新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/12/28-2010/1/10 第108期

网络记录器 / IR系列报导

技术浅谈与应用 - 内容稽核的正规表示法使用方式

网络安全一直以来都是公司内部首要的课题之一，除了一般对外常用的资安设备之外，对内也渐渐的重视。正因为如此，不少公司纷纷导入网络侧录设备来管理内部资源，一方面可加强内部网络信息的安全，另一方面也可管理员工于公司内的种种网络使用行为，更可有效降低员工利用上班时间来滥用网络资源之情况发生，藉此让公司能够达到更好的生产效益。

新软系统所推出的网络记录器 - IR，除了拥有强大侧录功能之外，还附有人性化及多元化的管理功能，可依照不同的环境来满足管理人员不同之需求。但身为一个网络管理人员又该如何有效的在全公司大量且众多记录结果中，去找到符合公司需要、老板需要、主管需要...等不同的记录来做有效之存查及呈现呢？虽然管理人员可利用搜寻功能找出所需之记录数据，不过这还得亲自进入系统来耗费时间操作，倘若往后又有相关之记录需要查核，就必须再做一次相同的搜寻动作，既然要如此不断重复相同搜寻动作，管理人员又该如何让系统自行处理呢？

利用『内容稽核』功能可轻松分别针对 IR 所记录的 SMTP、POP3、HTTP / HTTPS、IM、Web SMTP、Web POP3、FTP、TELNET 数据内容设定相关的比对机制，完成特定所需审查传送的文字、文件...是否符合既定的网络安全政策。但重点在于管理人员所设定的稽核条件为何、是否能正确制定稽核条件，虽然该功能可直接使用输入关键词来做为稽核条件的设定方式，但面对于需要较有变化性之稽核条件时，单纯只利用关键词方式就显的不是如此方便。因此管理人员则可进一步使用正规表示法来做为搜寻稽核的条件，藉此来达到更多样变化之条件设定方式。

服务名称	可支持使用正规表示法部份
SMTP	信件主旨、信件内容
POP3 / IMAP	信件主旨、信件内容
HTTP / HTTPS	网页内容
IM	聊天内容
Web SMTP	信件主旨、信件内容
Web POP3	信件主旨、信件内容

『内容稽核』各服务内容可支持使用正规表示法部份

正规表示法（Regular Expression），是指透过一些特殊字符的排列，用以『搜寻/取代/删除』一列或多列文字字符串，而『内容稽核』该项功能则是利用来做为搜寻使用。但对于不常使用或不曾使用「正规表示法」的管理人员而言，较容易搞错相关之字符串意义及使用方式，所以以下将分别说明使用者较常使用之符号。

符号	说明	范例
^	代表启始字符	^A 代表以 A 开头的字符串 Abc，Aaa。
$	代表结束字符	A$ 代表以 A 结尾的字符串 bca，aaA
.	1.代表任意字符，但不包括换行字符 \n。 2. n 个 .表示任意 n 个任意字符 (注意: 并非任意长度的字符串)。	a.b 代表 a 带一个任意字符，後面接着一个 b，字符串可以是 azb、aab、abb、a b 等，a 与 b 中间『一定』仅有一个字符，而空格字符也是字符。
\	将其後的字符跳脱，使其回归原字符的涵义。	\. 代表将其後字元特殊符号『.』之特殊意义去除。此时的『.』代表条件是包含有『.』这个符号的字符串，例如：www.tw.yahoo.com、168.95.1.1、…，而非其符号原本所代表的『任意字符』。
*	重复零个或多个的前一字符。	ess* 代表含有 es, ess, esss 等等的字符串(因为 * 可以是 0 个，所以 es 也是符合带搜寻字串)。 * 为重复『前一个字符』的符号；因此，在 * 之前必须要紧接着一个字符(例如：a*)。
?	『零个或一个』的前一字符。	go?d 代表 gd，god 这两个字符串。o? 代表『空的或 1 个 o 』。

