Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Microsoft Forefront TMG – Logging options in Forefront TMG

Abstract

In this article I will show you how Forefront TMG can be configured to log network traffic to various log file formats like Microsoft SQL Server 2008 SP1 Express, text file logging or to a central Microsoft SQL Server instance.

Let's begin

During a Microsoft Forefront TMG installation the setup programs installs a local Microsoft SQL Server 2008 Express Edition with SP1 so this is the default option for logging data in Microsoft Forefront TMG. The logging options in Forefront TMG can now be found in a separate Logs & Reports container in the Microsoft Forefront TMG console as you can see in the following screenshot.

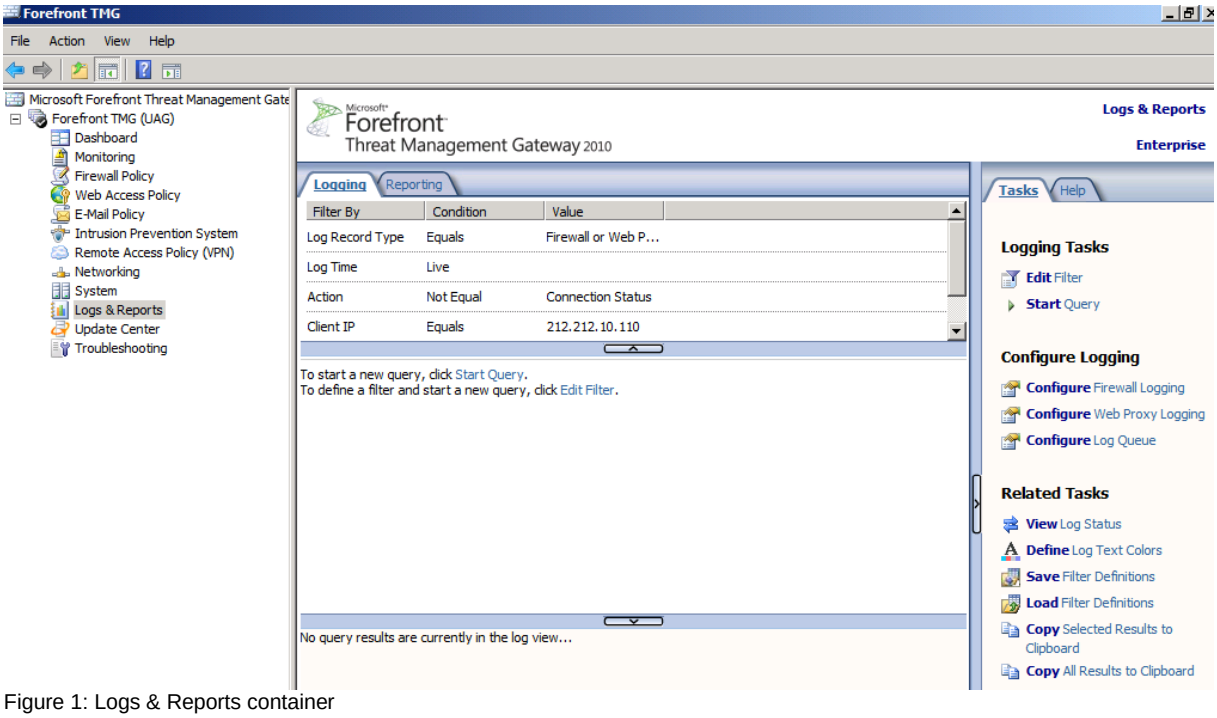

Figure 1: Logs & Reports container

Logging options

Forefront TMG Administrators can configure logging for the Firewall and Webproxy service and for each logging option you can choose between the following Log Storage Formats:

- SQL Server Express database
- Microsoft SQL Server database
- File logging

Each of these options has different pros and cons which are explained in detail in the link I provided in the link section at the end of this article.

In general Microsoft SQL Server Express logging is the best option if you have only one Forefront TMG Server or you don't need central logging capabilities. SQL Server and SQL Server Express logging is also the first option when you want to query the Forefront TMG log data with the help of external tools. One of the cons of SQL Express or SQL Server logging is that this type of logging requires more CPU power and for external SQL Logging a central SQL Server and a reliable network connection to the SQL Server. The following screenshot shows how to change the Log Storage format in Forefront TMG.

