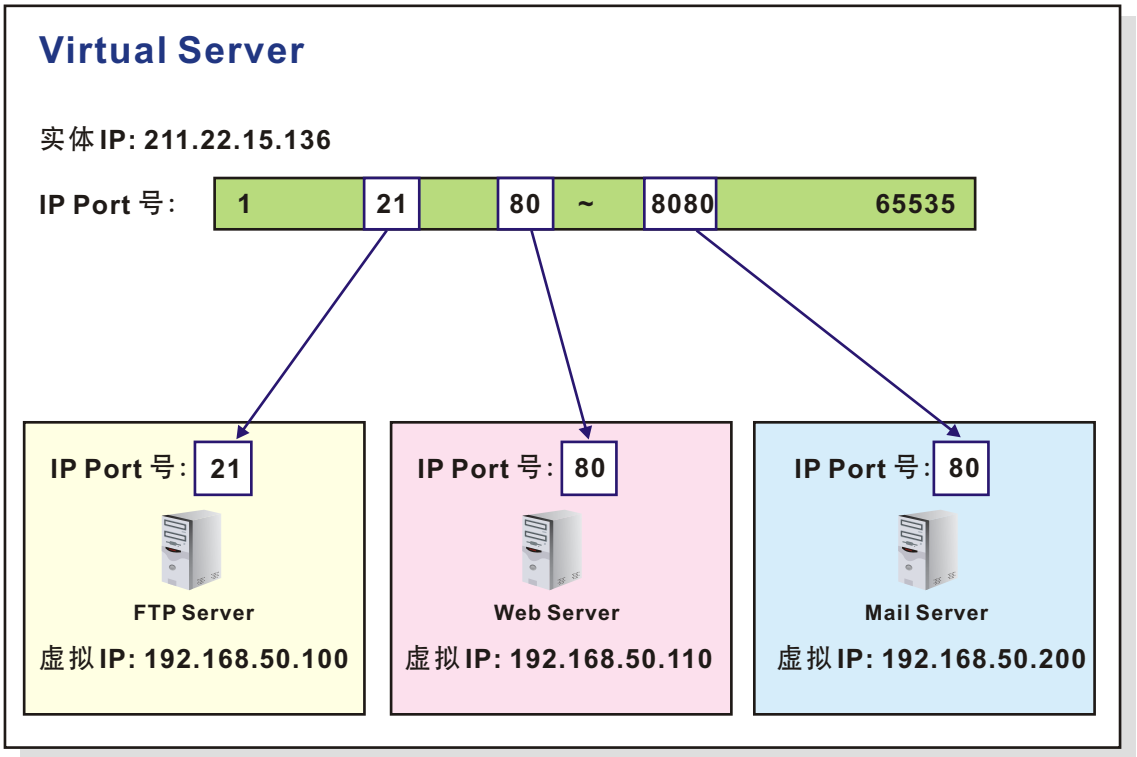
图一 IP 对映会将实体 IP 的服务端口“全数”对映至“单一”虚拟 IP

虚拟服务器

倘若「IP 对映」是实体 IP 与虚拟 IP 之间的对映，则「虚拟服务器」就是属与“端口的对映（Port Mapping）”；它可以将一个实体 IP 的服务端口分配给多个服务器所使用。因此适合用于实体 IP 有限的公司，企业只需用单一实体 IP 就可架设多种服务器（例如：把实体 IP 的 80 port 对映至 Web Server；21 port 对映至 FTP Server ...），可将实体 IP 的利用价值运用的淋漓尽致。

而且，新软系统所提供的「虚拟服务器」亦拥有“服务器负载平衡”机制－每个实体 IP 的服务端口可以循环分配方式对映至四个内容相同的服务器。有效分散各服务器的负载量，以维持这些服务器的运作效能，让客户联机至服务器时能更加顺畅、更加稳定。

