Owner of the content within this article is www.isaserver.org

Written by Marc Grote – www.it-training-grote.de

Advanced Forefront TMG debugging

Abstract

This article will show you how to collect advanced Forefront TMG information for documentation and debugging purposes with the TMG Data package and advanced Forefront TMG logging.

Let's begin

Microsoft Forefront TMG creates a large amount of logging data for the Web proxy and Firewall service by default into a local Microsoft SQL 2008 SP1 Server Express instance. These log files should help Firewall Administrators to see what happens at the Firewall to enforce the allowed or disallowed Firewall policy rules and to see the reason why some legitimate traffic is not allowed or vice versa. For general information about the health of the Forefront TMG Server you can use the Forefront TMG dashboard and the Windows event logs.
For some more advanced logging you can use the built in Diagnostic logging in Forefront TMG which collects some more helpful information. If these information are not enough you can use some more advanced tools which are all part of the well-known Microsoft Forefront Best Practices Analyser tool.

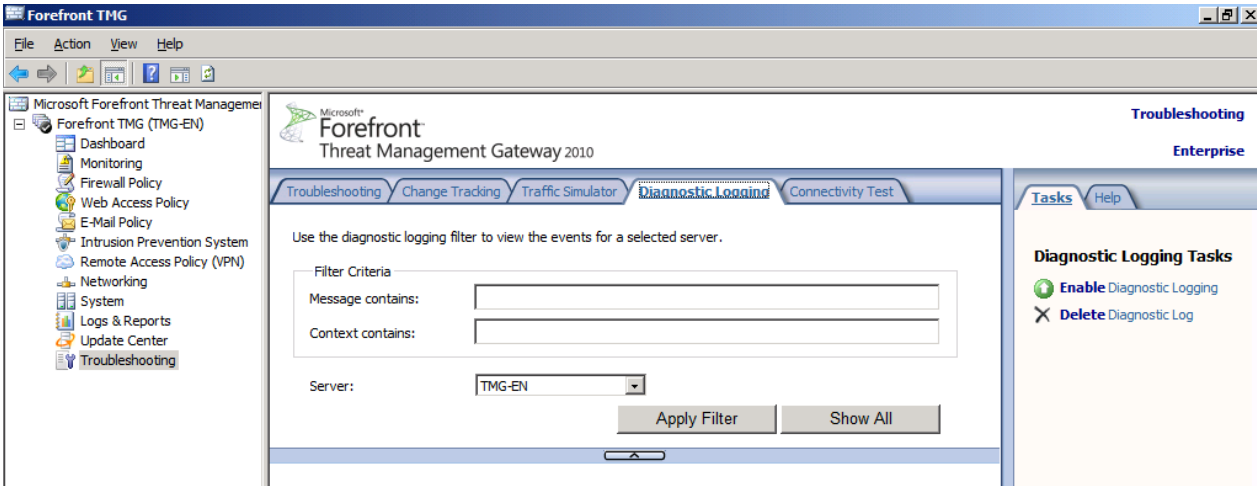
The TMG BPA comes with these (and some more tools):

- TMG Data packager
- Isainfo
- ISAtrace
- TMGBPApack

In this article I will give you a high level overview about these tools and how to use them but first let us start with the built in Diagnostic Logging in Forefront TMG.

Diagnostic logging

You can start the Forefront TMG Diagnostic logging feature in the Troubleshooting node in the Forefront TMG Management console as shown in the following screenshot.



Use the diagnostic logging filter to view the events for a selected server.

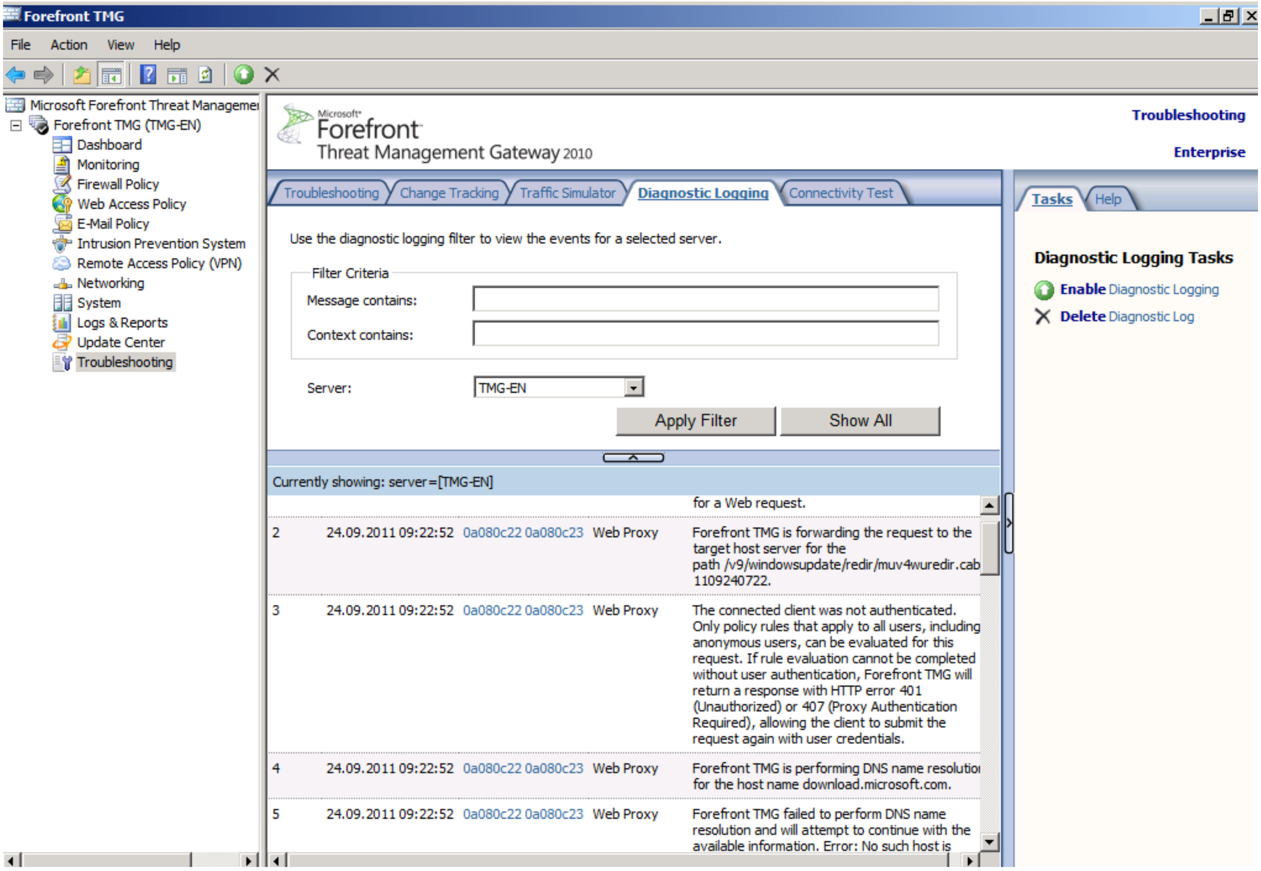
Message contains:

Context contains:

Server: TMG-EN

Figure 1: Forefront TMG Diagnostic Logging

Click *Enable Diagnostic Logging* to start the collection process
Forefront TMG starts now collecting running information from the TMG Server. After you decided that the collection process has collect enough data, you must disable the Diagnostic Logging to display the collected information.
As shown in the next screenshot, the Diagnostic logging process collected some more information which might be helpful for you to find the cause of a problem with Forefront TMG.



Use the diagnostic logging filter to view the events for a selected server.