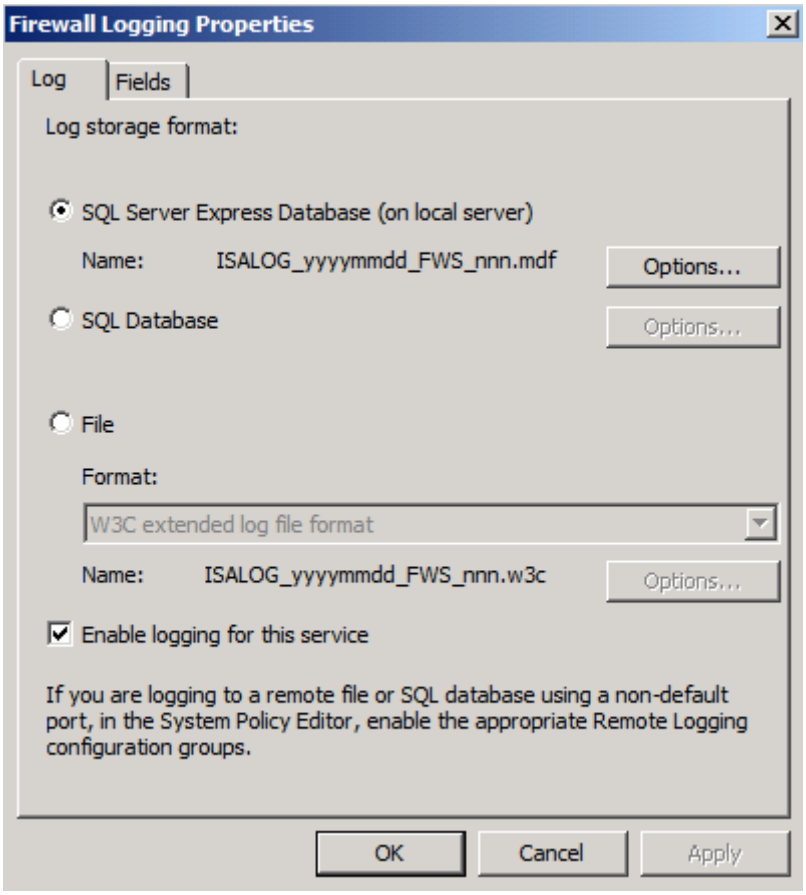

Figure 2: Log storage format

If you choose the "Fields" tab in the Log storage format settings you can select which fields should be logged in the appropriate log file. At the end of this article I will show you how to reduce the amount of logged data by deselecting some log fields.

