新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2006/11/13 - 2006/11/19 第3期

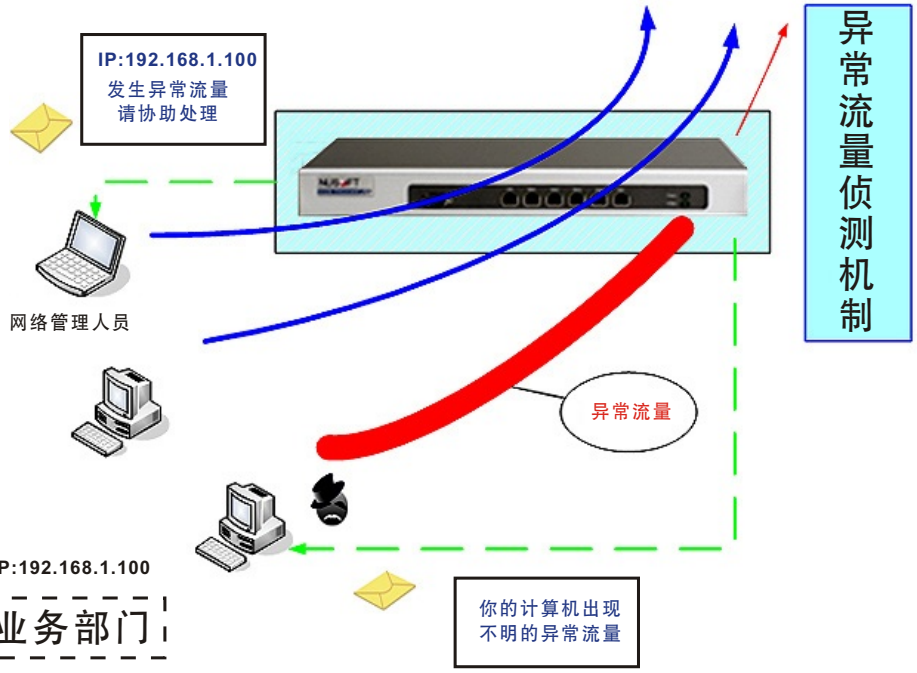
多功能UTM、负载均衡器 / MS、MH系列报导

技术浅谈与应用 - 异常流量IP

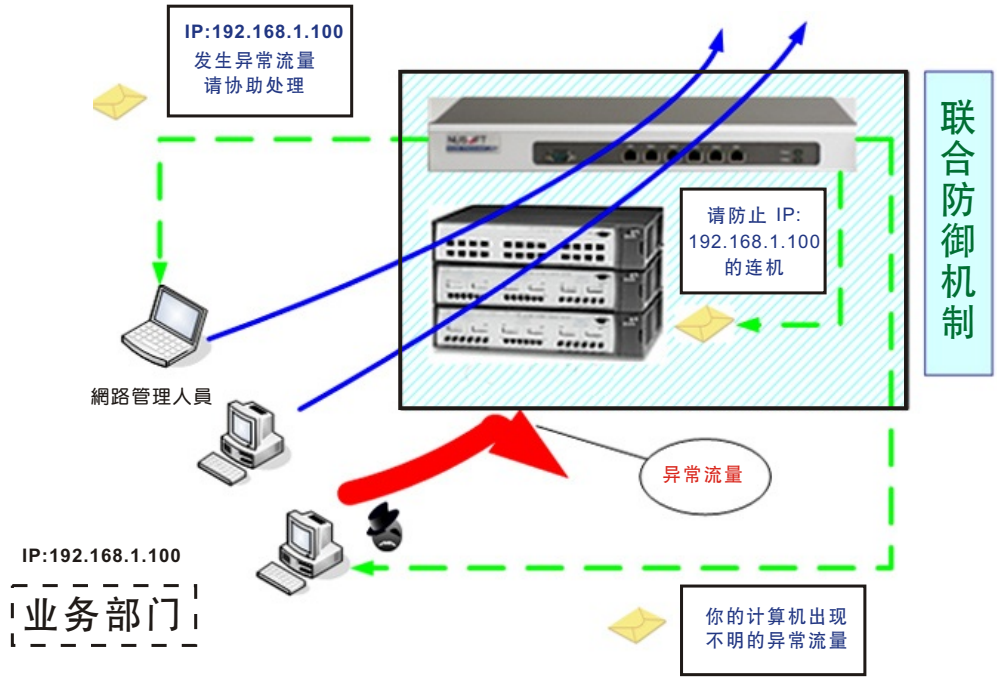
◎内部异常流量侦测与建置联合防御网络机制

新软公司另一独创巨作 — 『内部异常流量侦测与联合防御机制』，拒绝网络瘫痪与杜绝病毒扩散的唯一选择。

长期以来，企业的安全防护措施，大致都有着「防外有余、防内不足」的弊病，解决方案不外乎是防火墙、UTM、网关防毒、IDS 等网关防护，虽然在防范来自外部的各类威胁攻击时，皆有相当程度的防御能力，但面对企业内部网络的恶意攻击，因而产生的大流量或高联机数时却往往无法有效杜绝，造成企业网络频宽阻塞。而在恶意程序扩散蔓延方面，以往的管理人员总是在众多计算机中，花上好几天的时间一台一台找一台一台扫，增加了寻找中毒计算机的时间，因而导致整个网络瘫痪影响企业信息安全。



