新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/12/28- 2010/1/10 第108期

網路記錄器 / IR 系列報導

技術淺談與應用 - 內容稽核的正規表示法使用方式

網路安全一直以來都是公司內部首要的課題之一，除了一般對外常用的資安設備之外，對內也漸漸的重視。正因為如此，不少公司紛紛導入網路側錄設備來管理內部資源，一方面可加強內部網路資訊的安全，另一方面也可管理員工於公司內的種種網路使用行為，更可有效降低員工利用上班時間來濫用網路資源之情況發生，藉此讓公司能夠達到更好的生產效益。

新軟系統所推出的網路記錄器 - IR，除了擁有強大側錄功能之外，還附有人性化及多元化的管理功能，可依照不同的環境來滿足管理人員不同之需求。但身為一個網路管理人員又該如何有效的在全公司大量且眾多記錄結果中，去找到符合公司需要、老闆需要、主管需要…等不同的記錄來做有效之存查及呈現呢？雖然管理人員可利用搜尋功能找出所需之記錄資料，不過這還得親自進入系統來耗費時間操作，倘若往後又有相關之記錄需要查核，就必須再做一次相同的搜尋動作，既然要如此不斷重覆相同搜尋動作，管理人員又該如何讓系統自行處理呢？

利用『內容稽核』功能可輕鬆分別針對 IR 所記錄的SMTP、POP3、HTTP / HTTPS、IM、Web SMTP、Web POP3、FTP、TELNET 資料內容設定相關的比對機制，完成特定所需審查傳送的文字、檔案…是否符合既定的網路安全政策。但重點在於管理人員所設定的稽核條件為何、是否能正確制定稽核條件，雖然該功能可直接使用輸入關鍵字來做為稽核條件的設定方式，但面對於需要較有變化性之稽核條件時，單純只利用關鍵字方式就顯的不是如此方便。因此管理人員則可進一步使用正規表示法來做為搜尋稽核的條件，藉此來達到更多樣變化之條件設定方式。

服務名稱	可支援使用正規表示法部份
SMTP	信件主旨、信件內容
POP3 / IMAP	信件主旨、信件內容
HTTP / HTTPS	網頁內容
IM	聊天內容
Web SMTP	信件主旨、信件內容
Web POP3	信件主旨、信件內容

『內容稽核』各服務內容可支援使用正規表示法部份

正規表示法（Regular Expression），是指透過一些特殊字元的排列，用以『搜尋/取代/刪除』一列或多列文字字串，而『內容稽核』該項功能則是利用來做為搜尋使用。但對於不常使用或不曾使用「正規表示法」的管理人員而言，較容易搞錯相關之字串意義及使用方式，所以以下將分別說明使用者較常使用之符號。

符號	說明	範例
^	代表啟始字元	^A 代表以 A 開頭的字串 Abc，Aaa。
$	代表結束字元	A$ 代表以 A 結尾的字串 bca，aaA
.	1.代表任意字元，但不包括換行字元 \n。 2. n 個 .表示任意 n 個任意字元 (注意: 並非任意長度的字串)。	a.b 代表 a 帶一個任意字元，後面接著一個 b，字串可以是 azb、aab、abb、a b 等，a 與 b 中間『一定』僅有一個字元，而空白字元也是字元。
\	將其後的字元跳脫，使其回歸原字元的涵義。	\. 代表將其後字元特殊符號『.』之特殊意義去除。此時的『.』代表條件是包含有『.』這個符號的字串，例如：www.tw.yahoo.com、168.95.1.1、…，而非其符號原本所代表的『任意字元』。
*	重複零個或多個的前一字元。	ess* 代表含有es, ess, esss 等等的字串(因為 * 可以是 0 個，所以 es 也是符合帶搜尋字串)。 * 為重複『前一個字元』的符號；因此，在 * 之前必須要緊接著一個字元(例如：a*)。
?	『零個或一個』的前一字元。	go?d 代表 gd，god 這兩個字串。o? 代表『空的或 1 個 o 』。

