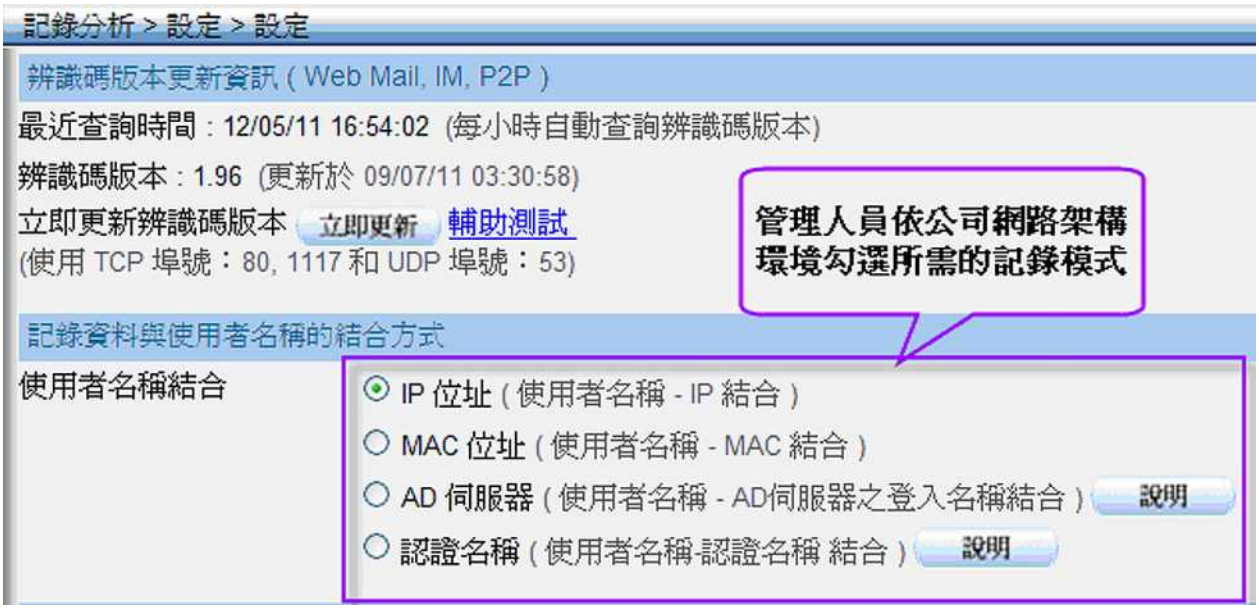
新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2012/1/1-2012/1/15 第135期

網路記錄器 / IDR 系列報導

新軟網路記錄器提供各種資料整合方式，適用各企業環境

網際網路已是現代社會在商業及生活上不可或缺的工具，帶給企業不少商機，但也為員工帶來了一個方便摸魚的管道，舉凡即時通訊聊天、傳送私人電子郵件等各種損害企業利益，以及網路資源的網路行為相對地也日益遽增。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“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。

網路架構環境越來越複雜，管理人員有限的雙眼並無法及時地監看無限的網路，惟有選擇正確的網路側錄設備才能夠幫助網路管理者、企業經營者，以最精簡的人力及最少的時間下滿足完整的記錄存證與資安方面的需求。新軟系統『網路記錄器-IDR系列』除了提供常用的『By IP』、『By MAC』兩種記錄模式來記錄使用者上網之內容外，尚還有針對擁有AD Server的企業所提供之『By AD Server』模式，以及適合用於中小型企業的記錄依據模式－『By Authentication names』模式，讓管理人員能夠有效率的為公司選擇最適當的記錄模式。



圖一　四種記錄資料與使用者整合方式的UI介面操作

依IP位址記錄模式(By IP Addresses)