于是，新软公司为强化实时异常流量侦测，以提升区域内网的安全性。推出的各项产品中皆拥有独创的【异常流量 IP】侦测机制，如上图所示，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，不仅可针对较高流量之主机或主机群设定【不侦测 IP】来符合网络需求，更可以针对各企业网络环境需求制订异常流量临界值，来达到中毒计算机对外联机有效管制及零误判的企业需求。



此外，一般的侦测机制着重于侦测并未能达成实时阻断的效果。新软公司研发团队凭借多年对市场需求的研究与了解，不仅在各产品均拥有优异的零误判异常流量侦测机制，更开发出一般市售产品所欠缺的联合防御机制。如上图范例所示，当业务部门IP：192.168.1.100的计算机中毒时，导致区域内网中产生大量且不明的对外联机，系列产品将于第一时间内主动侦测出异常流量（中毒计算机）并将相关信息记录于设备中，且立即通知事先指定的交换器（Core Switch），共同组成联合防御联机，实时阻断发生问题的使用者，以最快速的时间达到实时阻绝的效果确保网络安全。在发生异常流量的同时，系列产品均能在第一时间内根据管理人员所设定的警讯通知形式发出警讯（如：E-Mail、SNMP Trap、NetBIOS），通知该使用者及管理人员协助处理，使资安事件的发生达到实时且有效的控管，以避免异常流量对于企业网络造成危害。

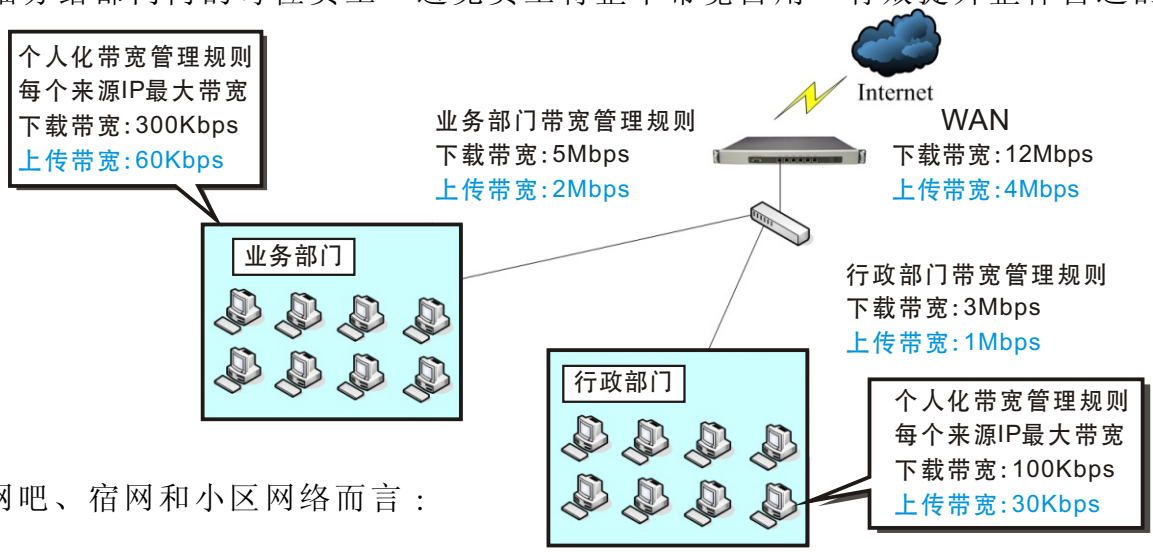
文 赖鸿文 tony@nusoft.com.tw

市场营销报导 - 如何有效管理有限的带宽？

A.以公司单位来说：

一般企业都设有许多部门，掌管着整体的运作，在企业 e 化后，业务的往来几乎由网络来传递。但往往会发生带宽不敷使用的问题，导致讯息传递窒碍和使用者怨声载道。最后，都只能以提升对外带宽这种治标不治本的做法，来暂时性解决问题。原因就出在带宽的分配上过于笼统，又无法有效阻绝带宽的滥用。

