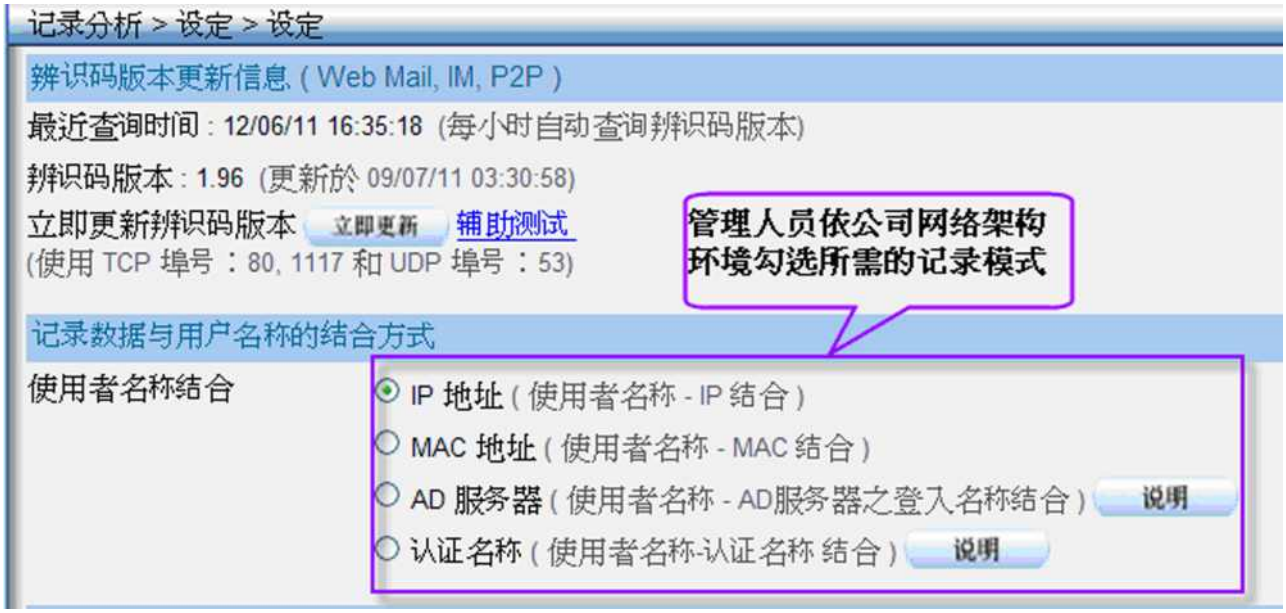
新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2012/1/1-2012/1/15 第135期

网络记录器 / IDR系列报导

新软网络记录器提供各种数据整合方式，适用各企业环境。

因特网已是现代社会在商业及生活上不可或缺的工具，带给企业不少商机，但也为员工带来了一个方便摸鱼的管道，举凡实时通讯聊天、传送私人电子邮件等各种损害企业利益，以及网络资源的网络行为相对地也日益遽增。因此现代的公司为了保护自身企业财产安全以及有效提升公司运作生产力，纷纷采购“网络侧录设备”，藉以来协助企业达到有效保护、提升产能之目的。

网络架构环境越来越复杂，管理人员有限的双眼并无法及时地监看无限的网络，惟有选择正确的网络侧录设备才能够帮助网络管理者、企业经营者，以最精简的人力及最少的时间下满足完整的记录存证与资安方面的需求。新软系统『网络记录器-IDR系列』除了提供常用的『By IP』、『By MAC』两种记录模式来记录使用者上网之内容外，尚还有针对拥有AD Server的企业所提供之『By AD Server』模式，以及适合用于中小型企业的记录依据模式－『By Authentication names』模式，让管理人员能够有效率的为公司选择最适当的记录模式。



图一　四种记录数据与使用者整合方式的UI接口操作

依IP地址记录模式(By IP Addresses)

