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

Explaining the Microsoft Forefront TMG Firewall Lockdown Mode

Abstract

In this article, I will show you how to configure the Microsoft Forefront TMG Firewall Lockdown Mode and the new TMG Log queue feature (LLQ).

Let's begin

Before we start with this article please note that Microsoft Forefront TMG (Threat Management Gateway) is still a beta version as I wrote this article and some things could be changed in the final version of Microsoft Forefront TMG.

As another note keep in mind that much of this article can also be used for ISA Server 2004 and ISA Server 2006, because the Firewall Lockdown mode is nearly the same in all versions. Only the TMG Log queue feature is only available in Forefront TMG.

The first question that you might be asking is: What is the Firewall Lockdown Mode? The answer is simple. All ISA Server versions have a function that disables the ISA Server Firewall service when logging from ISA to the logging destination is interrupted. This is also true for Microsoft Forefront TMG except that TMG comes with a new feature to extend the Firewall Lockdown mode which is called the Log queue feature. I will give you more information about this feature later in this article.

The next question you might be asking is: Why has ISA/TMG a Firewall Lockdown Mode – Isn't it contra productive?

No it isn't. A critical function of TMG is to react to an attack. If there is an attack and the TMG logs fills and fills and fills it could take only a short time after TMG overwrites older log files and if you try to analyze the attack after the attack has gone, you will not find any information in the log file of the attacker. This and some other scenarios are the reason why TMG enters the Firewall Lockdown Modus when logging is interrupted, with one exception, the new Log queue feature.

Forefront TMG tries to combine the need for a not connected TMG Server to the Internet during the logging failure and the need for TMG Administrators to remotely administer the machine from the trusted LAN.

When Forefront TMG enters the Lockdown mode, the following occurs:

- An event triggers an alert to shutdown the Firewall service. It is possible to specify other operations when TMG cannot log to the log destination.
- The Firewall shutdown is logged into the Alert section in the monitoring feature of Microsoft Forefront TMG

When TMG is in Lockdown mode the following functionality applies:

FWENG.SYS (the Kernel Mode packet filter driver) applies the Firewall policy.
Outgoing traffic from the LOCAL HOST network to all networks is allowed.
The following system policy rules allow incoming traffic to the LOCAL HOST network unless a TMG Administrator disabled it:

- Allow remote management from selected computers using MMC.
- Allow remote management from selected computers using Terminal Server.
- Allow DHCP replies from DHCP servers to Forefront TMG.
- Allow ICMP (PING) requests from selected computers to Forefront TMG.
- VPN remote access clients cannot access Forefront TMG. Similarly, access is denied to remote site networks in site-to-site VPN scenarios.

DHCP (Dynamic Host Configuration Protocol) traffic is always allowed. DHCP requests on port 67 UDP are allowed from the LOCAL HOST network to all networks, and DHCP replies on UDP port 68.

Any changes to the network configuration that are made in lockdown mode are applied only after the Firewall service restarts and Forefront TMG exits lockdown mode. Forefront TMG does not issue any alerts.

Leaving lockdown mode

Leaving the Firewall lockdown mode is easy. You only have to restart the Firewall service. This automatically exits the lockdown mode and brings TMG back to normal operating state. Any changes made to the Forefront TMG configuration are applied after Forefront TMG lockdown mode has removed.

Large Logging Queue

LLQ (Large Logging Queue) is a new feature in Microsoft Forefront TMG which helps reducing 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.

The following diagram shows all components used by the Large Logging Queue feature.

