# **Troubleshooting Forefront TMG**

# Abstract

In this article I will show you some helpful Forefront TMG troubleshooting tools for general and special troubleshooting issues with Forefront TMG. We will have a look into Forefront TMG log files, Windows Event viewer, TMG Best Practice Analyzer (TMG-BPA), TMG Data packager, PAL and some other tools and techniques.

# Let's begin

Troubleshooting Forefront TMG problems can be complicated and time consuming because of the various possible types of problems. Independently from available tools and techniques for troubleshooting Forefront TMG problems, you should follow the concept called <u>KISS</u> (Keep it simple, Stupid!). KISS in my opinion means; start with some simple troubleshooting approaches before you start with Kernel debugging ©. With KISS in mind you can start troubleshooting with simple questions like: Does it work from other clients? Is the problem repeatable? Does it worked a while ago?

**Please keep in mind**: This article doesn't give you solutions for specific problems. This guide was written to give you an overview about troubleshooting technologies and tools with the goal that you can use some tools to troubleshoot your specific problems.

For this article I will give you some insights into the following tools and techniques:

- Forefront TMG Dashboard
- Forefront TMG Logging
- Windows Event viewer
- Forefront TMG log files
- Forefront TMG Best Practice Analyzer
- Forefront TMG Data Packager
- Microsoft Network Monitor (Netmon)
- TMG built in tools
- NETSH
- Forefront TMG Diagnostic Logging
- FWENGTRACE
- ISATRACE
- Perfmon
- PAL (Performance Analysis of Logs)
- TMG Superflow

## Forefront TMG Dashboard

The Forefront TMG Dashboard should be one of the first places where a Forefront TMG Administrator should spend some time, because it is the central point to see the health status of your Forefront TMG Server.

Forefro	ont										Dashboar
	lanageme	ent Ga	iteway	2010							Enterpris
Dashboard		_									
🔇 Alerts				8	Sessions						8
Severity	Count				Server	Total	Web Pr	Forefro	Secure	VPN Re	VPN Qu
🐼 Error	2 (2 new)				TMG-EN	3	1	0	2	0	0 0
🔔 Warning	3 (3 new)										
(i) Information	7 (7 new)				(i) Protection	Technology					8
-					Name	recimology		Activity			Va 🔺
					Network Insp	ection System		Blocked atta	acks		0
					Web Protecti	on		Blocked infe	ected downlo	ads	0
-					Web Protecti	00		Blocked poli	cy violations		0
Network Stat				8	URL Filtering			Blocked URL	-		0 /
Object	Stat	us U	ptime	Bytes/Sec					Lifequests		
					HTTPS Inspe			Disabled			
					E-Mail Protec	tion		Blocked infe	ected messag	jes	0
					Snam Eilterin	n		Blocked sna	m messaries		×
Services 👘				8	2 Definition	Updates					8
Service	Status 9	Servers	Up		Protection Mech	nanism 🔺		Status			A
🖉 Firewall	Started 1	out of	1		🛛 🐼 E-Mail An	tivirus		Failed			_
🖉 Job Sched	Started 1	out of	1		🐼 Malware 1	Inspection		Failed			
SQL Serv	Started 1	out of	1								
					i) Cache Utili	Cache Type	Conte	n Cache	Conter	n Cache	e Conter 🔺
					TMG-EN	Hosted Cache	0,0	0.0%	0,0	0,0%	0,0
					TMG-EN	Combined Cad	-	0.0%	0,0	0,0%	0,0

Figure 1: Forefront TMG Dashboard

From the Forefront TMG Dahsboard you can easily navigate to the Alert section, which gives you more details about the specific alerts. If you want to be informed via e-mail it is possible to create alert <u>notifications</u>.



#### Threat Management Gateway 2010

Alerts Sessions Connectivity Verifiers Services Configuration							
Alert	Latest 🔺	Status	Category	Server			
🗄 🧻 Malware Inspection Definitio	. 04.06.2011 12:26:24	New	Other	TMG-EN			
🗉 🛕 IP Spoofing	04.06.2011 12:27:29	New	Security	TMG-EN			
🗉 i Service Started	04.06.2011 12:33:38	New	Firewall Service	TMG-EN			
🗉 🚫 Definition Updating Failed	04.06.2011 12:48:18	New	Security	TMG-EN			
∃ (i) Network Inspection System	. 04.06.2011 14:00:02	New	Firewall Service	TMG-EN			
🖃 🕂 Routing (chaining) failure	04.06.2011 14:01:25	New	Routing	TMG-EN			
Routing (chaining) failure	04.06.2011 12:28:35	New	Routing	TMG-EN			
Routing (chaining) failure	04.06.2011 14:01:25	New	Routing	TMG-EN			
🖃 🔇 Definition Updates Checking	. 04.06.2011 14:15:11	New	Security	TMG-EN			
Definition Updates Checking .	04.06.2011 14:15:11	New	Security	TMG-EN			

# Alert Information Description: The Web Proxy filter detected that the upstream proxy server '192.9.200.240' is not available.

Figure 2: Forefront TMG Alerts

# Forefront TMG logging

One of the most used functionality in Forefront TMG is the TMG real time logging functionality which will give you a real time view about the traffic from your clients and Servers. The TMG logging is a wonderful tool if you want to allow network traffic from one application, Server or Client but you don't know the required communication ports to open.

Logging Report	ting					Tasks Help
Filter By	Condition	Value				
Log Record Type	Equals	Firewall or Web P				Logging Tasks
Log Time	Live					Edit Filter
Action	Not Equal	Connection Status				Stop Query
			1	1		Configure Logging
Log Time 🔺	Client IP	Destination IP	Destination Port	Protocol	Action Over	
04.06.2011 14:20:17	7 127.0.0.1	192.9.200.240	8080	http	Failed	Configure Firewall Logging
04.06.2011 14:20:17	7 192.9.200.28	192.9.200.240	8080	HTTP Proxy	Closed	Configure Web Proxy Logging
04.06.2011 14:20:19	9 127.0.0.1	127.0.0.1	8080	HTTP Proxy	Closed	Configure Log Queue
04.06.2011 14:20:19	9 127.0.0.1	127.0.0.1	8080	HTTP Proxy	Initiate	Related Tasks
04.06.2011 14:20:19	9 10.80.16.176	10.80.16.80	53	DNS	Initiate	View Log Status
04.06.2011 14:20:19	9 192.9.200.28	192.9.200.240	8080	HTTP Proxy	Closed	A Define Log Text Colors
04.06.2011 14:20:19	9 192.9.200.28	192.9.200.240	8080	HTTP Proxy	Initiate	Save Filter Definitions
•						Doad Filter Definitions
						Copy Selected Results to
Initiated Co	nnection			TMG-EN 04	4.06.2011 14:20:19	Clipboard
Log type: Firewall s						Copy All Results to Clipboard
Status: The operation Source: Local Host (						
Destination: Extern	•	•				
Protocol: HTTP Prox	•	,000)				