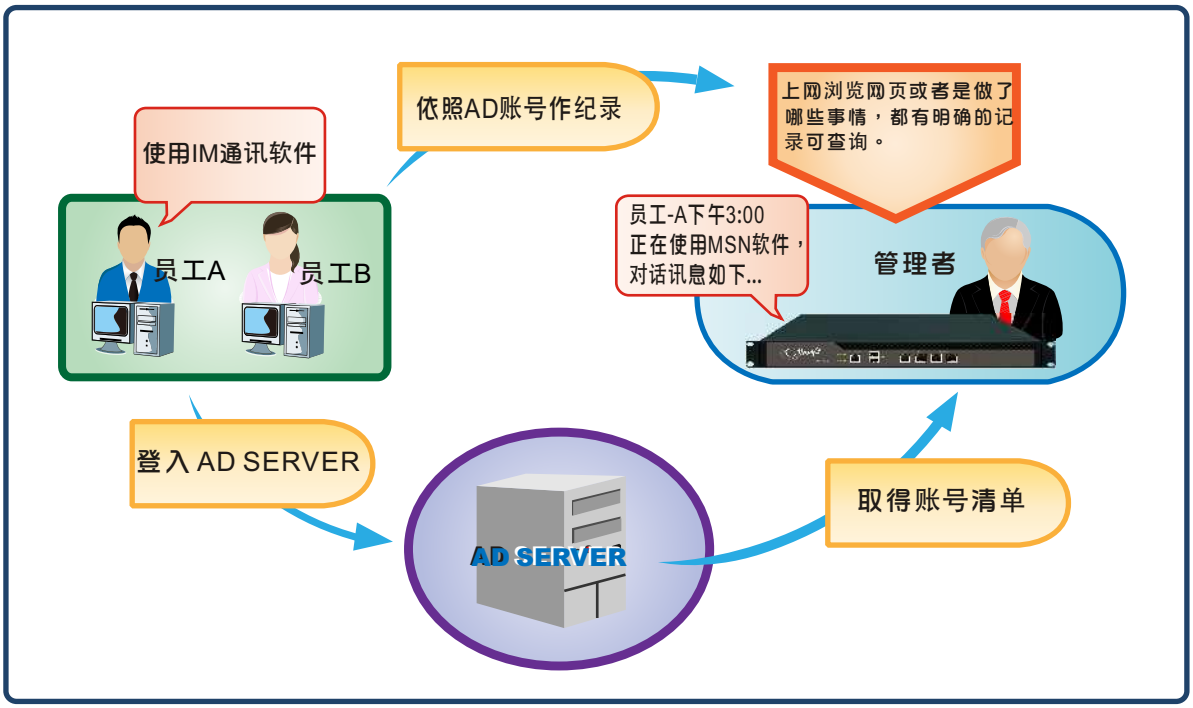
以每位使用者的IP地址做为纪录数据的依据，适用于企业内部的网络环境为固定IP分配。倘若使用者所使用的IP可任意作变更，或是所使用为浮动式IP(使用DHCP)情况下，采用此种模式时易发生所记录下的内容不易分辨该项记录IP当时为谁所使用，导致误判的情形增加。

依MAC地址记录模式(By MAC Addresses)

针对上述问题，管理人员采用使用者之MAC地址做为记录数据的依据，可有效避免有心人士任意变换IP逃避查缉的问题发生，适用于企业内部使用者随意变更IP，IP为非固定使用(如：DHCP)。若企业内部网络环境有架设路由器时，则透过路由器传递的封包其MAC会被路由器之MAC取代，所以网络记录器的记录基准需采用IP记录模式，才不会发生路由器后端使用者上网记录错误的情况。

依AD服务器记录模式(By AD Server)

对于部份企业已经拥有AD Server的网络环境，选取AD Server记录模式，能够有效将其『网络记录器 - IDR』之记录依据结合企业内部所架设的AD Server；若使用者名单有所变动时(如：新进员工、员工离职…等)，也只需更改AD Server中的设定，而『网络记录器』上的记录就跟着改变，完全不用管理人员再费时于机器设备上调整与变动。



图二　藉由AD Server登入账号记录所有上网记录

管理人员要如何才有办法使用『网络记录器 - IDR』来与企业的AD Server作结合运用呢？当『网络记录器』以使用者的AD Server之登入名称做为记录数据的依据时，需搭配系统中所另附之外挂辅助程序「IR_Plugin」使用，利用「IR_Plugin」来统整结合AD Server上使用者的账号数据。

依认证名称记录模式(By Authentication names)

若公司规模为中小型企业且经费有限，但是又希望能够做到类似AD Server如此方便的账号管理方式，则可使用新软系统『网络记录器 - IDR』所提供的『认证名称』记录方式。此记录模式仅适用于『网络记录器』采用Bridge模式架设时使用。当管理人员启用『认证名称』记录模式时，使用者如欲上网，必须先通过系统认证(符合IDR内建认证表的账号，或与外部结合之RADIUS、POP3、LDAP Server中的账号之一)方能使用网络服务，网络记录器则会以使用者所输入的认证账号来做为记录之依据。

	By IP	By MAC	By AD server	By 认证名称
记录方式	依照使用者计算机的『IP』作为记录依据。	依使用者计算机上网卡的『MAC』作为记录依据。	与企业的AD服务器结合，并依『AD Server』内的账号作为依据。	依照使用者所『认证通过』的账号(名称)作为依据。
适用环境	使用固定IP之企业网络环境。	使用固定IP、浮动IP(DHCP)之企业网络环境。	企业内部有架设AD Server之网络环境。	无架设AD服务器网络环境之中小型企业。
注意	使用者任意变更其使用IP或浮动IP(DHCP)时，不建议使用该模式。	若封包之传递有透过路由器时其MAC会被路由器之MAC取代，不建议使用此模式。	需搭配『外挂辅助程序-IR_Plugin』配合使用。	此记录模式仅适用于『网络记录器』采用Bridge模式架设时使用。
备注	当企业网络内部有使用路由器时必须使用By IP模式。	可有效避免有心人士任意变换IP逃避查缉的问题发生。	以AD服务器内之账号为记录依据，可正确记录使用者的上网内容。	以「认证名称(账号)」为记录依据，可正确记录使用者的上网内容。

表一　各种记录依据比较表

文 余光明 kongmeng@nusoft.com.tw