

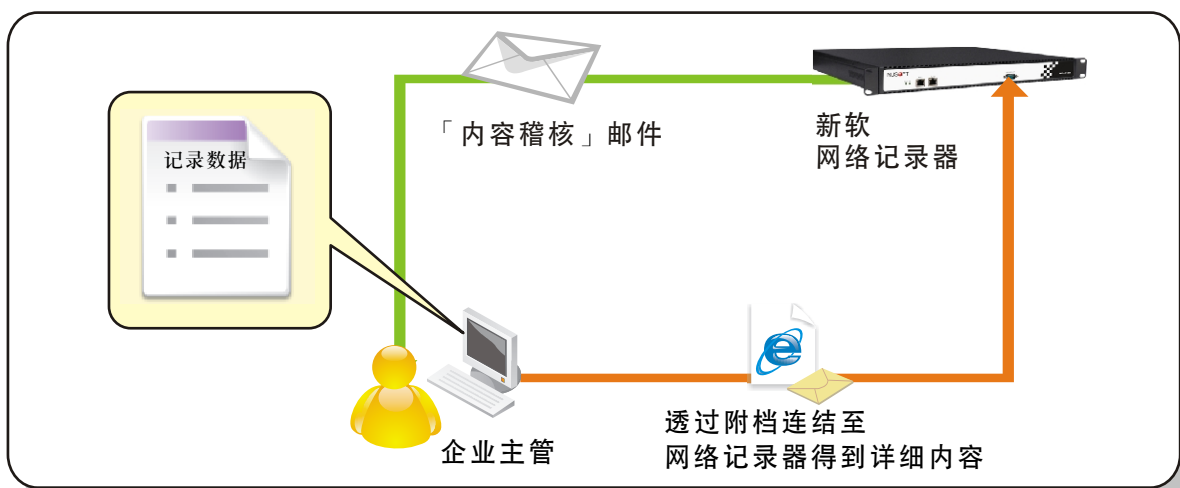
## 网络记录器 / IR 系列报导

### 技术浅谈与应用 - 记录数据不必找，「内容稽核」自动呈上来

目前有越来越多的企业在内部架设网络记录器，不论是为了监督员工网络行为、防止企业机密外泄或者备份企业往来邮件...等目的，最终都是为了所需要的那几笔记录数据，但是网络记录器所记录的是全公司的网络行为呀，在记录器里找寻需要的记录数据就有如大海捞针一般十分困难，虽然可利用搜寻功能找出记录数据，不过这还得进入系统耗费一些时间呢，而且若之后有相关的记录需要查核，就必须再做一次相同的搜寻动作，然而每天都做相同的动作何不让系统自行来做呢。

为此新软网络记录器在最新的韧体版本中新增「内容稽核」功能，可按需求在稽核条例中设定搜寻的服务种类、使用者名称、传输方向...等参数（关键词 / 字符串），系统将根据稽核条例中的设定，自动于每天凌晨 0 点 30 分搜寻前一天的记录数据，并将这些符合稽核规则的数据以附电子邮件的方式寄送给特定的收件者，收件者收到附有 HTML 文件的邮件后，便可从邮件附档中所提供的连结查看详细的记录内容。简单的说，「内容稽核」就是代替使用者每天搜寻特定记录数据的功能，这对于忙碌的主管来说，每天例行性的记录筛检也就轻松了许多。

举例来说，假使目前公司正准备进行一场获利可观的标案，为了防范内神通外鬼将投标金额泄漏给竞争对手，项目主管可在「内容稽核」中设定稽核规则，使网络记录器自动于每天凌晨，把含有与标案相关的文字或投标金额的记录数据皆筛选出来，以邮件的方式寄送给主管查看，当主管收到此邮件时，再藉由邮件中所夹带的 HTML 文件浏览记录，并进一步从文件中的连结联机至网络记录器而得到详细的记录内容，如此一来不需再花费多余的精神进入系统中查寻记录，只要每天接收邮件就能确保投标计划是否遭到泄密，大大省去每天巡察记录的时间。



