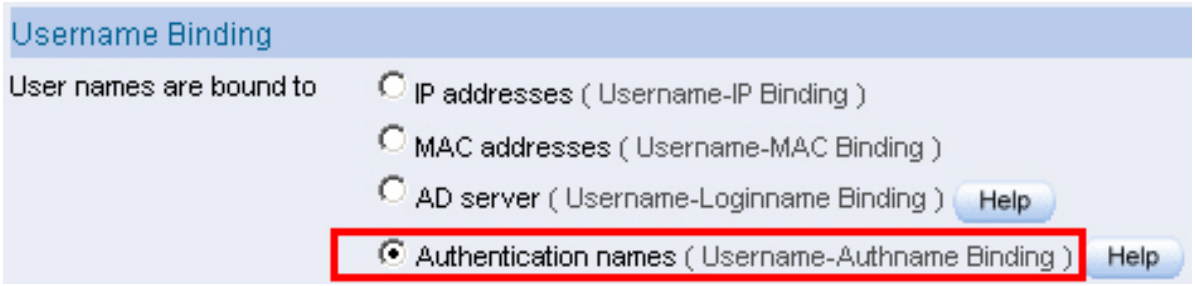
新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/6/15- 2009/6/28 第94期

网络记录器 / IR系列报导

技术浅谈与应用 - ”使用者名称 - 认证名称 结合”记录方式

为了能更有效的管理及规范内部员工的因特网使用行为，网络记录器早已经是公司、企业所广为使用的侧录设备。对于资安方面而言，网络记录设备中的各项记录，举凡讯息传递、实时通讯、电子邮件…等，于现今社会中仍然是项重要的凭证依据，所以能够选择正确的网络侧录设备才能有效帮助网络管理者、企业经营者，满足记录存证方面之需求。

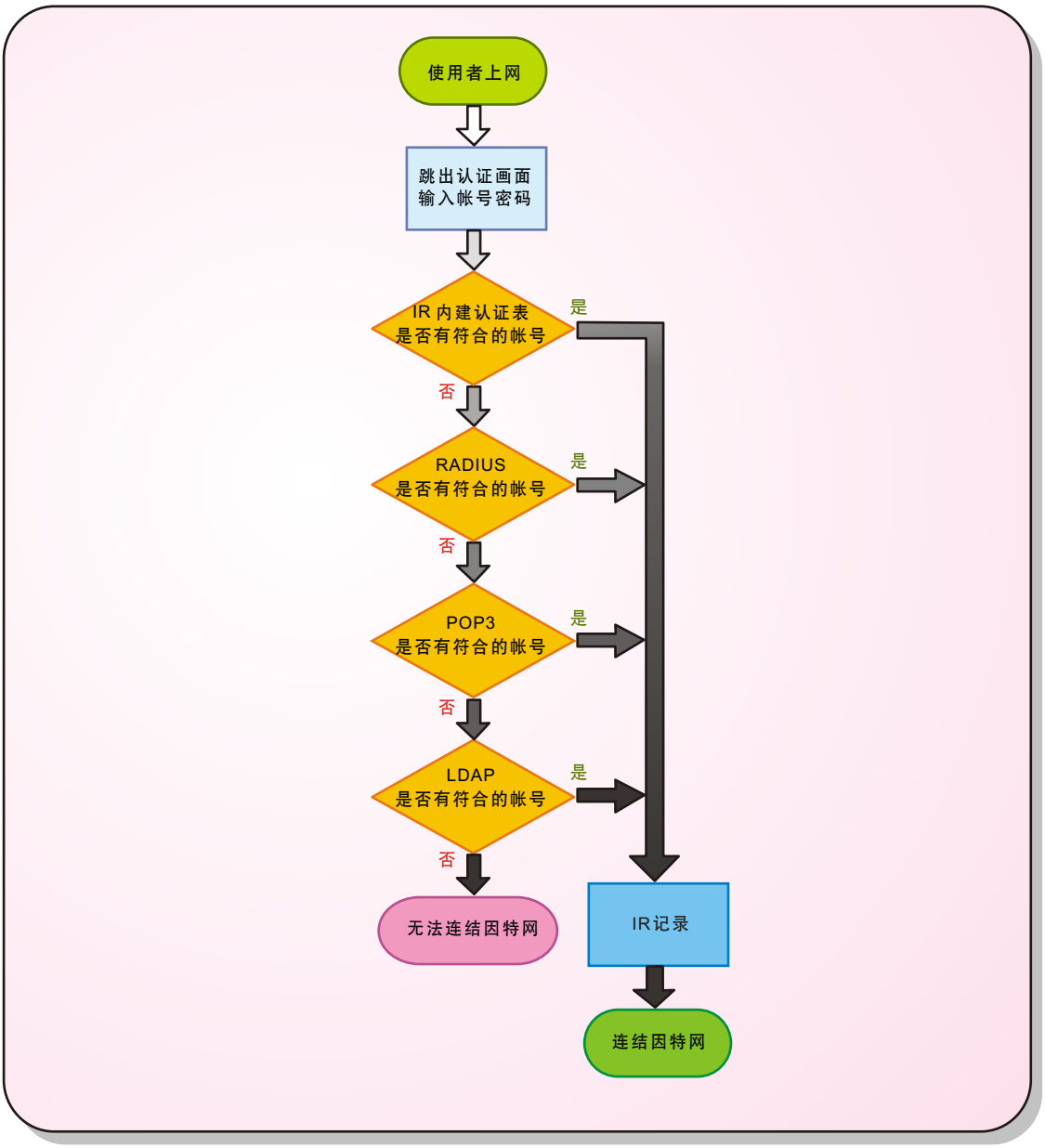
而网络记录设备中所记录下的内容，当然也必须清楚且完整的标示出该项记录为何人所使用，如此一来所记录的内容才能成为有力的证据。新软系统网络记录器-IR上，新增了新的使用者记录方式『认证名称』记录模式，此记录模式是将使用者所使用的认证账号来做为记录之依据。而认证的账号来源可分别为『网络记录器-IR』中管理人员所设定之内建认证表里的使用者账号，以及外部 POP3 Server、RADIUS Server、LDAP Server 上使用者的账号，来做为通过此项机制的认证账号。



