新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2006/12/4 - 2006/12/10 第6期

网络记录器 / IR系列报导

技术浅谈与应用 - 记录数据备份

网络记录器每天不停的记录数据，会不会发生硬盘空间不足而无法再记录的问题呢？以 NUS-IR2000 来说，它的硬盘虽然多达 250G，但也会有用完的时候。因此 NUS-IR2000 可让管理员自行分配各种记录的储存期限。旧记录一旦过了储存期限，就会自动将它移除，腾出硬盘空间，以便能再记录新的数据。倘若这些记录十分重要，需要保存个三五年才能销毁时，那该怎么办？（欧美各国已立法要求部份行业必须保存往来电子邮件 三 至 五 年，以供日后调阅。）这时，就需要依靠 NUS-IR2000 独特的远程备份功能来保存这些记录。

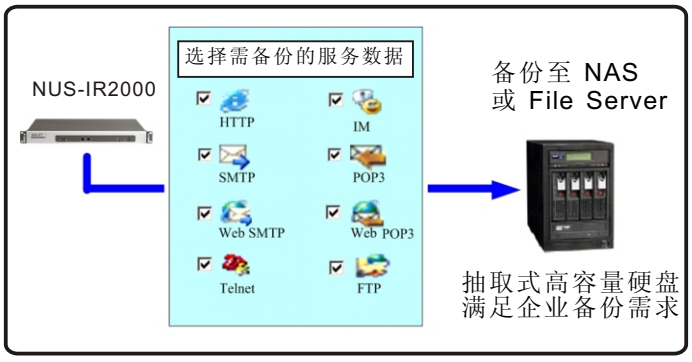
利用 NUS-IR2000 的远程备份机制，管理人员可视需求，将记录内容备份至远程的 NAS 或是 File Server 中。不仅可选择所需备份之服务（如：E-Mail、I M…服务），更可以订定自动备份之时间，使企业可自由选择网络离峰时间进行备份，避免在备份时无法记录数据的窘境。而将记录数据备份至远程 NAS 或 File Server 中的抽取式高容量硬盘，不但能使 NUS-IR2000 的硬盘空间，可得到充分灵活的运用，更能提高数据保存的安全性。

总括来说，NUS-IR2000 的远程备份机制，拥有下列特点：

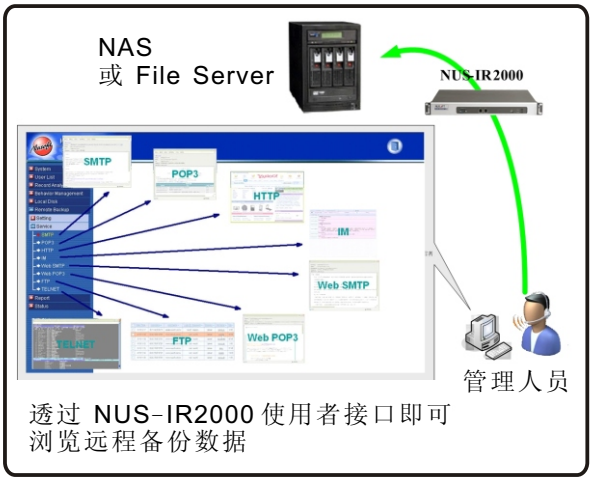
1.延伸硬盘空间，使储存容量不受限于本机硬盘的限制。（如图 一）

2.避免纪录遗失，例如误删、记录超过储存期限后被自动删除、系统发生问题。

3.网络记录器仍可浏览远程 NAS / File Server 所备份的记录。浏览简单、方便。（如图 二）



（图一）



（图二）

就「备份机制」来说，新软 IR 系列产品和市售产品的比较（如下表）：

	新软公司 NUS-IR2000	市售其它侧录设备(采用光盘烧录备份)
备份所需时间	6 分钟可备份 2G 的数据容量。	一张光盘需 6 分钟或更长的烧录时间。
备份空间大小	视 NAS 或 File Server 硬盘决定，多数为 250G 以上。可备份大型企业约 85 天的记录数据。	一张光盘仅能备份 600M，约大型企业 4 小时的纪录容量。
专人操作	可选择自动备份，无须专人操作。	由于需人工更换光盘片所以仅能专人操作。
备份时机	可选择半夜或网络离峰时间自动备份，不会影响正常记录。	由于需专人操作，所以仅能于上班时间作业。而备份时将占用大量系统效能干扰数据之正常侧录。
存放空间	无须另辟空间存放。	需有足够的空间保存光盘。
数据保护机制	NAS 或 File Server 可使用磁盘阵列，避免硬盘损毁、造成数据遗失。	增购光盘保存设备，但无法100%保证光盘堪用，一旦光盘损毁数据将无法还原。
硬盘空间占用	直接备份至远程 NAS 或 File Server，无数据重复与占用设备硬盘空间之虞。	光盘烧录时需先将记录数据转换为 ISO 格式，储存于设备中造成数据重复与占用设备硬盘空间。