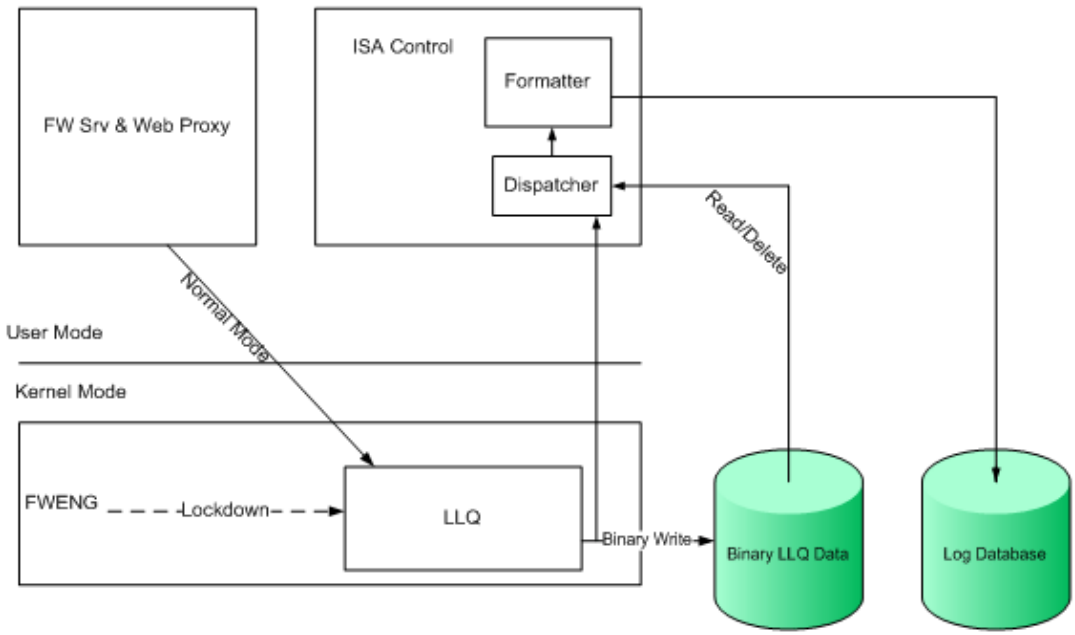

Figure 1: The new log Queue feature – Source: http://technet.microsoft.com/en-us/library/dd183731.aspx

The LLG is stored in RAM and on the Hard disk. If the Dispatcher (the read component) sees no delay in writing log files, the log data will be directly written to the log database.
It is possible to configure the amount of time and the amount of data that can be held in memory by the help of the Registry. There are two configurable Registry settings:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Fweng\Parameters\LogQueueMaxLossCount
HKYEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Fweng\Parameters\LogQueueMaxLossTimeInSeconds

Attention: Microsoft explicitly doesn't recommend changing these settings without calling Microsoft PSS!

It is possible to configure the Log Queue Storage folder in the TMG Management console in the Logs & Reports tab. It is possible to use the Standard folder in the TMG installation folder or another directory on the TMG Server. If you use a custom folder, the folder must exist before you change the LLQ directory to this path.

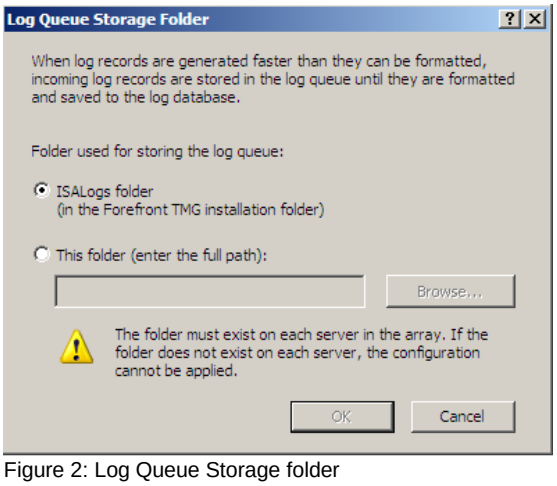

Figure 2: Log Queue Storage folder

In the same tab in the TMG Management console it is possible to view the log status of LLQ. The log queue should empty when logging is correctly working.