认证名称记录模式功能选项截图

当管理人员在启用『认证名称』记录模式后，假如使用者要进行连上因特网的动作时，必须先要通过系统之认证后才能正常连上因特网及使用网络上之各项服务。而当使用者所使用的其中一种账号(IR 内建认证表、POP3、RADIUS、LDAP)来登入并且连上因特网后，网络记录器则会以使用者所输入的认证账号来作为记录之依据。

该项认证记录模式，使用者认证账号的搜寻优先级则是依照：IR 内建认证表(Auth user) → RADIUS → POP3 → LDAP。当发生有相同名称账号情况时，例如：内建认证表中设有“ABC”这个使用账号，而 POP3 中也同样有位使用者账号为“ABC”，当使用者要用该账号登入时，系统会依照先搜寻到的账号为使用者登入的依据，换句话说 IR 内建认证表(Auth user)优先权大于 POP3，所以在使用“ABC”这个账号做认证时，必须输入 IR 内建认证表(Auth user)中的账号 & 密码做登入认证，而无法使用 POP3 中的账号 & 密码做登入认证。特别需要注意的地方则是，此种记录模式仅适用于网络记录器采用 Bridge 模式架设时使用。



认证流程示意图

管理人员也可自行设定联机闲置时间，让没在持续进行联机行为的使用账号，于限定之时间到达时，系统会自动将该账号注销，以防遭有心人事盗用。对于特定的使用者 or 机器(如：公司内部所架设之邮件服务器)而言，管理人员可将其 IP 位置输入免认证列表中，让该使用者 or 机器设备不需经过认证即可联机至因特网。但特别要注意的是设定于免认证列表上的使用者, 往后所有上网动作，在网络记录器-IR 上的记录皆会以 IP 为主。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 新软网络记录器 - 新增「认证上网」新机制

随着时代的变迁，现代人使用网络已经成为生活中不可或缺的一种习惯，也渐渐的变成一种依赖，这样依赖的习惯也不知不觉中带入了公司的工作环境里。然而在上班中使用网络偷上网对企业来说，不但是资源公器私用、上班不专心降低工作产能更是有使公司机密外流的可能发。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，纷纷采购相关“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。

但是一家公司内所架设的网络设备一定不会只有一台网络侧录设备，林林总总的服务器所使用的账号数量将不在少数，因此现在许多大型公司企业为了达到以「人」为本的管理需求，皆在公司里架设 AD Server，来进行所有员工的使用账号管理。然而，若公司规模属于中小型企业且相关经费有限，但是又希望能够做到类似 AD Server 如此方便的账号管理方式，该如何才能实现此类企业需求？

一般市面上的网络侧录设备，所提供之记录依据不外乎只有「By IP」、「By MAC」两种记录模式来记录使用者上网之内容。而新软系统网络记录器除了此两种记录模式外，尚还有针对拥有AD Server 的企业所提供之「By AD」模式。但是若像无 AD Server 之中小型企业用户的话，目前新软系统在 v5. 05 新版本上新增适合用于中小型企业的记录依据模式－「认证模式」。此记录方式适用于 IR 网络记录器采用 Bridge 模式架设时使用。当启用此记录方式，使用者如欲上网，必须先通过系统认证（可使用内建的认证表 Auth User 或是使用与外部结合之 RADIUS、POP3、LDAP Server）方能使用网络服务。而网络记录器将会以使用者的认证账号作为记录之基准。不仅可以排除「By IP」与「By MAC」两种记录模式下，使用者上网身份常被冒用的情形；也让许多中小企业在实施账号管理上，确实做到以「人」为本的政策推行。

记录依据	By IP	By MAC	By AD	By 认证
记录方式	依照使用者计算机之「IP」作为记录依据	依照使用者计算机上网卡的「MAC」作为记录依据	与企业之AD server结合，并依照「AD server」内的帐号作为记录依据	依照所「认证通过」的帐号作为记录依据
适用环境	适合每人配发固定IP	固定 IP、采用 DHCP 之浮动 IP	公司内部有架设 AD server 之环境	无架设 AD 服务器环境之中小型企业
备□□注	可能会发生使用者冒用他人计算机 IP 上网，冒充其上网内容	若电脑遭他人使用，则记录到的上网内容将不会是原使用者的记录	以「AD server 内之帐号」为记录依据，可正确记录使用者的上网内容	以「认证帐号」为记录依据，可正确记录使用者的上网内容

各种记录依据比较表

新软系统在「IR 网络记录器」系列产品里，秉持着“不断进步、永续经营”的理念持续成长，搜集目前市场上一些主流的新趋势走向，进而以现代企业所有可能需求的环境为架构，设计出贴心又实用的记录功能，一步一步的走在信息安全的前端，成为领导市场需求的主流。

文 黄政铭 ming@nusoft.com.tw