新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2006/12/11 - 2006/12/17 第7期

网络记录器 / IR系列报导

技术浅谈与应用 - 记录数据检索

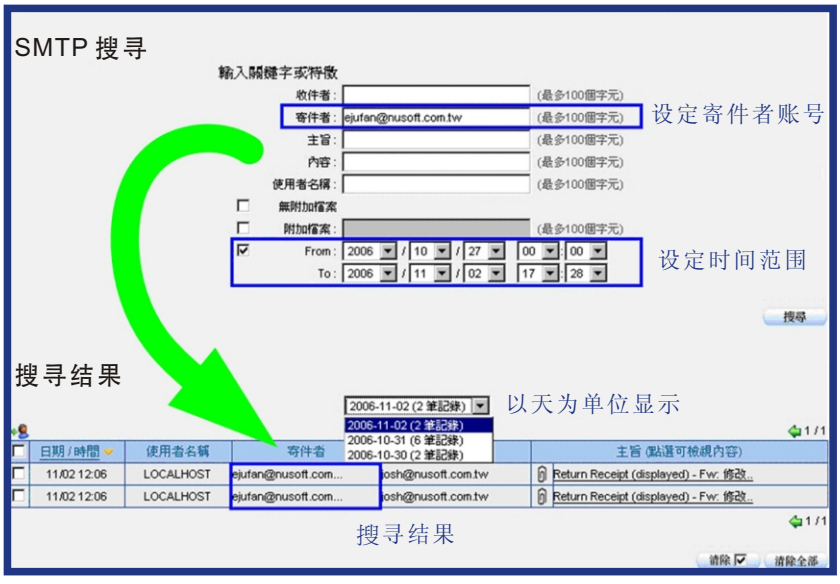
在做事愈来愈讲求效率的趋势中，拜科技之赐，许多方便的通讯和数据传输方式，以网络为媒介蓬勃发展。但，伴随而来的是，有心人士的滥用，导致耗费工时、机密外泄…，众多危害企业利益的行为。

因此，了解员工上网行为，严然成为企业管理上的一个新兴课题。为了提供所需的数据，新软公司研发了有别于市售行为管理防火墙的网络记录器（NUS-IR2000、NUS-IR1500、NUS-IR1000），着重于内部上网行为的侧录。

以 NUS-IR2000 来说，对于上网封包的撷取和还原，皆以详尽、深入为原则。于记录数据之初，即依其性质，将可供检阅的特征提取出来，发展出方便调阅记录内容的使用接口。独特的 **全方位搜寻** 和 **内容检索** 技术，由此应运而生：

1.全方位搜寻：

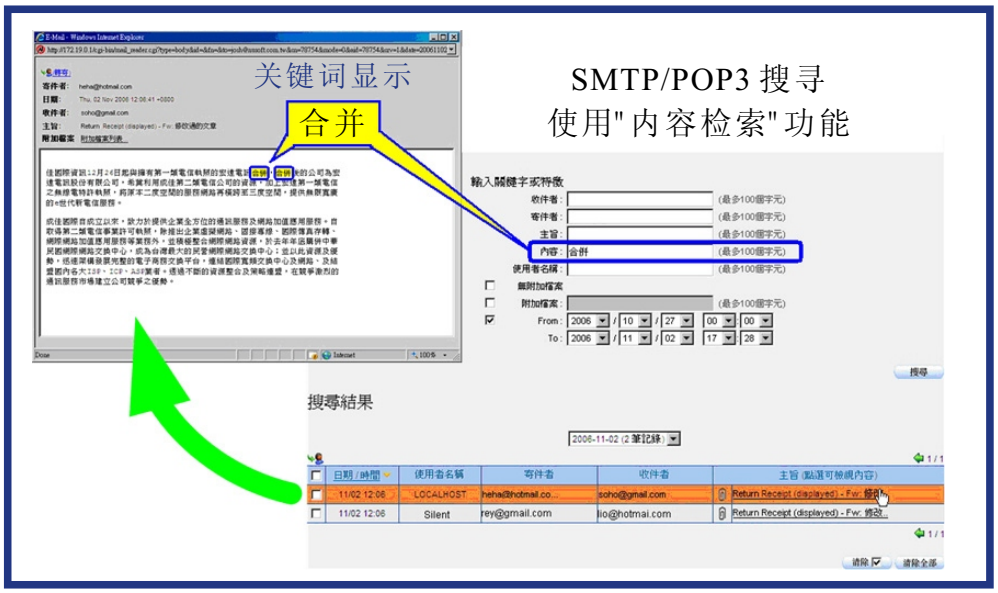
由于 NUS-IR2000 将常用的网络行为（例如：HTTP、SMTP、POP3、Web Mail『Web SMTP & Web POP3』、IM、FTP 和 TELNET）详细记录，必须运用庞大的数据库做为储存媒介。为了在大量的数据中做重点搜寻，NUS-IR2000 提供管理人员输入关键词和特征的搜寻接口，深入广大的数据库中一一比对数据库内容，快速且正确找到所需的记录。



