How to configure Forefront TMG logging into a central Microsoft SQL Server database

Abstract

This article will show you in details how to change the local SQL Server express logging of Forefront TMG into a central Microsoft SQL Server database.

Let's begin

The default settings for Forefront TMG are to log into a local Microsoft SQL Server Express 2008 SP1 database. During a Forefront TMG installation a local Microsoft SQL Server Express database will be installed. If you want to change the local SQL Server logging to a central SQL database instance, you have to do several steps before you can change the logging in Forefront TMG. The high level steps are:

- 1) Create the Forefront TMG databases in your central SQL Server
- 2) Execute the Forefront TMG SQL scripts to create the necessary SQL tables in the database
- 3) Configure permissions for the TMG Server to access the SQL database
- 4) Change the SQL logging in Forefront TMG
- 5) Optional: Force data encryption between the TMG and the SQL Server
- 6) Test the connection

As a first step, we have to locate the SQL scripts of Forefront TMG which creates the required fields, tables, views and more for the SQL database. You can find the SQL scripts in the Forefront TMG installation directory. Copy the scripts to your SQL Server.

Hicrosoft Forefront Threat Management Gateway				
🚱 ◯ マ 🔰 ▼ Computer ▼ Local Disk (C:) ▼ Prog	ram Files 🝷 Microsoft Forefront Threat Management Gat	eway 🔹	- 🐼	Search Microsoft Fore
File Edit View Tools Help				
Organize 👻 Include in library 👻 Share with 💌	New folder			
☆ Favorites	Name	Date modified	Type *	Size
Nesktop	i fwengprf.h	13.10.2009 23:26	H File	6 KB
鵑 Downloads	hfperf.h	13.10.2009 23:26	H File	1 KB
🔢 Recent Places	IsaManagedCtrlPrf.h	13.10.2009 23:25	H File	1 KB
	socksprf.h	08.09.2009 12:16	H File	1 KB
🔁 Libraries	w3pctrs.h	13.10.2009 23:26	H File	14 KB
Documents	wspperf.h	13.10.2009 23:26	H File	4 KB
J Music	🕖 Secure.htm	15.06.2010 19:34	HTML Document	5 KB
Videos	ent_0608.i	12.09.2010 12:07	I File	93 KB
	enterprise.i	12.09.2010 12:07	I File	244 KB
🖳 Computer	EnterpriseStandalone.i	12.09.2010 12:07	I File	14 KB
all Local Disk (C:)	objects.i	12.09.2010 12:07	I File	1.105 KB
DVD Drive (D:) Label Iso	objectsEnt.i	12.09.2010 12:07	I File	1.031 KB
	server_objects.i	12.09.2010 12:07	I File	4 KB
🙀 Network	Microsoft.Isa.ManagedPerfCounters.InstallS	16.06.2011 08:20	INSTALLSTATE File	7 KB
	📝 fwsrv.sql	13.10.2009 23:23	Log File	3 KB
	w3proxy.sql	15.06.2010 19:01	Log File	3 KB
Figure 1: Locate the TMG .SQL scripts	I			

The FWSRV.SQL file is for the Firewall logging, the W3PROXY.SQL file is for the Web Proxy logging.

The following screnshot shows the content of the W3PROXY.SQL file.

📕 w3proxy.sql - Notepad	. E
File Edit Format View Help	
<pre>IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_batch_insert' AND type = 'P') exec sp_executesql N'CREATE PROCEDURE sp_batch_insert @tempTableName nvarchar(100), @tableName nvarchar(100) AS</pre>	_
IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_batch_discard' AND type = 'P') exec sp_executesql N'CREATE PROCEDURE sp_batch_discard @tempTableName nvarchar(100) AS EXECUTE (''truncate table ['' + @tempTableName + '']'')' GO	
<pre>CREATE TABLE webproxyLog { [c]ientTP] uniqueidentifier, [c]ientUserName] nvarchar(128), [c]ientUserName] nvarchar(218), [c]ientUserName] nvarchar(218), [c]ientUserName] nvarchar(25), [referredserver] varchar(25), [DestHostIP] uniqueidentifier, [DestHostIP] uniqueidentifier, [DestHostIP] uniqueidentifier, [bytessent] bigint, [bytessent] bigint, [bytessent] bigint, [bytessent] bigint, [resultcode] varchar(23), [resultcode] int, [result</pre>	

Next, start the SQL Server Management Studio application to create the databases for Firewall and Web Proxy logging.