就「数据浏览」来说，新软IR系列产品和市售产品的比较（如下表）：

	新软公司 NUS-IR2000	市售其它侧录设备(采用光盘烧录备份)
浏览方式	直接于管理接口浏览。	需使用档案辨识软件解读取光盘数据后方能浏览。
浏览地点、时间	在任何地点、时间，只需联机至网络记录器之控制接口即可浏览。	需在特定安装辨识软件的计算机中，读取光盘数据，无法随时随地浏览。
数据找寻	可透过管理接口中搜寻机制，在第一时间找出所需数据	需于众多光盘中找寻出所需数据光盘。如无法确定数据位于那片光盘，则必须每片光盘一一寻找。
多人同时使用	可提供多人同时查阅	同一时间内仅能提供一人查阅
软件安装	无须另外安装软件，仅需网页浏览器皆可完成相关查询动作	需安装特定的档案辨识软件

文 程智伟 rayearth@nusoft.com.tw

市场营销报导 - 网络记录器需包含的基本功能

在目前网络信息传递蓬勃发展的环境中，运用得当可做为商场竞争的一大利器。反之，则成为企业向前迈进的绊脚石。而目前对企业最大的冲击，无疑是内部员工想尽办法利用公司网络，从事私人或非法的活动（例如：利用实时通讯软件聊天怠工、持续占用宽传送大型档案、泄漏公司机密数据…）。

在以往企业只能耗费大量的人力，做收效有限的查缉和吓阻动作。为了因应上述的需求，网络侧录设备如雨后春笋般充斥在市场上。这些商品无不标榜能完整记录或控管员工的网络行为，但往往呈现出来的是，不够清楚或难以阅读的数据，且模糊了原有的产品定位。

有鉴于此，新软公司在开发网络记录器时，则特别着重于数据的搜集、探勘和分析：

1. 详实纪录 8 种常用的服务：
   HTTP、SMTP、POP3、WEB Mail(Web SMTP & Web POP3)、IM、FTP 和 TELNET。
2. 将记录依使用者和服务名称分类呈现：

产品 / 数据分类方法	新软网络记录器	一般市售网络侧录设备
使用者	可依据使用者名单找到特定使用者，了解其所有上网行为，并提供今日记录功能，使管理人员能在第一时间内查询特定使用者今日所有记录数据。	仅能透过服务名称搜寻相关使用者，使管理人员欲查寻单一使用者网络行为时，往往浪费许多的时间在搜寻特定使用者上，降低了工作效率。
服务名称	可以依照服务名称搜寻各项服务记录，了解哪些使用者使用该项服务，大大减少搜寻的时间。	

3. 提供全方位的检索接口：

产品 / 查阅能力技术	新软网络记录器	一般市售网络侧录设备
搜寻功能	透过强大的搜寻系统，能以网站、使用者、网页内容、时间区间等信息，在庞大的数据中重点搜寻。当管理人员对其所需条件输入关键词时，皆可迅速、轻易的找到所要的记录。	无法针对标题搜寻，必须经由管理人员一一确认。
内容检索	利用此独创技术，在庞大的数据库中快速且正确找到所需的数据，有效提高管理效能。	

4. 实时和历史性的网络流量排序：

产品 / 流量排行方式	新软网络记录器	一般市售网络侧录设备
今日排行榜	利用时间滚动条拖曳至所需的时段，即可分析时段内的各项流量，藉此揪出危害网络频宽的使用者。	仅能针对单一时间点内的记录做分析，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排除危害网络的使用者。
历史排行榜	记录企业网络所有流量分析信息，全方位的分类查询有助于企业实时掌握所有网络流量信息。	

5.过网络备份完整数据：

	新软网络记录器	一般市售网络侧录设备
备份机制	可视管理需求，将要备份的服务记录内容，以定期或立即的方式，传送至远程的 NAS 或是 File Server 储存，可选择离峰时间备份，有效避免了备份时无法记录的危机。	多半采用光盘烧录输出方式进行备份，必须于上班时间内由专人进行备份工作。在备份时往往需停止记录动作，于备份完成时在进行记录工作。

根据上述五大项特性，再辅以异常流量侦测和群组管理机制，将管理的权责分担给各部门负责人，减轻管理员的负担，并随时监视网络使用情形，避免异常流量损及使用者的权益。使网络记录器无形中成为资安系统中，不可或缺的管理利器。

文 陈昱升 josh@nusoft.com.tw