如上图所示，以 NUS-IR2000 的 SMTP 搜寻为例，搜寻出来的数据是以天为单位呈现，并利用一目了然的窗体方式呈现搜寻结果。

2.内容检索：

NUS-IR2000 不仅能依标题、使用者、时间等条件搜寻，更可以针对记录的网络行为内容进一步搜索，不必一笔一笔的比对查阅，就能使管理人员快速查询相关数据，有效的为企业机密信息严密把关，以降低信息外流的危机，并提高管理效能。



如上图所示，在 NUS-IR2000 的 SMTP 搜寻功能中，以“合并”为关键词，做邮件「内容」搜寻，符合条件的部份，便会以黄色方块清楚标示出来，让查阅者一目了然。

就「搜寻机制」来说，新软 IR 系列产品和市售产品的比较（如下表）：

产品 / 查阅能力技术	新软公司 **NUS-IR2000**	一般市售网络侧录设备
搜寻功能	能依指定的条件和特征，于庞大的数据中搜寻，迅捷的找到所需的记录。	1. Mail：无法针对信件的内容，附加档案的档名检索。 2. Web Mail：常用网页快照方式记录 Web Mail，导致无法利用收件者、寄件者、主旨、信件内容…方式搜寻。 3. IM：大多仅能对聊天的账号搜寻。无法针对聊天的内容、传递的档案加以搜寻。 4. HTTP：通常只能针对 URL 搜寻，而不能搜寻网页内容与网页标题。
内容检索	可深入搜寻各项数据的「内容」，对往来的数据严密把关，并有效管理。	

文 陈昱升 josh@nusoft.com.tw

市场营销报导 - 行为管理功能

随着近年来因特网的快速发展，企业 e 化提升了整体的竞争力；但也因为过于便利的网络传输，而容易发生企业网络资源遭到滥用、员工上网摸鱼等问题，造成无形的损失。因此，各家业者纷纷推出网络侧录设备来因应这个企业 e 化的后遗症。

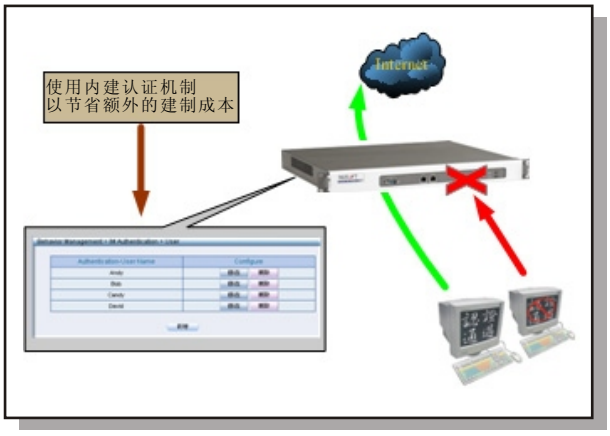
而部份厂商所推出的设备是以**关联器**再加上**记录数据功能**的方式滥竽充数，并称之为“行为管理器”。宣称可以记录、管控员工之上网情况，甚至拥有防火墙功能与负载平衡机制！！殊不知，其往往呈现的是一团乱的记录数据、简单的管控功能、阳春的防火墙机制、不堪使用的负载平衡功能…，完全模糊了网络侧录设备之产品定位。