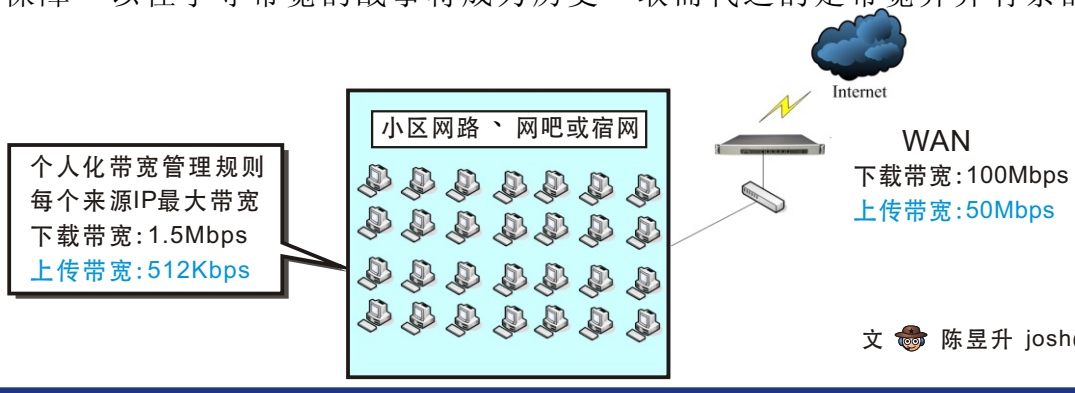
有鉴于此，新软系统将带宽管理扩及到各个层面，利用原有的 QoS 功能，让企业可以依照各部门的特性，规画带宽使用的原则，使彼此间在对外传递数据时，不会相互影响和冲突。同时，独创的个人化带宽管理(Personal QoS)，可将 QoS 所保留的带宽，再细分给部门内的每位员工，避免员工将整个带宽占用。有效提升整体营运的效率。



B.针对网吧、宿网和小区网络而言：

在一个共享网络的的环境中，常常上演网络资源的攻防战，只要有人打破正常使用原则，往往搞的人仰马翻。不仅是网管人员焦头烂额，使用者也会弥漫在一股攻讦的气氛当中。在顾客至上的原则下，既无法完全阻绝用户的异常需求，又要承担来自于各方的压力。

基于公平原则，新软系统针对个人使用网络的特性，独具匠心的个人化带宽管理(Personal QoS)设计，不再只是异常行为的侦测与防堵。而是，制定可供各种正常需求运作的通则，不再需要针对每个用户设定 QoS，让每位使用者在网络带宽的使用上都有保障。以往争夺带宽的战事将成为历史，取而代之的是带宽井井有条的应用。



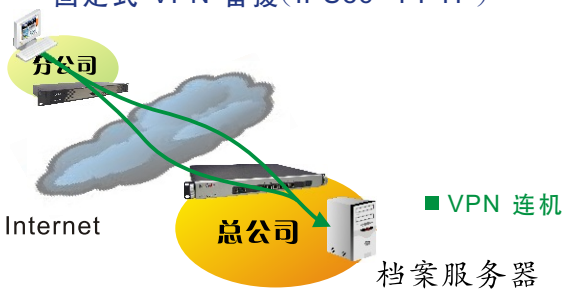
文 陈昱升 josh@nusoft.com.tw

市场营销报导 - 如何从远端存取企业内档案？

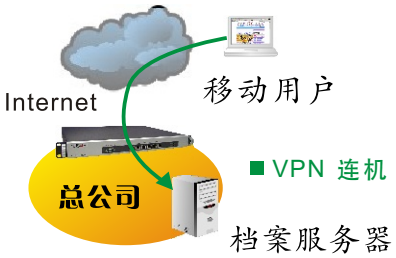
一般企业需要从远程来存取档案时，都会以安全性为第一考虑。而在以往，通常是以企业专线来达到安全传输档案的目的。这种传输方式安全性高，但价格昂贵。目前，较为大众所能接受的方式是采用 VPN 联机。而 VPN 联机分为两大类：固定式 VPN，还有移动式 VPN。

固定式的 VPN 就是已经使用多年的 IPSec 与 PPTP。这两种 VPN 大多是用在两个子网络之间的传输，像是总公司与分公司。在过去，这两种 VPN 都是联机后就无法有效控管两个子网络之间的传输。这样的传输方式对企业网络安全性，也是一大隐忧。现在，新软系统特地将”管制条例”的概念，导入了 IPSec 与 PPTP 中。管理员可以利用”管制条例”轻松达到控管（甚么人、甚么时候、去哪里、使用何种服务…）两个子网络之间的传输。甚至可以做到利用病毒过滤、入侵防御侦测等方式达到超高安全性的档案传输。至于在固定式 VPN 的线路连接方面，新软系统独创的 VPN 负载平衡功能，可做到多条 VPN 线路频宽的合并、VPN 断线备援…，让 VPN 的联机永无后顾之忧。