正規表示法符號列表

符號	說明	範例
[ ]	1. 代表在 [ ] 中一個會出現的字元	例 1：a[bc] 代表含有 ab 或 ac 的字串。 需特別留意的是，在 [ ] 當中『謹代表一個待搜尋的字元』，亦即 [bc] 代表 b 或 c 的意思。 例 2：[0-9] 代表含有任意數字的字串。在字元集合 [ ] 中的減號 - 是有特殊意義的，他代表介於兩個字元之間所有連續的字元（例如：所有大寫英文字元則為 [A-Z] 、所有小寫英文字元則為 [a-z] ）。 例 3：ab[^c] 代表字串 ab 後方不能是 c，^ 在 [ ] 內時，代表的意義是『反向選擇』的意思(例如：我不要大寫字元，則為[^A-Z])。
|	『或』、『or』的意思。	gd|good 代表 gd 或 good 這兩個字串
+	重複『一個或一個以上』的前一字元。	go+d 代表 god，good，goood，. . . 的字串。 o+ 代表『一個以上的 o 』。
{ }	限制一個範圍區間內的重複字元數	因為 { 與 } 的符號在 shell 是有特殊意義的，因此，必須要使用跳脫字符 \ 來讓他失去特殊意義才行。 例 1：ab\{3\}c 代表 a 後有 3 個 b 最後是 c，如：abbbc 例 2：go\{2,4\}d 代表在 g 與 d 之間有 2 個到 4 個的 o 存在的字串，亦即 good、goood、gooood。 例 3：go\{2,\}d 則是連續 2 個以上的前一字元，如：good、goood、gooooooood (此時也可利用 gooo*d 來表示)
( )	群組	例 1：g(la|oo)d 代表 glad 或 good 這兩個字串，因為 g 與 d 是重複的，所以， 我就可以將 la 與oo 列於 ( ) 當中，並以 | 來分隔開來。 例 2：A(xyz)+C 代表開頭是 A 結尾是 C，中間有一個以上的 "xyz" 字串的意思。

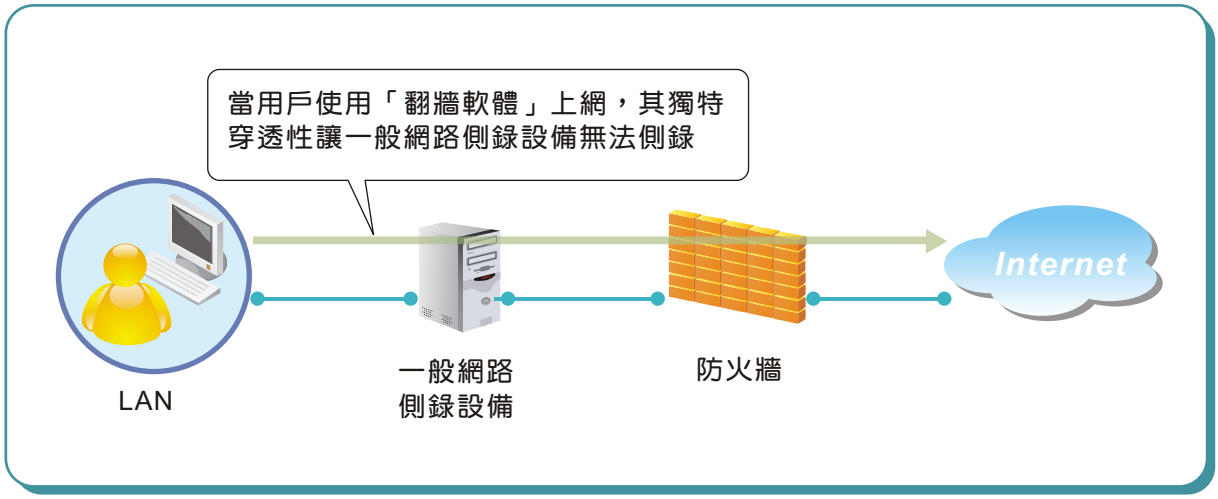
正規表示法符號列表

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新軟網路記錄器協助企業防火牆補足資安漏洞

網路世界進步速度一日千里，而科技也隨著人類的求知慾，不斷地進化成長。現今許多企業為了維護企業資訊安全及提升公司生產效率，因而使用相關網路管制設備來管制員工，避免員工於上班時間利用公司網路資源從事工作之餘外的私人事務；甚至還有公司採購網路側錄設備來記錄員工上班時的網路使用狀況，藉此了解是否有員工於上班時間混水摸魚。