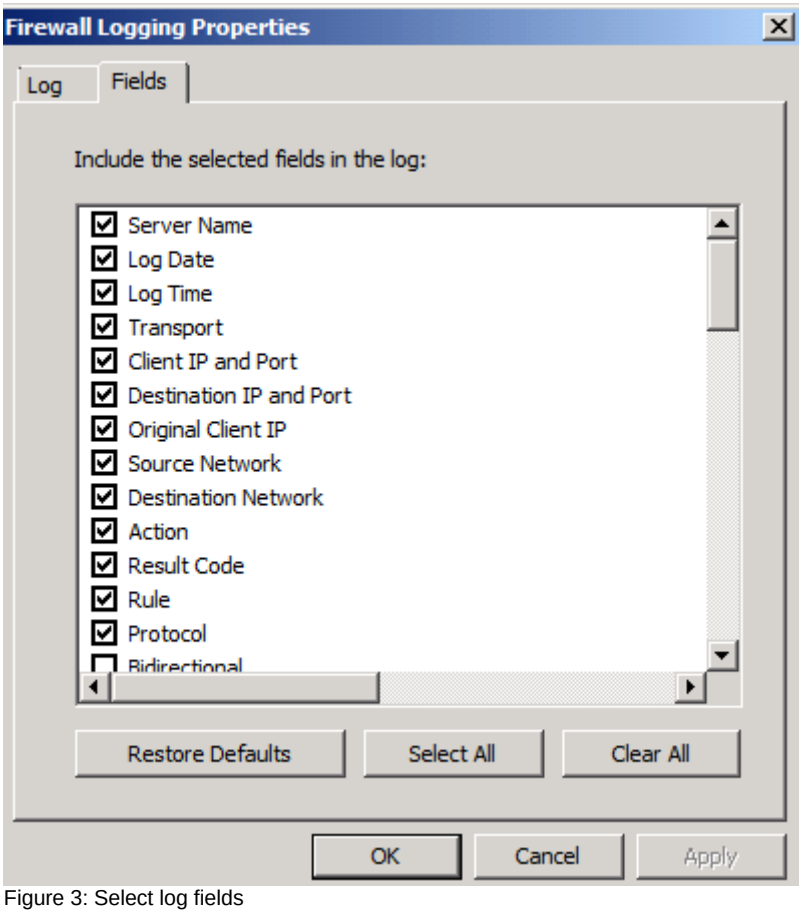

Figure 3: Select log fields

The default log file location is the system drive. If you want to change the location of the log files, click the Options tab and specify another folder for saving log files. It is also possible to specify log file storage limits, which can limit the amount of logging data or configure the amount of free disk space for other services running on the Forefront TMG machine.

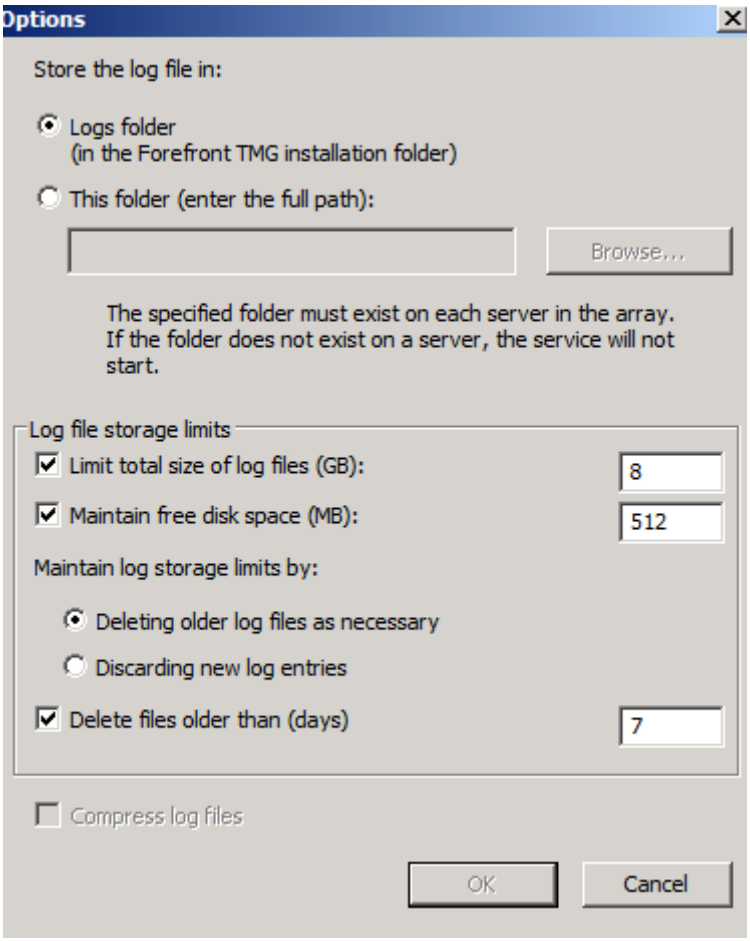

Figure 4: Log file storage limits

LLQ – Large Logging Queue

LLQ (Large Logging Queue) is a new feature in Microsoft Forefront TMG which helps reduce the number of times when TMG enters Firewall lockdown mode due to logging failures. Large Logging Queue is a local queue directory on your TMG Server which is used to save TMG log entries when TMG cannot log into the log destination – by default the SQL Server Express edition.
LLQ has two main components that run in the Kernel mode from TMG (FWENG.SYS) and the User mode (Dispatcher). The process in user mode only reads data from hard disk while the Kernel mode process Fweng writes to the hard disk.

