新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/6/15- 2009/6/28 第94期

## 網路記錄器 / IR 系列報導

# 技術淺談與應用 - "使用者名稱-認證名稱 結合" 記錄方式

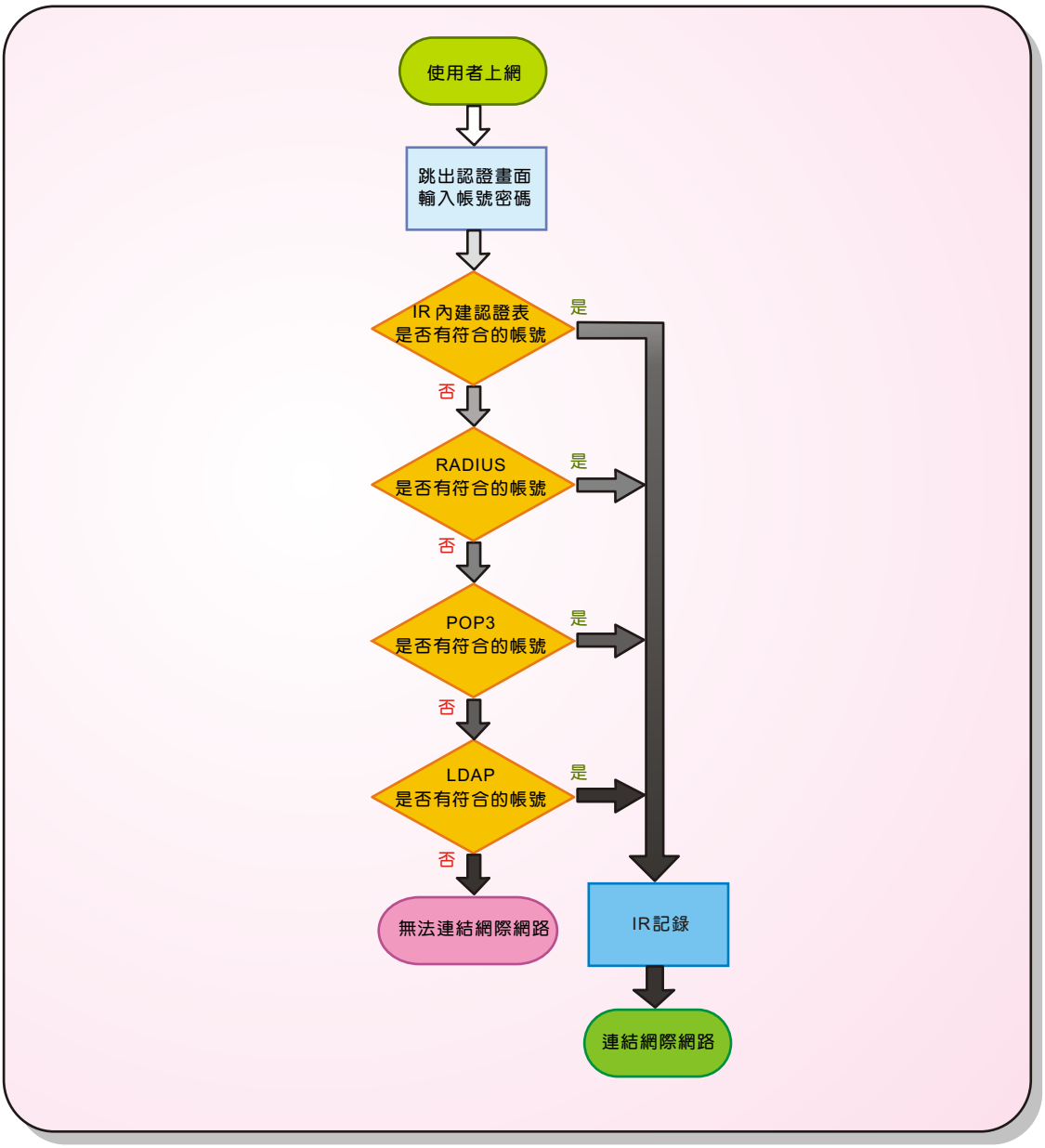
為了能更有效的管理及規範內部員工的網際網路使用行為，網路記錄器早已經是公司、企業所廣為使用的側錄設備。對於資安方面而言，網路記錄設備中的各項記錄，舉凡訊息傳遞、即時通訊、電子郵件…等，於現今社會中仍然是項重要的憑證依據，所以能夠選擇正確的網路側錄設備才能有效幫助網路管理者、企業經營者，滿足記錄存證方面之需求。

而網路記錄設備中所記錄下的內容，當然也必須清楚且完整的標示出該項記錄為何人所使用，如此一來所記錄的內容才能成為有力的證據。新軟系統網路記錄器-IR上，新增了新的使用者記錄方式『認證名稱』記錄模式，此記錄模式是將使用者所使用的認證帳號來做為記錄之依據。而認證的帳號來源可分別為『網路記錄器-IR』中管理人員所設定之內建認證表裡的使用者帳號，以及外部POP3 Server、RADIUS Server、LDAP Server 上使用者的帳號，來做為通過此項機制的認證帳號。