然而「上有政策、下有對策」，雖然公司斥資採購相關設備藉以監督員工上班情形，但是針對公司所採用的網路管理政策，員工自是有辦法可以躲避。最常遇到員工使用「翻牆軟體」及「遠端控制軟體」來躲避網路管制設備的管制及網路側錄設備的記錄。乃因這些通道軟體擁有獨特的 “穿透性” 讓前端防火牆、防毒牆無法達到準確的網路安全過濾，間接形成“資安防護漏洞”使網路上的駭客或病毒有機可趁；甚至於讓網路側錄設備無法真正記錄到該員工上網的內容，導致該員工能夠順利在上班時間利用公司網路資源上網摸魚，降低公司生產效率。

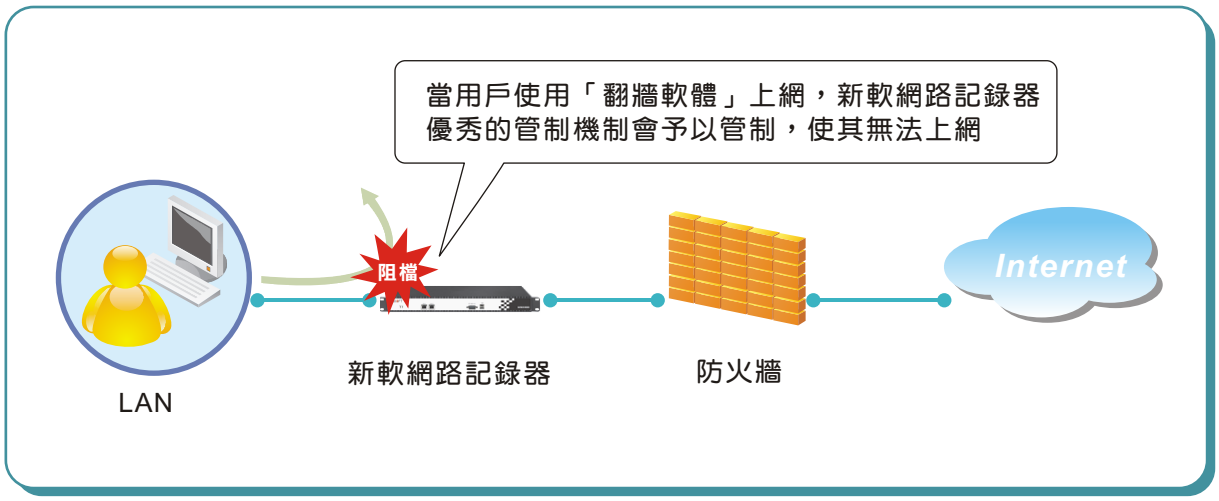


當用戶使用翻牆軟體上網時，一般市售網路側錄設備就完全束手無策

新軟系統網路記錄器 -IR 系列之原始產品設計概念就是以「協助一般企業防火牆補足資安漏洞」，因此針對像此類加以使用翻牆軟體或遠端控制軟體來躲避網路記錄器之問題，新軟網路記錄器 -IR 系列便能夠提供完善的解決方案：

只需將新軟系統網路記錄器以橋接模式架設於公司網路前端，此時只要任何通過公司網路進出的封包都會經過新軟網路記錄器並會被網路記錄器記錄且備份下來，其所能提供的網路記錄服務包括 HTTP、E-Mail、Web Mail、IM 即時通訊、FTP、TELNET…等多項常用服務，都能夠完整地將員工上網的行為一五一十的記錄下來。

倘若遇到員工企圖使用「翻牆軟體」及「遠端控制軟體」躲避網路記錄器之記錄時該如何處理呢？此時便是新軟系統網路記錄器 -IR 系列優於市面上許多網路側錄設備的地方；優勢在於：新軟網路記錄器有提供完善的“應用程式管制”機制（例如：翻牆 Tunnel 程式、遠端控制程式…等等），可針對網路架構底下用戶進行管制。因此只要將管制環境設定完成後，正常使用者仍可使用一般網路服務，此時若出現有心人士欲使用相關管制程式時，除了該使用者無法正常使用相關程式之狀況以外，管理者還可以於“IM /應用程式記錄”裡經由詳細的報表(UserName + IP + MAC)找出公司裡是誰違法使用相關應用程式。如此便可以完善保護公司企業資訊安全，也不怕公司網路資源遭人公器私用。



當用戶使用翻牆軟體上網時，新軟網路記錄器會予以管制，使其無法正常上網

文 黃政銘 ming@nusoft.com.tw