

Re: Errors Message from Webtrends Firewall Suite

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/12507.html>

From:

Date: 10/25/02

Date: 24 Oct 2002 19:48:58 -0700

Solution

The following article describes the issue in detail as well as a way to increase the out of order time so that fewer records are discarded.

<http://www.netiq.com/kb/esupport/consumer/esupport.asp?id=NETIQKB664>

Below is the article

Firewall Suite and Firewall Appliance Analyzer keep track of how many records in the log file were dropped due to being out of chronological order, and when this number of dropped records becomes high it may cause concern. All out of order records will affect visitor session statistics and in some cases, alters session numbers, lengths, etc.

Below is the method for manually setting the timeout value for Firewall Suite and Firewall Appliance Analyzer. Use this setting with careful thought and planning to avoid the problems above.

Locate the following file within the WebTrends product:

`\wtm_<cartridge>\<cartridge>.ini`

Open the file in a text editor and locate the following section:

[defaults]

Add the following line:

`MaxOutOfOrder=n`

[where n is any number of seconds, 1-359]

Save the changes.

Note: By default, all log analysis cartridges will throw out records that are more than thirty seconds out of order. This setting will change the amount of seconds the engine will allow records to be out of order. The greater this value, however, the more memory will be used.

The reason it takes more memory is because whatever setting is entered into the .ini file is the amount of time the WebTrends parsing engine will do automatic, in-memory sorting for you. The larger the time slice, more memory is needed to do this sorting. It is important to understand the results of this configurational change.

Example:

An example case where this might happen is if you had three Check Point FW-1 modules – two in the United States and one in Central America – all logging to the same console. The records coming from Central America could be written out more than thirty seconds past the other modules. Reasons for this:

One cause could be when multiple machines record to one log, and those machines have a system clock set more than 30 seconds different.

Another reason could be one in which multiple services write out records to a single log file on a machine, and the records are then dumped out from a buffer periodically. This has been known to cause problems.

-
- *Next message:* : "Re: NAPT(Linux 7.2 or ICS) and UDP clients"
 - *Previous message:* mhicaoidh: "Re: ZoneAlarm & Server Ports."
 - *In reply to:* Unbreakable: "Errors Message from Webtrends Firewall Suite"
 - *Messages sorted by:* [date] [thread] [subject] [author] [attachment]