No.30

Tech Overview : Configuring Content Auditing Settings Using Regular Expressions

Network security has been seen as the first priority among companies. What's more, the focus is no longer solely on the external network, but rather on the internal network. Therefore, businesses adopt Internet recording devices in order to manage their internal network. The Internet recording devices provide network management that can improve business productivity by reducing network resource abuse by the employees during work time.

Nusoft Internet Recorder provides you with a top-notch recoding mechanism with friendly and flexible management that can match any circumstance and satisfy any needs. However, it is not easy for the IT administrator to generate the specific logs that meet the demands of different superiors in the company. One solution is to log in the user interface and search the logs manually. However, it is time-consuming and repetitive because the IT administrator needs to do the search repeatedly every time he needs the logs. To avoid spending time on the search, a better approach would be for the device to generate the logs automatically itself.

Nusoft Internet Recorder features Content Auditing that facilitates gathering and organizing records. It generates the records of SMTP, POP3, HTTP(S), IM, Web SMTP, Web POP3, FTP and TELNET respectively and mails the records to the designated recipient periodically. To generate auditing reports that exactly meet the demands of the recipient, the defined criteria are the key. The IT administrator may enter the keywords to define the criteria, but solely relying on keywords is insufficient. Thus, utilizing keywords coupled with regular expressions can be more effective.

Service	Attributes that Support Using Regular Expressions
SMTP	Subject and Content
POP3 / IMAP	Subject and Content
HTTP / HTTPS	Content
IM	Content
Web SMTP	Subject and Content
Web POP3	Subject and Content

Table 1 Regular Expression Supported by Different Services

Regular Expressions can be used to search, replace or delete strings or lines by using the combination of symbols or characters. Regular expressions can be used in Content Auditing for creating flexible and concise criteria. The table below shows the usage of it.

NUSOFT

Symbol	Description	Example
^	Matches the start of the string or line.	^A matches the string or line beginning with "A", such as "Abc", "Aaa", etc.
$	Matches the end of a string or line.	A$ matches the string or line ending in "A", such as "bcA", "aaA", etc.
.	1. Matches all characters except for a new line (\n). 2. Multiple dots match a set of any characters. (A dot (.) matches a single character.)	a.b matches a string beginning with"a" and ending in "b". There must be only one character between "a" and "b". For example, "azb", "aab", "abb", "a b", etc. (A space is treated as a character.)
\	Ignores the regular expression meaning from the following character.	\. ignores the regular expression meaning of ".", so "." will be treated as a literal character. For example, www.tw.yahoo.com, 168.95.1.1, etc.
*	Matches the preceding character zero or more times.	ess* locates the string or line that contains "es", "ess", "esss", etc. (es matches the meaning because * can be more than one time or zero time.) * denotes the repetition of the preceding character, thus, there must be a character before *, such as a*.
?	Matches the preceding character zero or one time.	go?d denotes "gd" and "god" because "?" matches the preceding character zero or one time.
[ ]	Matches a single character that is contained within the brackets.	Example 1 : a[bc] locates "ab" or "ac" because [ ] matches a single character contained within it. Example 2 : [0-9] denotes the numbers zero to nine because the dash (-) inside the brackets matches the characters between two characters. For example, [A-Z] denotes the capital letters from A to Z. [a-z] denotes the lowercase letters from a to z. Example 3 : ab[^c] matches "aba", "abb", "abd", "abe", etc. except "abc" because the symbol (^) in the brackets matches all characters except the one in the brackets. For example, [^A-Z] matches lowercase letters from "a" to "z".
|	Represents the meaning: 'or'	gd|good matches "gd" or "good".

Table 2 Regular Expression Guidelines

Symbol	Description	Example
+	Repeatedly matches one or more of the preceding character.	go+d matches one or more "o" contained within e.g., "god", "good", "goood", etc.
{ }	Repeatedly searches for characters within the specified range.	The symbols "{" and "}" have a unique meaning within shell scripts, therefore when used as regular expressions they need to be proceeded with a "/" character. Example 1: ab\\{3\\}c represents three "b" characters between "a" and "c" i.e., "abbbc". Example 2: go\\{2,4\\}d represents two to four "o" characters between "g" and "d" i.e., "good", "goood" and "gooood". Example 3: go \\{2,\\}d represents two or more "o" characters between "g" and "d", e.g., good, goood, goooood, etc.
( )	Group	Example 1: g(la|oo)d matches the string "la" or "oo" located between "g" and "d" i.e., "glad" or "good". Example 2: A(xyz)+C matches one or more "xyz" strings located between "A" and "C".

Table 2 Regular Expression Guidelines

No.30

Product News : Nusoft Internet Recorder Resolves Your Network's Vulnerabilities

The growing need in information naturally stimulates the evolution of the Internet. A recent survey on Internet usage has shown that over 80 percent of users have incorporated the Internet into their daily life, whether it's at work or at home. Consequently, many business owners have purchased network-recording devices to avoid business secrets theft and the misuse of network resources.