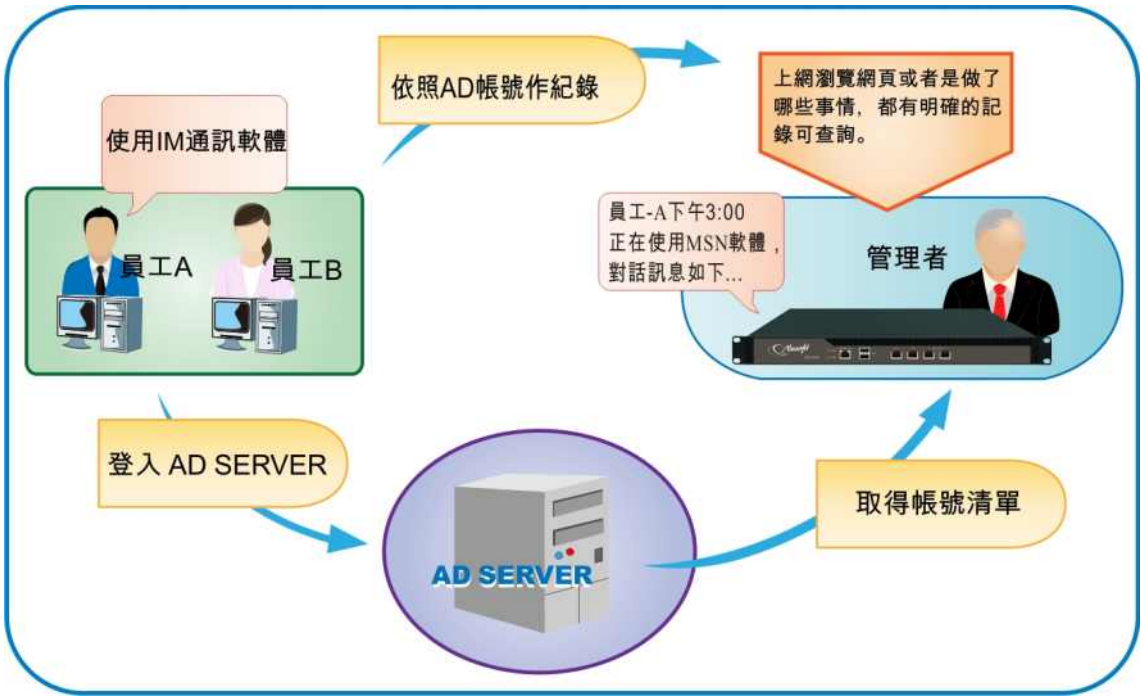
以每位使用者的IP位址做為紀錄資料的依據，適用於企業內部的網路環境為固定IP分配。倘若使用者所使用的IP可任意作變更，或是所使用為浮動式IP(使用DHCP)情況下，採用此種模式時易發生所記錄下的內容不易分辯該項記錄IP當時為誰所使用，導致誤判的情形增加。

依MAC位址記錄模式(By MAC Addresses)

針對上述問題，管理人員採用使用者之MAC位址做為記錄資料的依據，可有效避免有心人士任意變換IP逃避查緝的問題發生，適用於企業內部使用者隨意變更IP，或IP為非固定使用(如：DHCP)。若企業內部網路環境有架設路由器時，則透過路由器傳遞的封包其MAC會被路由器之MAC取代，所以網路記錄器的記錄基準需採用IP記錄模式，才不會發生路由器後端使用者上網記錄錯誤的情況。

依AD伺服器記錄模式(By AD Server)

對於部份企業已經擁有AD Server的網路環境，選取AD Server記錄模式，能夠有效將其『網路記錄器 - IDR』之記錄依據結合企業內部所架設的AD Server；若使用者名單有所變動時(如：新進員工、員工離職…等)，也只需更改AD Server中的設定，而『網路記錄器』上的記錄就跟著改變，完全不用管理人員再費時於機器設備上調整與變動。



圖二 藉由AD Server登入帳號記錄所有上網記錄

管理人員要如何才有辦法使用『網路記錄器 - IDR』來與企業的AD Server作結合運用呢？當『網路記錄器』以使用者的AD Server之登入名稱做為記錄資料的依據時，需搭配系統中所另附之外掛輔助程式「IR_Plugin」使用，利用「IR_Plugin」來統整結合AD Server上使用者的帳號資料。

依認證名稱記錄模式(By Authentication names)

若公司規模為中小型企業且經費有限，但是又希望能夠做到類似AD Server如此方便的帳號管理方式，則可使用新軟系統『網路記錄器 - IDR』所提供的『認證名稱』記錄方式。此記錄模式僅適用於『網路記錄器』採用Bridge模式架設時使用。當管理人員啟用『認證名稱』記錄模式時，使用者如欲上網，必須先通過系統認證(符合IDR內建認證表的帳號，或與外部結合之RADIUS、POP3、LDAP Server中的帳號之一)方能使用網路服務，網路記錄器則會以使用者所輸入的認證帳號來做為記錄之依據。

	By IP	By MAC	By AD server	By 認證名稱
記錄方式	依照使用者電腦的『IP』作爲記錄依據。	依照使用者電腦的『MAC』作爲記錄依據。	與企業的AD伺服器結合，並依『AD Server』內的帳號作為依據。	依照使用者所『認證通過』的帳號(名稱)作為依據。
適用環境	使用固定IP之企業網路環境。	使用固定IP、浮動IP(DHCP)之企業網路環境。	企業內部有架設AD Server之網路環境。	無架設AD伺服器網路環境之中小型企業。
注意	使用者任意變更其使用IP或浮動IP(DHCP)時，不建議使用該模式。	若封包之傳遞有透過路由器時其MAC會被路由器之MAC取代，不建議使用此模式。	需搭配『外掛輔助程式-IR_Plugin』配合使用。	此記錄模式僅適用於『網路記錄器』採用Bridge模式架設時使用。
備註	當企業網路內部有使用路由器時必須使用By IP模式。	可有效避免有心人士任意變換IP逃避查緝的問題發生。	以AD伺服器內之帳號爲記錄依據，可正確記錄使用者的上網內容。	以「認證名稱(帳號)」爲記錄依據，可正確記錄使用者的上網內容。

表一　各種記錄依據比較表

文 余光明 kongmeng@nusoft.com.tw