固定式 VPN 备援(IPSec、PPTP)



移动式 VPN 备援(SSL VPN)



移動式 VPN 就是近幾年來才崛起的 SSL VPN。大多是移動用戶、在外奔波的業務、出國洽公之人員所使用。不管使用者在哪裡，網咖、客戶公司、甚至在家裡。只要有網路，透過電腦的瀏覽器，短短 20 秒就能完成 SSL VPN 的連線。

也許有人會說：在外面使用 VPN，用 PPTP 就好了。簡單方便，何必再學一種新的 VPN。實際上，PPTP 的安全性在所有 VPN 中是最差的。況且使用者所在網路的閘道器若不支援PPTP Pass Through（PPTP 透通），使用者將無法成功建立 PPTP VPN。相較起來，SSL VPN 的資料加密能力比 PPTP 高出許多，且不會受限於網路環境，使用上安全且方便。

多功能 UTM 內建 VPN 比較

	固定式 VPN		移動式 VPN
	IPSec VPN	PPTP VPN	SSL VPN
安全性	高	中	高
架設難度	難	難	容易
VPN 負載平衡	○	○	×
Policy 管控	○	○	×
適用環境	總公司與分公司	總公司與分公司	移動使用者

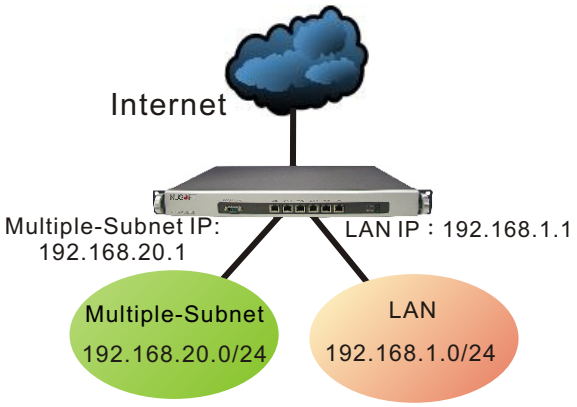
文 程智伟 rayearth@nusoft.com.tw

市场营销报导 - 如何管理企业内不同子网络？

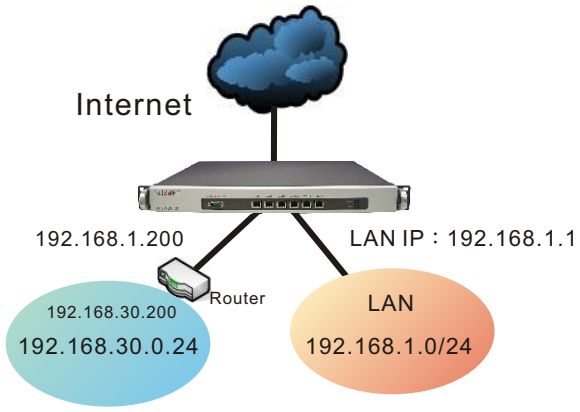
企业网络在规划时，往往为了管理方便，会把整个企业网络划分为多个不同子网络，并将这些子网络分配给各大部门所使用。在过去，建构这种企业网络架构的方法，就是在每个子网络前架设路由器。藉由路由器能够沟通不同子网络的特性来建构多子网络的企业网络环境。这种企业网络的建构方式，不只架设经费提高了，在网络维护方面也会变为复杂，增加管理上的困难度。事实上这个问题，可以利用新软多功能 UTM 内建的 Multiple-Subnet 功能轻松解决。

Multiple-Subnet 这功能适用在”企业有多个部门，而这些部门需要区分为不同的子网络”之网络环境。管理员只需要几个简单的设定，指定这些子网络在联机至外部网络时，需透过Multiple-Subnet机制所设定的网络接口，就可轻松完成设定。此后，位于这些子网络的用户就可直接透过多功能 UTM 上网，并完全能受到多功能 UTM 的管控。

Multiple-Subnet



指 定 路 由 表



假如企业网络环境必须使用路由器来连接不同的子网络时，多功能 UTM 也能利用内建的指定路由表功能达到建构多子网络环境之目的。指定路由表的功能就是在告诉多功能 UTM，如果收到需要传送至特定子网络的封包时，要往哪个路由器传送。

Multiple-Subnet 与指定路由表，这两的功能的使用环境其实是很相近的。都是企业网络中有多个不同的子网络。两者之间的差异就只有”指定路由表使用于有路由器环境”，而”Multiple-Subnet 则不需使用”。只需要弄清楚这一点，在建构多子网络的企业网络，就不会有选择错误的问题发生。

文 程智伟 rayearth@nusoft.com.tw