这看似平凡的「内容稽核」却是企业主管例行性查核记录的一大利器，而这新功能所带来的便利，只有等新版本的韧体发布后，使用过的人才能体会的到。

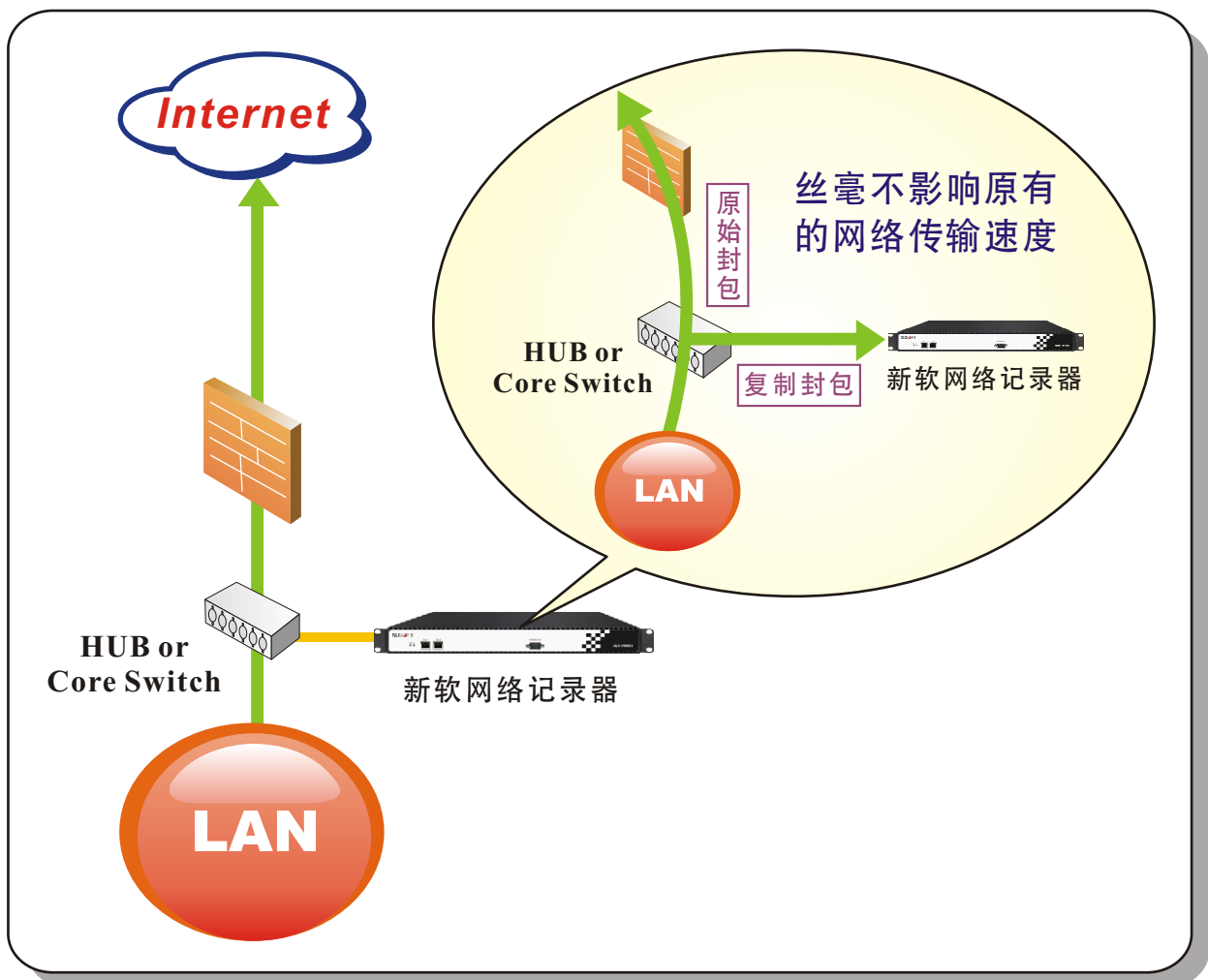
	旧有的记录「搜寻」功能	新增的「内容稽核」功能
可分析的记录种类	SMTP、POP3/IMAP、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET	SMTP、POP3/IMAP、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET
搜寻方式	使用者每日手动搜寻	系统根据稽核规则每日自动搜寻
显示方式	立即显示于操作介面	每天凌晨 0 点 30 分以附档邮件寄出
显示内容	依照所选择的日期	前一天的记录数据
方便性	对于立即需要查阅记录数据的使用者较为方便	对于每天需例行性查阅数据的使用者较为方便