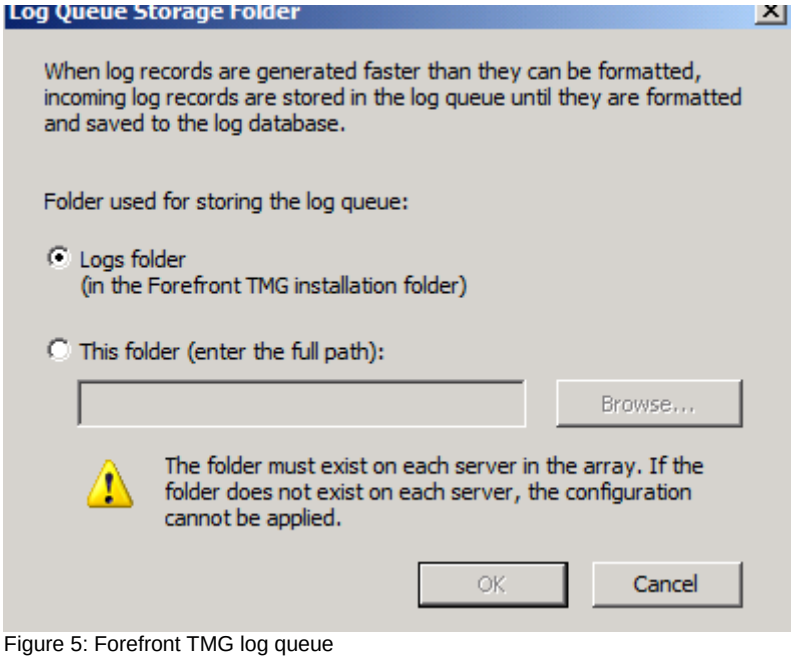

Figure 5: Forefront TMG log queue

There is an explicit Log status button to see the status of Forefront TMG logging. If the connection to the local or remote Microsoft SQL Server couldn't be established, the Log queue begins to grow. After the connection to the local or remote SQL Server has been reestablished, the data in the Log queue will be written to the SQL Server database.

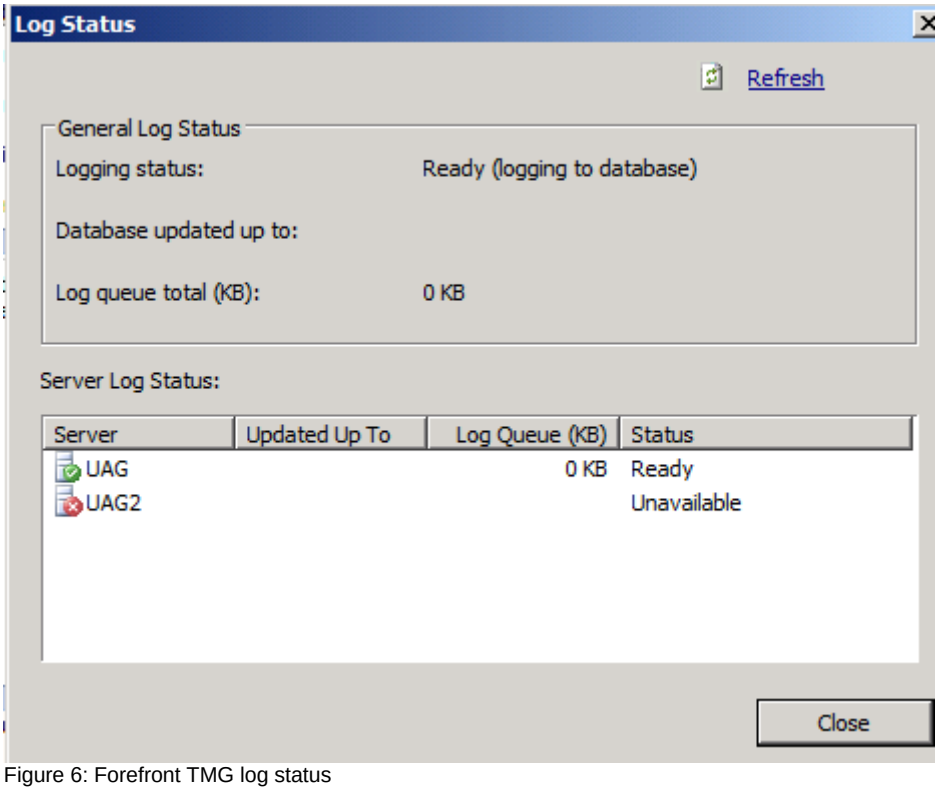

Figure 6: Forefront TMG log status

Garbage rule

Microsoft Forefront TMG logging can be very intensive compared to the amount of data being logged. This can quickly fill up the SQL Server database and if the

