新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/2/9- 2009/2/22 第85期

网络记录器 / IR系列报导

技术浅谈与应用 - 记录储存空间的分配问题

在目前的公司、企业中，为了保密防谍以及提升员工的工作效益，从过去网络侧录设备渐渐的被广范使用，一直到目前为止，对公司、企业而言，网络侧录设备几乎是项不可或缺的网络安全设备之一。网络侧录设备不只是要能够达到完整的分析、全面化的管理，当然最为重要的不外乎是要能够支持全方面的记录功能及详细的记录内容。

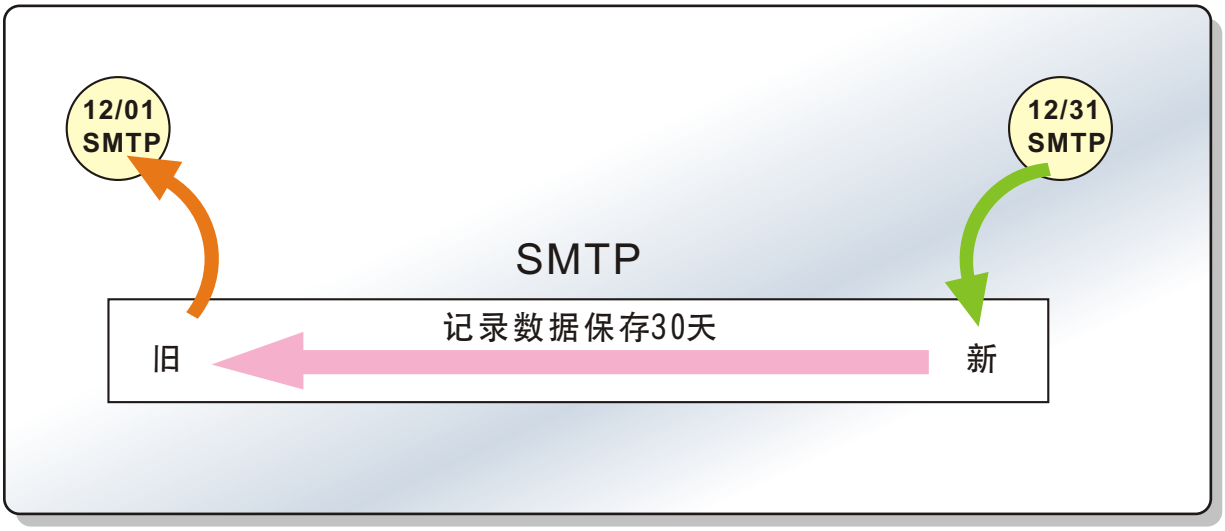
然而在详细记录内容下，数据一笔笔的不断增加，相对的若是没有足够的储存空间来将所记录下来的内容做妥善保存也是徒劳无功。但是只需要大量空间来提供储存记录就能够解决如此的问题吗？其实大量的空间固然是可以解决一时数据储存的需求，不过从长远的眼光来看这并不是一种最适当的解决方法。所以为了能做到最完善数据储存，同时还必需搭配有规画性的储存方式才是最佳的解决处理办法。

新软系统『网络记录器-IR』在记录储存空间方面，可以依各项服务类别之记录，依照对公司的重要性而言来自行灵活运用调配。记录数据所保留天数对公司而言，哪项记录服务类别重要性高，所分配的记录就可设定较长的天数；相对的重要性较低的记录数据，所设定的保留天数即可设定较短，例如 HTTP 这种看过即可的信息，可设定较短的保留天数；而像是 IM/MAIL（包含 SMTP、POP3、Web SMTP、Web POP3）此类较为重要的信息，就可设定较长的保存天数，如此一来即可大大的减省掉不必要浪费的储存空间。

新软网络记录器数据保存方式可分为两种情况，一种是内建硬盘尚未达上限，另一种则是内建硬盘已达上限。除了使用保存天数的方式来确保硬盘的空间外，同时也采用了储存空间临界值预防机制。当新软网络记录器的记录数据，达到设定的保存期限时，即会将其立即清除；若是在数据保存期满前，储存空间就已达上限，新软网络记录器会依照储存数据的历史排序，从目前保留最久、最早建立的记录开始删除的动作，腾出一定比例的空间，以维持后续侧录动作。

一．内建硬盘尚未达上限

新软网络记录器-IR 在记录储存空间方面可分为 SMTP、POP3/IMAP、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET 八大项类别，并且可依照每个公司的重视情况来自行决定记录之保存天数，以达到灵活运用及不浪费储存空间的最佳效果，换句话说则是将所记录之数据内容附上保存期限，依照保存天数来交由系统决定何时可将已达保存天数时效内的数据加以删除。例如：以 SMTP 这项类别为例，欲将此项服务类别中的记录数据设定保存为 30 天，而当 12/01 日所被记录的数据会一直保存到12/30 日，直到 12/31 这一天时，系统则会自动将 12/1 中所记录之 SMTP 记录全数删除。