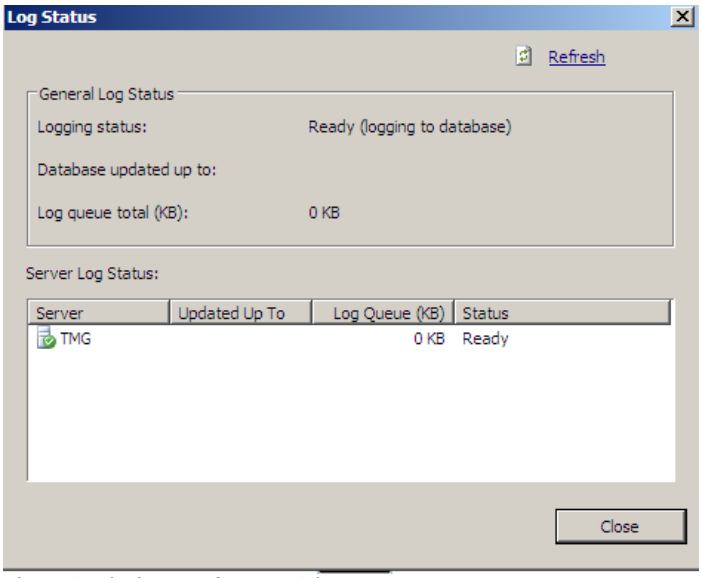

Figure 3: Display Forefront TMG log queue

Log file maintenance

During an attack to the TMG Server or your internal network, the number of log entries will be increasing dramatically and here starts the problem. If TMG Server logging fails, the default log failure alert is issued which shutdowns the Microsoft TMG Firewall service and TMG Server enters the Lockdown mode. This behavior is a great starting point for Denial of Service attacks (DoS).
To reduce the risk of a logging failure, you have several places to optimize the system:

- Use Disk Defragmenter to keep the Hard disk optimized for read and write access
- Use a fast and reliable system
- Optimize logging data
- You should review for which Firewall rules you would like to enable logging
- You should also review which SQL fields you want to log. It is possible to configure the log fields in the Firewall logging properties (see Figure 4 for more information)
- Create a deny rule with logging disabled which drops unwanted traffic like NetBIOS and DHCP traffic which fills the log files with these unwanted information
- Configure the Firewall log and the Web proxy log folders on different disks.
- If you are using SQL logging, modify the file growth size or file growth percentage for the logs database.

The following picture shows the Firewall logging properties:

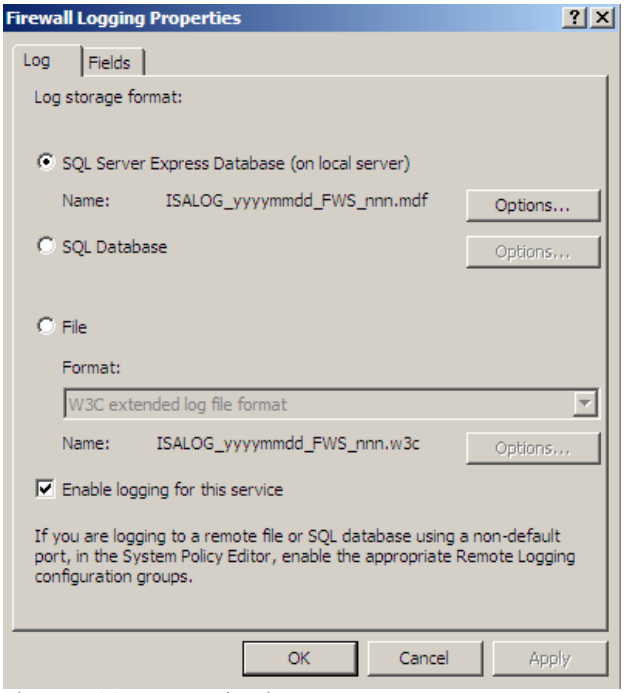

Figure 4: SQL Express logging

Flood mitigation

Beginning with ISA Server 2000, Microsoft implemented some rudimentary anti-spoofing and intrusion detection features. ISA Server 2004 introduced more features to fight against intrusion detection attacks. ISA Server 2006 adds additional techniques to fight against spam. New technologies included are the Flood Mitigation settings that should help protect against threats. With the help of the Flood Mitigation settings it will be possible to reduce the number of generated log entries. Flood Mitigation should be configured depending on your needs and you should often have a look at the Flood Mitigation settings if the are up to date depending on the actual situation.

TMG logging alerts

In the Monitoring tab in the TMG Management console it is possible to configure the Alert settings for all TMG alerts and in this case for a logging failure. In the action tab of the alert it is possible to stop the Microsoft Firewall service. This is the default setting in Microsoft Forefront TMG.