正规表示法符号列表

符号	说明	范例
[ ]	1. 代表在 [ ] 中一个会出现的字符	例 1：a[bc] 代表含有 ab 或 ac 的字符串。 需特别留意的是，在 [ ] 当中『谨代表一个待搜寻的字符』，亦即 [bc] 代表 b 或 c 的意思。 例 2：[0-9] 代表含有任意数字的字符串。在字符集合 [ ] 中的减号 - 是有特殊意义的，他代表介於两个字元之间所有连续的字符（例如：所有大写英文字符则为 [A-Z]、所有小写英文字符则为 [a-z]）。 例 3：ab[^c] 代表字符串 ab 後方不能是 c，^ 在 [ ] 内时，代表的意义是『反向选择』的意思（例如：我不要大写字符，则为[^A-Z]）。
|	『或』、『or』的意思。	gd|good 代表 gd 或 good 这两个字符串
+	重复『一个或一个以上』的前一字符。	go+d 代表 god，good，goood，...的字符串。 o+ 代表『一个以上的 o 』。
{ }	限制一个范围区间内的重复字符数	因为 { 与 } 的符号在 shell 是有特殊意义的，因此，必须要使用跳脱字符 \ 来让他失去特殊意义才行。 例 1：ab\{3\}c 代表 a 後有 3 个 b 最後是 c，如：abbbc 例 2：go\{2,4\}d 代表在 g 与 d 之间有 2 个到 4 个的 o 存在的字符串，亦即 good、goood、gooood。 例 3：go\{2,\}d 则是连续 2 个以上的前一字符，如：good、goood、gooooooood (此时也可利用 gooo*d 来表示)
( )	群组	例 1：g(la|oo)d 代表 glad 或 good 这两个字符串，因为 g 与 d 是重复的，所以，我就可以将 la 与 oo 列於 ( ) 当中，并以 | 来分隔开来。 例 2：A(xyz)+C 代表开头是 A 结尾是 C，中间有一个以上的 "xyz" 字符串的意思。

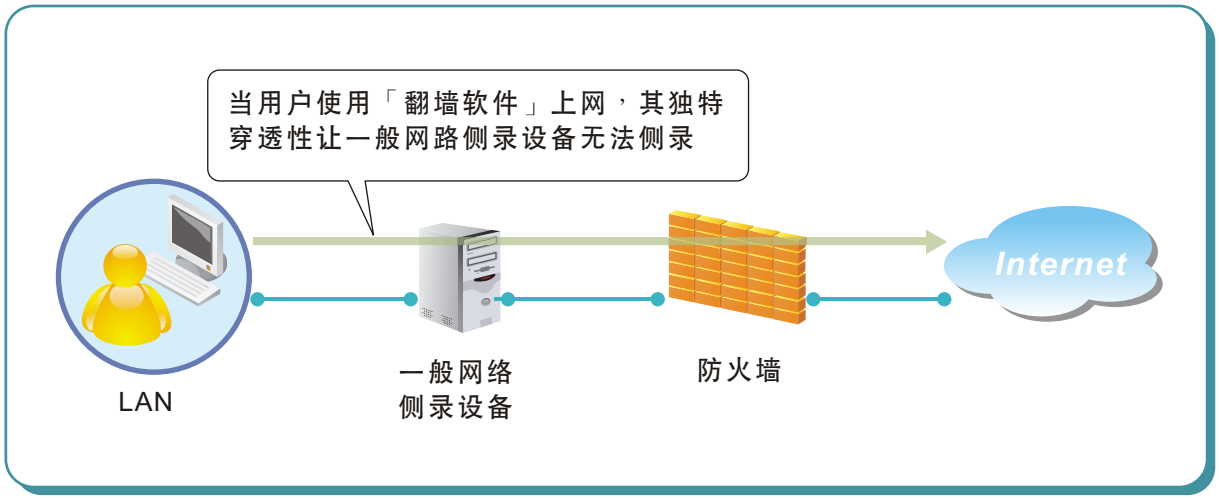
正规表示法符号列表

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 新软网络记录器协助企业防火墙补足资安漏洞

网络世界进步速度一日千里，而科技也随着人类的求知欲，不断地进化成长。现今许多企业为了维护企业信息安全及提升公司生产效率，因而使用相关网络管制设备来管制员工，避免员工于上班时间利用公司网络资源从事工作之余外的私人事务；甚至还有公司采购网络侧录设备来记录员工上班时的网络使用状况，藉此了解是否有员工于上班时间混水摸鱼。