## **Windows Event Viewer**

Figure 3: Forefront TMG Logging

Additional information

The next really important tool for troubleshooting TMG is the Windows Event Viewer. Forefront TMG logs many helpful information in the Application and System event log categories and specific information about ADAM (AD-LDS) in the Application and Services Log. The ISA Server Diagnostic Logging is empty by default, you have to activate the ISA/TMG Diagnostic logging manually, but more about this later.

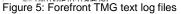
Application Application Setup Information O4.06.2011 13:49:11 ISA Server Dia System Information O4.06.2011 13:49:11 ISA Server Dia System Information O4.06.2011 13:49:11 ISA Server Dia Stystem Information	Action View Help						
Custom Views       Information       04.06.2011 13:49:11       ISA Server Dia       31394       None         Import System       Import System       04.06.2011 13:49:11       ISA Server Dia       31324       None         Import System       Import System       04.06.2011 13:49:11       ISA Server Dia       31324       None         Import System       Import System       04.06.2011 13:49:11       ISA Server Dia       31324       None         Import System       Import System       Import System       31324       None       Import Custom View         Import System       Import System       Import System       31324       None       Import Custom View         Import System       Import System       31324       None       Import Custom View       Import Custom View         Import System       Import System       31325       None       Import Custom View       Import System         Import System       Import System       Import System       31325       None       Import System         Import System       Import System       Import System       31325       None       Import System         Import System       Import System       Import System       31325       None       Import System         Import System <th>» 🖄 🗖 🛛 🖬</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	» 🖄 🗖 🛛 🖬						
Level       Date and Time       Source       Event ID       Task Categ       Date and Time         Application       04.06.2011 13:49:11       ISA Server Dia       31394       None       Source       Cate Digition         Security       Security       Security       116/mation       04.06.2011 13:49:11       ISA Server Dia       31324       None       Portade Events       Date and Time       Coexte Digitions         Applications       04.06.2011 13:49:11       ISA Server Dia       31324       None       Portade Events       Date and Time       Coexte Digitions         Applications       04.06.2011 13:49:11       ISA Server Dia       31324       None       Portade Events       Portade		ISA Server Diagno	stics Number of events: 440				Actions
Application       94.06.2011 13:49:11       ISA Server Dia       31394       None         Security       Security       11 Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Prowarded Events       Applications and Services Logs       11 Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Applications and Services Logs       11 Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Applications and Services Logs       11 Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Advam (MSExchange)       Hardware Events       11 Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Information       04.06.2011 13:49:11       I		Level	Date and Time	Source	Event ID	Task Cateo 🔺	ISA Server Diagnostics
Security Security Security Security Security System Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed System Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed System Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and M (MSExchange) Information O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation O 4.06.2011 13:49:11 ISA Server Dia Sitzed O and Thermation <		(i) Information	04.06.2011 13:49:11	ISA Server Dia			💰 Open Saved Log
Setue       Importantion       04.06.2011 3:49:11       ISA Server Dia       31324       None       Import Custom View         Provided Events       Information       04.06.2011 3:49:11       ISA Server Dia       31320       None       Import Custom View         Applications and Services Logs       Information       04.06.2011 3:49:11       ISA Server Dia       31320       None       Import Custom View         ADAM (MSExchange)       Information       04.06.2011 3:49:11       ISA Server Dia       31320       None       Import Custom View         ADAM (MSExchange)       Information       04.06.2011 3:49:11       ISA Server Dia       31320       None       Import Custom View       Clear Log       Import Custom View         ADAM (MSExchange)       Information       04.06.2011 3:49:11       ISA Server Dia       31320       None       Import Custom View       Import Custom View       Clear Log       Clear Log       Import Custom View       Clear Log       Clear Log       Clear Log       Clear Log       Import Custom View       Cle		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31324	None	
Forwarded Events       Information       04.06.2011 13:49:11       ISA Server Dia       31353       None         Applications and Services Logs       Information       04.06.2011 13:49:11       ISA Server Dia       31357       None         ADAM (ISASTGCTB)       Information       04.06.2011 13:49:11       ISA Server Dia       31357       None         ADAM (VESchange)       Information       04.06.2011 13:49:11       ISA Server Dia       31357       None         Hardware Events       Information       04.06.2011 13:49:11       ISA Server Dia       31357       None         Information       04.06.2011 13:49:11       ISA Server Dia       31357       None         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31323       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31321       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31321       None         Microsoft       Information       04.06.201		1 Information	04.06.2011 13:49:11	ISA Server Dia	31324	None	Treate Custom View
Applezations and Services Logs       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         ADAM (ISASTGCTR)       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         ADAM (ISASTGCTR)       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         ADAM (ISASTGCTR)       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         ADAM (ISASTGCTR)       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         ADAM (ISASTGCTR)       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None </td <td>😭 System</td> <td><ol> <li>Information</li> </ol></td> <td>04.06.2011 13:49:11</td> <td>ISA Server Dia</td> <td> 31320</td> <td>None</td> <td>Import Custom View</td>	😭 System	<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31320	None	Import Custom View
Applications and Services Logs       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         ADAM (ISASTGCTB)       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         ADAM (ISASTGCTB)       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         ADAM (MSExchange)       Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Information       04.06.2011 13:49:11       ISA Server Dia       31320       None       Properties         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31321       None         Windows PowerShell       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Windows PowerShell       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Windows PowerShell       Information       04.06.2011 13:49:11       ISA Server Dia       31324       N	Forwarded Events	<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31353	None	Classian
ADAM (ISASTGCTR)       Information       0.100.2011 13:49:11       I.B.A. GUE Dathin       3.1320       None         ADAM (NSExchange)       Information       0.4.06.2011 13:49:11       ISA Server Dia       31320       None         Information       0.4.06.2011 13:49:11       ISA Server Dia       31321       None         Microsoft       Information       0.4.06.2011 13:49:11       ISA Server Dia       31321       None         Windows PowerShell       Information       0.4.06.2011 13:49:11       ISA Server Dia       31324       None         Windows PowerShell       Information       0.4.06.2011 13:49:11       ISA Server Dia       31324       None         Windows PowerShell       Information       0.4.06.2011 13:49:11       ISA Server Dia       31324       None         Subscriptions       Microsoft       Information       0.4.06.2011 13:49:11		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31320	None	Clear Log
