新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/2/18-2008/3/2 第61期

多功能UTM / MS系列报导

技术浅谈与应用 - DMZ的透通路由模式(Transparent Routing)与透通桥接模式(Transparent Bridge)差异为何

新软Multi Security UTM以往在DMZ的接口拥有NAT及Transparent两种模式，可依照网络架构的需求做选择。在NAT模式下的DMZ为一个独立的虚拟网域，常用于实体IP不足的企业网络中，以Port Mapping或是IP Mapping的方式将连接在DMZ中服务器的虚拟IP对映至实体IP，以供其运作网络服务于Internet，而Transparent模式又称为透通模式，连接在DMZ中的服务器须以实体IP架设，由于使用上较为方便，固常用于实体IP足够的企业网络当中。

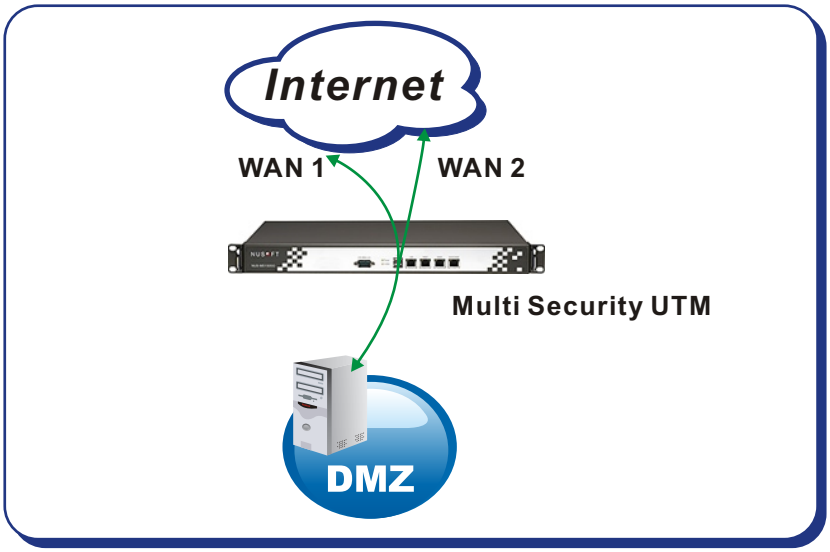
新软Multi Security UTM的韧体开发至今不断地新增、改善各项功能，其中NUS-MS1000以上型号在V.4.01的版本中，将DMZ细分为NAT、Transparent Routing、Transparent Bridge三种模式。在此之前我们已清楚了解NAT与Transparent模式的差异，那么Transparent Routing和Transparent Bridge这两种模式又有何区别呢？

Transparent Routing：

来自DMZ的封包经过新软Multi Security UTM时，会根据系统内的路由表决定此封包由哪一个界面传送。

适用环境：

当使用两条以上外线，需要运行负载平衡的机制时，可用此模式。系统会将来自DMZ的封包依照负载平衡机制分配至各个WAN Port。

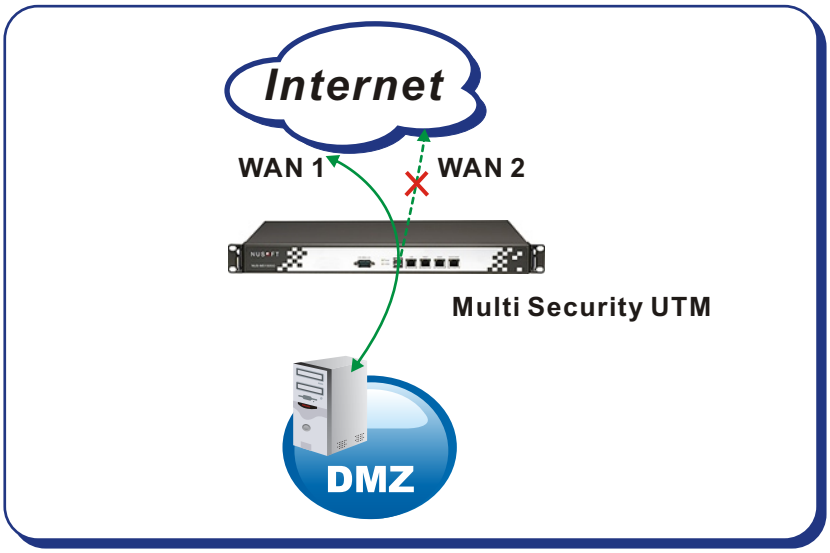


Transparent Bridge:

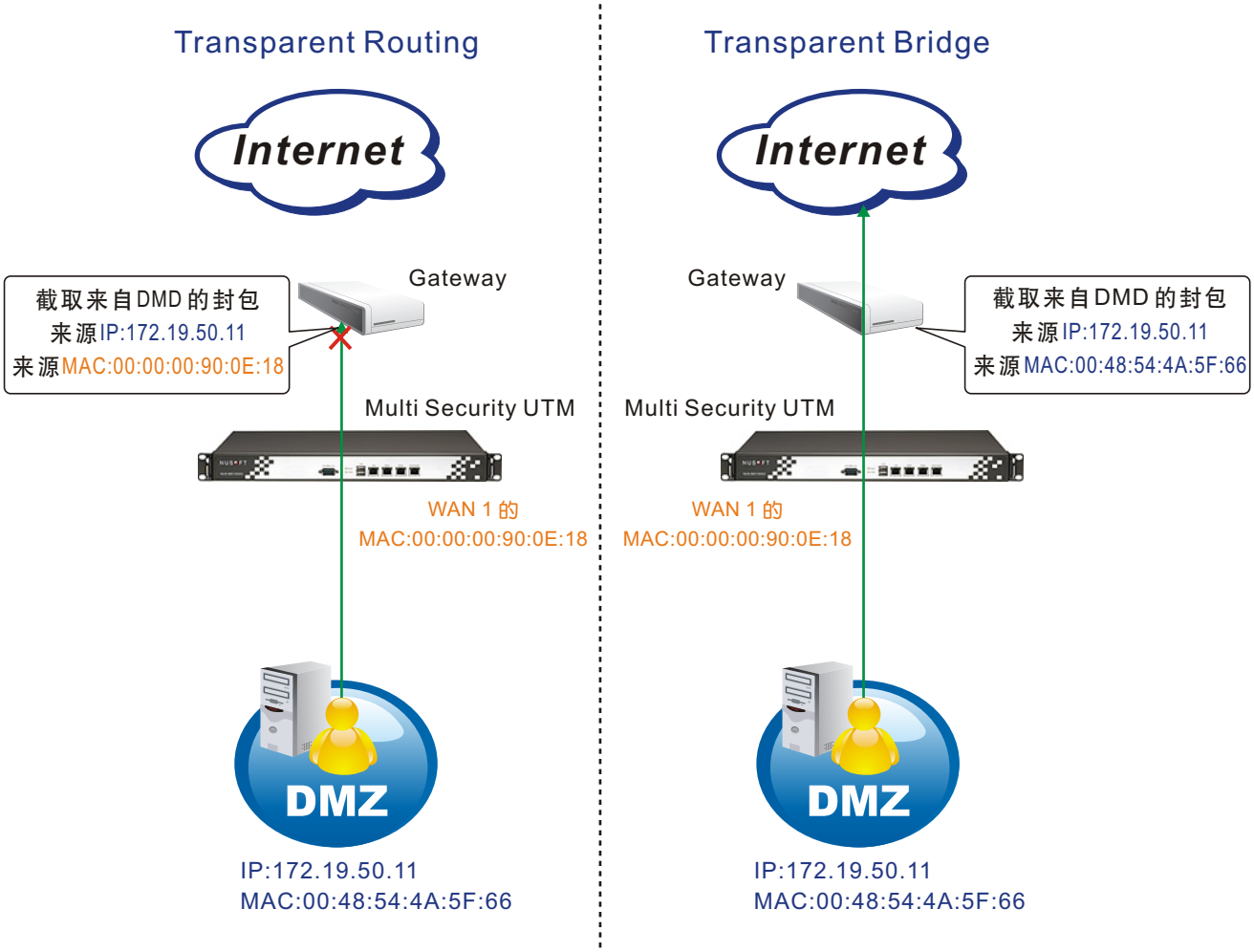
来自 DMZ 的封包并不经由系统内的路由表决定封包的传送界面，而是根据封包里目地端的 MAC 来决定由哪一个接口传送，运作方式如同一般的交换器（Switch）。

適用環境：

当只有一条外线或是只允许 DMZ 的封包固定通过一个 WAN Port，便可使用此模式。系统会将来自 DMZ 的封包全都导向固定的一个 WAN Port，这使得其它的 WAN Port 对 DMZ 来说变得无用武之地。



虽然此模式对 DMZ 无法提供负载平衡，但是在某些网络架构中此模式却是十分实用。如下图所示，若在 Multi Security UTM 前端的 Gateway 绑定底下的 PC 及服务器的 IP 及 MAC，只允许 IP 及 MAC 都符合的封包才能通过，那么在 Multi Security UTM 底下的 PC 及服务器就必须以出口端 Gateway 所允许通过的 IP 及 MAC 连至因特网。然而使用 Transparent Routing 模式，在出口端的 Gateway 将会看到 DMZ 下的每一个 IP 都搭配着 Multi Security UTM WAN1 Port 的 MAC 而无法通过，若选择 Transparent Bridge 模式则在出口端将会看到所有 DMZ 下的 PC 及服务器均以自己的 IP 及 MAC 通过 Gateway 连至 Internet。