Message contains:

Context contains:

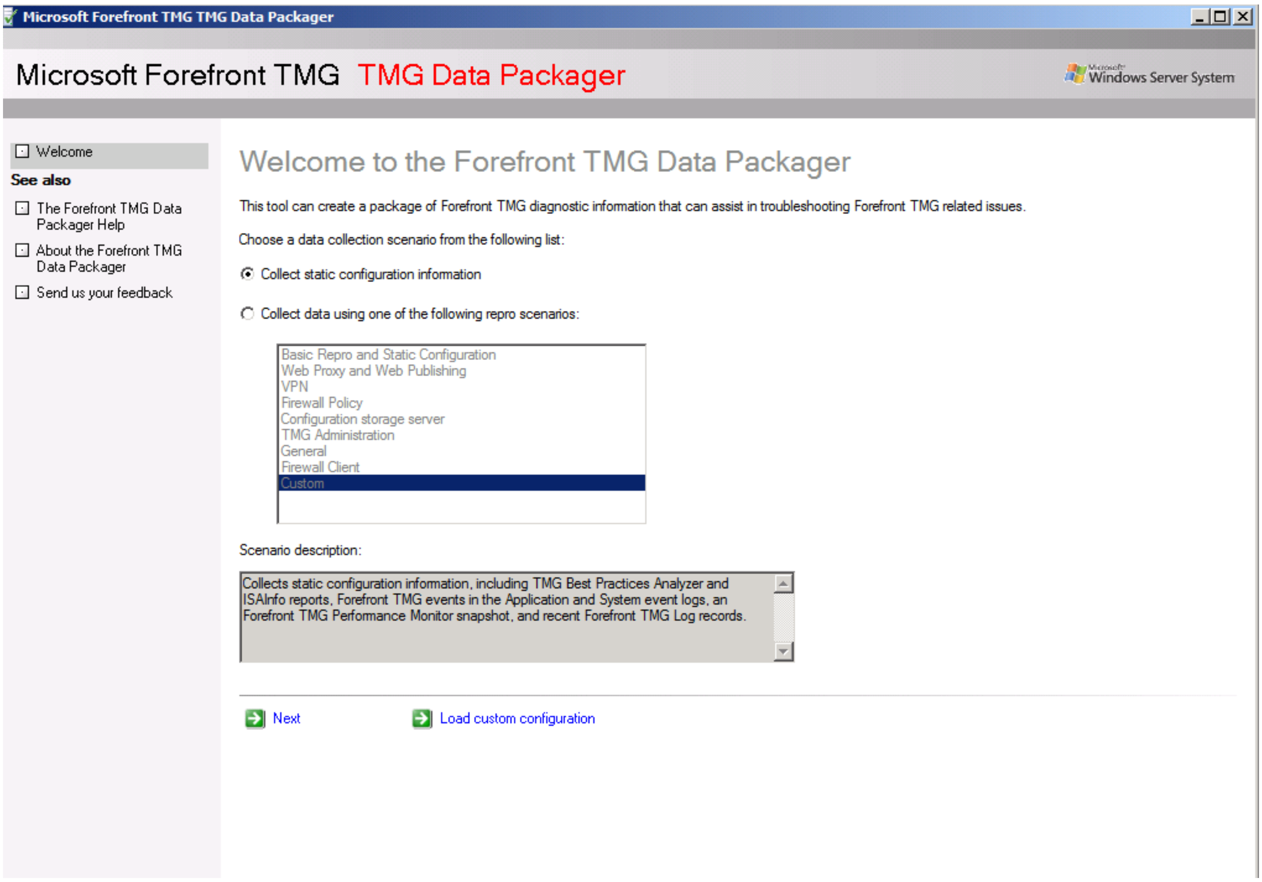
Server: TMG-EN

```
Currently showing: server=[TMG-EN]
                                                                  for a Web request.
2    24.09.2011 09:22:52  0a080c22 0a080c23  Web Proxy   Forefront TMG is forwarding the request to the
                                                         target host server for the
                                                         path /v9/windowsupdate/redir/muv4wuredir.cab
                                                         1109240722.
3    24.09.2011 09:22:52  0a080c22 0a080c23  Web Proxy   The connected client was not authenticated.
                                                         Only policy rules that apply to all users, including
                                                         anonymous users, can be evaluated for this
                                                         request. If rule evaluation cannot be completed
                                                         without user authentication, Forefront TMG will
                                                         return a response with HTTP error 401
                                                         (Unauthorized) or 407 (Proxy Authentication
                                                         Required), allowing the client to submit the
                                                         request again with user credentials.
4    24.09.2011 09:22:52  0a080c22 0a080c23  Web Proxy   Forefront TMG is performing DNS name resolutio
                                                         for the host name download.microsoft.com.
5    24.09.2011 09:22:52  0a080c22 0a080c23  Web Proxy   Forefront TMG failed to perform DNS name
                                                         resolution and will attempt to continue with the
                                                         available information. Error: No such host is
```

Figure 2: Analyze Forefront TMG Diagnostic Logging

Forefront TMG Data Packager

If the built in Diagnostic logging of Forefront TMG isn’t enough, you can use the Forefront TMG Data Packager which is part of the Forefront TMG Best Practices Analyzer. You will find the TMG Data Packager in the installation directory of the TMG BPA. Select the information you want to collect. We are starting with collecting static information. I will give you some information about the repro mode later in this article when we will use the TMGBPAPack.


Microsoft Forefront TMG TMG Data Packager
Microsoft Forefront TMG TMG Data Packager
Microsoft Windows Server System
Welcome
See also
The Forefront TMG Data Packager Help
About the Forefront TMG Data Packager
Send us your feedback
Next
Load custom configuration

Welcome to the Forefront TMG Data Packager

This tool can create a package of Forefront TMG diagnostic information that can assist in troubleshooting Forefront TMG related issues.

Choose a data collection scenario from the following list:

● Collect static configuration information

○ Collect data using one of the following repro scenarios:

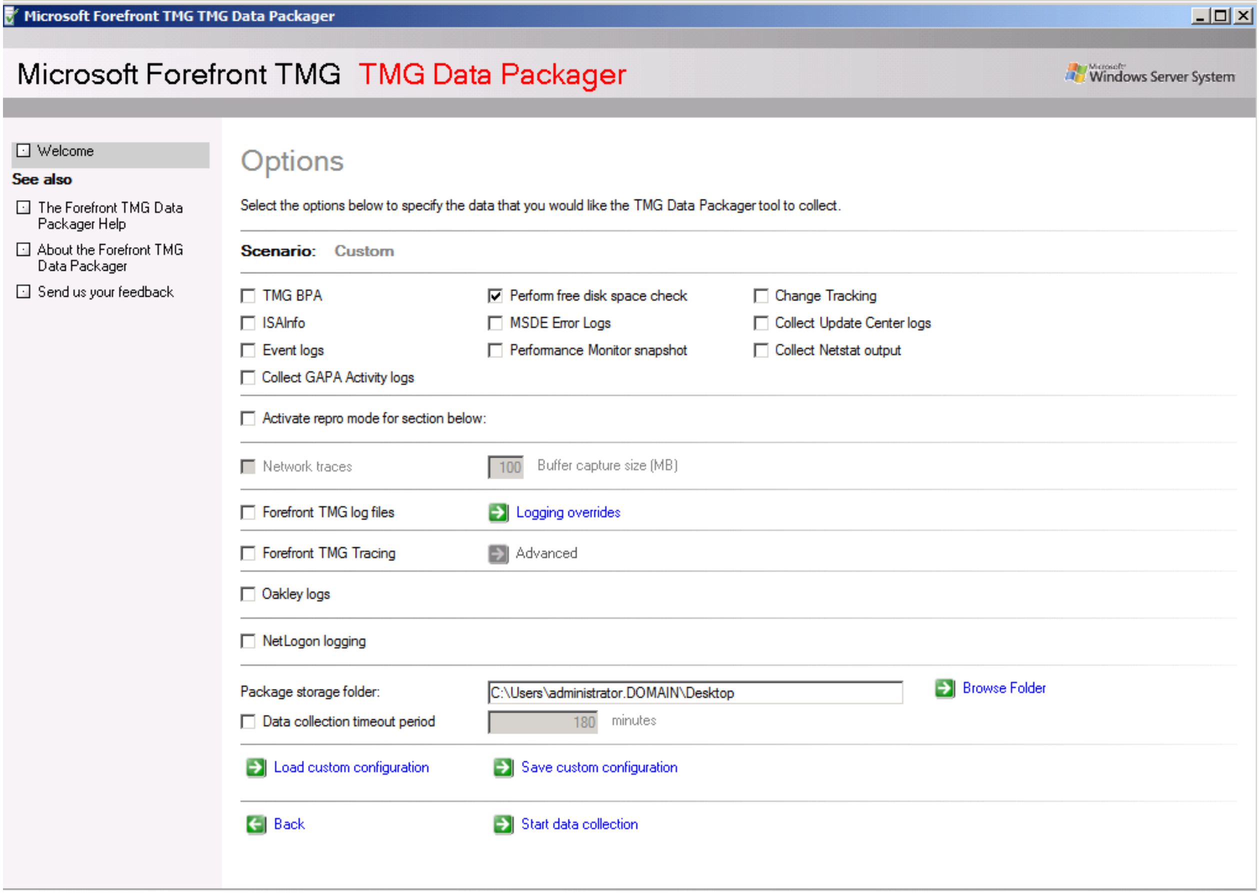
Basic Repro and Static Configuration
Web Proxy and Web Publishing
VPN
Firewall Policy
Configuration storage server
TMG Administration
General
Firewall Client
Custom

Scenario description:

Collects static configuration information, including TMG Best Practices Analyzer and ISAInfo reports, Forefront TMG events in the Application and System event logs, an Forefront TMG Performance Monitor snapshot, and recent Forefront TMG Log records.

Figure 3: Forefront TMG Data Packager

It is possible to customize which information the TMG Data Packager should collect.



Microsoft Forefront TMG TMG Data Packager

Microsoft Forefront TMG TMG Data Packager

Windows Server System
□ Welcome
See also
□ The Forefront TMG Data Packager Help
□ About the Forefront TMG Data Packager
□ Send us your feedback

Options

Select the options below to specify the data that you would like the TMG Data Packager tool to collect.