ADAM (MSExchange)       Information       0+00.5201112.49:11       ISA Server Dia       31357       None         Information       04.06.201113:49:11       ISA Server Dia       31357       None         Information       04.06.201113:49:11       ISA Server Dia       31327       None         Microsoft       01.nformation       04.06.201113:49:11       ISA Server Dia       31328       None         Microsoft       01.nformation       04.06.201113:49:11       ISA Server Dia       31324       None         Microsoft       01.nformation       04.06.201113:49:1		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31357	None	👕 🐺 Filter Current Log
Image: Stand (MSExtrange)       Imformation       04.06.2011 13:49:11       ISA Server Dia       31357       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31320       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Image: Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Image: Information       04		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31320	None	Properties
I tasee & Ergine       Difformation       0-100.2011 12.49:11       Difformation       31319       None         I Key Microsoft       Difformation       0-0.6.2011 13:49:11       ISA Server Dia       31327       None         Windows PowerShell       Difformation       0-0.6.2011 13:49:11       ISA Server Dia       31327       None         Subscriptions       0-0.6.2011 13:49:11       ISA Server Dia       31327       None         Windows PowerShell       Difformation       0-0.6.2011 13:49:11       ISA Server Dia       31324       None         Subscriptions       0-0.6.2011 13:49:11       ISA Server Dia       31324       None       Windows Comparison       0.0.6.2011 13:49:11         Subscriptions       0-0.6.2011 13:49:11       ISA Server Dia       31324       None       Windows Comparison       Refresh         Difformation       0-0.6.2011 13:49:11       ISA Server Dia       31324       None       Windows Comparison       Windows Comparison </td <td></td> <td><ol> <li>Information</li> </ol></td> <td>04.06.2011 13:49:11</td> <td>ISA Server Dia</td> <td> 31357</td> <td>None</td> <td>- · ·</td>		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31357	None	- · ·
ISA Server Diagnostics       Information       04.06.2011 13:49:11       ISA Server Dia       31329       None         Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31326       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31328       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Subscriptions       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31320	None	Find
Is Server Diagnostics       Attach a Task To the View         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Microsoft       Information       04.06.2011 13:49:11       ISA Server Dia       31327       None         Windows PowerShell       Information       04.06.2011 13:49:11       ISA Server Dia       31324       None         Subscriptions       04.06.2011 13:49:11       ISA Server Dia       31324       None       Attach a Task To the         Information       04.06.2011 13:49:11       ISA Server Dia       31324       None       Refresh         Information       04.06.2011 13:49:11       ISA Server Dia       31324       None       Refresh         Information       04.06.2011 13:49:11       ISA Server Dia       31324       None       Refresh         Information       04.06.2011 13:49:11       ISA Server Dia       31324       None       Refresh         Information       04.06.2011 13:49:11       ISA Server Dia       31324       None       Refresh         Date and time: 06/04/2011-13:49:12.783       Packet context: 00000bef       Source:		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31319	None	Save All Events As
Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31327	None	1-
MSExchange Management Windows PowerShell Subscriptions Windows PowerShell Windows PowerShell Windows PowerShell Subscriptions Windows PowerShell Sub		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31326	None	Attach a rask to this Log.
Windows PowerShell       Information       04.06.2011 13:49:11       ISA Server Dia       31323 None         Subscriptions       Information       04.06.2011 13:49:11       ISA Server Dia       31324 None         Information       04.06.2011 13:49:11       ISA Server Dia       31324 None       Image: Comparison of Comp		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31391	None	View
Subscriptions          Subscriptions       Information       04.06.2011 13:49:11       ISA Server Dia       31394       None         Information       04.06.2011 13:49:11       ISA Server Dia       31324       None       If Help         Event 31394, ISA Server Diagnostics       X       Image: Server Diagnostics       X       Image: Server Diagnostics       Image: Server Diagnostics       Image: Server Diagnostics       X       Image: Server Diagnostics       Image: Server Diagnostics       Image: Server Diagnostics       X       Image: Server Diagnostics       Image: Server Diagnostics       Image: Server Diagnostics       Image: Server Diagnostics       X       Image: Server Diagnostics       Image: Server Diagnostics </td <td></td> <td><ol> <li>Information</li> </ol></td> <td>04.06.2011 13:49:11</td> <td>ISA Server Dia</td> <td> 31323</td> <td>None</td> <td>B Bofroch</td>		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31323	None	B Bofroch
Information       04.06.2011 13:49:11       ISA Server Dia       31324 None       If Help         Information       04.06.2011 13:40:11       ISA Server Dia       12324 None       If Help         Event 31394, ISA Server Diagnostics       X       Image: Server Diagnostics		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31394	None	
Event 31394, ISA Server Diagnostics       Event 31394, ISA Server Diagnostics         General Details       Image: Details         Date and time: 06/04/2011-13:49:12.783       Image: Details         Packet context: 00000bef       Image: Details         Log Name:       ISA Server Diagnostics         Source:       ISA Server Diagnostics         Log Name:       ISA Server Diagnostics         Log Source:       ISA Server Diagnostics		<ol> <li>Information</li> </ol>	04.06.2011 13:49:11	ISA Server Dia	31324	None	Relp
Event 31394, ISA Server Diagnostics       Image: Comparison of the server Diagnostics         General Details       Image: Comparison of the server Diagnostics         Date and time: 06/04/2011-13:49:12.783       Image: Comparison of the server Diagnostics         Packet context: 00000bef       Image: Comparison of the server Diagnostics         Log Name:       ISA Server Diagnostics         Source:       ISA Server Diagnostics         Log Name:       ISA Server Diagnostics         Source:       ISA Server Diagnostics         Log Name:       ISA Server Diagnostics         Source:       ISA Server Diagnostics		Toformation	04.06.0011.12.40.11	TEA Conver Dia	21274	Manna L	F
General Details       Image: Originality of the data set of the data s							
Date and time: 06/04/2011-13:49:12.783 Packet context: 00000bef Log Name: ISA Server Diagnostics Source: ISA Server Diagnostics Logged: 04.06.2011 13:49:11		Event 31394, ISA Se	rver Diagnostics			×	Event Properties
Date and time: 06/04/2011-13:49:12.783       Image: Copy         Packet context: 00000bef       Image: Save Selected Even         Log Name:       ISA Server Diagnostics         Source:       ISA Server Diagnostics         Log Source:       ISA Server Diagnostics         Log Name:       ISA Server Diagnostics         Log Name:       ISA Server Diagnostics         Log Name:       ISA Server Diagnostics         Source:       ISA Server Diagnostics		General Details	1				Diagonal Attach Task To This Even.
Log Name: ISA Server Diagnostics Source: ISA Server Diagnostics Logged: 04.06.2011 13:49:11		l					Сору
Log Name: ISA Server Diagnostics Source: ISA Server Diagnostics Logged: 04.06.2011 13:49:11							Save Selected Events
Source: ISA Server Diagnostics Logged: 04.06.2011 13:49:11						•	Q Refresh
Source: ISA Server Diagnostics Logged: 04.06.2011 13:49:11		Log Name:	ISA Server Diagnostics				Help
			-	Logged: 04.0	6 2011 12:40:11		
Event ID: 31394 Task Category: None			-				
		Event ID:			e		
Level: Information Keywords: Classic		Level:	Information	Keywords: Clas	sic		
User: N/A Computer: TMG-EN.trainer.intern		User:	N/A	Computer: TMC	G-EN.trainer.intern		

