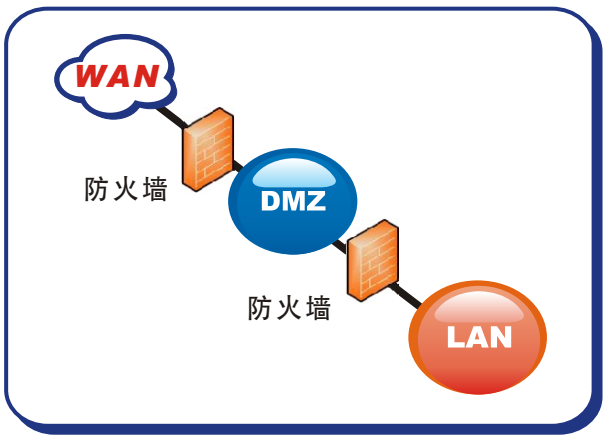
新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/9/3-2007/9/9 第41期

## 负载均衡器 / MH 系列报导

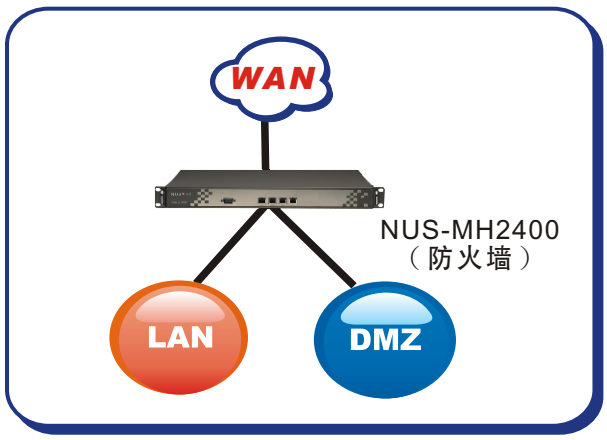
### 技术浅谈与应用 - 什麽是DMZ？使用DMZ有何好处？

当您在架设新软系统产品－多功能UTM、负载平衡器时，是否在其外观上发现其网络接口中除了拥有衔接内部网络的 LAN 端口、连接至因特网的 WAN 端口外，还有一个使用者较不常接触过的 DMZ 端口。甚么是 DMZ 端口呢？

DMZ 为英文 De-Militarized Zone 的缩写，一般称之为“非军事区”，本来是指军事上禁止战斗的区域，而在网络方面在过去是指内部网络和外部网络之间的一小段网络（如图一），常被用来架设服务器之用。此种 DMZ 的架设方式可使服务器的网络传输可受防火墙的监控，或受其它安全机制检测，安全性高。但因为企业需要采购两台防火墙，使得在架构与管理企业网络之成本大幅增加，令一般企业难以接受，所以绝大多数的企业已改采用另一种 DMZ 架构方式来建构企业网络（如图二，新软多功能UTM 与负载平衡器皆是这种 DMZ 架构）。此种方式仅需要架设一台防火墙即可保护内部网络与 DMZ 区，兼具安全性与成本效益，故广受企业喜爱。




图一 传统 DMZ




图二 新式 DMZ

| | 安全性 | 成本 | 难度 | 便利性 |
|---|---|---|---|---|
| 传统 DMZ | 高 | 高 | 高 | 低 |
| 新式 DMZ | 高 | 低 | 低 | 高 |

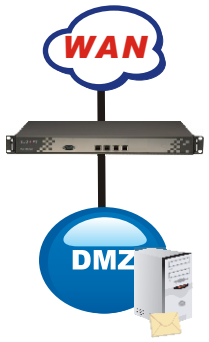
表一 两种 DMZ 架构比较

为何服务器放置于 DMZ 中会较为安全呢？放在内部网络不好吗？一样也可以受到防火墙的保护啊？实际上，服务器所受到的网络威胁不一定来自于外部网络，亦有可能来自于内部网络－内部网络的计算机中毒是很有可能会拖累架设在内部网络之服务器。将服务器架设于 DMZ 时，任何通往 DMZ 的联机皆需要受到管制条例之控管，甚至是受到 IDP 与病毒侦测的保护（多功能 UTM），大大提升了企业网络的安全性。

## 新软系统所提供的 DMZ

新软系统所推出的多功能UTM（MS 系列）、负载平衡器（MH 系列）产品，拥有实体的 DMZ 端口（可以物理方式区隔内部网络与 DMZ）。并且支持两种 DMZ 模式—NAT 模式 & Transparent 模式供企业选择。

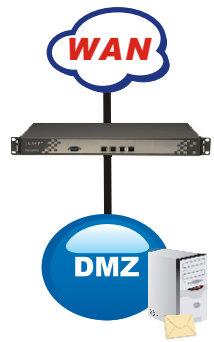
图三 DMZ 采用 NAT 模式




### 1.NAT 模式

在此模式中 DMZ 为一独立虚拟网域，其下服务器采用虚拟 IP 架设，常用于真实 IP 不敷使用的企业。倘若欲开放服务器供外部使用者联机时，需设定 IP 对应或虚拟服务器，将外部寻求服务的联机透过实体 IP 导到内部服务器的虚拟 IP。

图四 DMZ 采用 Transparent 模式




### 2.Transparent 模式

又称为透通模式，其下服务器采用实体 IP 架设。因使用上较为方便，所以企业真实 IP 假如足够，多使用此模式建构网络。倘若欲开放服务器供外部使用者联机时，仅需要开放管制条例。

## 常见於市面上的“伪”DMZ

除了上述 DMZ 之外，市面上还有些产品因硬件设计关系（无实体 DMZ 端口），导致无法实际提供 DMZ 功能，因此将可新增网段的 Multiple-Subnet 功能宣称为“软件 DMZ”。“软件 DMZ”并无法以物理方式区隔 DMZ 与内部网络，因此并无法确实保护架设于 DMZ 区域的服务器。