要知道，网络侧录设备应专注于网络数据的记录与分析，至于行为管理部分则是与企业原有的专业防火墙搭配使用；旨在弥补专业防火墙的不足，而不是凡事都想插一脚，最后变成功能样样都有，样样不精的设备。有鉴于此，新软公司在开发网络记录器的行为管理功能时，即依循上述之原则，特别着重于一般企业防火墙无法掌控的地方，让新软网络记录器与企业原有之防火墙能够相辅相成，来为企业解决这企业 e 化的后遗症。

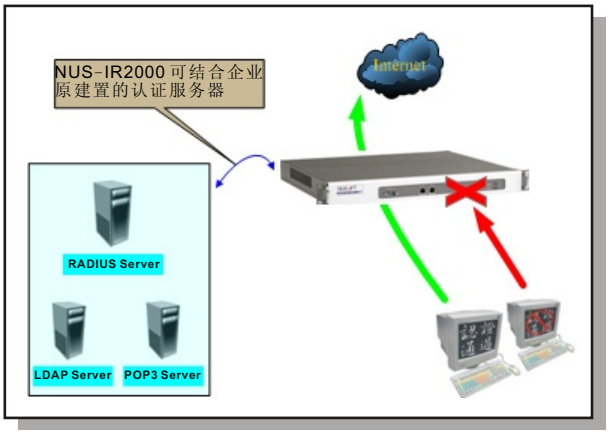
新软网络记录器的行为管理功能：

- **实时通讯认证**

实时通讯认证机制可协助企业有效掌握旗下员工的实时通讯使用。管理人员可要求员工在使用实时通讯前，必须通过网络记录器之认证否则将禁止使用。此外，网络记录器支持了多种认证账号数据。企业除了可使用其内建的认证用户表（不须再额外架设认证服务器，可节省建置之成本）之外，亦可结合企业原本已建置完成的现有认证服务器（如：RADIUS、POP3、LDAP 等），以达到账号整合的目标。



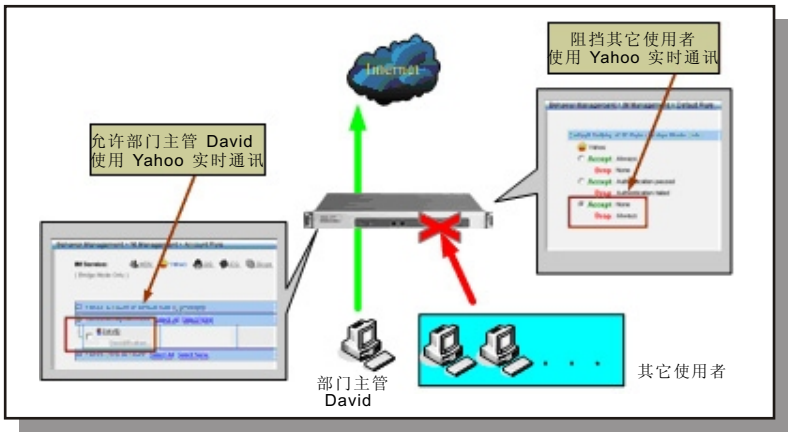
利用本机之认证表完成认证设置



利用外部服务器完成认证设置

实时通讯管理

可使企业能有效管理企业内部实时通讯之使用，弥补一般防火墙无法阻挡员工使用实时通讯软件之问题。它不仅可管控整个企业的实时通讯使用（如全部允许、仅有通过认证者允许或全部不允许等），更能针对个别账号制订规则，以符合企业的管理需求。



利用实时通讯管理掌控实时通讯之使用

P2P 管理

点对点软件的传输可以使用任何的 Service Port 来进行，因此一般防火墙根本无法阻挡这个企业频宽杀手。因此，新软公司在网络记录器里添加了 P2P 管理功能。P2P 管理功能不仅可以管控整个企业的点对点软件使用，也可针对个别使用者制订规则，以符合企业对于点对点软件的管理需求。