Figure 4: Windows Event Logging

#### TMG log files

During the Forefront TMG installation, the setup <u>process</u> creates some log files in the %windir%\temp directory and after a successful installation you will also find some log files like the ISA\_UpdateAgent log file which gives you detailed information about the TMG Web Protection platform updates.

🕌 Temp					_
G → ↓ • Computer • Local Disk (C:) • Winde	ows • Temp •		<b>-</b>	Search Temp	
File Edit View Tools Help					
Organize 🔻 🧾 Open 🔻 Print New folder					= -
☆ Favorites	Name	Date modified 👻	Туре	Size	
Nesktop	😰 b0992982-a982-4677-b519-a468c2f46a51	04.06.2011 14:20	XML Document	63 KB	
Downloads	📄 ed947b54-5fbe-42b3-ac3d-ad3e77de74fc	04.06.2011 14:21	XML Document	63 KB	
Recent Places	ISA_UpdateAgent	04.06.2011 14:15	Text Document	85 KB	
📜 Libraries	UpdateAgent.exe.22c.et	04.06.2011 14:00	ETL File	1.024 KB	
Documents	nvcbin.def.73a576cf.tmp	04.06.2011 12:28	TMP File	302.995 KB	
J Music	k8shioqc.vbt	04.06.2011 12:27	VBT File	1.119 KB	
E Pictures	sqlservr.exe.53c.etl	04.06.2011 12:26	ETL File	1.024 KB	
Videos	IsaManagedCtrl.exe.eac.et	04.06.2011 12:26	ETL File	1.024 KB	
· Commuter	W3Prefch.exe.edc.etl	04.06.2011 12:26	ETL File	1.024 KB	
P Computer	mspadmin.exe.8ec.et	04.06.2011 12:26	ETL File	1.024 KB	
	isastg.exe.654.etl	04.06.2011 12:25	ETL File	1.024 KB	



## Forefront TMG Best Practices Analyzer

Most of you are familiar with the TMG Best Practices Analyzer which compares your current Forefront TMG installation with Best Practices from Microsoft. Using the TMG

BPA should be the first tool to start after a Forefront TMG installation or when you consider problems with your TMG configuration.

Forefront TMG Best Practices	s Analyzer Tool	<u>_</u> _×
Forefront TMG	Best Practices Analyzer Tool	Windows Server System
Forefront TMG  Velcome Start a scan Select a Best Practices scan to view View a report Start BPAZVisio Schedule a scan See also Forefront TMG Best Practices Analyzer Help About the Forefront TMG Best Practices Analyzer Send us your feedback Updates and customer feedback	View Best Practices Report ISASERVER.ORG Select Report Type:  Ust Reports City Tree Reports City Connection Light Surger City City City City City City City City	Windows Server System
	<ul> <li>▲ A policy rule blocks FTP uploads</li> <li>▲ Forefront TMG Records Logs to the System Drive</li> <li>▲ Strict RPC compliance is enforced in an access rule that allows traffic to or from the Local H</li> <li>▲ Strict RPC compliance is enforced in an access rule that allows traffic to or from the Local H</li> <li>▲ The IP Spoofing warning alert was signaled 1 times</li> <li>▲ The Routing (chaining) failure warning alert was signaled 1 times</li> <li>▲ The Service Principal Names (SPNs) for the configuration storage server are not registered</li> <li>▲ DNS search order is blank</li> <li>▲ Forefront TMG is running on a virtual server</li> </ul>	

Figure 6: TMG BPA

# Forefront TMG Data Packager

The Forefront TMG Data Packager is a very helpful tool to collect all necessary information about your Forefront TMG configuration. You can use the Data Packager to send information to Microsoft product support for further analysis but you can also use this tool to document your Forefront TMG installation status. As an TMG consultant I sometimes use the TMG Data Packager to document the TMG configuration status for my customers.

Microsoft Forefront TMG TM	5 Data Packager	<u>_                                    </u>
Microsoft Foref	ont TMG TMG Data Packager	Windows Server System
<ul> <li>Welcome</li> <li>See also</li> <li>The Forefront TMG Data Packager Help</li> <li>About the Forefront TMG Data Packager</li> <li>Send us your feedback</li> </ul>	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	

Figure 7: TMG Data packager

It is possible to select the options to specify the data that you would like to be part of the TMG Data Packager collection process.