然而「上有政策、下有对策」，虽然公司斥资采购相关设备藉以监督员工上班情形，但是针对公司所采用的网络管理政策，员工自是有办法可以躲避。最常遇到员工使用「翻墙软件」及「远程控制软件」来躲避网络管制设备的管制及网络侧录设备的记录。乃因这些信道软件拥有独特的 “穿透性” 让前端防火墙、防毒墙无法达到准确的网络安全过滤，间接形成 “资安防护漏洞” 使网络上的黑客或病毒有机可趁；甚至于让网络侧录设备无法真正记录到该员工上网的内容，导致该员工能够顺利在上班时间利用公司网络资源上网摸鱼，降低公司生产效率。

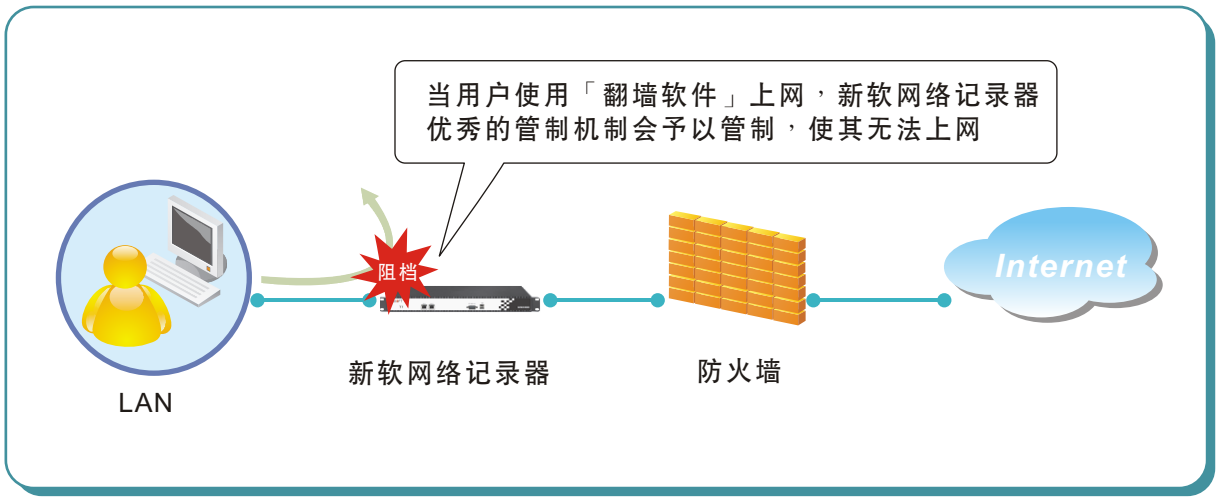


当用户使用翻墙软件上网时，一般市售网络侧录设备就完全束手无策

新软系统网络记录器 -IR 系列之原始产品设计概念就是以「协助一般企业防火墙补足资安漏洞」，因此针对像此类加以使用翻墙软件或远程控制软件来躲避网络记录器之问题，新软网络记录器 -IR 系列便能够提供完善的解决方案：

只需将新软系统网络记录器以桥接模式架设于公司网络前端，此时只要任何通过公司网络进出的封包都会经过新软网络记录器并会被网络记录器记录且备份下来，其所能提供的网络记录服务包括 HTTP、E-Mail、Web Mail、IM 实时通讯、FTP、TELNET...多项常用服务，都能够完整地将员工上网的行为一五一十的记录下来。

倘若遇到员工企图使用「翻墙软件」及「远程控制软件」躲避网络记录器之记录时该如何处理呢？此时便是新软系统网络记录器 -IR 系列优于市面上许多网络侧录设备的地方；优势在于：新软网络记录器有提供完善的“应用程序管制”机制（例如：翻墙 Tunnel 程序、远程控制程序...等等），可针对网络架构底下用户进行管制。因此只要将管制环境设定完成后，正常使用者仍可使用一般网络服务，此时若出现有心人士欲使用相关管制程序时，除了该使用者无法正常使用相关程序之状况以外，管理者还可以于“IM / 应用程序记录”里经由详细的报表（UserName + IP + MAC）找出公司里是谁违法使用相关应用程序。如此便可以完善保护公司企业信息安全，也不怕公司网络资源遭人公器私用。



当用户使用翻墙软件上网时，新软网络记录器会予以管制，使其无法正常上网

文 黄政铭 ming@nusoft.com.tw