新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/12/17- 2007/12/23 第54期

网络记录器 / IR系列报导

技术浅谈与应用 - 网络记录器的硬盘容量可以使用多久？如何得知硬盘容量快额满了？

随着网络科技的发达，企业每天透过网络传输的数据量相当庞大，网络俨然已成为企业最重要的沟通管道之一。在企业大量使用网络传递信息的同时，对于具相当规模的企业来说，旗下员工每天的网络行为所产生之数据量往往都过于庞大，导致一般网络侧录设备其所内建的硬盘容量经常不敷使用。同时机器所记录之数据也缺少分类的机制，当内建硬盘容量接近饱和时，系统便会自动将最旧的数据删除，如此无差别的硬盘储存管理方式，对于硬盘储存容量不仅没有做到有效分配的控管，也不符合企业须长时间保存数据的要求。

新软系统针对一般市售网络侧录设备此缺点，特别在新软网络记录器（IR 系列产品）上加入对于封包的传递做撷取、分析及归类的独特过滤技术，除了能够详细过滤封包的来源并加以归类之外，同时在数据储存上具有独家的「储存期限」机制；透过此机制，网管人员可依企业的需求在各项服务上设定欲储存的时间值，而 IR 即会依据网管人员所设定的「**数据储存时间**」与该服务的「**每日平均流量**」，计算各项网络服务的「**预估储存空间大小**」及该服务的「**硬盘容量占用百分比**」，藉由此方式来有效分配各项记录于 IR 内建硬盘的使用率。

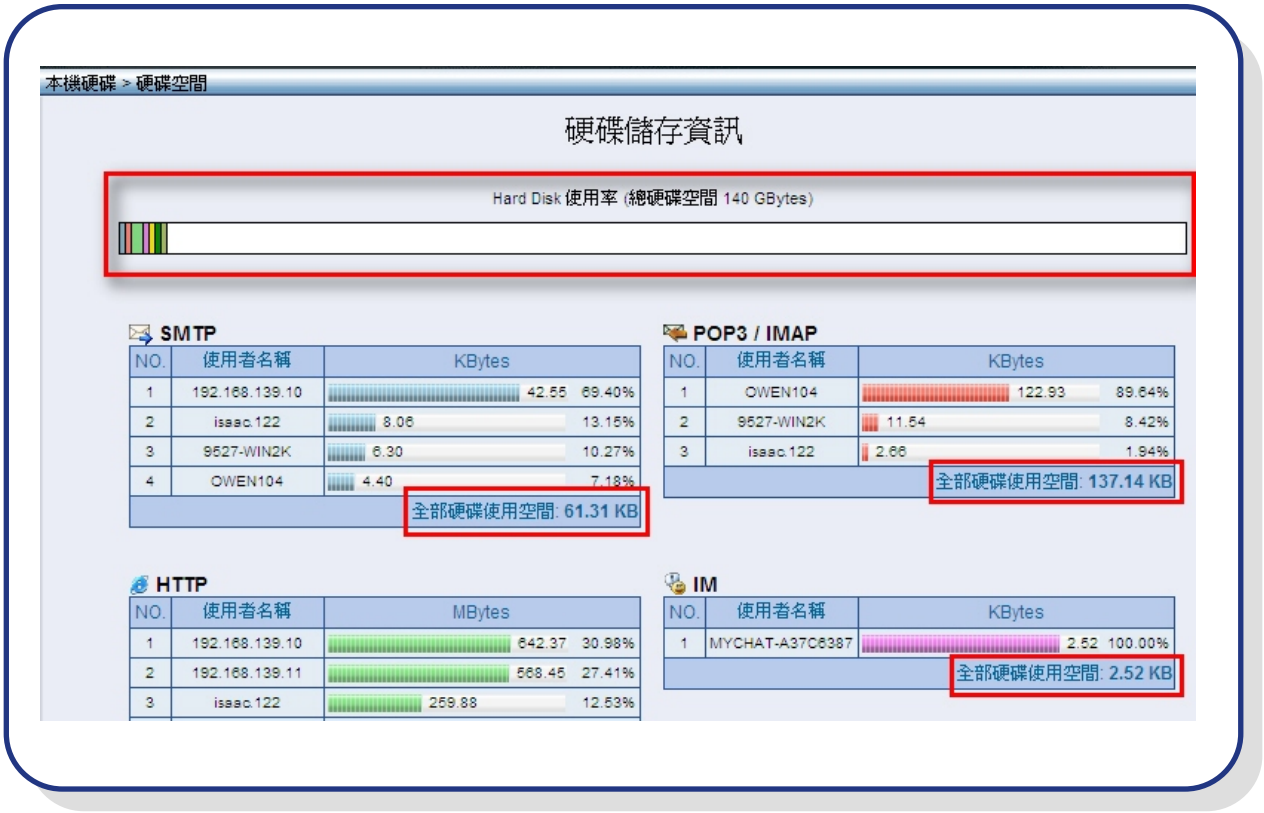
服務名稱	目前儲存時間範圍 (y/m/d)	平均流量 / 天	儲存時間 (0: 不記錄)	預估儲存空間* (百分比)
SMTP	07/12/06 ~ 07/12/10	12.26 KB	60 天	735.72 KB (0.00%)
POP3 / IMAP	07/12/06 ~ 07/12/10	27.43 KB	7 天	191.99 KB (0.00%)
HTTP	07/12/06 ~ 07/12/10	414.39 MB	60 天	24.86 GB (16.54%)
IM	07/12/07 ~ 07/12/10	1 KB	7 天	4.41 KB (0.00%)
Web SMTP	07/12/06 ~ 07/12/10	1 KB	7 天	1 KB (0.00%)
Web POP3	07/12/06 ~ 07/12/10	314.85 KB	7 天	2.20 MB (0.00%)
FTP	07/12/10 ~ 07/12/10	1 KB	7 天	1 KB (0.00%)
TELNET	07/12/10 ~ 07/12/10	85.32 KB	8 天	682.58 KB (0.00%)
全部				24.87 GB (16.54%)