Microsoft Forefront TMG TMG	a Data Packager			<u>_0×</u>			
Microsoft Forefr	ont TMG TMG Dat	ta Packager		Windows Server System			
		-					
. Welcome See also	Options						
<ul> <li>The Forefront TMG Data Packager Help</li> </ul>	Select the options below to specify the o	data that you would like the TMG Data Pac	kager tool to collect.				
About the Forefront TMG Data Packager	Scenario: Static Configurati	on Information					
Send us your feedback	TMG BPA	Perform free disk space check	Change Tracking				
	✓ ISAInfo	MSDE Error Logs	Collect Update Center logs				
	Event logs	Performance Monitor snapshot	Collect Netstat output				
	Collect GAPA Activity logs						
	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:\temp	Brows	e Folder			
	Data collection timeout period	180 minutes					
	Load custom configuration	Save custom configuration					
	🗲 Back	Start data collection					

Figure 8: TMG Data packager - Options

The TMG Data Packager creates a CAB file with a lot of log files as you can see in the following screenshot.

→ 🕞 → Computer → Local Disk (C	:) ▼ temp ▼ TmgPackage			👻 🚺 Search TmgPad	kage
e Edit View Tools Help					
Irganize 🔻					
🚖 Favorites	Name *	Size	Туре	Date	Path
🧮 Desktop	Application	3.140 KB	Classic Event Log	04.06.2011 14:03	EventViewerEvent
Downloads	🔮 array	18 KB	XML Document	04.06.2011 14:09	ChangeTracking \
📳 Recent Places	BpaDataPackagerLog	1 KB	Text Document	04.06.2011 14:09	BpaDataPackager
📜 Libraries	BPAReport_TMG-EN	3.348 KB	XML Document	04.06.2011 14:07	BpaReportFiles\
Documents	BPAReport_TMG-EN	6 KB	Text Document	04.06.2011 14:07	BpaReportFiles\
J Music	🚝 ChangeTracking	5 KB	XSL Stylesheet	14.01.2010 16:13	ChangeTracking\
E Pictures	ChangeTrackingTab	11 KB	HTML Document	14.01.2010 16:13	ChangeTracking\
Videos Videos	EventViewer_ErrorEv	23 KB	CSV File	04.06.2011 14:03	EventViewerEver
	EventViewer_IsaEve	4 KB	CSV File	04.06.2011 14:03	EventViewerEver
Computer Local Disk (C:)	GapaSigStub	9 KB	Text Document	01.06.2011 22:30	UpdateCenter\
DVD Drive (D:) Label Iso	ISA_UpdateAgent	84 KB	Text Document	04.06.2011 14:00	UpdateCenter\
0 010 0110 (01) 000 000	IsaBPA. 201106040203	5 KB	XML Document	04.06.2011 14:08	BpaReportFiles\
📮 Network	ISAInfo_tmg-en	86 KB	Text Document	04.06.2011 14:09	IsaInfoFiles\
	ISAInfo_tmg-en	16.346 KB	XML Document	04.06.2011 14:09	IsaInfoFiles\
	IsaLogs_Firewall_MS	500 KB	CSV File	04.06.2011 14:03	TmgLogs\
	IsaLogs_WebProxy	173 KB	CSV File	04.06.2011 14:03	TmgLogs\
	IsaPerformanceData	380 KB	Text Document	04.06.2011 14:08	TmgPerfmonCou
	🔤 minusImg	1 KB	GIF image	08.09.2009 12:09	ChangeTracking
	MpSigStub	7 KB	Text Document	02.06.2011 10:30	UpdateCenter\
	Netlogon	1 KB	Text Document	23.04.2011 20:03	Netlogon\
	NetStatOutput	14 KB	Text Document	04.06.2011 14:09	NetStatFiles\
	🔽 plusImg	1 KB	GIF image	08.09.2009 12:09	ChangeTracking
	🛃 System	2.116 KB	Classic Event Log	04.06.2011 14:03	EventViewerEver
gure 9: TMG Data packager	TDP.2011-6-4.14-3-3	383 KB	Text Document	04.06.2011 14:03	BoaDataPackage

Figure 9: TMG Data packager – CAB file content

# Netsh

Beginning with Forefront TMG Microsoft extended the Windows Netsh tool with some Forefront TMG commands. As some of you might know, some commands of the FWENGMON utility of ISA Server 2006 are now part of the Netsh tool. Netsh has now some options to give you a low level view about client connections with the Firewall and may be helpful in some situations.

	tmg>show al				
	ion Objects:				
D	Protocol	Source	Destination	One-Sh	ot
1 2 3 6 13	TCP(6) TCP(6) TCP(6) TCP(6) TCP(6) TCP(6)	0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 10.80.0:0 10.80.16.176:0 10.80.16.176:0	10.80.16.176:1745 10.80.16.176:8080 127.0.0.1:8080 10.80.16.80:6009 10.80.16.80:6011	No No No No No	
Crea	ations.				
ctive	e Sessions:				
		Source /	Destination /		
D	<b>Protocol</b>	Source Proxy	Dest. Proxy	2-way	Timeout
6	 TCP<6>	 10.80.16.176:10331	10.80.16.80:445	 Yes	 Yes
26	TCP(6)	10.80.16.176:12790	10.80.16.80:6009 10.80.16.176:10154	Yes	Yes
24	TCP<6>		10.80.16.80:6009	Yes	Yes
49	TCP(6)	10.80.16.176:12790 10.80.16.176:12845	10.80.16.80:6011	Yes	Yes
47	TCP(6)	10.80.16.176:12846	10.80.16.176:10154 10.80.16.80:6011	Yes	Yes
96	UDP(17)	10.80.16.176:12845 10.80.16.176:23803	10.80.16.80:53	Yes	Yes
92	UDP(17)	10.80.16.176:24567	10.80.16.80:53	Yes	Yes
91	UDP(17)	10.80.16.176:28858	10.80.16.80:53	Yes	Yes
89	UDP(17)	10.80.16.176:49731	10.80.16.80:53	Yes	Yes
93	UDP(17)	10.80.16.176:51683	10.80.16.80:53	Yes	Yes
90	TCP(6)	127.0.0.1:12823	127.0.0.1:8080	Yes	Yes
95	TCP(6)	127.0.0.1:12847		Yes	Yes
50 51	TCP(6) TCP(6)	192.9.200.28:12853 192.9.200.28:12854	192.9.200.240:8080 192.9.200.240:8080	Yes Yes	Yes Yes
.4 Coi	nnections.		172171200121010000	103	103
R	ule		urce range		Destinat:
n rai	nge				

Figure 10: NETSH TMG options

## Microsoft Network Monitor (Netmon)

As one of the last resorts in Forefront TMG troubleshooting (excepts Windows Kernel Debugging <sup>(i)</sup>) you can use the Microsoft Network Monitor to get deep inside into the network traffic. Netmon may be helpful when you couldn't find the cause of problems with the built in tools of Forefront TMG. You can use the Microsoft Network Monitor (Netmon) 3.3 version which is part of the TMG BPA installation or you can use the latest build 3.4 from the Microsoft website.