Forefront TMG Administrator starts the TMG realtime logging, a large amount of different data can be seen if the traffic is not filtered. To reduce the amount of logged data I often used a Garbage rule in Forefront TMG which allows the traffic for “Unnecessary” traffic like DHCP reply and requests, NetBIOS requests and something more, but in the Firewall rule I disabled the logging option. You must place the rule in front of other Firewall rules. The following screenshot shows a Garbage rule.

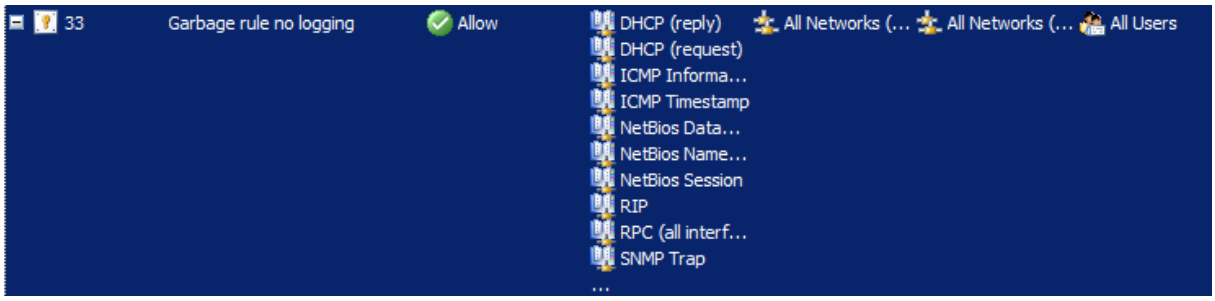

Figure 7: Forefront TMG Firewall rule for Garbage collection

If you click into the properties of the Garbage rule, select the Action tab and remove the flag from the “Log requests matching the rule” and from now on Forefront TMG will allow these type of traffic but it will not log these traffic.

