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

Forefront TMG and UAG services explained

Abstract

In this article we will talk about Forefront TMG and Forefront UAG services, which controls the main functionality of Forefront UAG and TMG. I will also show you the dependencies between Forefront TMG and UAG services and I will also list windows services which are essential for Forefront TMG and UAG functionality.

Let's begin

During a typical Forefront TMG installation, the setup routine installs several Forefront TMG services:

- Forefront TMG Control service
- Microsoft Firewall service
- Forefront TMG Storage
- Forefront TMG Job Scheduler
- SQL Server (MSFW)
- SQL Server (ISARS)

Forefront TMG Control Service

The Microsoft Forefront TMG Control service (ISACTRL) performs the following functions:

- Starting other Forefront TMG services
- Restarting other Forefront TMG services when changes are made through Forefront TMG Management or scripts
- Generating Forefront TMG alerts and running actions (displayed in the Forefront TMG monitoring dashboard)
- Updating the Forefront TMG Client (Firewall Client) configuration settings
- Deleting unused log files
- Synchronizing the configuration of a Forefront TMG computer with its Configuration Storage server.

Attention: You cannot use Forefront TMG Management console to stop or start the Microsoft Forefront TMG Control service. To stop the service you must use the following command from and elevated command prompt:
net stop isactrl

If you stop the Microsoft Forefront TMG Control service, all the other Forefront TMG services will also be stopped.

Microsoft Forefront TMG Storage

The Microsoft Forefront TMG Storage (ISASTG) provides local storage for the Forefront TMG configuration. By default Forefront TMG stores the configuration in a local AD-LDS (Active Directory Lightweight Directory Instance) and for the case that the AD-LDS instance is not reachable, a copy of the current configuration will also be stored in the Registry on the local machine. You can read more about the TMG configuration here.

Forefront TMG Job Scheduler Service

The Forefront TMG Job Scheduler Service is used to create a pre cache of Web content for often used websites by users.
Forefront TMG can be configured to cache websites in a local cache on the file system of the TMG Server. You can configure which content Forefront TMG should prefetch and schedule when the content should be cached, available for access directly from the Forefront TMG cache rather than from the Internet.

Microsoft Firewall Service

The Forefront TMG Firewall service (FWSRV) is a generic, circuit-level proxy for Windows Sockets applications. The Firewall service redirects the requesting clients / applications to the Forefront TMG server, thus establishing a communication path from the internal application to the Internet application through the Forefront TMG server. The Firewall service runs as a stand-alone service on the Forefront TMG Server. Forefront TMG provides a set of application filters which offers some functionalities, for example controlling RPC traffic through the RPC-filter or a FTP filter to control the FTP data and control channel communication. Third party vendors are able to extend Forefront TMG functionality with custom application filters.

The Firewall service can be stopped manually in the Forefront TMG Management console, or programmatically using a script. You can read more about the ISA Server 2006 Firewall service (which is almost identically with Forefront TMG) here.

Lockdown mode

Whenever the Firewall service shuts down, Forefront TMG enters lockdown mode.
In lockdown mode, the following functionality applies:
The kernel-mode packet filter driver (fweng) applies the firewall policy.
Only the following system policy rules continue to allow incoming traffic to the Local Host network:

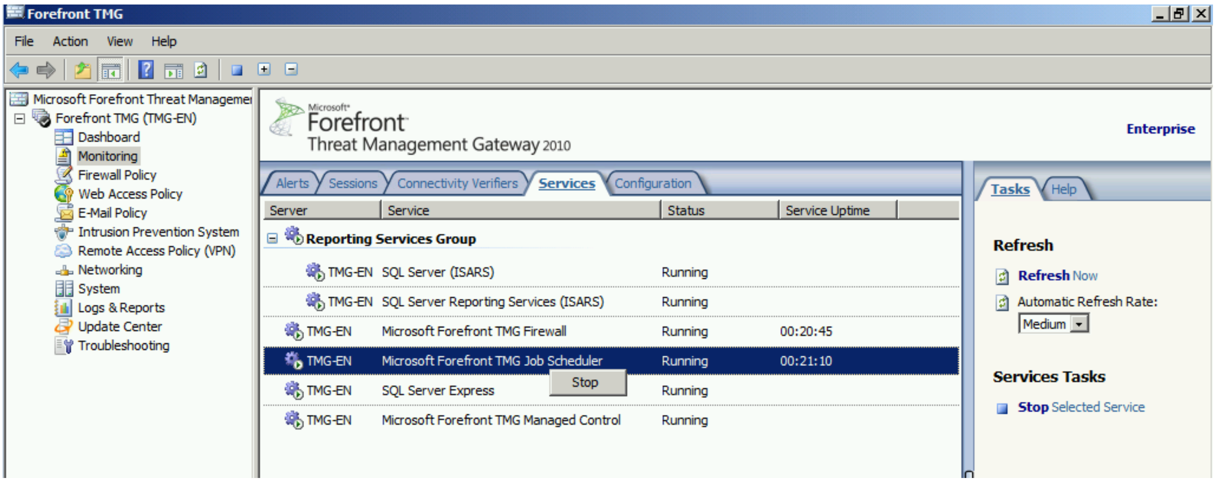
- Allow remote management from selected servers using MMC.
- Allow remote management from selected computers using Terminal Server.
- Allow DHCP replies from DHCP servers to Forefront TMG.
- Allow ICMP (PING) requests from selected computers to Forefront TMG.
- Allow access from trusted servers to the local Configuration Storage server (supported only in Enterprise Edition).
- Outgoing traffic from the Local Host network to all networks is allowed. If an outgoing connection is established, that connection can be used to respond to incoming traffic.
- VPN remote access clients cannot access Forefront TMG and site-to-site VPN does not work.

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

Microsoft SQL services

During a Forefront TMG installation, a local SQL Server 2008 SP1 express database will be installed. Forefront TMG uses the SQL Server by default to store log traffic for the Web proxy and Firewall service. The SQL Server reporting services are used to create one time and recurring reports for different TMG usage scenarios.
The SQL Server (MSFW) service (MSSQL$MSFW) is the instance of Microsoft SQL Server Express 2008 that is installed with Forefront TMG and is used for logging.
The SQL Server (ISARS) service (MSSQL$ISARS) is the instance of Microsoft SQL Server Express 2008 that is installed with Forefront TMG and is used for reporting.
Attention: If you stop the Microsoft SQL services, Forefront TMG use the LLQ (Large Logging Queue) feature to log traffic into the local file system until the Microsoft SQL services are started again.

You can use the Windows services console to start and stop Windows services or the Forefront TMG MMC to stop and start (but not to restart) Forefront TMG service. You should keep in mind that stopping services in the Forefront TMG MMC may disconnect you from Remote Management tools like the Remote TMG MMC or a connection through Microsoft Remote Desktop services, so the better way is to use the Windows Services Snap In to restart Forefront TMG services.



Server	Service	Status	Service Uptime
Reporting Services Group			
TMG-EN	SQL Server (ISARS)	Running	
TMG-EN	SQL Server Reporting Services (ISARS)	Running	
TMG-EN	Microsoft Forefront TMG Firewall	Running	00:20:45
TMG-EN	Microsoft Forefront TMG Job Scheduler	Running	00:21:10
TMG-EN	SQL Server Express	Running	
TMG-EN	Microsoft Forefront TMG Managed Control	Running	

Refresh
Refresh Now
Automatic Refresh Rate: Medium

Services Tasks
Stop Selected Service

Figure 1: Stopping services in the Forefront TMG MMC

Other (directly) related services

There are some other Windows services which are directly related to Forefront TMG functionality. Some of these services are:

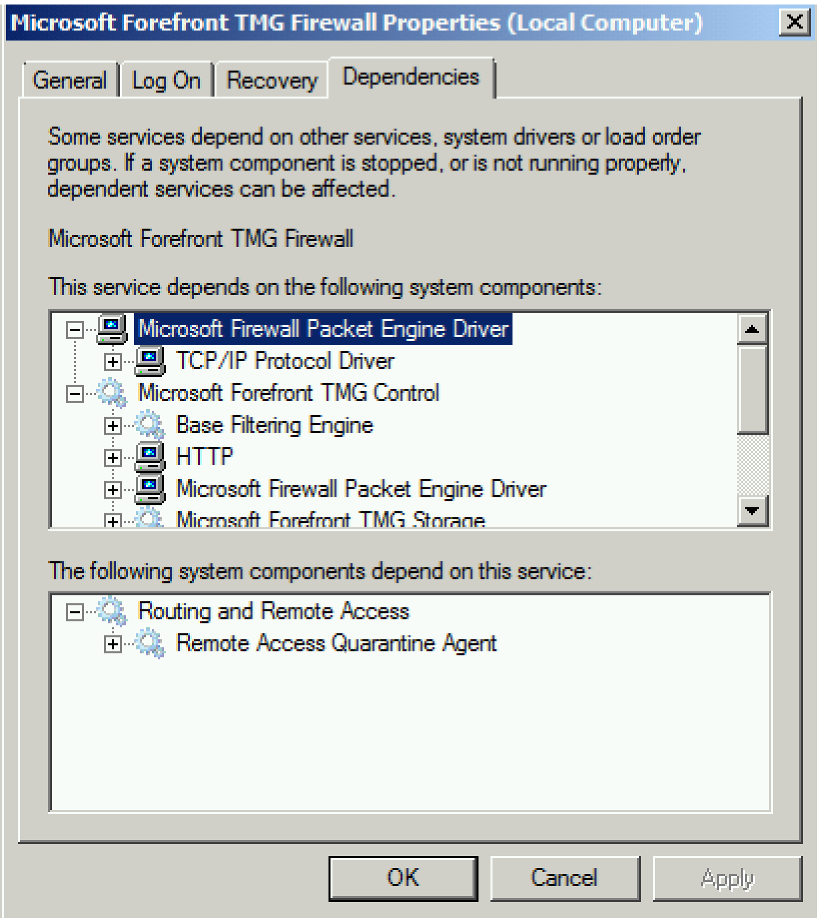
- IKE and AuthIP Ipsec Keying Modules
- IPsec Policy Agent
- ISASTGCTRL (AD LDS instance)
- Network Policy Server
- Routing and Remote Access
- SQL Server (ISARS)

- SQL Server (MSFW)
- SQL Server Reporting Services (ISARS)

Please note: There are some other important Windows services which are not directly related to Forefront TMG but these services are also important for the entire functionality of the underlying Windows operating system, so I recommend to monitor all services on the Forefront TMG Server for example with Microsoft System Center 2012 Operations Manager or other third party solutions.

Service dependencies

For a better understanding how Forefront TMG services interact with other TMG and Windows services you should have a look into each related Forefront TMG services to see the dependencies on other services or the dependencies of Forefront TMG services from other Windows and TMG services. To evaluate the service dependency you can use the Windows services Snap In as shown in the following screenshot.


Microsoft Forefront TMG Firewall Properties (Local Computer)
General
Log On
Recovery
Dependencies
OK
Cancel
Apply

Some services depend on other services, system drivers or load order groups. If a system component is stopped, or is not running properly, dependent services can be affected.

Microsoft Forefront TMG Firewall

This service depends on the following system components:

- Microsoft Firewall Packet Engine Driver
  - TCP/IP Protocol Driver
- Microsoft Forefront TMG Control
  - Base Filtering Engine
  - HTTP
  - Microsoft Firewall Packet Engine Driver
  - Microsoft Forefront TMG Storage

The following system components depend on this service:

- Routing and Remote Access
  - Remote Access Quarantine Agent

Figure 2: Forefront TMG Service dependencies

You can also use the Windows Registry to see Forefront TMG services dependencies. Start *Regedit.exe* and navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*.

