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

Unsupported configurations with Forefront TMG

Abstract

In this article I will explain the unsupported configuration scenarios with Forefront TMG based on the official Microsoft documentation and my experience in customer projects.

Let's begin

Before you install Forefront TMG you should carefully read on which platforms a Forefront TMG installation is supported. There are the following limitations:

- Forefront TMG is not supported on a 32-bit operating system
- Forefront TMG is not supported on Windows Server 2003
- Forefront TMG is not supported on all editions of Windows Server 2008
- Forefront TMG is not supported on Windows Server 2012 / R2.

If you want to install Forefront TMG in an array managed by an Enterprise Management Server (EMS), make sure that the EMS Server is installed on a supported machine without other Forefront TMG services installed.

If you try to upgrade your old ISA Server 2004 / 2006 machine to Forefront TMG keep in mind that there is no in Place upgrade supported. You must export the ISA 2004 / 2006 configuration, built a new Server with Forefront TMG and import the old configuration from ISA 2004/2006. If you want to upgrade from ISA 2000 to Forefront TMG you first have to install a temporary ISA 2004/2006 computer to import the ISA 2000 configuration and after that you can use the exported ISA 2004/2006 configuration to create a new Forefront TMG Server. An In place Update from Windows Server 2008 SP2 to Windows Server 2008 R2 is also not supported, so you have to create a fresh installation.

Some customers asked my in the past if it is possible to install Forefront TMG on a Domain Controller. The installation of Forefront TMG on a Domain Controller is not supported but with Forefront TMG SP1 Microsoft extends the support of Forefront TMG installed on a Read Only Domain Controller (RODC).

Many of my customers asked me in the past if it is better to install Forefront TMG as a member of a workgroup instead of being an Active Directory Domain Member. Regardless of the Pros and Cons, deploying Forefront TMG in a workgroup has the following limitations:

- Domain-based user authentication cannot be applied to an array
- Client certificates cannot be used as primary authentication
- User mapping is not supported (except for PAP and SPAP)
- Automatic Web proxy detection using Active Directory Auto Discover is not possible for TMG clients

- Group policy deployment of the HTTPS inspection trusted root certification authority (CA) certificate to client computers with the TMG client installed is not possible
- If you deploy a Forefront TMG array, EMS replication is not supported (only one EMS Server)

Please also keep attention with third party Firewalls installed on the Forefront TMG Server. Forefront TMG cannot coexist with a Third Party Personal Firewall and if you use the built in Windows Firewall make sure that the Firewall is NOT controlled by Active Directory Group Policies because Forefront TMG takes control over the Windows Firewall with the Web Filtering Platform (WFP).

Array issues

If you deploy Forefront TMG in an array please also be aware of the following restrictions:

- An array of Forefront TMG servers with different operating systems is not supported
- Forefront TMG and ISA Server cannot coexist in the same enterprise or array
- Forefront TMG does not support firewall chaining

ISP Redundancy issues

Few of my customers uses the ISP Redundancy feature of Forefront to load balance / aggregate the Bandwidth of two ISP links (Personally I prefer a dedicated Router for ISP Load Balancing). If you decided to use the ISP-R feature you should be aware of the following issues:

- ISP redundancy does not support more than two external interfaces
- Forefront TMG does not support more than two default gateways
- Multiple DHCP default gateways are not supported
- ISP redundancy does not support e-mail protection
- Protocol-based load balancing is not supported with ISP redundancy feature

Networking issues

Networking in Forefront TMG is one of the most importing tasks to consider. There are some pitfalls.
Forefront TMG doesn’t support defining networks that represents remote subnets which means you must include all IP address subnets from your LAN infrastructure in the logical network definition on your TMG Server.
If you decided to install Forefront TMG with a single Network adapter, there are some limitations in functionality. The following article explains these limitations. Other networking issues:

- Internationalized Domain Names are not supported
- Domain names that include wildcard characters are not supported with link translation enabled
- Protocol based Enhanced NAT is not supported

VPN issues

If you use Forefront TMG as a VPN server consider the following limitations:

If you use Forefront TMG in an array you cannot use DHCP to allocate IP addresses for VPN clients. You must use static non overlapping IP address ranges on every Forefront TMG Array member.
Be also aware that you cannot use IP filters configured on the NPS (Network Policy Server). Forefront TMG overrides most manually created NPS settings.
Last but not least outbound L2TP connections are not supported by Forefront TMG configured as an L2TP/IPsec VPN server.