Figure 3: Create a new database for SQL logging

The default database name for the Firewall logging is TMG-FWLOG. If you want to change the name you must also change the name of the database in the SQL script.

🚪 New Database					
Select a page	🔄 Script 🝷 📑 H	elp			
General Options Filegroups	Database name: Owner:		TMG-FWLC	G	
	Use full-text in Database files:	dexing			
	Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth
	TMG-FWLOG	Rows	PRIMARY	3	By 1 MB, unrestricted growth
	TMG-FWLO	Log	Not Applicable	1	By 10 percent, unrestricted growth
Connection					
Server: fep2010					
Connection: TRAINER\administrator					
View connection properties					
Progress					
Ready				Add	Remove
					OK Cancel

Figure 4: Specify location and other settings for the new database

Do the same for the Forefront TMG Web Proxy database.

Next we must execute the SQL script from Forefront TMG to create the required tables, views and fields for the SQL Server database. Start the SQL Server Management Studio application and start a new query and paste the entire SQL script into the query editor and execute the query. To the same for the TMG Web Proxy database.



Figure 5: Execute the SQL script to create tables and more

After executing the query control the results. For example navigate to the Columns tab and verify that there are new entries as shown in the following screenshot.

K Microsoft SQL Server Management Studio
File Edit View Project Debug Tools Window Community
😫 New Query 🕞 📑 📸 😘 🕞 🚔 🗐 🥌 💂
: 맨 맨 Execute 🕨 🖛 🗸 🗄
Object Explorer - 7 ×
Connect 🕶 📑 📑 🍸 🛃 🍒
🖃 📴 Columns 📃
servername (nvarchar(128), null)
📃 logTime (datetime, null)
protocol (varchar(32), null)
SourceIP (uniqueidentifier, null)
SourcePort (int, null)
📃 DestinationIP (uniqueidentifier, null)
DestinationPort (int, null)
OriginalClientIP (uniqueidentifier, null)
SourceNetwork (nvarchar(128), null)
DestinationNetwork (nvarchar(128), null)
Action (smallint, null)
resultcode (int, null)
🔳 rule (nvarchar(128), null)
ApplicationProtocol (nvarchar(128), null)
Bidirectional (smallint, null)
bytessent (bigint, null)
bytessentDelta (bigint, null)
bytesrecvd (bigint, null)
bytesrecvdDelta (bigint, null)
connectiontime (int, null)
Destination (unt, null)
Clean Harry (varchar(255), null)
ClientOserName (varchar(514), null)
ClientAgent (varchar(255), hull)
connectionid (int, null)
Interface (varchar(25) pull)
IPHeader (varchar(255), null)
Pavload (varchar(255), null)
GmtLogTime (datetime, null)
issScanResult (smallint, null)
issSignature (nvarchar(128), null)
I NATAddress (uniqueidentifier, null)

Figure 6: Database after script execution

Next, we must allow the TMG Server computer account access to the SQL Server and the created databases. Because we are using Windows integrated authentication on the SQL Server we create a new login based on Windows user accounts, in this case the computer account of the TMG Server. Because you cannot browse for computer objects in the object picker of the SQL Server, you must manually enter the TMG Server computer account with the notation DOMAIN\Computername\$ as shown in the following screenshot. Set the default database to the TMG-FWLOG database (optional) for example.