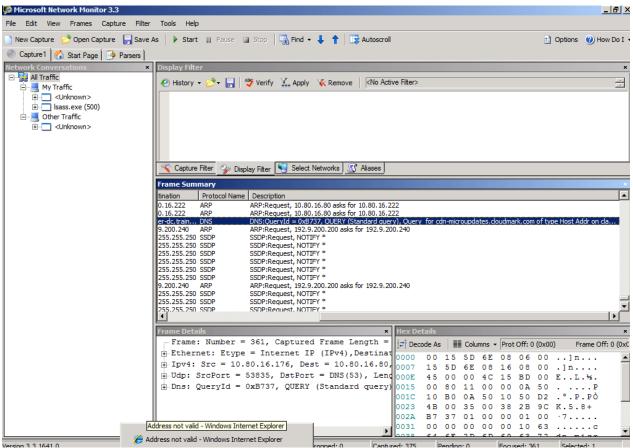


Figure 11: Microsoft Network Monitor

**Attention**: If you want to analyze network traffic between Forefront TMG and the ISA Firewall client, now called TMG client, you have to download a special Netmon Parser. You can download the Netmon parser <u>here</u>.

## Forefront TMG troubleshooting

The Forefront TMG Management console comes with some built in troubleshooting tools like the Traffic simulator, the change tracking feature and the connectivity test tool.

	Troubleshooting and Support
r	Use the Best Practices Analyzer
	The Best Practices Analyzer Tool for Forefront TMG scans the configuration settings of the local computer. This tool examines the local Forefront TMG computer, determining the status of the computer configuration and finding issues that do not conform to recommended best practices.
	View Forefront TMG Configuration Changes
	The Configuration Change Tracking feature records and displays changes applied to the Forefront TMG configuration. Click this link to open the Change Tracking tab in the Forefront TMG Monitoring options.
	View Forefront TMG Alerts
	Forefront TMG alerts notify you when specified events occur on the local Forefront TMG computer. Click this link to open the Alerts tab in the Forefront TMG Monitoring options.
	View Forefront TMG Logging
	Forefront TMG maintains logs of activity on the Forefront TMG computer. Click this link to open the Logging tab in the Forefront TMG Monitoring options.
	Use the Traffic Simulator
	Forefront TMG Traffic Simulator simulates network traffic in accordance with specified request parameters, and provides information about firewall policy rules evaluated for the request. Click this link to go to the Traffic Simulator tab.
	View Diagnostic Logging Events
	Forefront TMG Diagnostic Logging view allows you to query the diagnostic logging database according to the filter criteria. Click this link to go to the Diagnostic Logging tab.

For special TMG troubleshooting the TMG Diagnostic Logging feature might be helpful to find problems with the TMG configuration. Forefront TMG Diagnostic Logging is deactivated by default and you manually have to activate it.

Forefront	Troubleshooting
Threat Management Gateway 2010	Enterprise
Troubleshooting Change Tracking Traffic Simulator Diagnostic Logging Connectivity Test	Tasks Help
Use the diagnostic logging filter to view the events for a selected server.  Filter Criteria Message contains: Context contains: Server: TMG-EN Apply Filter Show All	Diagnostic Logging Tasks   Disable Diagnostic Logging  Delete Diagnostic Log
Figure 13: Forefront TMG Diagnostic logging	

After the TMG Diagnostic logging has run for a while you can stop the Diagnostic logging and filter the log for informations that might be of interest for you.

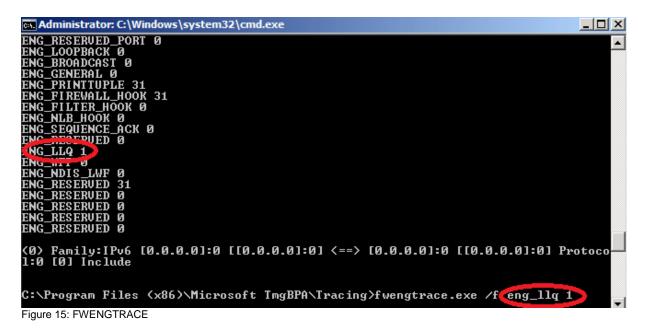
J.	Forefront Threat Managem	ent Gateway 2010	)			Troubleshooting Enterprise
Tr	roubleshooting Change T	racking Traffic Simu	lator Diagno	stic Logging Connectivity Test		Tasks Help
	Jse the diagnostic logging fi Filter Criteria Message contains: Context contains: Server:	Iter to view the events		y Filter Show All		Diagnostic Logging Tasks  Carlot Enable Diagnostic Logging  Delete Diagnostic Log
Cun	rently showing: server=[TN	IG-EN]				
29	04.06.2011 13:48:39	0e907329 0e90732a	Firewall service	Forefront TMG is looking for an applicable network rule.	···· 📥 ,	
30	04.06.2011 13:48:39	0e907329 0e90732a	Firewall service	Forefront TMG is evaluating the network rule Local Host Access.	···· U	
31	04.06.2011 13:48:39	0e907329 0e90732a	Firewall service	The source and destination in the packet match the source and destination specified in the network rule, which specifies a route relationship.		
32	04.06.2011 13:48:39	0e907329 0e90732a	Firewall service	The network rule Local Host Access matches the source and destination. A route relationship is specified.		
33	04.06.2011 13:48:39	0e907329 0e90732a	Web Proxy	Forefront TMG will connect to the Web server 192.9.200.240 on the IP address 192.9.200.240 and port 8080.		
34	04.06.2011 13:48:42	0e90732b 0e90732c	Web Proxy	Forefront TMG rejected the request with the HTTP status code 504 and will return the following error message to the Web client. "The connection timed out. (10060)"	<b>–</b>	Indu to Catting Startad

Figure 14: Forefront TMG Diagnostic logging content

The Diagnostic logging give you a deep insight how Forefront TMG works under the hood.