As the saying goes, "The more illumination, the more temptation." A network-recording device could be a "Right" answer to the cyberslacking, yet not necessarily always the "Best" one. To avoid being monitored or recorded, Internet anonymity and remote control software can be utilized. Generally, they enable users to evade detection by viruswalls/ firewalls, which may open a backdoor to allow unauthorized access to the internal network. This leaves a possibility for employees to remote into their computer at home during office hours and takes your employee productivity from bad to worse.
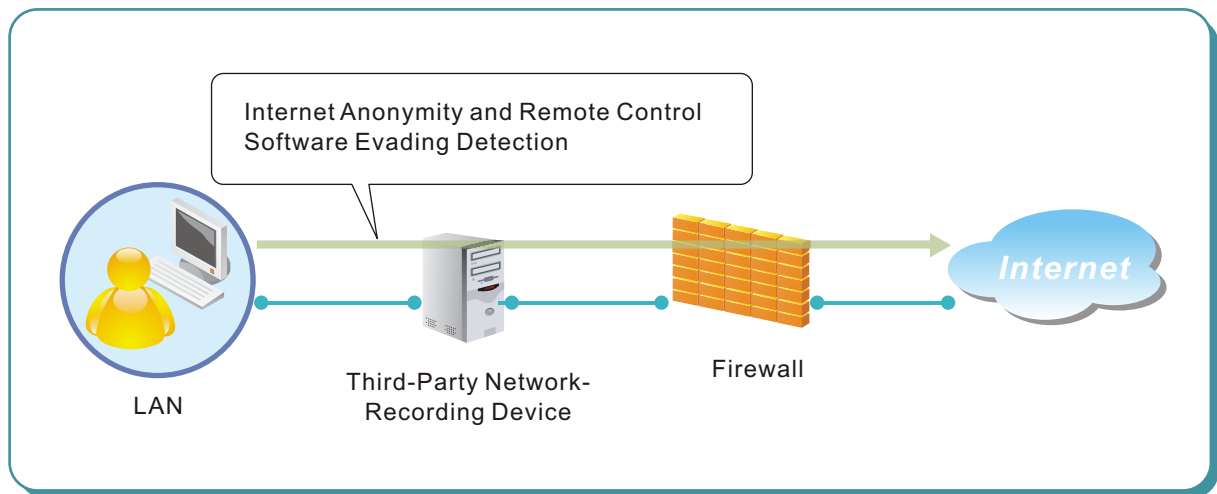

Figure 1. A LAN User Evading Detection

The Nusoft Internet Recorder (IR) series is designed around addressing the inadequacies with the vast majority of firewalls. To uphold a business' information security, the IR series regulates access to Internet anonymity and remote control software.

By deploying the Internet Recorder in bridge mode at the perimeter of the network, packets can be monitored and copied. The device's recording capabilities encompasses the most commonly used Internet activities and services used by employees such as HTTP, e-mail, Web-based mail, instant messaging, FTP, TELNET, etc., ensuring the company's network is not misused.

What sets the Nusoft Internet Recorder apart from third-party network-recording devices? To deal with employees attempting to discreetly use software such as Internet Anonymity and remote control software, the Internet Recorder provides comprehensive application blocking mechanisms. Once the desired regulation settings are in place, all the Internet services deemed essential to the business remain undisturbed. Employees are not only blocked from using applications designated as banned, but also any attempts are recorded in the device's IM / Application Log using the employee's Username, IP and MAC. Managers can now rest assured knowing that sensitive information remains secure and the network is used as it was intended for.

No.30

The Internet Recorder blocks a LAN user's attempt to use Internet anonymity and remote control software

Blocked!

Nusoft Internet Recorder
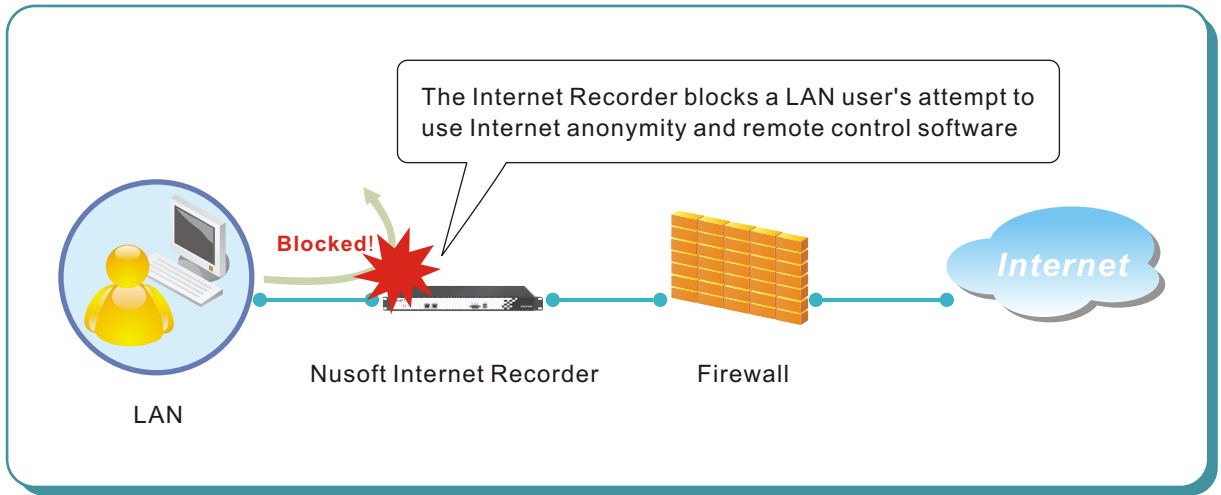
Firewall

Internet

LAN

Figure 2. A LAN User Attempting to Use Internet Anonymity and Remote Control Software