另外，部分 IP 分享器也宣称拥有 DMZ，但其与真正的 DMZ 功能天差地远－设定于这种“DMZ”下的计算机将失去任何保护，面临种种的安全风险。

文 周政达 zhengda@nusoft.com.tw

## 市场行销报导 - 任意IP路由-解决开放式网络环境的有效方案

在网络运用日益普及的趋势下，日常生活中所需之信息来源，也渐渐被此管道取代。然而，一但离开了所熟悉的环境，您是否会为了要使用网络而遇到许多窘境？

由于行动设备（例如：笔记型计算机）的广泛使用，所以无论在咖啡厅、餐厅、饭店、机场、休闲广场…中，皆开始提供有线或无线的上网环境。但在一个陌生的网络环境中，常常需要依循一堆繁杂的程序、设定后方能使用。而绝大部分的使用者只懂得如何浏览网页，如何收发信件，对于网络联机相关设定则是一窍不通，到最后还需要求助于相关服务单位来解决其问题。

在外洽公、旅游、…的网络使用者，基于上述的原因，在急于取得、传递所需的讯息时，只能耐着性子找出连通网络的方法，这种迫于无奈造成的时间延误，常常影响着这些使用者的利益。最明显的例子就是，一份急需审核的授权文件迟迟无法传输、欲获得信息随时调整行程…，无不因为这些因素导致许多无法弥补的后果。

有鉴于此，任意IP路由技术，就成为解决诸多问题的关键。不论使用者笔记型计算机的网络设定为何（IP是否隶属于既定的内部网段、预设网关是否设定为既定的IP），只要能在支持此技术的网络环境中获得存取点，就可立即上网。以往在异地使用网络的不便和困扰从此成为历史。（如下表）

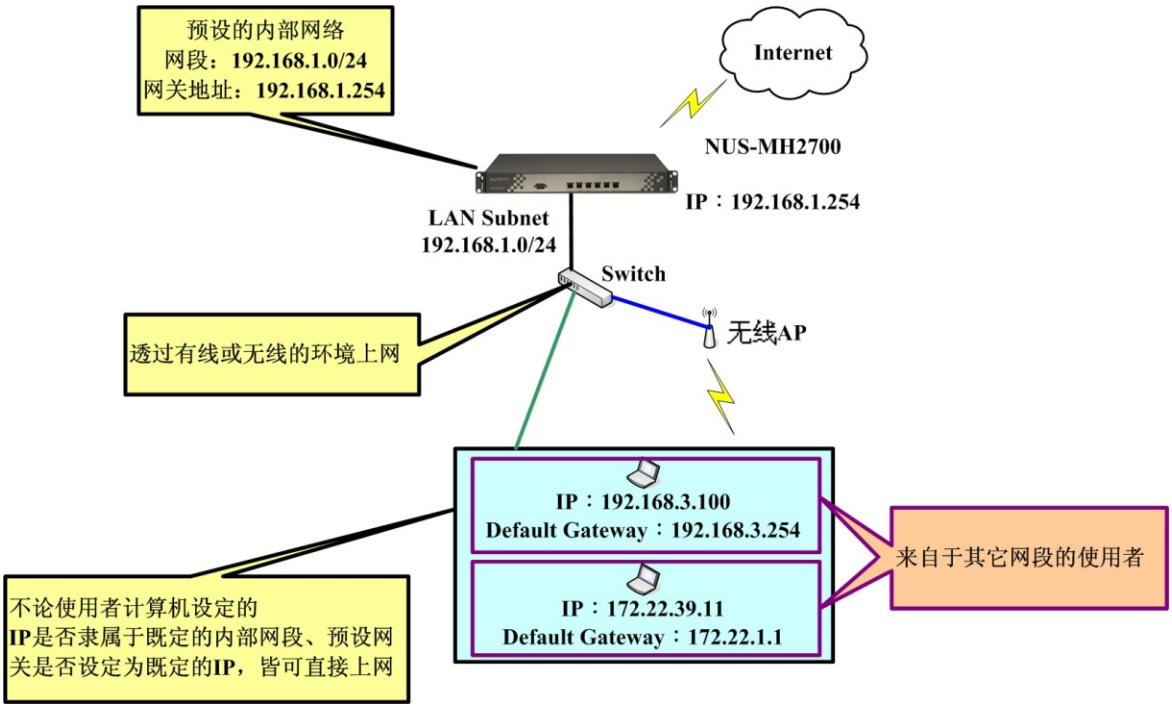
| | 任意IP路由器 | 传统路由器 |
|---|---|---|
| 使用环境 | 开放式环境（例如：咖啡厅、餐厅、酒店、机场、休闲广场…） | |
| 使用对象 | 持有行动设备（例如：笔记型计算机）在外洽公、旅游…的人 | |
| 使用方式 | 获得联机讯号直接上网 | 须依照指示说明，更改需多设备上的网络设定 |
| 便利性 | 可实时传递讯息 | 需耗费一定时间完成前置作业 |

任意IP路由和传统网络在开放式环境中的差异

以饭店为例－

在传统网络环境的情况下，房客如需上网，必须将其行动设备的IP地址、子网掩码、预设网关地址...依饭店网络的需求设定。倘若房客对于网络联机方式不甚了解，则需花费大量时间尝试联机，或是寻求饭店方面的协助。

而在任意IP路由的环境下，不管房客先前使用网络的联机设定为何，只要其行动设备可接上存取点（有线or无线网络）就可立即上网，不需要再变更行动设备的网络相关设定。（如下图）




文 陈昱升 josh@nusoft.com.tw