

网络记录器 / IR 系列报导

技术浅谈与应用 - 双向记录，让你彻底了解企业网络使用情况

在今日企业普遍 e 化的型态下，因特网已成为企业发展不可或缺的工具，主管及员工浏览网页及使用电子邮件传递信息，客服人员使用实时通讯软件为客户排解疑难及互动…，都得仰赖网络。但是，如此方便的网络环境如同双面刃般，一面可为企业带来丰厚的商机利益，另一面可能经由员工不当滥用企业网络带宽，导致网络阻塞、影响工作效率，严重则不慎泄漏商业机密损失惨重。

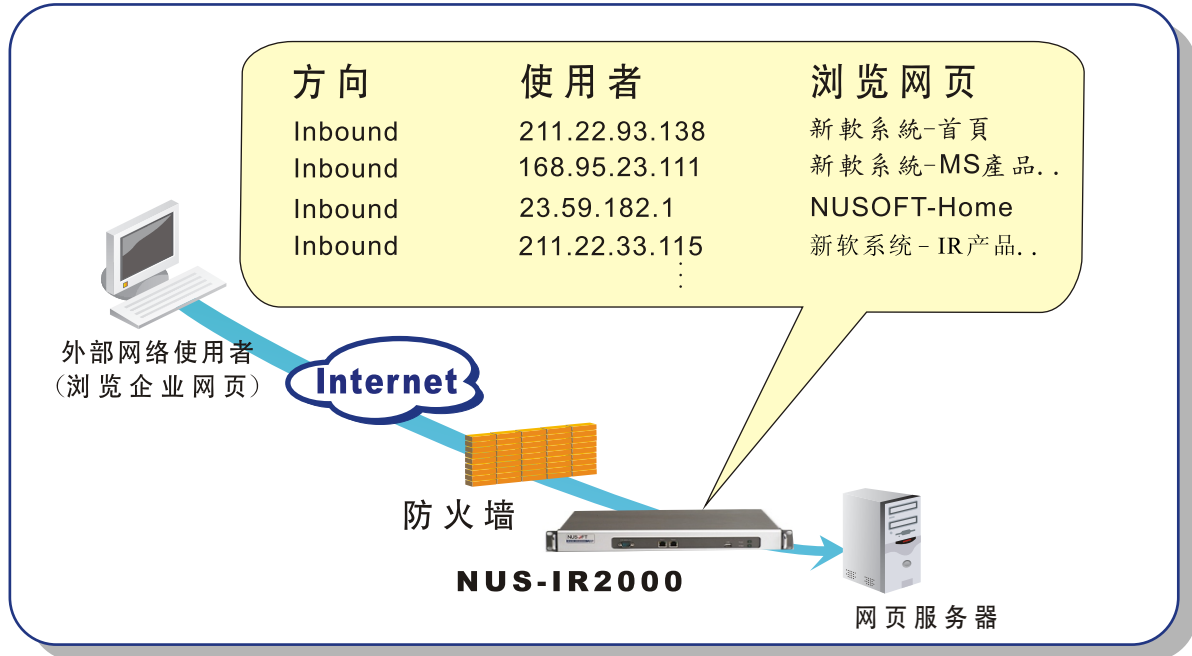
为了让员工谨慎地善用企业网络资源、遏止网络摸鱼，有越来越多的企业采用网络侧录设备。现今市场上的网络侧录设备，其功能重点都是侧录员工上网之情况，仅记录公司内部计算机对因特网上外部主机的服务联机（Outbound，内部至外部联机），而忽略了外部使用者联机至企业服务器之记录（Inbound，外部至内部联机）。要知道，仅有企业网络的 Outbound 记录而忽略了 Inbound 记录，是无法全面掌控企业网络之使用情况，难以确保是否有异常使用之行为。容易忽略资安漏洞的发生，让人不能不重视这项课题。