## FWENGTRACE

FWENGTRACE is part of the Forefront TMG Best Practice Analyzer and can be used to modify trace information for several Forefront TMG components, in this example the Forefront TMG LLQ (Large Logging Queue) feature of Forefront TMG.



# ISATRACE

Like Forefront <u>UAG</u>, Forefront TMG has some built in tracing capabilities, which give you the choice to modify the content of the ISALOG.BIN trace file which is located in the %windir%\Debug directory. Have you ever wondered about the large (about 400 MB) .bin file? This is the ISA/TMG trace file. Starting with ISA Server 2004 SP2 the ISALOG.BIN file is used to trace the status from a lot of Forefront TMG components. With ISATRACE you can change the information in the trace file.

<b>.</b> .	🔝 Release Bits Tracing							
	ISA Release Bits Tracing							
	Group	Erro	Warn	Info	Fund	Noise	Trace format search path:	
	+ GENERAL							
	+ ENG						Format As: Text	
	+ FWSRV						Trace File to Format	
	· VPN						C:\Windows\debug\jsalog.bin	
	+ WP						current C.Windows\debugysalog.bin	
	• STG						this file	
	· CTRL							
	· FWC						Tracing configuration file:	
	· COM						Browse	
	• UI						Load Save	
	· RPC							
	+ MONITOR						RT console colors	
	+ FLT						Light Yellow 💌 on Gray	
	• TEST							
	· SCHED							
	MIXER							
	DNSCACHE							
	APPCFGWZD							
FWeng Advanced Options Go GoRT Stop								
* WP_TRAFFIC filter Logging is currently ON								
-	, 							
	Circular log file of 4							
Auto enable tracing on startup								
Backup trace file on startup; Single Copy								

Figure 16: ISATRACE

# Windows Performance Monitor (Perfmon)

Perfmon is a great utility to analyze the performance of your Windows Server and the applications installed on the Server. A supported application like Forefront TMG extends the Windows Performance monitor with it's own counters that Forefront TMG Administrators can use to built baselines of the TMG Server to compare these baselines with current loads when they expect performance problems with their TMG Server.

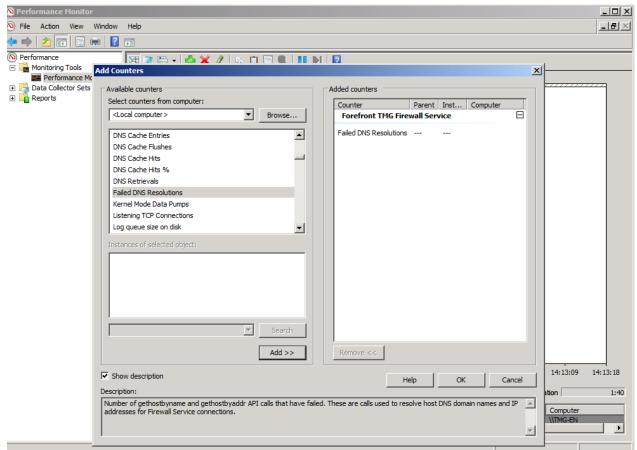


Figure 17: Windows Perfmon with TMG counters

Because there are a lot of performance counters for various Forefront TMG subsystems and it might be time consuming for Administrator to find the right counters, Microsoft has developed PAL (Performance Analysis of Logs) which can create XML files for specific applications with helpful Performance counters. You can use these XML files to import it into the Perfmon tool.

🔀 PAL Wizard v2.0.7			
1	Threshold File Questions Output Options File	Output Queue	Execute
captured. If an appropriate If the computer has multiple under different threshold file	is appropriate for the computer on which the log was threshold file doesn't exist, then choose System Overview. roles, then choose "All Thresholds" or analyze the log is. Optionally, the export button can be used to create a er to log all of the counters analyzed in the threshold file.		
Threshold File Title	System Overview		
Refresh Threshold File Name: Threshold File Description: Content Owner(s):	Microsoft Active Directory ASP.NET Microsoft BizTalk Server 2006/2009/2010 Citrix XenApp .NET Framework v1.1 or greater Dynamics AX 40/2009 Microsoft Exchange 2007 Microsoft Exchange 2003 Microsoft Exchange 2010 Win2008 R2 SP1 Hyper-V Microsoft Internet Information Services 5x/6x/7x Microsoft Office SharePoint Server (MOSS) 2007 and Searc Microsoft OCS 2007 R2 - Archiving Microsoft OCS 2007 R2 - CWA Microsoft OCS 2007 R2 - Edge Microsoft OCS 2007 R2 - Edge Microsoft OCS 2007 R2 - Mediation Microsoft OCS 2007 R2 - Monitoring Microsoft OCS 2007 R2 - Monitoring		
	Microsoft Threat Management Gateway		
	Nicrosoft Unject, Sonror Quick System Overview Microsoft Office SharePoint Server (MOSS) 2007 Microsoft SQL Server 2005/2008 System Overview	Previous	Next

Figure 18: PAL template

Export the XML file of PAL to a Perfmon template file. In the Windows Performance monitor navigate to the Data Collector Sets and create a new user defined Data collector set.

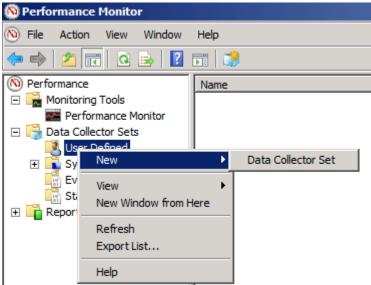


Figure 19: New Data Collectore Set with Perfmon

Select "Create from a template". Select the XML template exported from PAL and now you can see the performance counters for Forefront TMG.