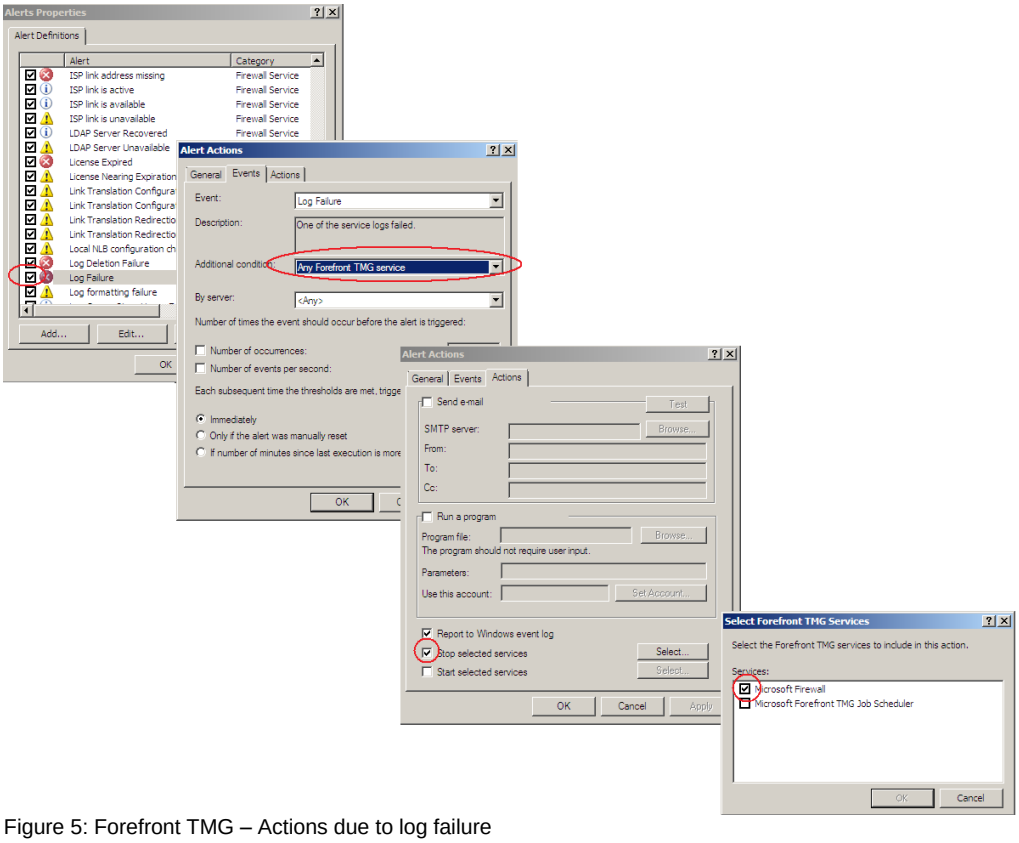

Figure 5: Forefront TMG – Actions due to log failure

Simulation of Logging failures

To simulate a logging failure, you only have to stop the Microsoft SQL Server Express service, and after the service has stopped, you can see that the Microsoft Firewall service is still running.

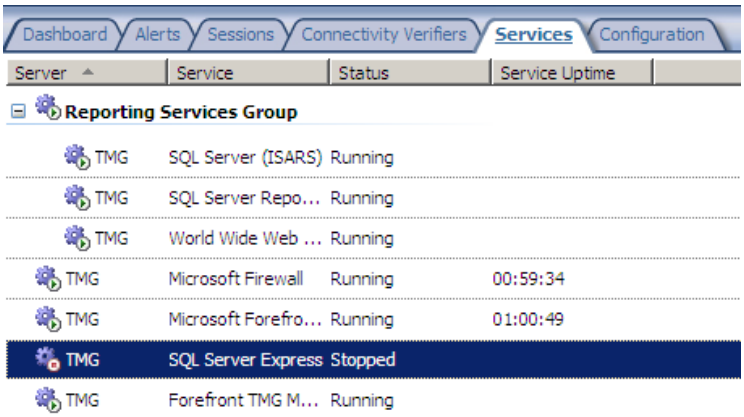

Figure 6: SQL Server Express Logging stopped

If you navigate to the Logs & Reports tab to view the LLQ status, you will see queue which is permanently filling up.