及时流量分析（NUS-IR1000 无此功能）

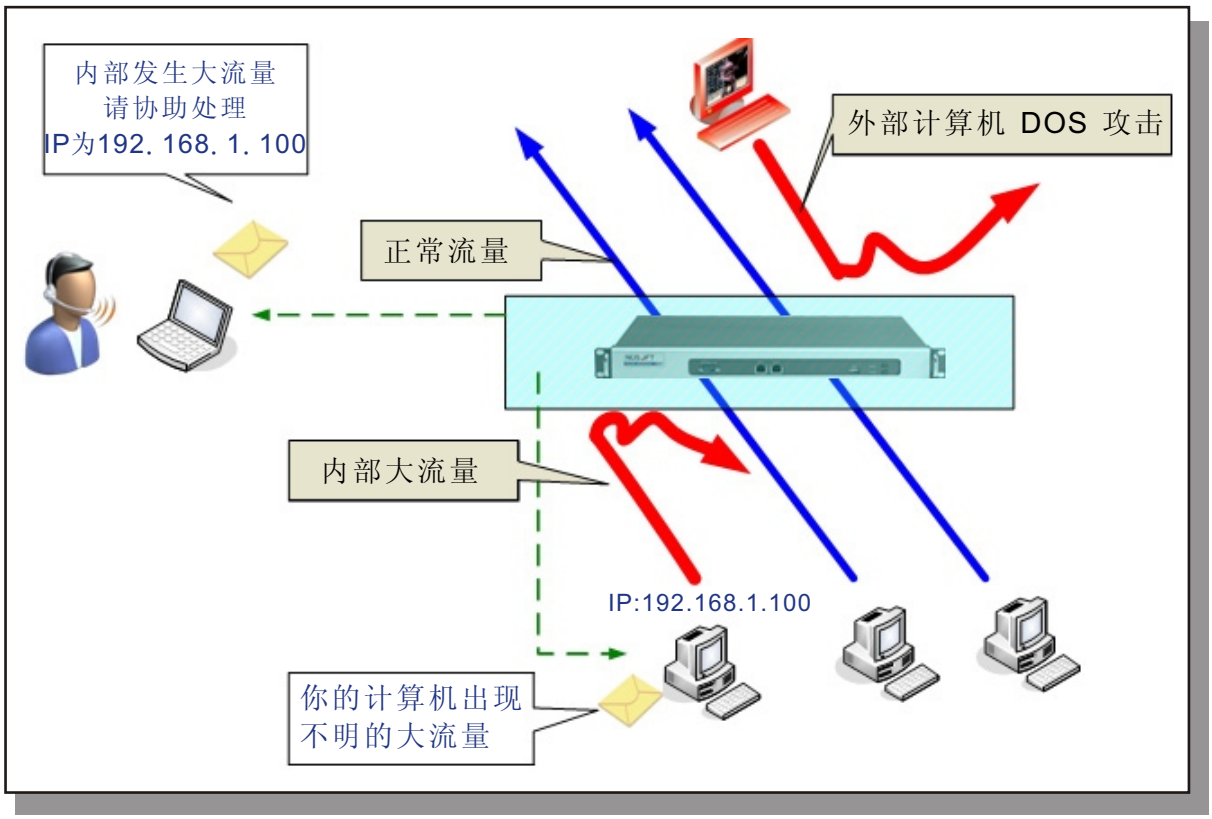
一般防火墙的流量记录功能较于阳春，管理人员较难从中得知重要讯息。而网络记录器的流量分析机制，可分析整个企业网络之流量，轻松得知目前企业网络的使用情况，是何人在何时使用何种服务占据企业网络频宽。再配合企业原有防火墙的阻挡功能、频宽管理…，有效控管企业的频宽利用。

流量分析机制分为三大功能：【流量统计】、【今日排行榜】、【历史排行榜】

产品 / 流量分析功能	新软网络记录器	一般网络测路设备
流量统计	以图表方式显示当日企业网络的实时流量，管理人员可从此得知在何时段有反常之流量发生。	仅提供特定时间点内的分析记录，且无法分析预设服务以外的各类型信息。不仅无法符合企业多元化的网络服务需求，更不能藉此协助企业揪出滥用企业网络的使用者。
今日排行榜	可统计今日任何时段的流量排行，并列出前十名。有助于管理人员，对于企业频宽之掌控。	
历史排行榜	可统计任何时段的流量排行，并全部列出。让管理人员，了解整个企业网络之运用情况。	

异常流量侦测

若企业网络内部之计算机发出异常之大流量时（DoS 攻击），网络记录器会先行阻挡此异常大流量之传送，确保整个企业网络的流畅。并可与 Core Switch 协同防御，将异常大流量封锁在局部范围。最后网络记录器会向管理人员与该计算机的使用者提出异常警告，让管理人员可迅速找到问题的所在。



文 程智伟 rayearth@nusoft.com.tw