文  黄智杰 alex@nusoft.com.tw

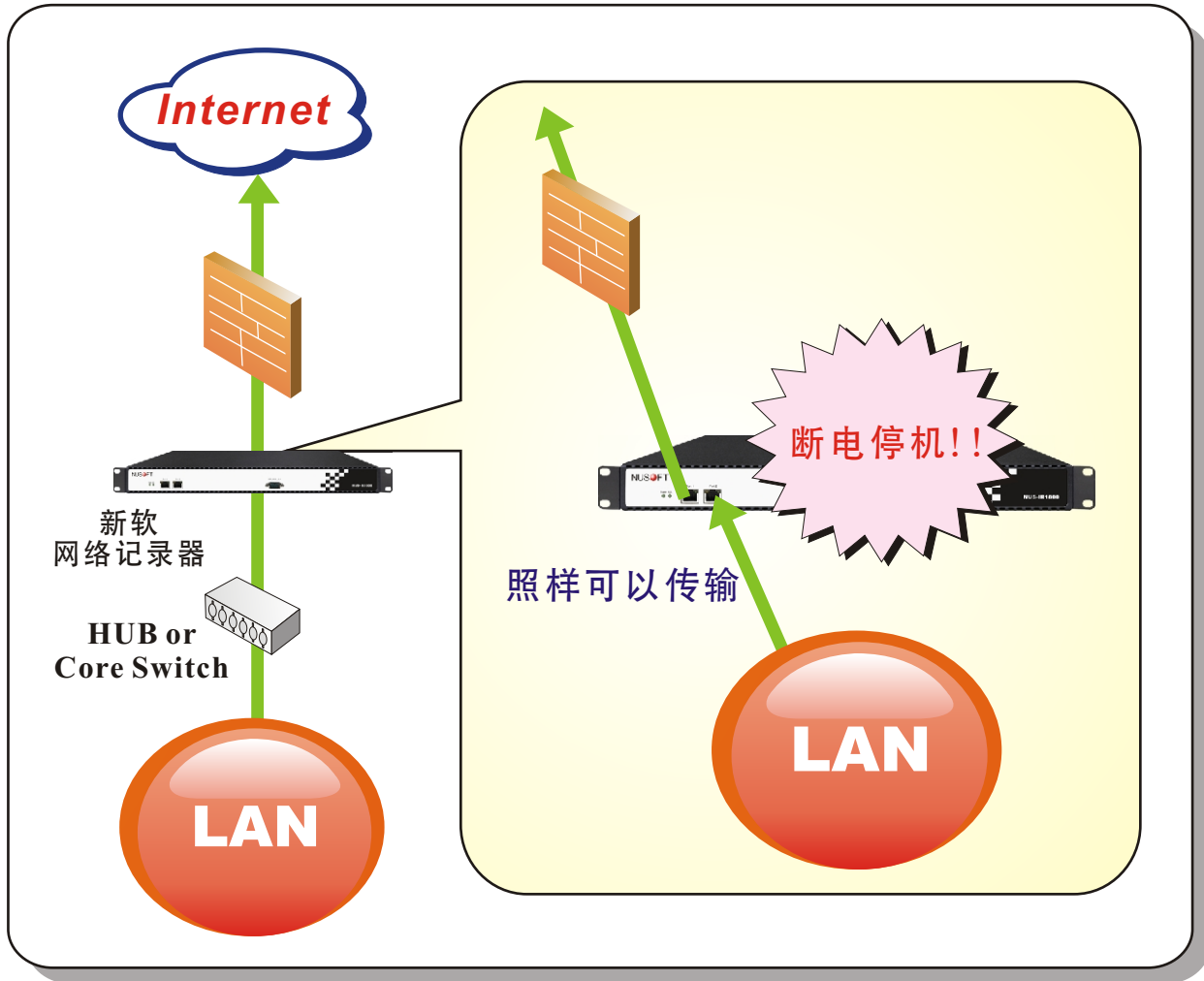
## 市场营销报导 - 网络记录器会影响企业网络的运作吗

许多企业为了记录企业内部网络活动情况，以确保信息安全并遏止员工滥用网络资源，通常会考虑在企业网络里架设网络记录器，但在购买网络记录器之前，往往心中都有一个疑虑，担忧一旦架设网络记录器便会影响网络的传输速度。

其实不然，以旁接方式架设网络记录器，进出企业网络的封包皆会复制一份传给网络记录器做为记录，而原来的封包在传输上并不会因网络记录器有任何的影响或停顿，所以并不会因为在固有的网络架构中架设网络记录器就造成线路壅塞，此外就算网络记录器故障甚至端口孔锈蚀损坏，也都丝毫不会影响企业网络原有的运作。



而另一方面企业更害怕的是万一以桥接的方式架设网络记录器，万一设备当机或是故障断电的时候，企业网络不就完全停摆了吗？对此新软网络记录器不仅在设备当机会自动重启系统回复原来的运作，也因新软网络记录器支持 By Pass 机制，就算设备故障断电也能让往来频繁的封包顺利通过，维持企业网络正常运行。



文  黄智杰 alex@nusoft.com.tw