🔊 Performance Monitor										
🔊 File Action View Window	Help									
🗢 🔿   🖄 📅   🗙 🗒 🗟	? 🖬									
N Performance	Name	Туре	Output							
🖃 🚰 Monitoring Tools	PAL_Microsoft_Threat_Manageme	Performance Counter								
Performance Monitor Data Collector Sets										
Data Collector Sets	PAL Microsoft Threat	Management_Gateway P	roperties X							
TMG-Performance										
🕀 📑 System	Performance Counters	File								
Event Trace Sessions	Performance counters:									
Startup Event Trace Sess     H	Forefront TMG Cache	Disk Failure Rate (failures	▲ Add							
		Il Packet Engine \Active Co								
		ll Packet Engine\Backlogge	Remove							
		Il Packet Engine Dropped								
		Il Packet Engine ReInject								
		Il Service Available Worker								
		Il Service DNS Cache Hits %								
	Log format:									
	Binary	-								
		-								
	Sample interval:	Units:	aximum samples:							
	15	Seconds	•							
	Data source name:									
	ОК	Cancel App	Help							

Figure 20: Perfmon eith PAL counters

You can now use the user defined Data Collector Set to start collecting informations. Right click the new Data collection and select Start.

After you stop the data collection process you can view the report of the collected data under the reports section of the Windows Performance monitor.

Performance Monitor									
) File Action View Window	Help								
╞ 🔿 🎢 📊 🎸 🤿	2 📷 🔤 🛄								
N) Performance	PAL Keport								
Monitoring Tools     Performance Monitor     Data Collector Sets     User Defined	Computer: Client Collected: Samstag, 4 Duration: 87 Seconds		28:59						
ITMG-Performance	Summary								
Event Trace Sessions	Disk Memory								
Startup Event Trace Sess	Disk Queue Length: 0	.057		Memory:	0 MB				
Reports				Top Process:					
TMG-Performance				Private Working Set:	КВ				
TMG-EN_2011060									
🕀 🚺 System	Diagnostic Result	\$					$\odot$		
	Performance						$\odot$		
	Resource Overvie	w							
	Component	Status	Utilization	Details					
	Network	Idle	0 %	Busiest network adapter is less	than 15%. 🗹				
	CPU						$\odot$		
	CFO								
	Network			Ħ			۲		
	Interface						۲		
	Network Interfac		Тор	o:18 of 18					
	counter	Ins	stance		Mean	Minimum	Maximum		
	Bytes Received/sec	Mi	crosoft Virtual Mach	ine Bus Network Adapter _3	217	48	576		
	Bytes Sent/sec	Mi	crosoft Virtual Mach	ine Bus Network Adapter _3	151	0	684		
	Bytes Total/sec	Mi	crosoft Virtual Mach	ine Bus Network Adapter _3	368	48	1,259		
	Current Bandwidth	Mi	crosoft Virtual Mach	ine Bus Network Adapter _3	10,000,000,000 10	000 000 000 1	0 000 000 000		

Figure 21: Perfmon data collector report

# Forefront TMG SuperFlow application

This article ends with a quick overview about the Forrefront TMG Superflow application. You can use this tool to troubleshoot a failed Forefront TMG installation. TMG Superflow contains some helpful links and resources to troubleshoot a failed Forefront TMG installation. You can read more about the TMG Superflow utility <u>here</u>.

📰 SuperFlow Application										
Troubleshooting Forefront TMG Services	Forefront Threat Management Gateway 2010									
Overview Preparation Tool Issues Setup Issues Resources										
This SuperFlow is designed to help you troubleshoot and resolve Forefront TMG installation issues. It takes you through the steps required to: Determine the root cause of your issue. Perform the appropriate resolution steps. Verify that the resolution fixed the issue. Navigating the SuperFlow You can navigate the SuperFlow You can navigate the SuperFlow by using the Preparation Tool Issues, Setup Issues, and Resources tabs: The Preparation Tool Issues tab helps you troubleshoot issues you may encounter when running the Preparation Tool. The Setup Issues tab helps you troubleshoot issues you may encounter when running the Installation Wizard. The Resources tab contains links to additional information to help you troubleshoot Forefront TMG installation issues.										
SuperFlow Icons The following table lists the icons that might display in the SuperFlow.										
Icon Description										
Send feedback about this SuperFlow.										
Opens the current topic in another window.										
Prints the current topic.										
Keyboard Shortcuts Keyboard shortcuts are combinations of keystrokes that can be used to perform a task that would you can use in the SuperFlow.	typically require a mouse or other pointing device. The following table lists the keyboard shortcuts that									
Press this key To do this										
TAB Move to the next object.										
SHIFT+TAB Move to the previous object.										
CTRL+TAB Move to the next SuperFlow tab. Figure 22: TMG Superflow										

#### 0

## Conclusion

Troubleshooting Forefront TMG problems can be very complicated because of the various reasons why Forefront TMG doesn't work as expected, but on the other hand there are lot of troubleshooting guides and tools to find the reason for the problem. In my opinion the most important aspect is to have an analytic approach when you start troubleshooting. You should always start with the easiest troubleshooting steps and walk through the other steps if the previous analytics wasn't successful.

## **Related links**

Forefront TMG Troubleshooting Survival Guide http://social.technet.microsoft.com/wiki/contents/articles/forefront-threatmanagement-gateway-tmg-2010-troubleshooting-survival-guide.aspx Forefront TMG Performance Troubleshooting with PAL v2.x Part 1 – Data Collection http://tmgblog.richardhicks.com/2011/02/06/forefront-tmg-performancetroubleshooting-with-pal-v2-x-part-1-data-collection/ Forefront TMG Setup log files http://technet.microsoft.com/de-de/library/ee781947.aspx Forefront TMG Troubleshooting http://technet.microsoft.com/en-us/library/dd897100.aspx SuperFlow for Troubleshooting Forefront TMG Installation http://www.microsoft.com/downloads/en/details.aspx?FamilyID=f1ebfda1-da51-44cc-99cb-96ad0fd40bdf Troubleshooting Forefront TMC 2010 Performance insues Chapt Shoet

Troubleshooting Forefront TMG 2010 Performance issues Cheat Sheet

http://social.technet.microsoft.com/wiki/contents/articles/troubleshooting-forefronttmg-2010-performance-issues-cheat-sheet.aspx TMG BPA download http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8aa01cb0-da96-46d9-a50a-b245e47e6b8b PAL download http://pal.codeplex.com/releases/view/51623