为了协助企业能完全掌握其网络使用情形，新软系统的 IR 系列（网络记录器）产品除了拥有完整之 Outbound 记录，特别增加了 Inbound 记录。让企业可全面掌握网页浏览（HTTP）、收发电子邮件（E-mail、Webmail）、实时通讯（MSN、Yahoo Message、ICQ、QQ…）、文件传输（FTP）、远程登入（Telnet）... 这八大项常用网络服务之使用情况。不管是内部员工上网，还是外部使用者联机进入。让管理者不仅可随时查阅记录，透过管理接口也清楚显示流量来源去向之 IP 地址、网页连结网址、聊天讯息字符串…，使得企业在网络管理上更能得心应手。

就电子邮件（E-mail）来说，新软网络记录器可以详细记录邮件接收与发送时间、寄件者与收件者、信件内文与附加文件，除了 Outbound 记录功能外，藉由 Inbound 联机记录功能，可得知外部使用者寄至公司内部邮件服务器、透过 Webmail 或 SMTP、POP3 联机至公司内部邮件服务器传输信件的情况。

以网页浏览（HTTP）而言，新软网络记录器则会详细记录内部使用者浏览网页时间、浏览目的网站…，并撷取当时浏览之画面存档备查；对于 Inbound 记录部份，则可详细记录外部使用者是透过哪个 IP 联机至企业网页，并从中得知企业网页哪些连结流量较高、哪些则乏人问津。可用来改善公司网页架构，提升整体浏览人气及企业形象。另外，像是搜寻引擎所提供的“关键词广告”（例如：Yahoo、Google），也可藉由新软网络记录器独特的 Inbound 联机记录优点，完全掌握点选此关键词广告连

结之外部计算机 IP 地址及点击次数；假若有人恶意多次点选广告连结，欲造成公司网络广告费用剧增，即可追查是哪个来源地址的恶意联机。



图一 外部使用者浏览企业网页时，新软网络记录器可详细记录其点选之网页

在文件传输 (FTP) 服务上，透过新软网络记录器内建的记录分析机制，可清楚地记录上传 / 下载计算机之双方主机名称及 IP 地址、登入者账号及密码、下载文件及传输流量大小。当公司内部有架设 FTP 服务器，亦可经由 Inbound 记录，网络管理者可清楚得知外部使用者何时从服务器下载哪些文件。至于在远程登入 (Telnet) 方面，藉由 Inbound 记录，网络管理者可清楚查阅来源计算机连至公司内部服务器主机执行哪些指令及动作，查阅哪些信息及公司机密，因而来进行数据控管。

文  黄赞中 isaac@nusoft.com.tw

市场营销报导 - 实时通讯管理策略 - 完全开放、全面封锁、积极开放，有效管理

自从 1996 年 ICQ 问世至今，实时通讯 (Instant Message，简称 IM) 的应用已经跨越了第 11 个年头。就因为其安装简单、沟通方便、实时迅速...，使它在近年来使用人数快速攀升。从一开始学生族群常用的聊天工具，转变为上亿网络使用者之主要沟通管道，且其普遍性甚至有超越电子邮件之趋势。这现象不只出现在一般计算机使用者，也出现在企业当中；实时通讯在企业间已经是一种非常普遍的电子沟通方式，员工透过实时通讯与客户沟通的比例越来越高。

就是因为实时通讯所带来的快速与便利，使得用实时通讯与客户沟通之效果甚至比电子邮件或是电话来的好。而且实时通讯又不需付费使用，对于合作伙伴、客户分布于世界各地的企业，可大幅减少通讯方面之成本。所以部分企业对实时通讯采取全面开放的态度。