🚪 Login - New			
Select a page	🛒 Script 👻 📑 Help		
General			
User Mapping	Login <u>n</u> ame:	TRAINER\TMG-EN\$	S <u>e</u> arch
Securables	Windows authentication		
Status	O SQL Server authentication		
	Password:		_
	Confirm password:		_
	Specify old password	,	
	Old password:		_
	Enforce password policy	1	
	Enforce password expira	ation	
	User must change passv	word at next login	
	Mapped to certificate		-
	O Mapped to asymmetric key		
	Map to Credential	,	Add
Connection	Mapped Credentials	Condential Derivider	
Connection		Provider	
fep2010			
Connection: TRAINER\administrator			
View connection properties			
Progress			Remo <u>v</u> e
Ready	Default database:	TMG-FWLOG	•
To a a so	Default language:	<default></default>	•
-		ОК	Cancel

Figure 7: New Windows login for the Forefront TMG computer account

In the login properties for the new SQL login we must configure the user mapping so that the TMG Server computer account has the necessary permissions to access the SQL database(s).

Login Properties - TRAINER\TMG-EN\$					
Select a page	🕵 Script 👻 📑 Help				
😭 General					
Server Roles	Users mapped to this login:				
Securables	Map	Database	User	Default Schema	
Status		EIMSynchronizationSer			
		master			
		model			
		msdb			
		ReportServer			
		Report Server Temp DB			
		SMS_FEP			
		SUSDB			
		tempdb			
	I	TMG-FWLOG	TRAINER\TMG-EN\$		
	Guest account enabled for: TMG-FWLOG Database role membership for: TMG-FWLOG				
Connection	✓ db_ac	cessadmin			
Server:	☐ db_ba	ckupoperator tareader			
lepzoto	db_dat	tawriter			
Connection: TRAINER\administrator	db_dd	admin			
	db_der	nydatareader ovdatawriter			
View connection properties	db_ow	ner			
	db_sec	curityadmin			
Progress	✓ public				
Ready					
				ОК	Cancel

Figure 8: Configure permissions for the account

After all requirements on the SQL Server are configured, we can change the Forefront TMG logging from local SQL Server Express to central SQL Server logging. Start the Forefront TMG MMC and navigate to the *Logs & Reports* node and in the Task pane *Configure Firewall Logging* or *Configure Web Proxy Logging*. Click the radio button *SQL database* and click the *options* button.

	×
Log Fields	
Log storage format:	
SQL Server Express Database (on local server)	
Name: ISALOG_yyyymmdd_FWS_nnn.mdf	Options,
SQL Database	Options
C File	
Format:	
Format: W3C extended log file format	_
Format: W3C extended log file format Name: ISALOG_yyyymmdd_FWS_nnn.w3c	Options,
Format: W3C extended log file format Name: ISALOG_yyyymmdd_FWS_nnn.w3c Finable logging for this service	Options
Format: W3C extended log file format Name: ISALOG_yyyymmdd_FWS_nnn.w3c ✓ Enable logging for this service If you are logging to a remote file or SQL database using a port, in the System Policy Editor, enable the appropriate R configuration groups.	Options options

Figure 9: Change TMG logging to central SQL logging

Enter the FQDN of the SQL Server, the port to use (default is 1433).

Attention: Make sure that SQL Server listens to port 1433 from remote connections. Enter the name of the database previously created on the SQL Server and the name of the SQL table (created by the SQL script). For additonal security it is also possible to enable the force Data encryption option but this requires additonal settings. I will tell you more about that later.

Firewall Logging Prop	erties	x		
Options		×		
Database Connection	on Parameters			
Ser <u>v</u> er:	FEP2010.TRAINER.INTERN	Browse		
Port:	1433			
Data <u>b</u> ase:	TMG-FWLOG			
<u>T</u> able:	FirewallLog			
Eorce data encryption				
Authentication Deta Use Windows au Use S <u>Q</u> L server	ails ut <u>h</u> entication authentication			
<u>U</u> ser:		Bro <u>w</u> se		
Pa <u>s</u> sword:	•••••			
-	Test OK	Cancel		
	OK Cancel	Apply		

Figure 10: Specify the SQL Server and additonal parameters

After the configuration has been finished, you can click the Test button to test the SQL connection. After you click the *OK* button, Forefront TMG will inform you that a Forefront TMG system policy will be activated which allows a SQL connection from LOCAL HOST to the internal network. For security reasons you should limit the system policy to allow access to only the SQL Server.