*預估儲存空間 = 平均流量 X 儲存時間 Help

（图一）预估储存时间＝使用者设定的【储存时间】× 系统分析的【平均流量】

当 IR 内部的各项服务记录一旦过了网管人员所设定的储存时间期限，系统则会自动将超过保存期限的数据删除。倘若，在尚未到达数据储存时间之前，硬盘储存空间就已经额满，则 IR 系列产品会依照数据储存的时间先后顺序，从时间最久的记录数据做删除的动作，空出储存空间，如此一来不仅 IR 产品内建的硬盘储存空间能不断地重复储存使用，同时系统侧录机制也能够持续地维持运作。

那网管人员要如何得知硬盘的使用状况呢？很简单~！网管人员只要从 IR 内部的『硬盘空间』管理接口上即可清楚得知内建硬盘的使用状况。在『硬盘空间』的管理接口中，除了可以看到各项服务所使用的硬盘空间之外，更能透过画面上的硬盘储存信息及横条图，清楚得知内建硬盘的总空间大小与硬盘的使用率。藉由这样一目了然的硬盘储存信息接口，不仅让网管人员轻松地得知 IR 系列产品内建硬盘的空间使用情形，同时能清楚地看到各项服务的员工使用排行榜，进而掌握企业的网络使用概况。



（图二）各项服务的硬盘使用率与总使用率情形

文 黃贊中 isaac@nusoft.com.tw

市场行销报导 - 流量排行榜可以帮网管人员解决哪些问题？

拜近年的因特网快速发展之赐，并透过企业e化的结合，使企业整体竞争力不断提升，网络科技的百家争鸣时期就此因应而生。但在过度依赖网络便捷性的同时，可经常发现网络资源遭到有心人士的不当滥用、员工网络摸鱼等问题层出不穷。虽然，坊间出现许多号称可协助网管人员监督企业网络使用的网络侧录设备，不过这些网络侧录设备仅能提供网络总流量记录之类的阳春功能，对于网管人员欲藉此揪出滥用企业网络资源害虫的需求，根本无济于事！