認證名稱記錄模式功能選項截圖

當管理人員在啟用『認證名稱』記錄模式後，假如使用者要進行連上網際網路的動作時，必須先要通過系統之認證後才能正常連上網際網路及使用網路上之各項服務。而當使用者所使用的其中一種帳號(IR 內建認證表、POP3、RADIUS、LDAP)來登入並且連上網際網路後，網路記錄器則會以使用者所輸入的認證帳號來作為記錄之依據。

該項認證記錄模式，使用者認證帳號的搜尋優先順序則是依照：IR 內建認證表(Auth user) → RADIUS → POP3 → LDAP。當發生有相同名稱帳號情況時，例如：內建認證表中設有 “ABC” 這個使用帳號，而 POP3 中也同樣有位使用者帳號為 “ABC” ，當使用者要用該帳號登入時，系統會依照先搜尋到的帳號為使用者登入的依據，換句話說 IR 內建認證表(Auth user)優先權大於POP3，所以在使用 “ABC” 這個帳號做認證時，必須輸入 IR 內建認證表(Auth user)中的帳號 & 密碼做登入認證，而無法使用 POP3 中的帳號 & 密碼做登入認證。特別需要注意的地方則是，此種記錄模式僅適用於網路記錄器採用 Bridge 模式架設時使用。




認證流程示意圖

管理人員也可自行設定連線閒置時間，讓沒在持續進行連線行為的使用帳號，於限定之時間到達時，系統會自動將該帳號登出，以防遭有心人事盜用。對於特定的使用 or 機器(如：公司內部所架設之郵件伺服器)而言，管理人員可將其 IP 位置輸入免認證列表中，讓該使用者 or 機器設備不需經過認證即可連線至網際網路。但特別要注意的是設定於免認證列表上的使用者，往後所有上網動作，在網路記錄器-IR上的記錄皆會以 IP 為主。

文 陳殿鴻 kim@nusoft.com.tw

## 市場行銷報導 - 新軟網路記錄器- 新增「認證上網」新機制

隨著時代的變遷，現代人使用網路已經成為生活中不可或缺的一種習慣，也漸漸的變成一種依賴，這樣依賴的習慣也不知不覺中帶入了公司的工作環境裡。然而在上班中使用網路偷上網對企業來說，不但是資源公器私用、上班不專心降低工作產能更是有使公司機密外流的可能發。因此現代的公司為了保護自身企業財產安全以及有效提升公司運作生產力，紛紛採購相關“網路側錄設備”，藉以來協助企業達到“有效保護、提升產能”之目的。

但是一家公司內所架設的網路設備一定不會只有一台網路側錄設備，林林總總的伺服器所使用的帳號數量將不在少數，因此現在許多大型公司企業為了達到以「人」為本的管理需求，皆在公司裡架設 AD Server，來進行所有員工的使用帳號管理。然而，若公司規模屬於中小型企業且相關經費有限，但是又希望能夠做到類似 AD Server 如此方便的帳號管理方式，該如何才能實現此類企業需求？

一般市面上的網路側錄設備，所提供之記錄依據不外乎只有「By IP」、「By MAC」兩種記錄模式來記錄使用者上網之內容。而新軟系統網路記錄器除了此兩種記錄模式外，尚還有針對擁有 AD Server 的企業所提供之「By AD」模式。但是若像無 AD Server 之中小型企業用戶的話，目前新軟系統在 v5.05 新版本上新增適合用於中小型企業的記錄依據模式－「認證模式」。此記錄方式適用於 IR 網路記錄器採用 Bridge 模式架設時使用。當啟用此記錄方式，使用者如欲上網，必須先通過系統認證（可使用內建的認證表 Auth User 或是使用與外部結合之 RADIUS、POP3、LDAP Server）方能使用網路服務。而網路記錄器將會以使用者的認證帳號作為記錄之基準。不僅可以排除「By IP」與「By MAC」兩種記錄模式下，使用者上網身份常被冒用的情形；也讓許多中小企業在實施帳號管理上，確實做到以「人」為本的政策推行。

| 記錄依據 | By IP | By MAC | By AD | By 認證 |
|---|---|---|---|---|
| 記錄方式 | 依照使用者電腦之「IP」作為記錄依據。 | 依照使用者電腦上網卡的「MAC」作為記錄依據。 | 與企業之AD server結合，並依照「AD server」內的帳號作為記錄依據。 | 依照所「認證通過」的帳號作為記錄依據。 |
| 適用環境 | 適合每人配發固定IP | 固定IP、採用DHCP之浮動IP | 公司內部有架設AD server之環境 | 無架設AD伺服器環境之中小型企業 |
| 備　　註 | 可能會發生使用者冒用他人電腦IP上網，冒充其上網內容。 | 若電腦遭他人使用，則記錄到的上網內容將不會是原使用者的記錄。 | 以「AD server內之帳號」為記錄依據，可正確記錄使用者的上網內容。 | 以「認證帳號」為記錄依據，可正確記錄使用者的上網內容。 |

各種記錄依據比較表

新軟系統在「IR 網路記錄器」系列產品裡，秉持著“不斷進步、永續經營”的理念持續成長，蒐集目前市場上一些主流的新趨勢走向，進而以現代企業所有可能需求的環境為架構，設計出貼心又實用的記錄功能，一步一步的走在資訊安全的前端，成為領導市場需求的主流。

文 黃政銘 ming@nusoft.com.tw