Figure 11: Warning message that TMG system polices rules must be activated

One of the limitation of the central SQL Server logging is that from now on you cannot create Forefront TMG reports, so you have to use/create your own reports with SQL Server utilities.



Figure 12: Warning message that no reports can be generated when central SQL logging is used

As previously said, it is possible to encrypt the data connection between the SQL Server and the TMG Server, if you enable the appropriate option.

Options			×		
Database Connection	on Parameters				
Server:	FEP2010.TRAINER.	INTERN	Browse		
Port:	1433				
Database:	TMG-FWLOG				
Table:	FirewallLog				
Force data encryption					
Authentication Details Use Windows authentication					
C Use SQL server authentication					
User:			Browse		
Password:	•••••				
	Test	ОК	Cancel		
	ОК	Cancel	Apply		

Figure 13: Optional: It is possible to enable data encryption between TMG and SQL Server

If you want to enforce encryption between the SQL Server and the TMG Server (and all other servers accessing the SQL Server) you must force encryption in the SQL Server instance properties in SQL Server Management studio. If you don't want to enforce encryption for all connections, you can leave the default setting unchanged, so the SQL Server will negotiate encryption with only clients which request encryption.

Protocols for MSSQLSERVER I	Properties		? ×
Flags Certificate Advanced			
General			
Force Encryption	Yes		-
Hide Instance	No		
Force Encryption			
Turns encryption on or off for t	the selected i	nstance of SQL S	Server.
ОК	Cancel	Apply	Help

Figure 14: Force encryption on the SQL Server

You must use a computer certificate on the SQL Server which is used to create the secure channel between the SQL Server and the TMG Server. The certificate must be issued by a trusted certification authority (CA) which the TMG and SQL Server trusts. For more information about configuring SQL Server for SSL encryption, please read the following <u>article</u>.

rotocols for MSSQLSERVER Properties			
Flags Certificate Advanced			
Certificate:	View Clear		
fep2010.trainer.intem	•		
Expiration Date	25.12.2011		
Friendly Name	fep2010.trainer.intern		
Issued By	intern, trainer, RootCA		
Issued To	FEP2010.trainer.intern		
Expiration Date			
OK Can	cel Apply Help		

Figure 15: Select the appropriate certificate

Conclusion

In this article I tried to show you how to reconfigure the local Forefront TMG SQL logging to a central Microsoft SQL Server. Central SQL logging has some pros like central management, backup, restore, but also some cons like the loose of some reporting capabilities in Forefront TMG, so you have to create your own reporting with Microsoft SQL Server or third party tools.

Related links

Configuring Forefront TMG logs <u>http://technet.microsoft.com/en-us/library/bb794937.aspx</u> Microsoft Forefront TMG – Logging options in Forefront TMG <u>http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Logging-options-Forefront-TMG.html</u> How to View TMG Logs when using SQL Server Express for Logging <u>http://blogs.technet.com/b/isablog/archive/2010/03/31/how-to-view-tmg-logs-whenusing-sql-server-express-for-logging.aspx</u> Relocating SQL Database Files on Forefront TMG 2010 <u>http://tmgblog.richardhicks.com/2011/04/11/relocating-sql-database-files-on-forefront-tmg-2010/</u> Firewall Logging using a Microsoft SQL database <u>http://www.isaserver.org/tutorials/Firewall-Logging-Microsoft-SQL-database.html</u> SQL Server encryption configuration <u>http://support.microsoft.com/kb/316898</u>