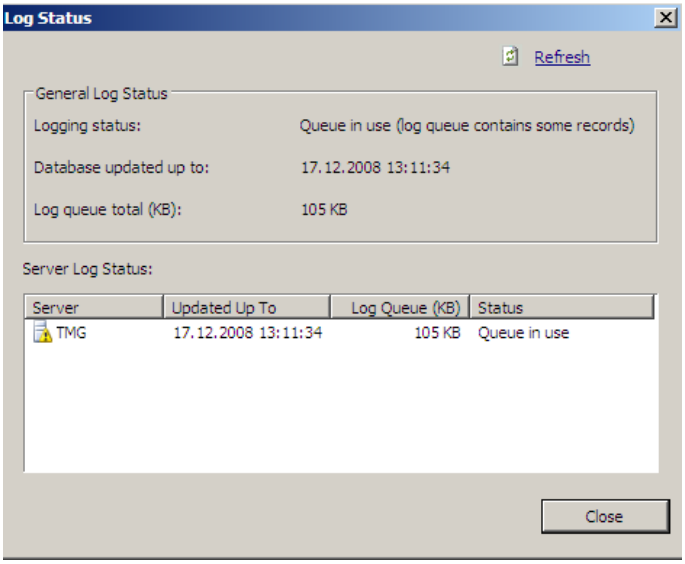

Figure 7: Log queue status – Log queue is filling

The default alert setting when the Log Queue usage starts is to report this into the Windows event log. You have to create an Event trigger or something else that send you a notice about the LLQ use.

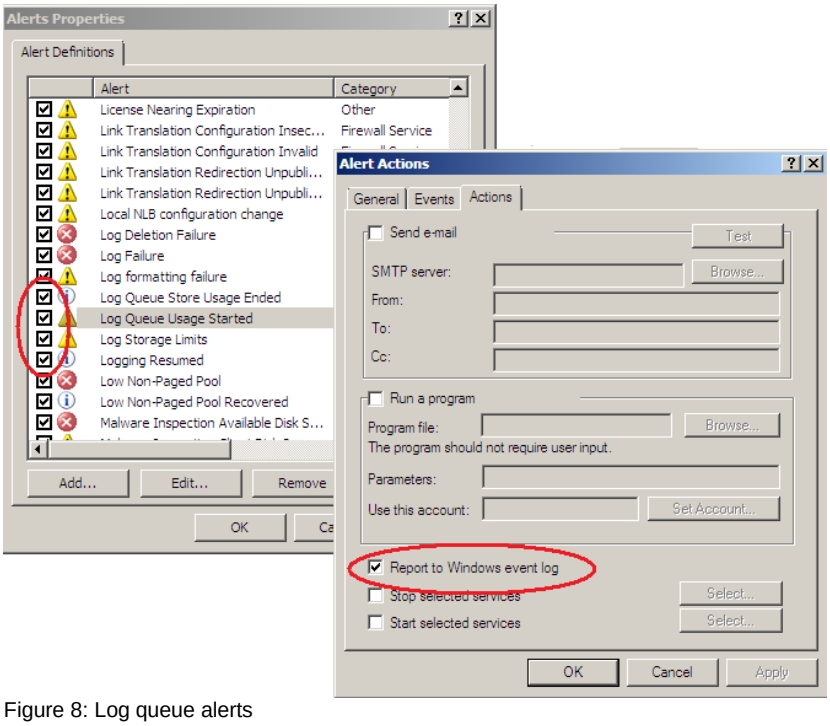

Figure 8: Log queue alerts

Conclusion

In this article, I tried to give you an overview about the new Microsoft Forefront TMG logging queue to avoid or reduce a Firewall lockdown when logging is interrupted. I also gave you an overview about the Forefront TMG logging mechanism and how Microsoft Forefront TMG will be configured for logging and how the log queue will be handled.

Related links

Forefront TMG - About lockdown mode
http://technet.microsoft.com/en-us/library/cc441609.aspx
Overview of the Logging Improvements in Forefront Threat Management Gateway (TMG)
http://technet.microsoft.com/en-us/library/dd183731.aspx
ISA Server 2006 Flood Mitigation
http://www.isaserver.org/tutorials/ISA-Server-2006-Flood-Mitigation.html