Protocol and application issues

Forefront TMG is an Application Layer Firewall and is able to filter many protocols with the help of application filter installed on the Forefront TMG Server. You must be aware of some protocol and application limits.
If you publish Outlook Anywhere with Forefront TMG, the TMG RPC filter cannot filter RPC-over-HTTP traffic.
If you use the HTTPS inspection feature, be aware of the following limitations:

- Extended Validation (EV) SSL certificates.
- Connections to external SSTP servers.
- CNG certificates.
- Servers that require client certificate authentication

Forefront TMG doesn't support Secure FTP connections. There are some community solutions to make SFTP connections possible but in my experience they doesn't work in every TMG implementation.
Many customers implemented client access with the use of Web Proxy Clients. A Web Proxy client hast some limitations if he tries to access FTP sites:

- Web Proxy client FTP requests are passed over HTTP. Therefore you cannot use FTP upload from a Web Proxy client, and only FTP downloads are supported
- To access FTP sites that require authentication, credentials should be specified in the address bar using the following format: ftp://username:password@FTP_Server_Name.
- By default, Forefront TMG uses PASV mode for FTP requests

Some customers asked me if they could use Forefront TMG as a router with dynamic routing protocols. Keep in mind that Forefront TMG does not support Routing Protocols like IGRP, BGP, RIP and OSPF.

Forefront TMG support in a virtual environment. Forefront TMG is supported to run as a Virtual Machine on a supported Hypervisor platform which is listed in the Microsoft Server Virtualization Validation Program (SVVP). If you want to implement Forefront TMG as a Virtual Machine, you should carefully read the whitepaper for Security considerations in a Virtual environment.

The most important limitation in Forefront TMG networking is that TMG does not support IPv6 traffic. Forefront TMG cannot filter IPv6 traffic. You have the option to hide the IPv6 logging entries in the Forefront TMG MMC if doesn't want to see this traffic. Don't be confused with IPv6 support in Forefront TMG for Direct Access traffic. There are some scripts and Registry keys which can be enabled on the TMG Server to allow Forefront TMG to act as a Direct Access Server.

The last important notice is, that Forefront TMG doesn't support CNG (Cryptographic Next Generation) certificates. This is a very important information because in the past I often had customer request who tries to install CNG certificates on the TMG Server for reverse publishing or HTTPS inspection.

Other limitations:

- Live Communications Server not supported on the Forefront TMG computer
- Forefront TMG does not support SIP traffic from an OCS server
- WCCP, ICP and ICAP protocols are not supported in Forefront TMG

Conclusion

After reading this article and the additional informations I mentioned you should now have a good understanding about unsupported configurations with Forefront TMG and how to avoid these limitations when you implement Forefront TMG in your environment.

Related links

Unsupported configurations
http://technet.microsoft.com/de-de/library/ee796231.aspx
Microsoft Forefront TMG - Installing Forefront TMG on a RODC
http://www.isaserver.org/articles-tutorials/installation-planning/Microsoft-Forefront-TMG-Installing-Forefront-TMG-RODC.html
About single network adapter limitations
http://technet.microsoft.com/en-us/library/cc995236.aspx
Publishing Secure FTP Servers behind ISA Firewalls
http://www.isaserver.org/articles-tutorials/configuration-general/Publishing-Secure-FTP-Servers.html
Configuring Forefront TMG as a Direct Access Server
http://www.isaserver.org/articles-tutorials/configuration-general/Microsoft-Forefront-TMG-How-configure-Forefront-TMG-DirectAccess-Server.html
Security Considerations with Forefront Edge Virtual Deployments
http://technet.microsoft.com/library/cc891502.aspx