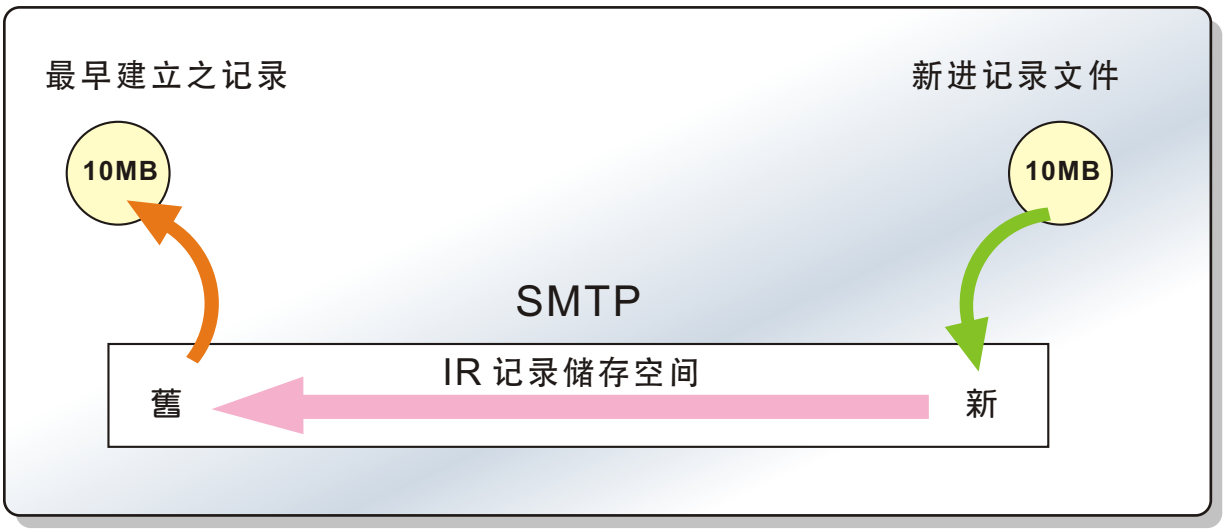


数据保存天数示意图

二．内建硬盘已达上限

第二种情况则是 IR 所内建之硬盘若是在数据尚未超过保存天数时硬盘空间就已经达到上限时，IR 的记录空间储存分配方式。IR 在遇到内建硬盘已达上限时，记录空间的储存分配方式会依照先进先出的原则方式，以储存数据的历史排序，将最早记录于内建硬盘中的记录**不分服务类别项目**的加以删除，而这方式和内建硬盘未达上限的处理方式到底不同于哪里呢？

内建硬盘未达上限时，系统所删除的记录是依照该项类别（如：SMTP 的记录在到期后只会删除 SMTP 该项服务类别中所到期的记录）。但遇到内建硬盘已达上限时，系统则会依照下笔新进来记录的容量大小，将最早建立保存于 IR 中的记录删除相对之容量大小，腾出空间来支付新进记录所需要容量，如：硬盘已饱和时，下笔新进入 IR 的记录数据为 10MB(不分类别)，系统则会删除最早存于 IR 中的记录 10MB(不分类别)，此时所删除的记录并不一定会是与新进记录所属同类别的数据，所删除之数据是以建立的时间早晚来做定论，换句话说，新进入的记录数据若为 SMTP，而被删除的记录有可能为其它服务类别。



空间分配示意图

为了因应企业在各法规的实行下，要达到长时间保留所有往来数据以供查阅的需求；并且同时防止用使用者邮件遗失或误删的情形发生，同时也可利用 IR 系统中所内建的 NAS 远程备份机制来进行数据的备份，将欲长期保存之记录数据储存到 File Server、NAS、Samba Server、Windows 网络芳邻…等备份设备中，来达到空间无上限及长期保存的效果。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 有规划的实时通讯控管，也可有效预防病毒入侵

信息科技发达的时代下，网络病毒层出不穷，几乎只要有牵扯到网络的东西，都会有病毒的踪影出现，而利用病毒来达到入侵、窃取及破坏的事件也是持续不断的在发生。然而，近期发现新型态的窃取数据犯罪手法，是一种黑客控制傀儡网络的新方式。