Forefront UAG services

During a Forefront UAG installation, Forefront TMG will also be installed on the Server. Forefront TMG Firewall functionality is used to protect the local Server and Forefront UAG uses many of the Forefront TMG functions to provide Forefront UAG functionalities. In addition to the Forefront TMG services, the following Forefront UAG services will be installed:

Name: Microsoft Forefront UAG Configuration Manager
Functionality: Manages the Forefront UAG configuration. Interacts between local Forefront UAG configuration and the Forefront TMG configuration.

Name: Microsoft Forefront UAG DNS64 Service
Functionality: This service complements a NAT64 deployment by translating IPv4 DNS responses to IPv6 DNS and is used when Forefront UAG has been deployed as a Direct Access Server.

Name: Microsoft Forefront UAG Endpoint Component Manager
Functionality: Manages Forefront UAG endpoint components. UAG Endpoint components can be used to control clients which wants to access a Forefront UAG portal.

Name: Microsoft Forefront UAG File Sharing
Functionality: Provides remote access to internal file structures, published through a Forefront UAG portal.

Name: Microsoft Forefront UAG Log Server
Functionality: Collects log messages and performs automatic cleanup of log files.

Name: Microsoft Forefront UAG Monitoring Manager
Functionality: Collects monitoring information and forwards it to the Web Monitor. Forefront UAG Administrators can use the Web Monitor to monitor and control portal usages and user sessions.

Name: Microsoft Forefront UAG Quarantine Enforcement Client
Functionality: Reports client health status when Forefront UAG portal or Direct Access has been configured to enforce NAP (Network Access Protection).

Name: Microsoft Forefront UAG Quarantine Enforcement Server
Functionality: Evaluates endpoint settings against NAP policies.

Name: Microsoft Forefront UAG Session Manager
Functionality: Manages data from endpoint sessions through UAG clients.

Name: Microsoft Forefront UAG SSL Network Tunneling Server
Functionality: Manages a virtual network on the server-side for remote VPN clients which connects through SSTP to the UAG Server.

Name: Microsoft Forefront UAG Terminal Services RDP Data
Functionality: Generates RDP data for the Terminal Services Client which connects through the Remote Desktop Gateway Server functionality.

Name: Microsoft Forefront UAG User Manager

Functionality: Authenticates users and provides user information against configured Forefront UAG authorization/authentication repositories like Active Directory domain services.

Name: Microsoft Forefront UAG Watch Dog Service
Functionality: This service is responsible for shutting down unresponsive critical services. These critical services should be configured to automatically restart to allow recovery.

As with Forefront TMG services, Forefront UAG services depends on other Forefront UAG and Windows services, so you should be familiar with these dependencies.

Conclusion

In this article I explained the several Forefront TMG services and related Windows services for Forefront TMG services. I also explained the functionality of a lot of Forefront UAG services and the service dependencies between different Forefront TMG and UAG services.

Related links

About Forefront TMG Services
http://msdn.microsoft.com/en-us/library/ff823916(v=vs.85).aspx
Firewall Lockdown mode
http://technet.microsoft.com/en-us/library/cc995069.aspx
TMG Storage 101
http://www.isaserver.org/articles-tutorials/configuration-general/Microsoft-Forefront-TMG-Storage-101.html
ISA Server 2006 Firewall Core
http://download.microsoft.com/download/e/7/6/e76fdda3-5c2c-4fbb-9c6f-3bcd0ed4b8ef/Firewall_Corewp.doc
Large Logging Queue (LLQ)
http://blogs.technet.com/b/isablog/archive/2012/09/18/tmg-logging-to-llq.aspx