



828 West Taft Avenue
Orange, CA 92865
714-282-6111
714-282-6117 Fax
www.8e6.com

8e6 3000 | Enterprise Filter



R3000 Logging

Scope

The scope of this white paper is to give a technical description as to what is logged by the R3000.

Product Definition

8e6 R3000 Enterprise Filter

The 8e6 R3000 Enterprise Filter is a hardware-based appliance solution that allows users to monitor, filter and log an organization's Internet traffic. Through user-defined parameters based on 8e6's 75+ categories of Web content, an R3000 filter will help improve employee productivity, reduce liability and preserve network resources.

8e6 Enterprise Reporter 3.0

The 8e6 Enterprise Reporter (ER) 3.0 is a standalone server appliance dedicated to monitoring and reporting on Internet access. Using a proprietary processing approach, the ER is able to produce detailed or summarized reports in minutes or even seconds without compromising other server/network functions.

Introduction

When filtering Internet traffic, the R3000 will log each Internet request it handles, regardless of whether the site was filtered. The log file is a line fed log that consists of one Internet request per line.

The log file itself is a comma delimited file that contains the following information, in the following format:

Source IP,Group\Username,Date,Time,Category,Requested URL

For example, if a user was not assigned to a group or NT/AD profile (i.e. using the default filtering level), was surfing from a workstation with an IP address of

10.11.12.13, and he requested the web page <http://www.espn.com/> at 1:30:35PM on October 29, 2003, the log file entry would appear as follows:

10.11.12.13,DEFAULT,2003/10/29,13:30:35,SPORTS,http://www.espn.com/

In the event that the users IP address exists in an IP Group, which has been created by the Global Administrator, the log file will include the name of the IP Group in the group field of the log file. Using the example above, if the user was a member of an IP Group named Sales, the log entry would reflect it as follows:

10.11.12.13,Sales,2003/10/29,13:30:35,SPORTS,http://www.espn.com/

If the user receives their filtering level from the R3000 Transparent Authentication using their NT/LDAP username, then the domain, group and username information would be included in the group field of the log file. Using the example above, if the user was logged into the domain LOGON, in the NT Group Sales, and had a username of joeuser, the log file would appear as follows:

10.11.12.13,LOGON/Sales/joeuser,2003/10/29,13:30:35,SPORTS,http://www.espn.com/

Once this information is collected by the R3000, the next step is to use this data for the purposes of reporting. There are two file transfer options available for the R3000 log file.

The primary option is to send the logs to an 8e6 Enterprise Reporter (ER) using the Reporting configuration option in the R3000 GUI. The ER will then process these logs into a high-speed database allowing an administrator to quickly generate reports on the Internet usage of the Internet users.

Since all of the information is included in this log, it is very easy to break the information down based on any of the available fields. For example, a report could be run on all users in the NT Group Sales. This information could then be broken down even further to show all users in the NT Group Sales, that visited web sites in the category SPORTS.

The secondary option is to export the log files to an existing FTP server using the reporting configuration option in the GUI. Using this option will FTP the logs to a server of the administrator's choice on a schedule that the administrator selects. The log files can then be manipulated at the administrator's choosing, utilizing any tool that the administrator wishes to use.