对于现在大多数人仰赖实时通讯软件便利的情况下，越来越多黑客开始透过植入实时通讯机器人程序（Bot，也称为傀儡程序），此方式让黑客可随心所欲的利用下达相关指令来偷取使用者计算机中的数据、回传该台计算机上的所有文件，甚至是使用者目前正在操作中的计算机屏幕截图；使用者计算机将完全赤裸裸的呈现给欲窃取文件数据的有心人士。对公司而言遭受入侵所造成的影响，情况小的可能是计算机设备系统被破坏，因此使得公司无法正常的照进度营运，情况大的则可能发生公司内部相关机密被窃取，甚致因此而损失掉巨额的商机。

此种病毒的传播路径依旧是透过软件的各种漏洞、植入各种后门程序，或者是透过恶意连结及利用文件传送的方式让使用者下载并安装此类恶意程序。因此，实时通讯软件就成了最佳传播途径之。

在面对实时通讯软件病毒如此泛滥的问题，身为公司管理人员又该如何去处理呢？就目前现况而言，公司内部人数众多的环境下，最佳解决办法就是有效的控管底下使用者对于网络实时通讯软件的使用，藉此来预防及降低病毒入侵的机率。公司倘若不能够有效的控管内部实时通讯软件的使用，及在使用上规则的限制时，相对的就必须得承担随时突然发生病毒藉由实时通讯软件此种管道入侵的风险。

但公司内部员工的人数众多，对于网络通讯软件的使用需求又不尽然的全都相同。内部人员、部门有些是完全不必要用到网络通讯软件，但有些部门或是特定人事必需开放使用实时通讯软件来跟外部子公司或是客户间作联系，因此而无法做到全面性顾及的限制，但却又不能因此而放任所有人员去滥用实时通讯软件，甚至是任意藉此做文件的传输动作…等，管理人员又该如何去限制及规范？

新软系统『网络记录器-IR』，便可以轻松的解决相关的问题，网络记录器-IR 除了拥有详细的记录内容、简单易懂的操控接口，更是支持了市面上多数通讯软件的控管机制，并且还可细分是否允许登、是否允许传档、仅允许使用未加密之实时通讯软件及仅允许使用通过认证的实时通讯软件…等设计，让管理者能应付各种不同的使用者需求，同时还支持 Web IM 的相关管制与使用。除此之外，新软系统 IR 对于实时通讯软件是利用软件中的特征码来进行阻挡及控管，因此能达到高准确率管制效果。

对于不同部门、不同人员，不同的需求下，管理人员只需要搭配利用 IR 中所内建的群组功能、认证管理功能来加以应用，即可针对不同部门、不同人员来做到不同的限制控管规则，有效的帮助公司轻松的解决实时通讯控管的种种问题，同时也帮助公司创造一个良好、有规律的网络使用环境，帮助公司带来丰厚的商机及减少员工利用实时通讯软件摸鱼的情况。让管理人员可轻松掌握整个企业网络的实时通讯。

目前所支持的 IM 应用程序		
可记录内容	阻挡登入	阻挡文件传输
MSN	MSN	MSN
Yahoo Messenger	Yahoo Messenger	Yahoo Messenger
QQ	QQ	QQ
ICQ	ICQ	ICQ
AIM	AIM	AIM
Gadu-Gadu	Gadu-Gadu	Gadu-Gadu
Skype	Skype	Google Talk
官方 Web MSN	Google Talk	
目前可阻挡的 Web IM 网站		
官方 Web MSN、Buddy、I Love IM、Meebo、IM haha、Kool IM、Messenger FX、Communication Tube、IMUnitive、Goowy、MSN2Go、TotMoMo、Mabber、Wablet、Mobile、webQQ. . . 等		

网路记录器实时通讯支援表格

	MSN	Yahoo	QQ	ICQ/AIM	Skype	Gadu-Gadu	Google Talk
仅允许使用未加密之即实通讯软件	○	–	–	–	–	○	–
仅允使用认证成功且未加密即实通讯软件	○	–	–	–	–	○	–
仅允许使用通过认证的即实通讯软件	○	○	○	○	–	○	–
全部允许使用即实通讯软件	○	○	○	○	○	○	○
全部禁止使用即实通讯软件	○	○	○	○	○	○	○
仅允许使用密码正确的即实通讯软件	–	–	○	–	–	–	–
仅允许使用认证成功且密码正确之即时通讯软件	–	–	○	–	–	–	–
仅允许安装“外挂辅助程序”之计算机	–	–	–	–	○	–	–
仅允许使用官方版本 Web IM	○	–	–	–	–	–	–
允许使用 Web IM	○	○	○	○	–	–	–
禁止使用 Web IM	○	○	○	○	–	–	–
实时通讯软件文件传输管理	○	○	○	○	–	○	○

实时通讯软件支持管理菜单

『实时通讯文件传输管理』（仅适用於网络记录器采用桥接方式架设）

文 陈殿鸿 kim@nusoft.com.tw