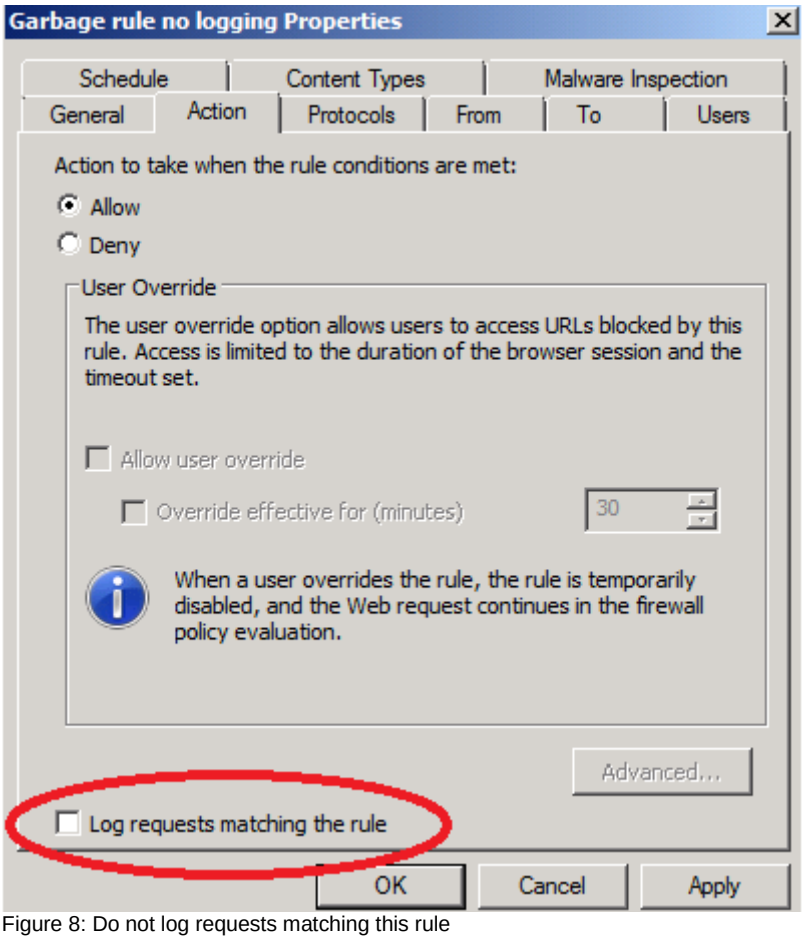

Figure 8: Do not log requests matching this rule

Another way to reduce the amount of logged traffic in Forefront TMG it is possible to select which fields for the Firewall and Webproxy Logging should be logged. Depending on the requirements of the IT department or legal justice it is possible to

deselect some Logging fields as you can see in the following screenshot. I marked some logging fields which might be unnecessary to include in the appropriate log fields. In your productive environment you might have to choose more or other logging fields depending on your needs.

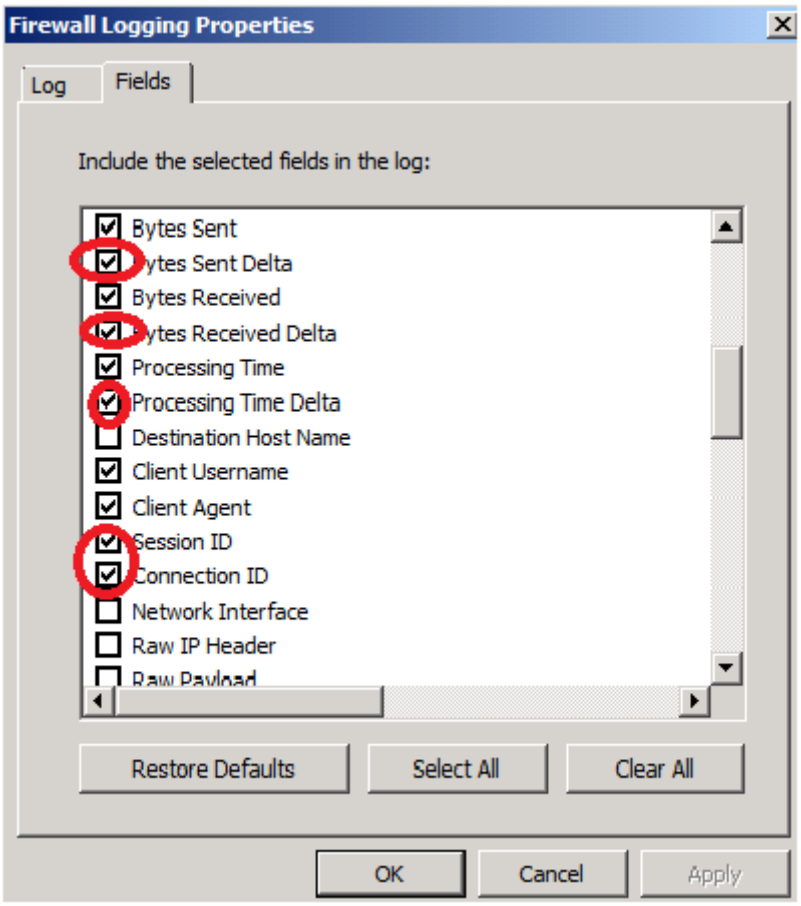

Figure 9: Disable logging fields

Conclusion

In this article, I gave you an overview about the different logging mechanisms in Forefront TMG. I showed you the advantages and disadvantages about the logging options. We had a special look into the options how to reduce the amount of logging data with the help of a garbage rule which allows traffic but doesn't log unnecessary traffic in Forefront TMG. I also showed you how to reduce the amount of logged data by disabling the logging of several log fields.

Related links

Best practice for performance in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794835.aspx
Logging enhancements in Forefront TMG
http://www.isaserver.org/articles/Logging-Enhancement-Microsoft-Forefront-Threat-Management-Gateway-TMG-2010.html
How to configure ISA Server 2004, ISA Server 2006, and Microsoft Forefront Threat Management Gateway, Medium Business Edition to log data to an SQL Server database
http://support.microsoft.com/kb/838710/en-us

Firewall logging using a Microsoft SQL database
http://www.isaserver.org/tutorials/Firewall-Logging-Microsoft-SQL-database.html