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

Microsoft Forefront TMG and UAG – A feature comparison

Abstract

In this article I will give you some detailed information about the differences between Forefront TMG and Forefront UAG, the supported and unsupported configurations with TMG and UAG and the operational areas of each product.

Let's begin

First of all let us have a brief description about Forefront TMG and Forefront UAG.

Forefront TMG

Forefront Threat Management Gateway 2010 (TMG) is the successor of ISA Server 2006. For a detailed comparison between ISA Server 2006 and Forefront TMG read the following article. Forefront TMG is a Multilayer Enterprise Firewall with several features like:

- Stateful Packet filtering
- Application Layer Firewalling
- HTTP Filter
- HTTPS Inspection
- URL Filtering
- Malware Inspection
- VPN Server (Client VPN and Site to Site VPN)
- Web proxy and Web caching Server
- Forward- and reverse Proxy
- E-Mail Protection Gateway
- Intrusion Prevention (IPS) and Intrusion Detection (IDS) system

Forefront TMG is available in two versions: Standard and Enterprise. For an overview about the Forefront TMG editions read the following article.

System requirements for Forefront TMG:

Component	Minimum requirements
CPU	64-bit, 1.86 GHz, 2 core (1 CPU x dual core) processor
Memory	2 GB, 1 GHz RAM
Hard Disk	2.5 GB available space. This is exclusive of the hard disk space required for caching or for temporarily storing files during malware inspection. One local hard disk partition that is formatted with the NTFS file system
Network adapters	One network adapter that is compatible with the computer's operating system, for communication with the Internal network
Operating system	Windows Server 2008 Version: SP2 or R2 Edition: Standard, Enterprise or Datacenter
Windows Roles and	These Roles and Features are installed by the Forefront TMG

Features	Preparation Tool: Network Policy Server Routing and Remote Access Services Active Directory Lightweight Directory Services Tools Network Load Balancing Tools Windows PowerShell
Other software	Microsoft .NET Framework 3.5 SP1 Windows Web Services API Windows Update Microsoft Windows Installer 4.5

Forefront UAG

Forefront Unified Access Gateway 2010 (UAG) is the successor of Microsoft IAG (Intelligent Application Gateway) and is designed for inbound access to corporate resources from several client types like Windows, Linux, Macintosh clients and mobile devices. Forefront UAG decides between managed and unmanaged clients. One of the strengthen of Forefront UAG are so called Endpoint access policies which can be used to give clients access to internal resources only when a predefined set of rules, defined from UAG administrators are fulfilled. You can think about Forefront UAG Endpoint access Policies as a much enhanced version of NAP (Network Access Protection). Forefront UAG enhances the basic Webserver publishing options from Forefront TMG by integrating a deep understanding of the applications published, the state of health of the devices being used to gain access, and the user's identity. Forefront UAG provides portal support for gaining access to internal resources. A portal is a website access by clients where users can gain access to different published applications like OWA, Remote Desktop connections, SSL VPN, Microsoft CRM, Sharepoint and many others.
Forefront UAG also supports several authentication providers like Active Directory, Netscape, LDAP, RADIUS, OTP and many more.
Another primary development goal of Forefront UAG is remote access via SSL VPN and a technique called DirectAccess.

System requirements for Forefront UAG:

Component	Minimum requirements
CPU	2.66 gigahertz (GHz) or faster processor. Dual core CPU
Memory	4 GB
Hard Disk	2.5 gigabyte (GB) (in addition to Windows requirements)
Network adapters	Two network adapters that are compatible with the computer operating system. These network adapters are used for communication with the internal corporate network, and the external network (Internet). Note that deploying Forefront UAG with a single network adapter is not supported
Operating system	Forefront UAG can be installed on computers running the Windows Server 2008 R2 Standard or Windows Server 2008 R2 Enterprise 64-bit operating systems. Forefront UAG must be a domain member
Windows Roles and Features	Network Policy Server Routing and Remote Access Services Active Directory Lightweight Directory Services Tools

	Message Queuing Services Web Server (IIS) Tools Network Load Balancing Tools Windows PowerShell
Other software	Microsoft .NET Framework 3.5 SP1 Windows Web Services API Windows Update Microsoft Windows Installer 4.5 SQL Server Express 2005 Forefront TMG is installed as a firewall during Forefront UAG setup. Following setup, Forefront TMG is configured to protect the Forefront UAG server. The Windows Server 2008 R2 DirectAccess component is automatically installed

Comparing Forefront TMG and Forefront UAG

During my work as a Consultant and Trainer for Forefront products, I often heard from customers that they are not aware of the differences between Forefront TMG and UAG and when they have to implement Forefront TMG or Forefront UAG.