另外，假如企业需要架设两个网站（企业网站、Web Mail），却只有一个实体 IP 要怎么办呢？一个实体 IP 只有一个 80 端口啊！「虚拟服务器」提供的“端口号变换”机制－可将实体 IP 的其中一个服务端口对映至虚拟 IP 的另一个服务端口。以上面的例子来说：企业可用实体 IP 的 80 端口对映至企业网站服务器的 80 端口，再将实体 IP 8080 端口对映至 Web Mail 服务器的 80 端口。如此一来，客户只要从实体 IP 的 80 端口就可进入企业网站；而员工只要从实体 IP 的 8080 端口及可进入 Web Mail 中。（图二）



图二 虚拟服务器将实体 IP 的服务端口分给多个服务器所使用

从上面的文章看起来「虚拟服务器」好像比「IP 对映」好用的多啊？那为甚么新软系统还要两种功能都提供呢？这是因为「虚拟服务器」的功能虽然强大，不过却有使用数量的限制（新软系统产品提供四组「虚拟服务器」），而且设定上也比「IP 对映」繁琐。所以当内建的四组「虚拟服务器」不敷使用时企业即可应用「IP 对映」，而对于拥有足够实体 IP 架设服务器的企业，也较偏好使用「IP 对映」这种设定较为简便的功能。

	IP 对映	虚拟服务器
设定流程	简便	需设定项目较多
可对应实体 IP 数量	64 组	4 组
一个 IP 可对映的服务器数	一个	多个
服务器负载平衡机制	无	有
是否支持端口号变换	否	是
适用时机	当四组虚拟服务器不敷使用时	当所需架设的服务器多於实体 IP 时
适用对象	拥有足够实体 IP 架设服务器的企业	实体 IP 不足的企业

表一 IP 对映与虚拟服务器之差别（以 NUS-MH2400G 为例）

文 黄智杰 alex@nusoft.com.tw

市场营销报导 - 新软系统推出「One-Step IPSec」机制，让您 IPSec VPN 一个步骤就建置完成

在以往，企业如需与其分公司、海外驻点... 透过网络传递重要信息时，为了安全起见，会架设专线做为沟通管道。唯专线之价格不斐，并非一般企业可负担的起，因此大部分之企业会采用 VPN（Virtual Private Network）的方式来取代专线。

在各种 VPN 联机当中，IPSec VPN 因适用在“地点固定的公司间传输”，所以企业常用在总公司与分公司的重要信息传递上。但 IPSec VPN 在架设上素来复杂，且在近年来新软系统为了提升其产品内建的 IPSec VPN 之传输安全性、管控灵活度...特别加入了「VPN Trunk」机制，将 IPSec VPN 列入「管制条例」控管。但也却使得其设定上更加复杂，让部分不常接触 IPSec VPN 的管理人员不知该如何设定。难道，鱼（安全、灵活管控...）与熊掌（设定简单）不可兼得吗？

为了让管理人员能够轻松使用架设 IPSec VPN 之环境，新软系统特别在其负载平衡器（MH 系列产品）、多功能 UTM（MS 系列产品）加入了「One-Step IPSec（IPSec 一步设定）」功能，来协助管理人员架设 IPSec VPN。什么是「One-Step IPSec」呢？简单的来讲，「One-Step IPSec」将大部分在 IPSec VPN 架设时所要设定之数据以默认值替代，管理人员仅需要填入少数几个必需自订的设定值，其它像是「VPN Trunk」、「管制条例」...的设定则由系统代劳完成；管理人员只要一个步骤，即可完成 IPSec VPN 之建置工作，大幅降低其困难度。

	以往 IPSec VPN 所需设定步骤	One-Step IPSec VPN 所需设定步骤
1	IPSec 自动加密设定 名称、外部网络接口、到目的位置、认证方法、加密金钥、加密或认证方式、进阶加密、ISAKMP 更新周期、加密金钥更新周期、GRE / IPSec...	One-Step IPSec 设定 名称、来源位置、目的地址、加密金钥
2	VPN Trunk 设定 名称、来源地址、目的地址、信道、保持联机 IP...	系统自动完成 VPN Trunk 相关设定
3	管制条例设定 建立由内至外管制条例 建立由外至内管制条例	系统自动完成管制条例相关设定

表一 以往 IPSec 与 One-Step IPSec 设定上之差别

文 程智伟 rayearth@nusoft.com.tw