Transparent Routing & Transparent Bridge 差异表

	Transparent Routing	Transparent Bridge
负载平衡	可	否
最佳适用环境	拥有两条外线以上	只有使用一条外线
来自 DMZ 封包中的 MAC	WAN1 Port 的 MAC	属于 PC 及服务器自己的 MAC

文 黄智杰 alex@nusoft.com.tw

市场行销报导 - UTM 应包含哪些基本功能

随着网络科技不断演进、数据传输也越来越发达，相对衍生出来的信息安全问题也随之增多，为因应此情形，各家网络设备厂商不断推出解决方案及相关产品（ex：防火墙、防毒墙、入侵侦测防御、VPN...）来满足企业需求。但是，随着企业网络架构日益复杂，所添购的网络设备也愈来愈多，导致企业 IT 人员不仅必须随时熟悉不同网络设备繁杂的管理接口，同时因不断添购设备，使得建置资金增加，造成企业预算负担。

于是，近年出现了相当热门的『整合式威胁管理（United Threat Management，UTM）』产品。UTM 产品的出现，不仅顺利解决企业 IT 人员必须熟悉管理多台不同接口网络设备的问题；同时 UTM 产品将网络管理「简单化」，透过单一设备及单一管理接口，即可满足企业多方面的功能需求。

而『UTM』设备应该包含哪些基本功能？根据 IDC 于 2004 年的市场研究报告中所提出的定义，UTM 设备应包含的基本功能如下：

UTM 基本功能	說明
完整『防火墙』功能	在一道完善的防火墙机制下，其不仅能阻挡 99% 的网络外在攻击，还兼备封包过滤及代理服务器（proxy）的功能，有些甚至还提供友善的操作设定介面，让使用者能依个人需求来开放管制相关网络安全功能。
具备『入侵防御侦测（IDP）』防护机制	当企业受到外来的黑客网络入侵、阻断服务/分散式阻断服务（DoS / DDoS）、恶意病毒...等网络攻击时，IDP 功能会发挥来源攻击特徵侦防动作，将这些恶意攻击有效拦截阻挡，并通知网管人员，使其能在关键时刻处理危机情形。
提供『VPN』安全联机解决方案	「IPSec VPN」：在总公司与分公司等两固定地点间建立 VPN 安全机，彼此存取内部网络文件。 「PPTP VPN」：外勤工程师在客户公司 or 家里使用个人常用的笔记型计算机，透过网络与公司建立 VPN 安全联机，下载内部文件服务器数据。 「SSL VPN」：无论任何地点，只要计算机可以上网，透过浏览器即可与公司建立 VPN 安全联机，存取公司内部文件。
内建『网关防毒』功能	企业最担心网络传输的数据文件含有病毒了！深怕其危害企业内部个人主机或重要服务器数据，对於常用的 HTTP 与 FTP 上传/下载文件、实时通讯软件聊天交流（MSN、Yahoo Message...）、Web Mail 收发信等网络行为更是步步为营！透过 UTM 内建的病毒过滤机制，可有效侦测拦截文件的病毒，维护企业资讯安全。

随着时间演进与企业成长，企业对于UTM功能的要求也不断增加，于是各厂商无不卯足全力将更多更强大的功能加入UTM产品中，ex：网页内容过滤、IM/P2P软件管制、邮件安全机制（垃圾邮件过滤、病毒邮件过滤）、多WAN port带宽管理（负载平衡、带宽分流、断线备援）、QoS、认证服务、容易判读的Log...。

但，令人惋惜的是，市面上有太多厂商都仅仅是将软件功能不断地加入UTM产品中，却从未考虑到硬件的执行兼容性及是否能承受负荷，也没有想过功能是否在硬件上能正常运作的可行性，这样不仅使UTM产品无法发挥所长，严重的是造成客户的不信任。

新软系统观察到市场此情形的严重性，谨慎评估企业的真实需求，将企业最常用的网络防护功能妥善规划分配，并经由管制条例（Policy）依功能特性与硬件做适当搭配，充分发挥硬件效能，不再出现资源浪费的情形发生。新软系统UTM产品不再只是号称多合一功能的资安防护设备，其目的在于将企业网络资源做最适当的分配，同时有效减少网管人员的工作负担，以「简单管理」的方式来完成企业所交付的工作责任。

文 黄赞中 isaac@nusoft.com.tw