Scenario: Custom

□ TMG BPA
□ ISAInfo
□ Event logs
□ Collect GAPA Activity logs
☑ Perform free disk space check
□ MSDE Error Logs
□ Performance Monitor snapshot
□ Change Tracking
□ Collect Update Center logs
□ Collect Netstat output

□ Activate repro mode for section below:

□ Network traces — 100 Buffer capture size (MB)

□ Forefront TMG log files — Logging overrides

□ Forefront TMG Tracing — Advanced

□ Oakley logs

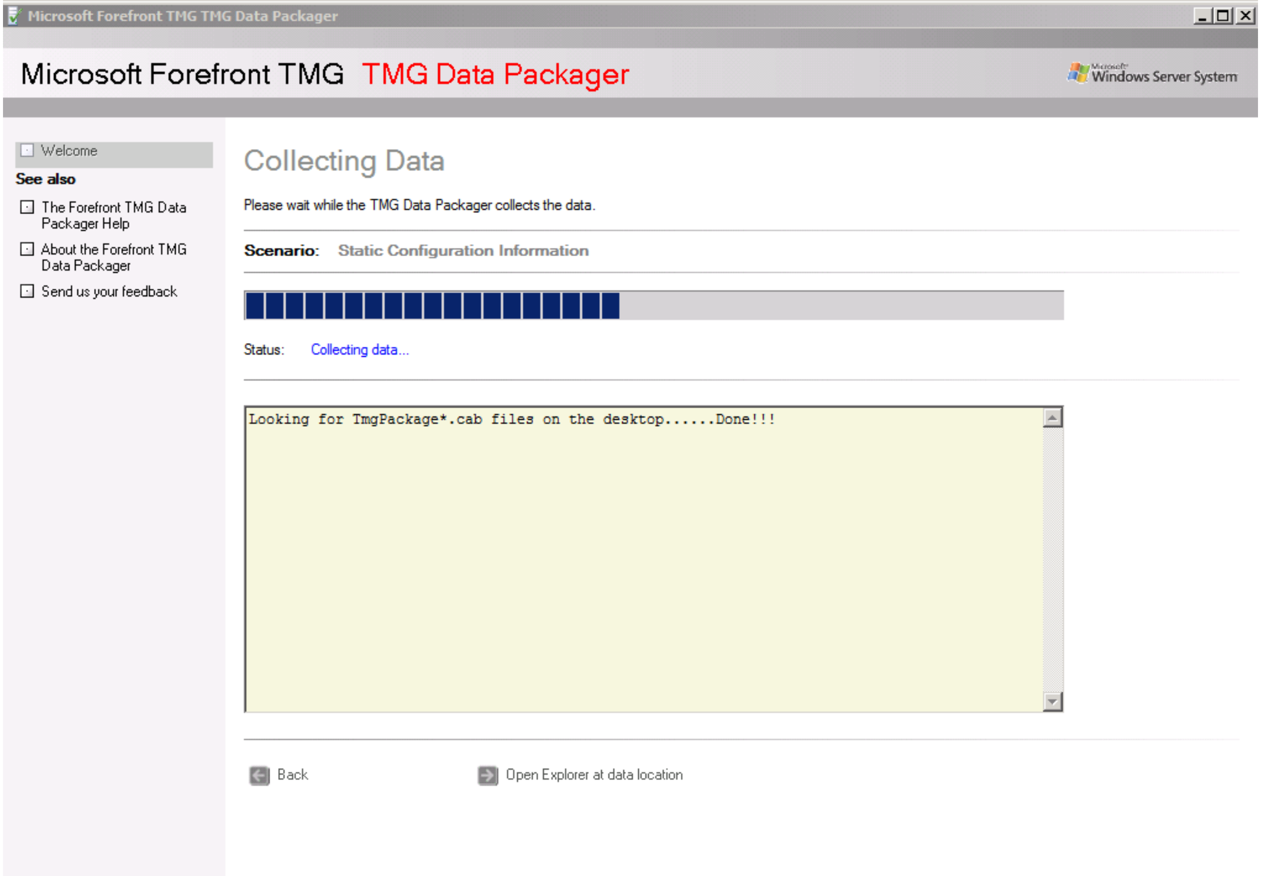
□ NetLogon logging

Package storage folder: C:\Users\administrator.DOMAIN\Desktop — Browse Folder

□ Data collection timeout period — 180 minutes

Figure 4: Forefront TMG Data Packager – Specify information to collect

Start Data collection. It could take some times until the TMG Data Packager has collected all information.



Microsoft Forefront TMG TMG Data Packager

Microsoft Forefront TMG TMG Data Packager

Windows Server System
Welcome
See also
The Forefront TMG Data Packager Help
About the Forefront TMG Data Packager
Send us your feedback
Back
Open Explorer at data location

Collecting Data

Please wait while the TMG Data Packager collects the data.

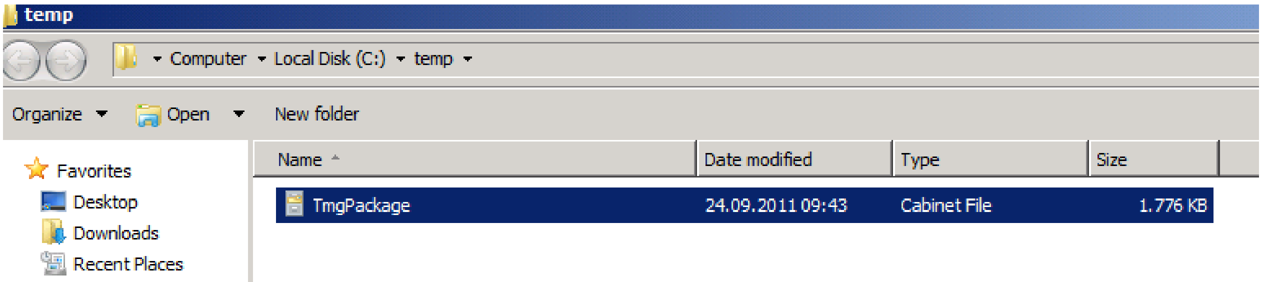
Scenario: Static Configuration Information

Status: Collecting data...

```
Looking for TmgPackage*.cab files on the desktop......Done!!!
```

Figure 5: Forefront TMG Data Packager – Collecting data

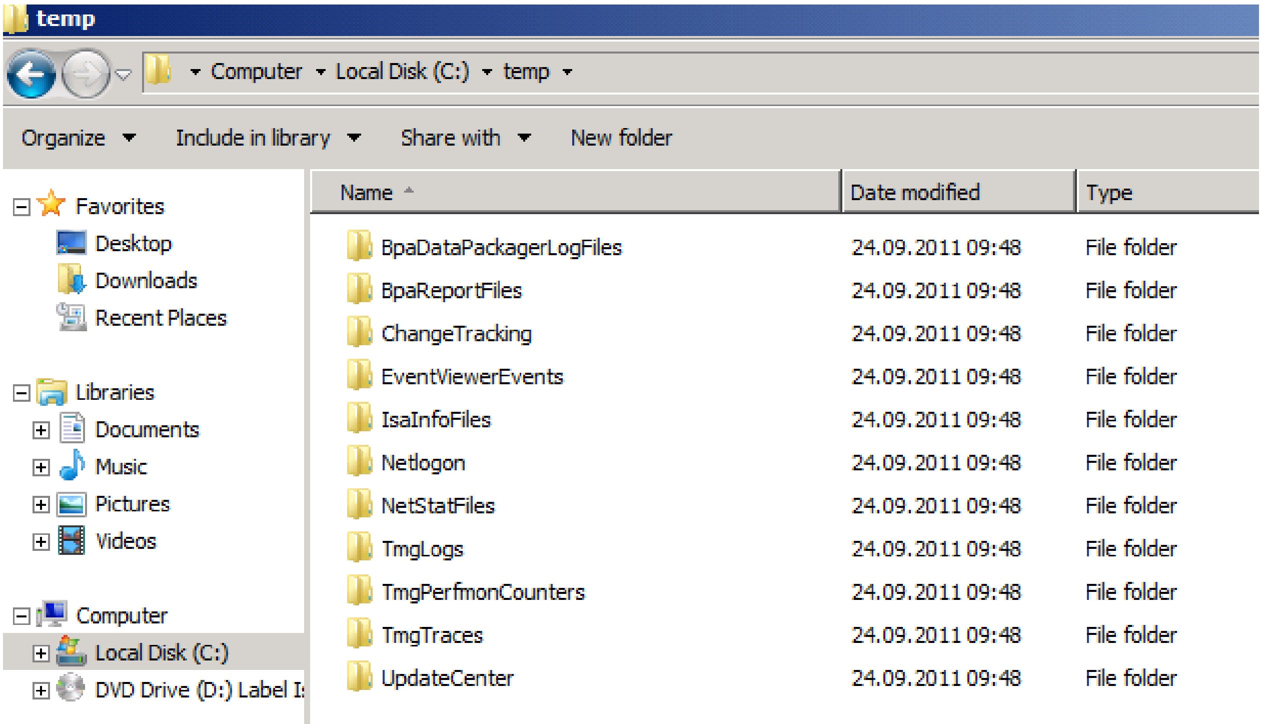
After the collection process has been finished you will find a .cab file with all collected information in the directory you specified earlier. You can now use this .cab file to archive the information or to send it to Microsoft Product Support service or if you want to analyze the collected information you have to use a tool which extracts the information of the .cab file.