实时通讯的正面效益：

1. 互动性佳，节省沟通往来时间。
2. 不需通讯成本。
3. 可实时得知需联络对象是否在线。

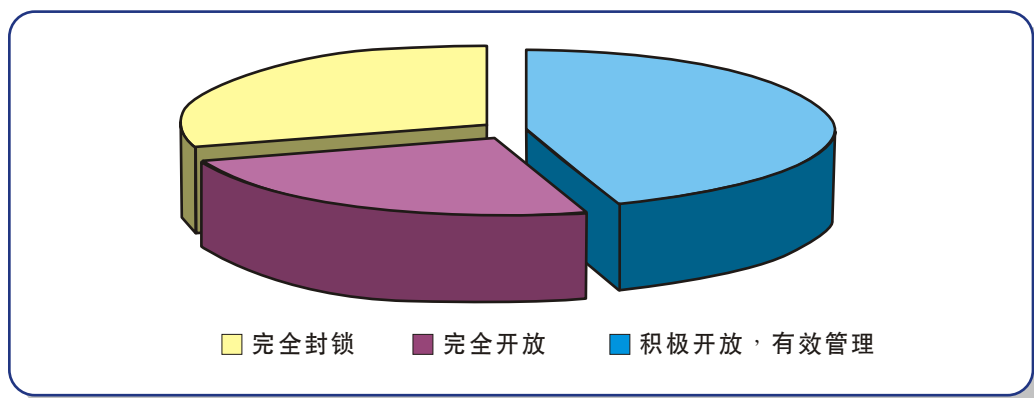
但是，也因为实时通讯实在是太方便了，导致企业员工利用它来聊天摸鱼的例子不胜枚举。或是透过实时通讯传输企业机密文件，而导致泄密的问题时有耳闻。甚至近年来，透过实时通讯散布病毒也不是甚么新鲜事了。因此，部分企业宁愿放弃实时通讯的方便性，而全面封锁实时通讯的使用。

实时通讯的负面隐忧：

1. 员工聊天摸鱼，降低工作效率。
2. 任意传递文件，易造成泄密（传递企业机密文件）或是法律上的问题（传递 MP3、非法文件）。
3. 病毒、黑客、钓鱼... 问题层出不穷。

难道对企业来说，实时通讯就只有全面开放或是完全封锁两种选项吗？难道不能妥善运用，为企业带来更多的商机？其实，除了全面开放或是完全封锁外，您还有更好的选择！！

虽然，实时通讯的负面隐忧为数不少，但如因此放弃这极具价值的沟通管道却有点因噎废食。如何管理实时通讯，让它为企业获得最大利益，是目前大部分的企业处理实时通讯之倾向。



图一 目前企业处理实时通讯问题之倾向

如何管理实时通讯，方能达到企业最大利益呢？

- 订定实时通讯使用范围（何人有权使用）—
管理人员可透过新软系统多功能 UTM、负载平衡器 或是 网络记录器的实时通讯管理机制，按企业之网络政策制定每位员工的实时通讯权限。
- 限定实时通讯软件种类，并随时注意实时通讯软件漏洞更新讯息—
统一限定企业所使用的实时通讯种类，以便于管理。并需注意实时通讯软件的漏洞更新，确保软件安全无虞。
- 使用企业统一申请之账号—
绝大部分的员工使用私人之实时通讯账号做为与客户沟通管道。倘若该员工离职，则接替人员无法再用此管道与客户联络，且企业无法制止离职员工继续使用此账号作出伤及企业利益之事情（假冒公司窗口，散布不实讯息给客户）。
- 架设防毒墙或是安装防毒软件，检测透过实时通讯所传递的文件—
新软多功能 UTM 的 IDP 扫毒机制可针对实时通讯所传递之文件扫毒，确保文件传输安全。
- 使用实时通讯记录机制—
要如何确定员工的实时通讯内容是聊天摸鱼，还是洽谈公事？新软网络记录器可记录员工使用实时通讯内容，其中详细记载对话内容、对象、时间、传送文件...，协助企业掌握员工使用实时通讯之情况。
- 公告企业实时通讯使用规则，并教育员工—
公告企业所订定的实时通讯使用办法，内容应包括为何管理实时通讯、员工使用权限、允许 / 禁止项目、实时通讯内容记录原则...。最好是要求员工签署“实时通讯使用同意书”，以避免日后不必要的麻烦。（尤其是记录实时通讯内容这一部份，最好明确告知员工）

文 程智伟 rayearth@nusoft.com.tw