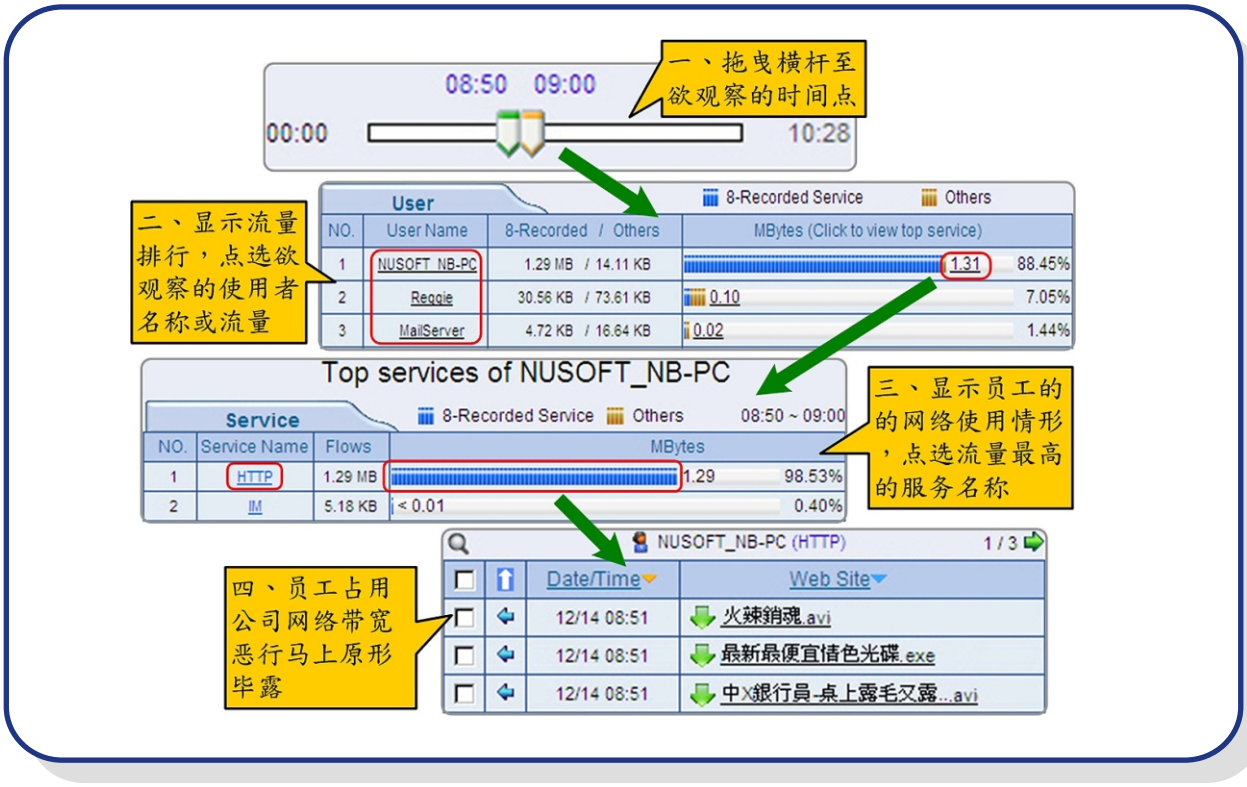
而新软系统了解企业此一需求，于网络记录器（IR系列产品）的流量分析功能特别加入『流量排行榜』的设计。流量排行榜是以「使用者的网络流量」与「各项网络服务的使用量」两种类型以排名的方式排序，并透过简单明了的图表呈现企业网络的使用情形。透过流量排行榜，不仅可轻松掌握企业任何时段的网络使用情形，更能够得知「是谁」在「哪个时段」使用「何种服务」占据企业网络带宽。

流量排行榜分为两种，各别为「**今日排行榜**」与「**历史排行榜**」：

- **今日排行榜：**

今日排行榜最大的特点就是－网管人员可观察当天任一时段网络流量前10名的记录，并透过新软独家的「**横移滑动拉杆**」时间轴设计，网管人员可以轻松地利用拖曳方式来选择欲观察之时段，并从画面排名结果中得知在这一时段内「何人」使用「何种服务」占用企业带宽。甚至可以深入了解该使用者透过此项服务到底做了些不法勾当，导致如此大量占用企业带宽。

另外值得注意的是，「今日排行榜」的观察时间是以每“10分钟”为单位，当然，网管人员也可依个人需求调整观察时间。会有这样的设计想法主要是因为过长的观察时间虽然可以累积记录较多的数据，但反而造成网管人员无法清楚得知该从何处找出问题发生的时间点，同时网络的异常流量也容易被其它服务信息所掩埋。这就是为什么新软网络记录器的「流量排行榜」机制远远优于他牌网络侧录设备的缘故。



【图一】透过今日排行榜，简单四个步骤即可轻松查阅使用者的网络使用情形

历史排行榜：

「历史排行榜」虽然也可让网管人员了解企业带宽的使用情形，但与「今日排行榜」不同的是，「历史排行榜」所观察的对象不是「当天的流量」，而是「企业从以往至当天的所有网络使用情况」。网管人员可依需求浏览指定时间日期范围内的所有网络流量信息，随时皆能掌握企业带宽的使用动态。

流量排行方式	新软网络记录器	一般网络侧录设备
今日排行榜	可观察当日任何时段的网络流量排行，并列出流量最高的前10名，使网管人员轻松掌握企业带宽之使用情形。	仅能提供单一特定时间点内的分析记录，也无法提供预设网路服务之外的分析记录。网管人员要找出滥用带宽者如同大海捞针。
历史排行榜	显示全时段的所有流量排行，网管人员可完整了解企业整体网络带宽的运作情况，无一遗漏。	

【表一】新软网络纪录器 VS. 一般网络侧录设备的流量分析记录差异

文 黄赞中 isaac@nusoft.com.tw