Name	Date modified	Type	Size
TmgPackage	24.09.2011 09:43	Cabinet File	1.776 KB

Figure 6: Forefront TMG Data package

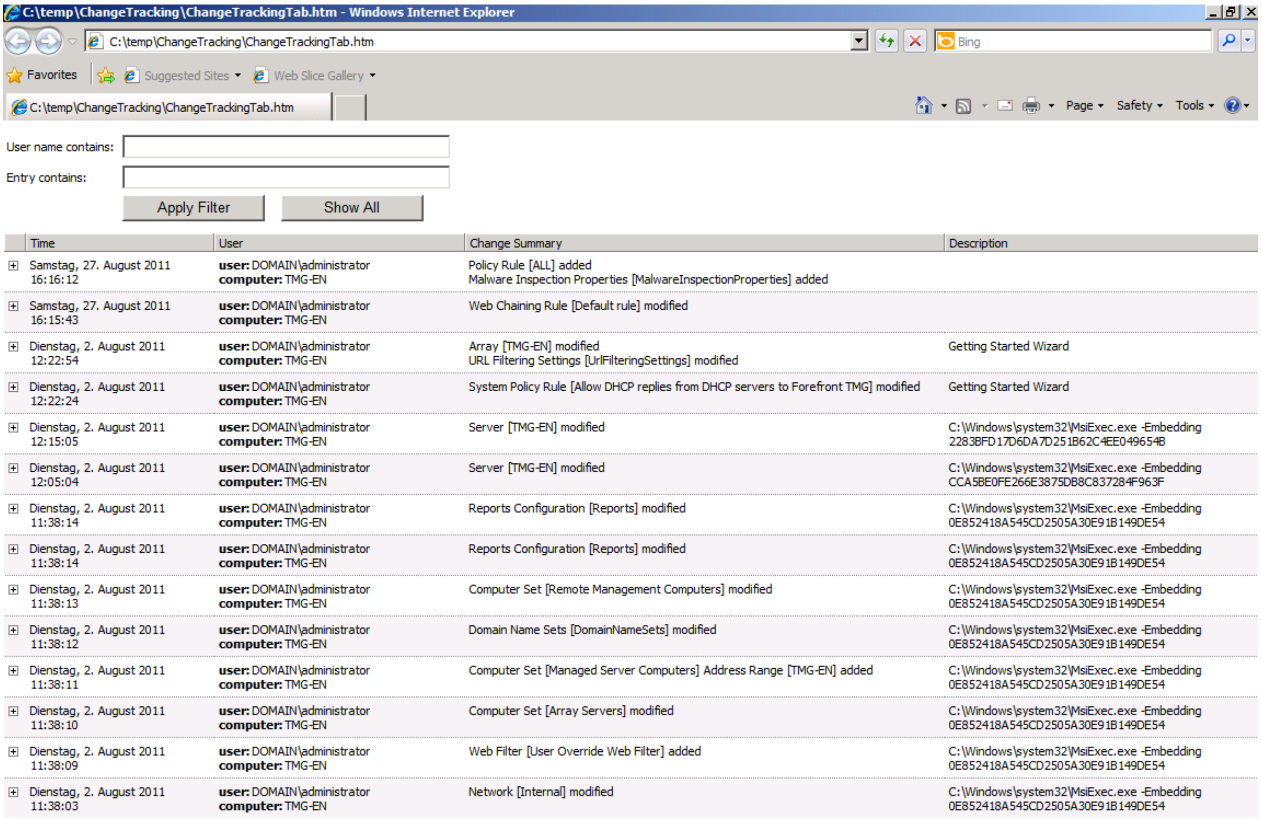
As shown in the following screenshot you can see the extracted cab file. I will give you some examples about the content of the cab file in the following screenshots.



Name	Date modified	Type
BpaDataPackagerLogFiles	24.09.2011 09:48	File folder
BpaReportFiles	24.09.2011 09:48	File folder
ChangeTracking	24.09.2011 09:48	File folder
EventViewerEvents	24.09.2011 09:48	File folder
IsaInfoFiles	24.09.2011 09:48	File folder
Netlogon	24.09.2011 09:48	File folder
NetStatFiles	24.09.2011 09:48	File folder
TmgLogs	24.09.2011 09:48	File folder
TmgPerfmonCounters	24.09.2011 09:48	File folder
TmgTraces	24.09.2011 09:48	File folder
UpdateCenter	24.09.2011 09:48	File folder

Figure 7: Content of Forefront TMG Data Packager

The TMG Data Packager collects information about the Forefront TMG Change tracking feature which contains all information which Administrator changed the Forefront TMG configuration.


C:\temp\ChangeTracking\ChangeTrackingTab.htm - Windows Internet Explorer
C:\temp\ChangeTracking\ChangeTrackingTab.htm
Bing
Favorites
Suggested Sites ▾
Web Slice Gallery ▾
C:\temp\ChangeTracking\ChangeTrackingTab.htm
Page ▾
Safety ▾
Tools ▾
Apply Filter
Show All

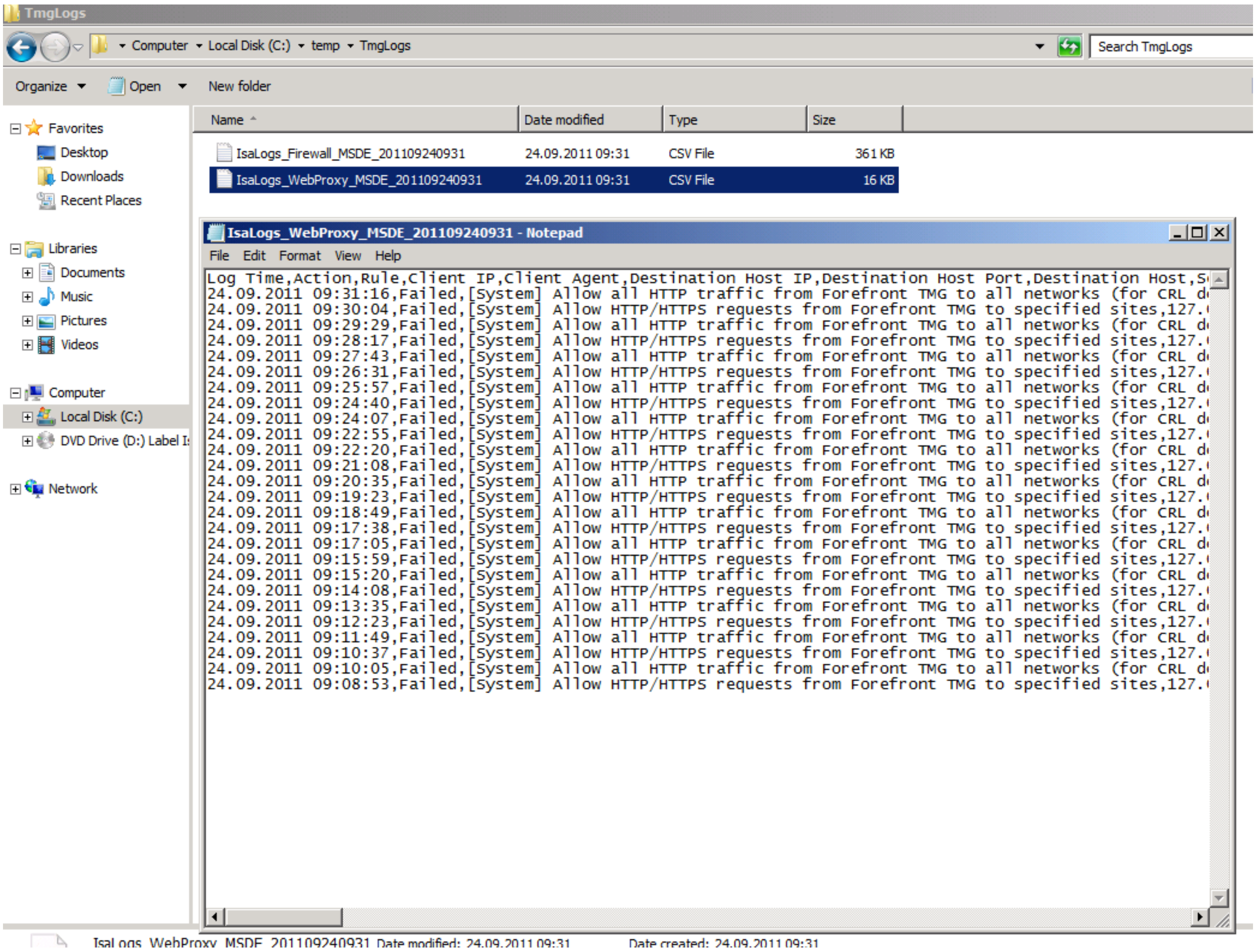
User name contains:

Entry contains:

Time	User	Change Summary	Description
Samstag, 27. August 2011 16:16:12	**user:** DOMAIN\administrator **computer:** TMG-EN	Policy Rule [ALL] added Malware Inspection Properties [MalwareInspectionProperties] added	
Samstag, 27. August 2011 16:15:43	**user:** DOMAIN\administrator **computer:** TMG-EN	Web Chaining Rule [Default rule] modified	
Dienstag, 2. August 2011 12:22:54	**user:** DOMAIN\administrator **computer:** TMG-EN	Array [TMG-EN] modified URL Filtering Settings [UrlFilteringSettings] modified	Getting Started Wizard
Dienstag, 2. August 2011 12:22:24	**user:** DOMAIN\administrator **computer:** TMG-EN	System Policy Rule [Allow DHCP replies from DHCP servers to Forefront TMG] modified	Getting Started Wizard
Dienstag, 2. August 2011 12:15:05	**user:** DOMAIN\administrator **computer:** TMG-EN	Server [TMG-EN] modified	C:\Windows\system32\MsiExec.exe -Embedding 2283BFD17D6DA7D251B62C4EE049654B
Dienstag, 2. August 2011 12:05:04	**user:** DOMAIN\administrator **computer:** TMG-EN	Server [TMG-EN] modified	C:\Windows\system32\MsiExec.exe -Embedding CCA5BE0FE266E3875DB8C837284F963F
Dienstag, 2. August 2011 11:38:14	**user:** DOMAIN\administrator **computer:** TMG-EN	Reports Configuration [Reports] modified	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:14	**user:** DOMAIN\administrator **computer:** TMG-EN	Reports Configuration [Reports] modified	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:13	**user:** DOMAIN\administrator **computer:** TMG-EN	Computer Set [Remote Management Computers] modified	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:12	**user:** DOMAIN\administrator **computer:** TMG-EN	Domain Name Sets [DomainNameSets] modified	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:11	**user:** DOMAIN\administrator **computer:** TMG-EN	Computer Set [Managed Server Computers] Address Range [TMG-EN] added	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:10	**user:** DOMAIN\administrator **computer:** TMG-EN	Computer Set [Array Servers] modified	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:09	**user:** DOMAIN\administrator **computer:** TMG-EN	Web Filter [User Override Web Filter] added	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54
Dienstag, 2. August 2011 11:38:03	**user:** DOMAIN\administrator **computer:** TMG-EN	Network [Internal] modified	C:\Windows\system32\MsiExec.exe -Embedding 0E852418A545CD2505A30E91B149DE54

Figure 8: Forefront TMG Change tracking extracted from the TMG Data Packager

The TMG Data Packager also collects log information about the Webproxy and Firewall Service of Forefront TMG.



Name	Date modified	Type	Size
IsaLogs_Firewall_MSDE_201109240931	24.09.2011 09:31	CSV File	361 KB
IsaLogs_WebProxy_MSDE_201109240931	24.09.2011 09:31	CSV File	16 KB

IsaLogs_WebProxy_MSDE_201109240931 - Notepad

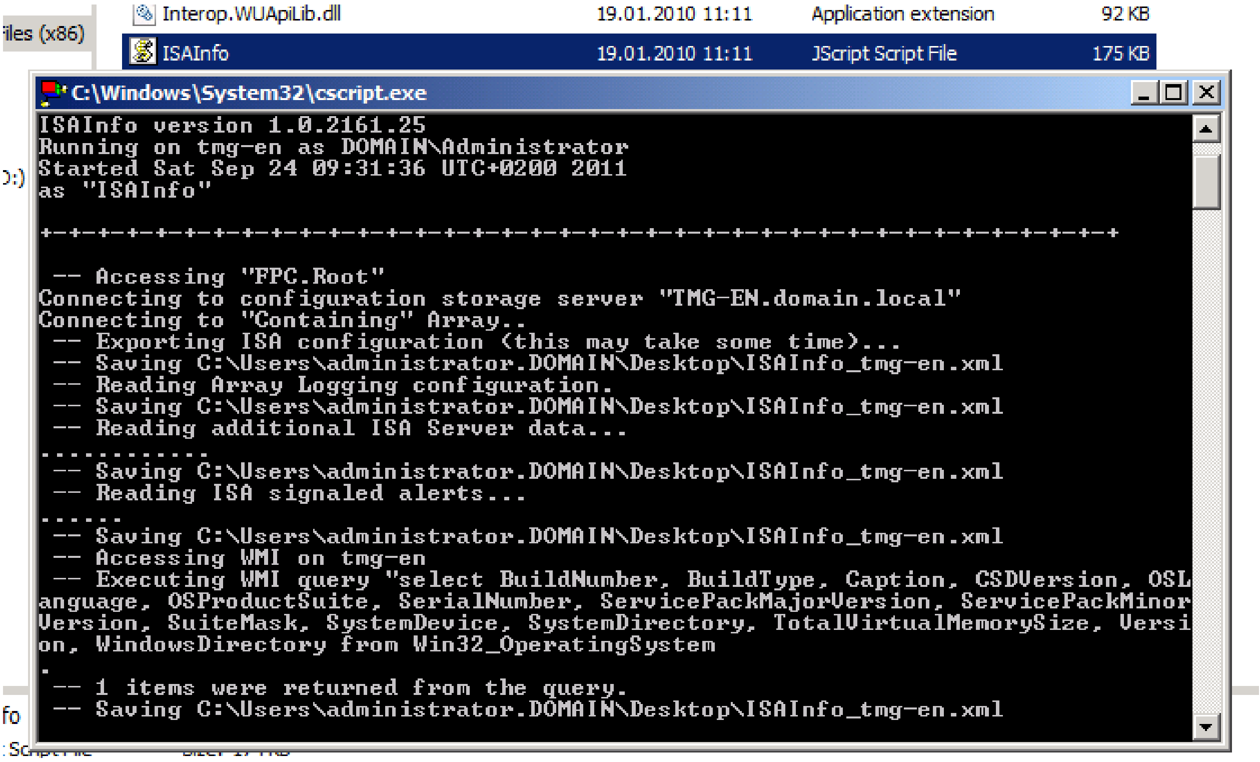
```
Log Time,Action,Rule,Client IP,Client Agent,Destination Host IP,Destination Host Port,Destination Host,S
24.09.2011 09:31:16,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:30:04,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:29:29,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:28:17,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:27:43,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:26:31,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:25:57,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:24:40,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:24:07,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:22:55,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:22:20,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:21:08,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:20:35,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:19:23,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:18:49,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:17:38,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:17:05,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:15:59,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:15:20,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:14:08,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:13:35,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:12:23,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:11:49,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:10:37,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
24.09.2011 09:10:05,Failed,[System] Allow all HTTP traffic from Forefront TMG to all networks (for CRL d
24.09.2011 09:08:53,Failed,[System] Allow HTTP/HTTPS requests from Forefront TMG to specified sites,127.
```

IsaLogs_WebProxy_MSDE_201109240931 Date modified: 24.09.2011 09:31 Date created: 24.09.2011 09:31

Figure 9: Forefront TMG Data Packager – Firewall and Webproxy log

ISAInfo

The next tool is ISAInfo. Most of you might be familiar with ISAInfo which is available at www.isatools.org. This website is hosted by Jim Harrison. ISAInfo in ISA Server times was a very helpful tool to collect information about your ISA Server machines. This tool is also included in the Forefront TMG Best Practices Analyzer tool.

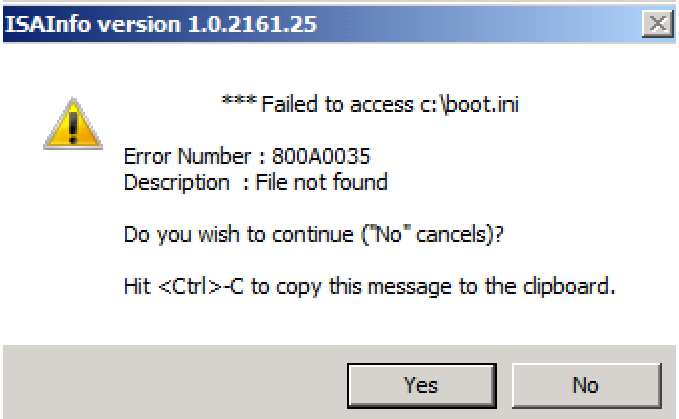


```
Interop.WUApiLib.dll    19.01.2010 11:11    Application extension     92 KB
ISAInfo                 19.01.2010 11:11    JScript Script File      175 KB
```

```
ISAInfo version 1.0.2161.25
Running on tmg-en as DOMAIN\Administrator
Started Sat Sep 24 09:31:36 UTC+0200 2011
as "ISAInfo"

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

 -- Accessing "FPC.Root"
Connecting to configuration storage server "TMG-EN.domain.local"
Connecting to "Containing" Array..
 -- Exporting ISA configuration (this may take some time)...
 -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
 -- Reading Array Logging configuration.
 -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
 -- Reading additional ISA Server data...
............
 -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
 -- Reading ISA signaled alerts...
......
 -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
 -- Accessing WMI on tmg-en
 -- Executing WMI query "select BuildNumber, BuildType, Caption, CSDVersion, OSL
anguage, OSProductSuite, SerialNumber, ServicePackMajorVersion, ServicePackMinor
Version, SuiteMask, SystemDevice, SystemDirectory, TotalVirtualMemorySize, Versi
on, WindowsDirectory from Win32_OperatingSystem
.
 -- 1 items were returned from the query.
 -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
```

Figure 10: Forefront TMG – ISAInfo is collecting data

Because the tool seems not to be completely redesigned to work with Forefront TMG you will get some error message popup boxes until the ISAInfo collection process is running but you can ignore the messages.



*** Failed to access c:\boot.ini

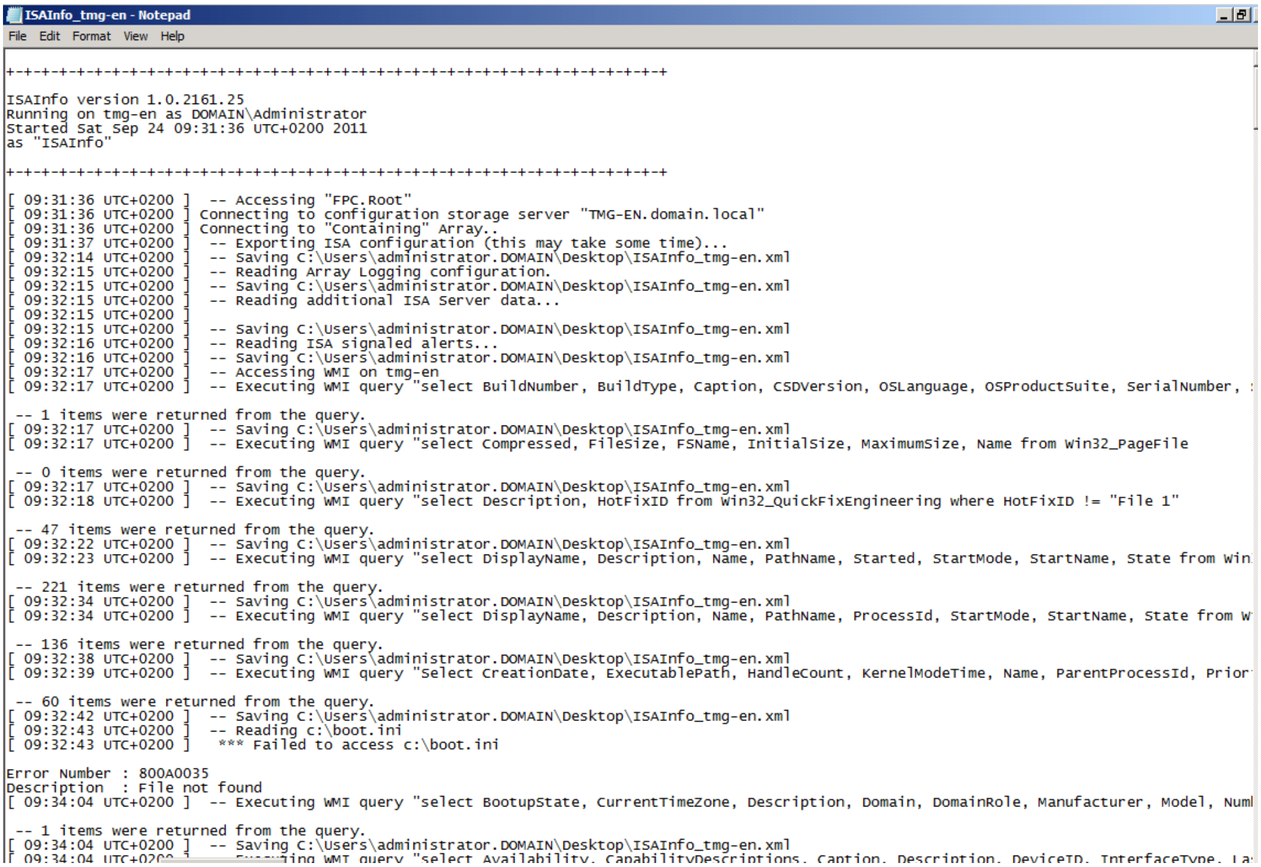
Error Number : 800A0035
Description : File not found

Do you wish to continue ("No" cancels)?

Hit <Ctrl>-C to copy this message to the clipboard.

Figure 11: Forefront TMG ISAInfo . Ignore warning message

ISAInfo creates two files. A log file with ISAInfo tools information and a XML file with the entire information about your Forefront TMG Server.



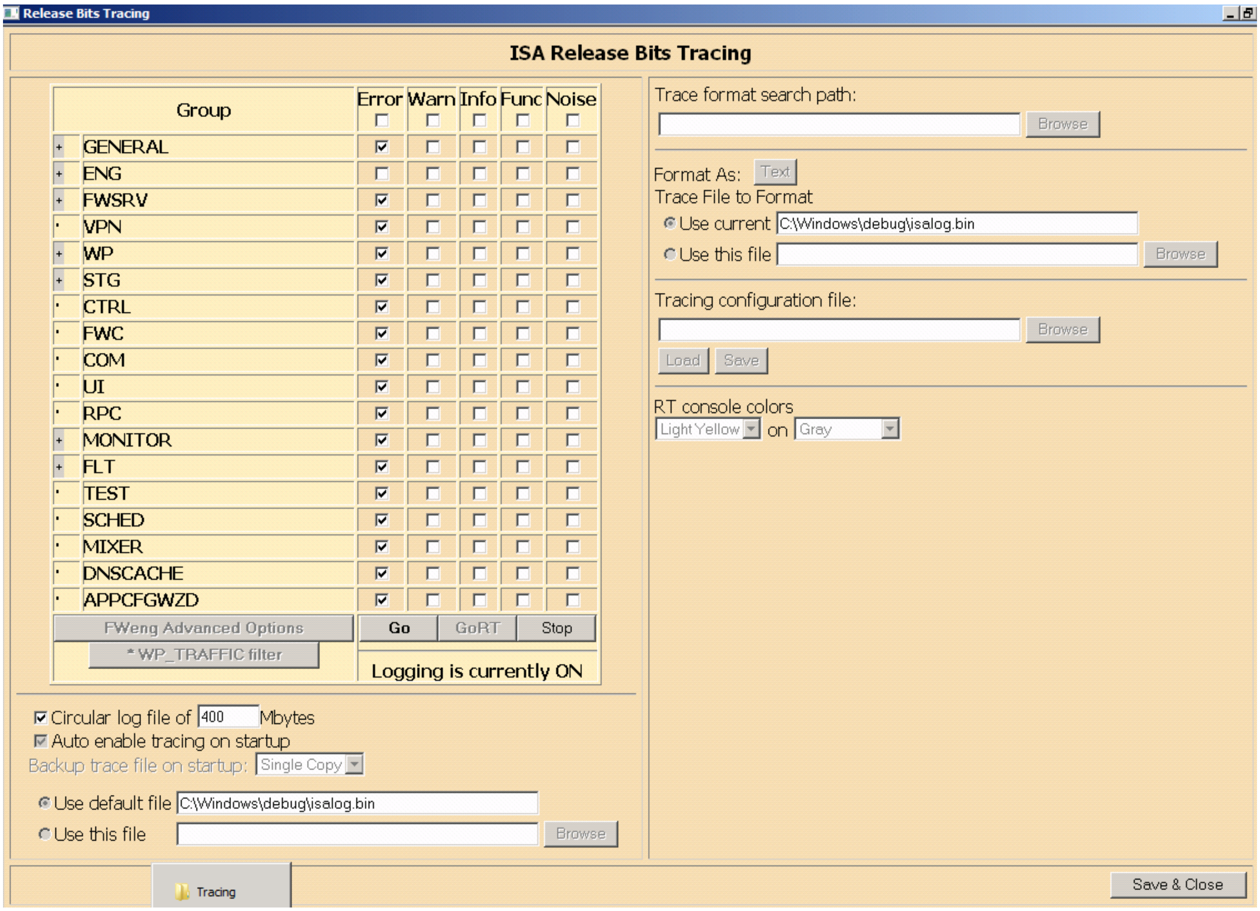
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

ISAInfo version 1.0.2161.25
Running on tmg-en as DOMAIN\Administrator
Started Sat Sep 24 09:31:36 UTC+0200 2011
as "ISAInfo"

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

[ 09:31:36 UTC+0200 ]  -- Accessing "FPC.Root"
[ 09:31:36 UTC+0200 ] Connecting to configuration storage server "TMG-EN.domain.local"
[ 09:31:36 UTC+0200 ] Connecting to "Containing" Array..
[ 09:31:37 UTC+0200 ]  -- Exporting ISA configuration (this may take some time)...
[ 09:32:14 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:15 UTC+0200 ]  -- Reading Array Logging configuration.
[ 09:32:15 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:15 UTC+0200 ]  -- Reading additional ISA Server data...
[ 09:32:15 UTC+0200 ]
[ 09:32:15 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:16 UTC+0200 ]  -- Reading ISA signaled alerts...
[ 09:32:16 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:17 UTC+0200 ]  -- Accessing WMI on tmg-en
[ 09:32:17 UTC+0200 ]  -- Executing WMI query "select BuildNumber, BuildType, Caption, CSDVersion, OSLanguage, OSProductSuite, SerialNumber, :

 -- 1 items were returned from the query.
[ 09:32:17 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:17 UTC+0200 ]  -- Executing WMI query "select Compressed, FileSize, FSName, InitialSize, MaximumSize, Name from Win32_PageFile

 -- 0 items were returned from the query.
[ 09:32:17 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:18 UTC+0200 ]  -- Executing WMI query "select Description, HotFixID from Win32_QuickFixEngineering where HotFixID != "File 1"

 -- 47 items were returned from the query.
[ 09:32:22 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:23 UTC+0200 ]  -- Executing WMI query "select DisplayName, Description, Name, PathName, Started, StartMode, StartName, State from Win

 -- 221 items were returned from the query.
[ 09:32:34 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:34 UTC+0200 ]  -- Executing WMI query "select DisplayName, Description, Name, PathName, ProcessId, StartMode, StartName, State from W

 -- 136 items were returned from the query.
[ 09:32:38 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:39 UTC+0200 ]  -- Executing WMI query "Select CreationDate, ExecutablePath, HandleCount, KernelModeTime, Name, ParentProcessId, Prior

 -- 60 items were returned from the query.
[ 09:32:42 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:32:43 UTC+0200 ]  -- Reading c:\boot.ini
[ 09:32:43 UTC+0200 ]   *** Failed to access c:\boot.ini

Error Number : 800A0035
Description  : File not found
[ 09:34:04 UTC+0200 ]  -- Executing WMI query "select BootupState, CurrentTimeZone, Description, Domain, DomainRole, Manufacturer, Model, Numl

 -- 1 items were returned from the query.
[ 09:34:04 UTC+0200 ]  -- Saving C:\Users\administrator.DOMAIN\Desktop\ISAInfo_tmg-en.xml
[ 09:34:04 UTC+0200 ]  -- Executing WMI query "select Availability, CapabilityDescriptions, Caption, Description, DeviceID, InterfaceType, La
```

Figure 12: Forefront TMG – ISAInfo log file

ISATRACE

The next tool is ISATRACE. Beginnig with ISA Server 2004 SP2 (if I remember correctly), Microsoft started to collect advanced ISA information in a .bin file on the local file system (ISALOG.BIN). The Forefront TMG Best Practices Analyzer contains a GUI tool which you can use to customize the amount of information which should be logged. You can find the tool in the directory named *Tracing* under the installation directory of the TMG BPA.

The tool allows you to select if you want to collect information for the several Forefront TMG components like Firewall service, Webproxy service, Firewall Control Channel (client), User Interface and many more. It is also possible to change the default directory for the log file and the size of the ISATRACE file.



Release Bits Tracing

ISA Release Bits Tracing

	Group	Error	Warn	Info	Func	Noise
		☐	☐	☐	☐	☐
+	GENERAL	☑	☐	☐	☐	☐
+	ENG	☐	☐	☐	☐	☐
+	FWSRV	☑	☐	☐	☐	☐
·	VPN	☑	☐	☐	☐	☐
+	WP	☑	☐	☐	☐	☐
+	STG	☑	☐	☐	☐	☐
·	CTRL	☑	☐	☐	☐	☐
·	FWC	☑	☐	☐	☐	☐
·	COM	☑	☐	☐	☐	☐
·	UI	☑	☐	☐	☐	☐
·	RPC	☑	☐	☐	☐	☐
+	MONITOR	☑	☐	☐	☐	☐
+	FLT	☑	☐	☐	☐	☐
·	TEST	☑	☐	☐	☐	☐
·	SCHED	☑	☐	☐	☐	☐
·	MIXER	☑	☐	☐	☐	☐
·	DNSCACHE	☑	☐	☐	☐	☐
·	APPCFGWZD	☑	☐	☐	☐	☐

Logging is currently ON

☑ Circular log file of 400 Mbytes
☑ Auto enable tracing on startup
Backup trace file on startup: Single Copy

● Use default file C:\Windows\debug\isalog.bin
○ Use this file

Trace format search path:

Format As: Text
Trace File to Format
● Use current C:\Windows\debug\isalog.bin
○ Use this file

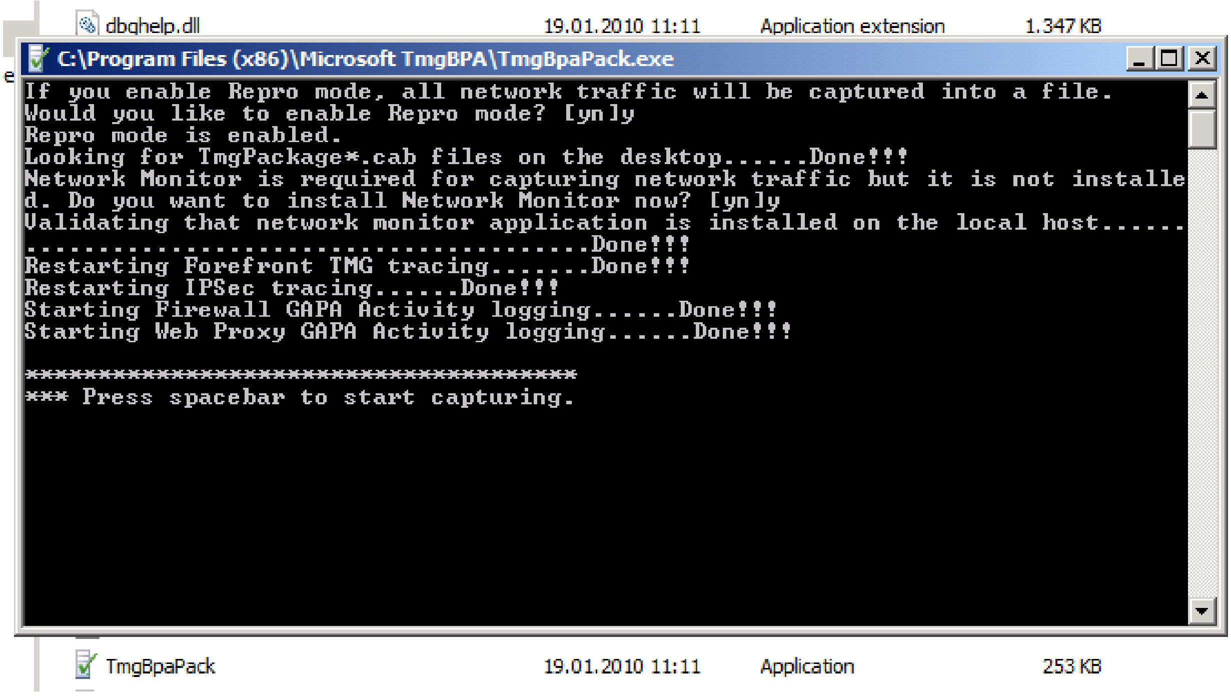
Tracing configuration file:

RT console colors
LightYellow on Gray

Figure 13: Forefront TMG – "ISA" Release Bits tracking

TMGBPAPack

The TMGBPAPack is also part of the Forefront TMG Best Practices Analyzer. It is a command line tool very similar to the TMG Data Packager with some exceptions (the only difference I'm aware of is that this tool also collects network traffic with the help of Microsoft Netmon 3.3). If you enable the Repro Mode all network traffic will be captured into Netmon trace files.

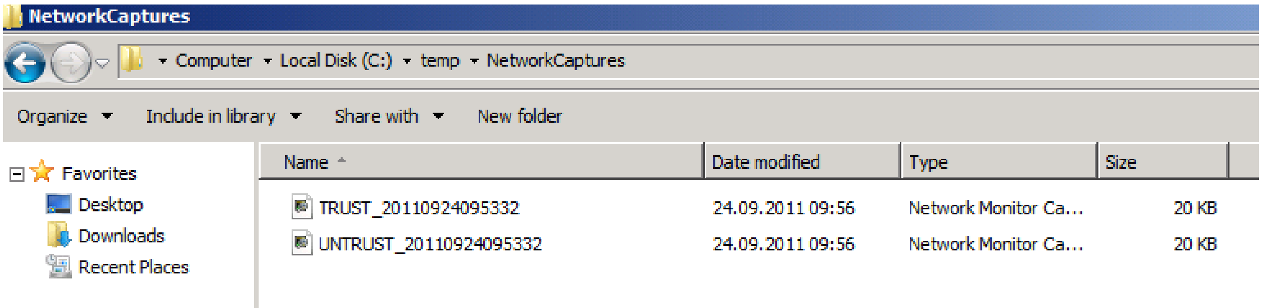


dbghelp.dll	19.01.2010 11:11	Application extension	1.347 KB
TmgBpaPack	19.01.2010 11:11	Application	253 KB

```
If you enable Repro mode, all network traffic will be captured into a file.
Would you like to enable Repro mode? [yn]y
Repro mode is enabled.
Looking for TmgPackage*.cab files on the desktop......Done!!!
Network Monitor is required for capturing network traffic but it is not installe
d. Do you want to install Network Monitor now? [yn]y
Validating that network monitor application is installed on the local host......
.........................................Done!!!
Restarting Forefront TMG tracing.......Done!!!
Restarting IPSec tracing......Done!!!
Starting Firewall GAPA Activity logging......Done!!!
Starting Web Proxy GAPA Activity logging......Done!!!

****************************************
*** Press spacebar to start capturing.
```

Figure 14: Forefront TMG BPA Pack is collecting informations

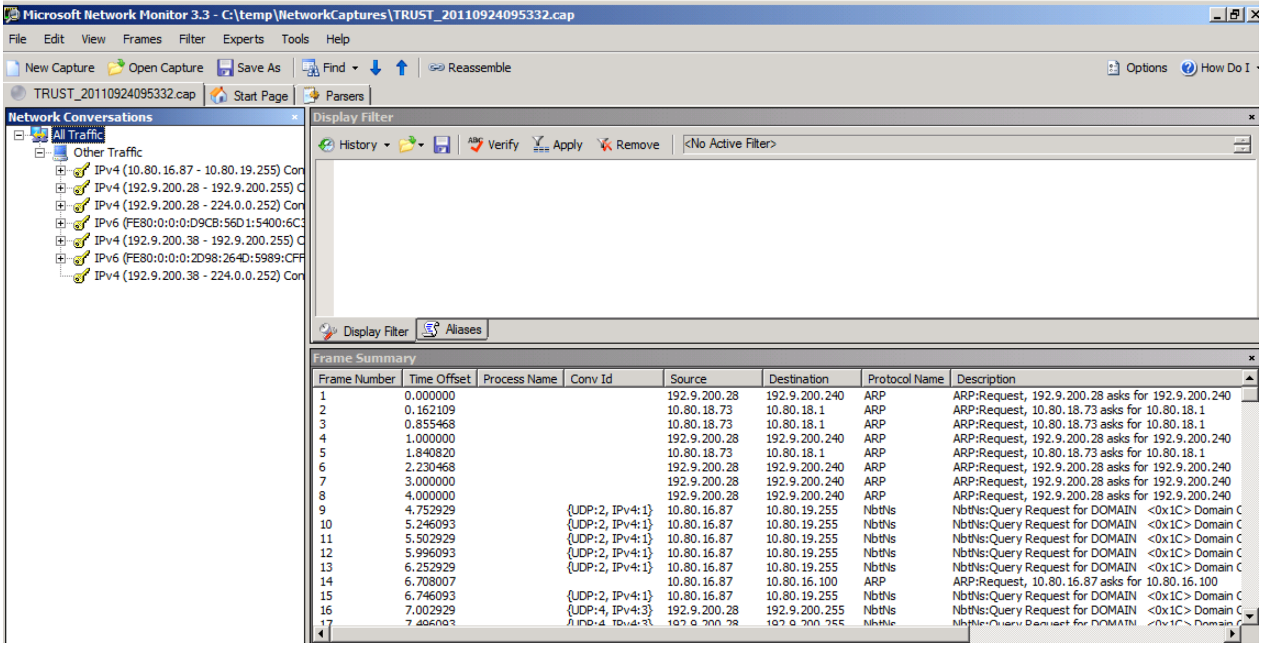
If the Microsoft Network Monitor is not installed, the TMGBPAPack installs Microsoft Netmon 3.3 (the latest available version of Netmon on the Internet is 3.4).
After you stopped the Netmon trace, the TMGDATAPack creates a single .cab file on the Desktop which you can extract to the local file system and there you will find one additional directory called *NetworkCaptures* which contains the Netmon Capture files.



Name	Date modified	Type	Size
TRUST_20110924095332	24.09.2011 09:56	Network Monitor Ca...	20 KB
UNTRUST_20110924095332	24.09.2011 09:56	Network Monitor Ca...	20 KB

Figure 15: Forefront TMG BPA Pack – collected Netmon traces

You can now use the installed version of the Microsoft Network Monitor to analyze the Netmon capture files as shown in the following screenshot.



All Traffic
Other Traffic
IPv4 (10.80.16.87 - 10.80.19.255) Con
IPv4 (192.9.200.28 - 192.9.200.255) C
IPv4 (192.9.200.28 - 224.0.0.252) Con
IPv6 (FE80:0:0:0:D9CB:56D1:5400:6C3
IPv4 (192.9.200.38 - 192.9.200.255) C
IPv6 (FE80:0:0:0:2D98:264D:5989:CFF
IPv4 (192.9.200.38 - 224.0.0.252) Con

Frame Number	Time Offset	Process Name	Conv Id	Source	Destination	Protocol Name	Description
1	0.000000			192.9.200.28	192.9.200.240	ARP	ARP:Request, 192.9.200.28 asks for 192.9.200.240
2	0.162109			10.80.18.73	10.80.18.1	ARP	ARP:Request, 10.80.18.73 asks for 10.80.18.1
3	0.855468			10.80.18.73	10.80.18.1	ARP	ARP:Request, 10.80.18.73 asks for 10.80.18.1
4	1.000000			192.9.200.28	192.9.200.240	ARP	ARP:Request, 192.9.200.28 asks for 192.9.200.240
5	1.840820			10.80.18.73	10.80.18.1	ARP	ARP:Request, 10.80.18.73 asks for 10.80.18.1
6	2.230468			192.9.200.28	192.9.200.240	ARP	ARP:Request, 192.9.200.28 asks for 192.9.200.240
7	3.000000			192.9.200.28	192.9.200.240	ARP	ARP:Request, 192.9.200.28 asks for 192.9.200.240
8	4.000000			192.9.200.28	192.9.200.240	ARP	ARP:Request, 192.9.200.28 asks for 192.9.200.240
9	4.752929		{UDP:2, IPv4:1}	10.80.16.87	10.80.19.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
10	5.246093		{UDP:2, IPv4:1}	10.80.16.87	10.80.19.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
11	5.502929		{UDP:2, IPv4:1}	10.80.16.87	10.80.19.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
12	5.996093		{UDP:2, IPv4:1}	10.80.16.87	10.80.19.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
13	6.252929		{UDP:2, IPv4:1}	10.80.16.87	10.80.19.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
14	6.708007			10.80.16.87	10.80.16.100	ARP	ARP:Request, 10.80.16.87 asks for 10.80.16.100
15	6.746093		{UDP:2, IPv4:1}	10.80.16.87	10.80.19.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
16	7.002929		{UDP:4, IPv4:3}	192.9.200.28	192.9.200.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C
17	7.496093		{UDP:4, IPv4:3}	192.9.200.28	192.9.200.255	NbtNs	NbtNs:Query Request for DOMAIN <0x1C> Domain C

Figure 16: Microsoft Netmon 3.3 trace of Forefront TMG traffic on the internal network interface

Conclusion

In this article I tried to show you how to use several helpful tools of Forefront TMG and the TMG Best Practice Analyser to collect advanced information about the Forefront TMG configuration and the log files generated from Forefront TMG or the underlying Windows operating system. You can use this information for documentation purposes or to analyse problems with the TMG configuration. The created data is also helpful for Microsoft if you open a case with the Microsoft product support.

Related links

Forefront TMG BPA Download
http://www.microsoft.com/download/en/details.aspx?id=17730
Forefront TMG Best Practices Analyzer
http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Best-Practice-Analyzer.html
New Options on TMG Data Packager
http://blogs.technet.com/b/yuridiogenes/archive/2010/03/07/new-options-on-tmg-data-packager.aspx
Using TMG BPA Data Packager to Troubleshoot Exchange / Lync / Sharepoint connectivity
http://blogs.technet.com/b/brennan-crowe/archive/2011/03/02/using-tmg-data-packager-to-troubleshoot-exchange-web-lync-web-and-sharepoint-connectivity.aspx