I will try to give a short decision help:
Forefront TMG is the Enterprise Edge Firewall to protect the internal network from the Internet and also provides protected access from internal resources to the Internet. Forefront TMG has powerful publishing features to publish internal services to the Internet like Outlook Web Access, Exchange Active Sync and a lot of more services, but is limited in intelligent publishing and only gives a limited control about client devices which should access the internal published resources. In fact Forefront TMG acts as a Firewall for **incoming** and **outgoing** requests.
Forefront UAG is used to extend and enhance the basic publishing features of Forefront UAG and comes with extended features like portals, SSL VPN (Please note: Forefront TMG also supports SSL VPN in form of SSTP), DirectAccess and powerful Endpoint Access Policies to control the client devices, accessing the Forefront UAG server. During a Forefront UAG installation, Forefront TMG will also be installed **but only** to protect the Forefront UAG Server. In fact Forefront UAG acts as an Application Layer Gateway and is the solution for **incoming** access to resources from the Internet.

The following screenshot gives a clear explanation about the Forefront TMG and Forefront UAG usage scenarios:

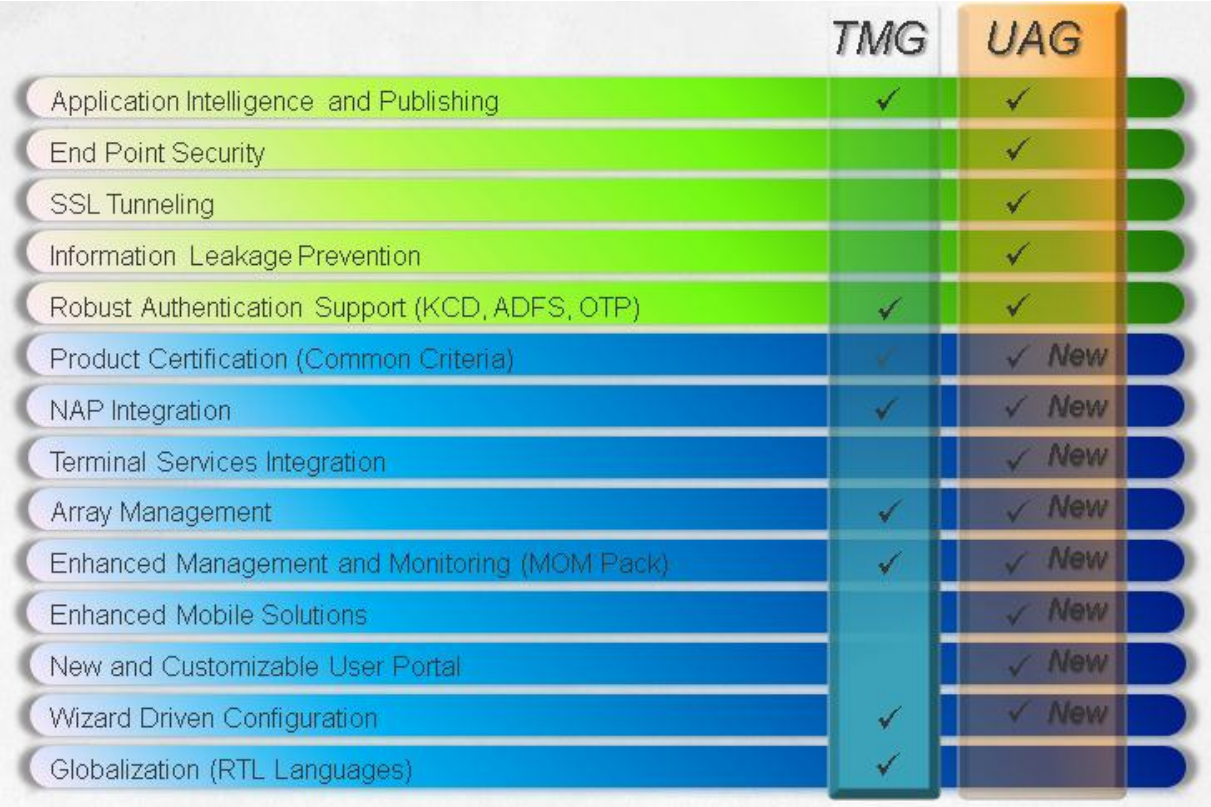

Figure 1: Forefront TMG and Forefront UAG comparison (Source: Microsoft)

Forefront TMG unsupported configurations

As with every solution there are supported and unsupported configurations. The unsupported configurations with Forefront TMG are:

- Forefront TMG is not supported on a 32-bit operating system
  - Forefront TMG can only be installed on a 64 Bit Operating system (2008 SP2 and 2008 R2)
- Forefront TMG is not supported on Windows Server 2003
- Forefront TMG is not supported on all editions of Windows Server 2008
  - Installation of Forefront TMG is only supported in Standard, Enterprise and Datacenter Edition and also not supported on Windows Server Core!
- Installing EMS on a Forefront TMG computer is not supported
  - EMS is the Enterprise Management Server (formerly known as CSS)
- In-place upgrade from ISA Server 2004/2006 to Forefront TMG is not supported
  - You have to export the ISA Server configuration and to import this configuration on a fresh TMG installation
- In-place upgrade from Windows Server 2008 SP2 to Windows Server 2008 R2 is not supported
  - Forefront TMG does not support upgrading to Windows 2008 R2 while Forefront TMG is installed.
- Forefront TMG installed on a domain controller is not supported, except with Forefront TMG SP1 where the installation of TMG is allowed on a Read Only Domain Controller (RODC)
- Forefront TMG Client is not supported on Windows 2000
- Forefront TMG does not support Firewall Client 2000

- Workgroup deployment limitations
  - user group authentication only with the use of LDAP (for publishing scenarios) or RADIUS (for in and outgoing access)
  - Client certificates cannot be used as primary authentication
  - User mapping is not supported (except for PAP and SPAP)
  - Group policy deployment of certificates for HTTPS inspection is not available
  - Automatic Web proxy detection using Active Directory Auto Discover is not possible.
- Multiple firewalls products
  - Installing other firewall products (such as a personal firewall) on a Forefront TMG Server is not supported

Forefront UAG support boundaries

Forefront UAG has also some supported and unsupported configurations. These support boundaries are:

Forefront UAG and Forefront UAG DirectAccess

Forefront UAG can be used to publish internal servers via Web portal or directly (like in Forefront TMG).
Forefront UAG can be used as a DirectAccess Server to extend the DirectAccess functionality which comes with Windows Server 2008 R2. Please note the following:

- Forefront UAG can be configured as a publishing Server and as a DirectAccess Server on the same machine
- Servers in an Forefront UAG Array can be configured to provide remote access to published servers and as a DirectAcccess server at the same time
- It is not possible to use the Network Connector application (a form of VPN) when Forefront UAG is configured as a DirectAccess server.

IPv6 support

In order to support DirectAccess, which is IPv6-based, Forefront UAG allows the following IPv6 traffic:

- Inbound authenticated IPv6 traffic (using IPsec).
- Native IPv6 traffic from and to the Forefront UAG DirectAccess server.
- Inbound and outbound IPv6 transition technologies (6to4, Teredo, IP-HTTPS and ISATAP).

No other IPv6 traffic is supported by Forefront UAG.

Forefront TMG running on Forefront UAG

A frequent misunderstanding is the role of Forefront TMG on Forefront UAG. I talked with many customers in the past which want to replace their Forefront TMG servers with Forefront UAG to participate from the Forefront UAG features, but Microsoft has clear statements about supported and unsupported configurations, which are:
Forefront TMG is installed during a Forefront UAG installation
Forefront TMG is installed as a complete product, and is not modified to run on a Forefront UAG server
Forefront UAG uses Forefront TMG, as follows:

Forefront TMG acts as a firewall, protecting **only** the Forefront UAG server.

Forefront UAG uses Forefront TMG infrastructure and functionality in some deployment and monitoring scenarios.
Changes made through the Forefront UAG console are processed to the Forefront TMG configuration and only in this way!

It is possible to configure some parts of Forefront TMG through the Forefront TMG Management console (MMC), but the following is **not** supported:

- Forefront TMG will be automatically installed during a Forefront UAG installation, a manual Forefront TMG installation is not supported
- Forefront UAG must be installed on a clean Windows Server 2008 SP2/R2 machine without Forefront TMG installed
- Forefront TMG will be removed if you remove Forefront UAG
- A manual uninstallation of Forefront TMG is not supported
- Forefront TMG as a forward proxy for **outbound** Internet access
- Forefront TMG as a site-to-site VPN server
- Forefront TMG as an intrusion protection system
- Publishing Forefront TMG via Forefront UAG

Supported Forefront TMG configurations

You can use the Forefront TMG Management console (MMC) for the following configurations:

- Creating access rules to limit access for users, groups, and networks for VPN remote access. These access rules must be place under the automatically created Firewall policies from Forefront UAG
- Monitoring, logging and reporting
- Modifying Forefront TMG system policies to enable access from Forefront TMG to internal Servers and to give access from internal Servers to Forefront TMG
- Publish Exchange SMTP/SMTPS
- Publish Exchange IMAP/IMAPS
- Publish Exchange POP3/POP3S
- Publish Office Communications Server (OCS) (except the OCS web access which should be published with Forefront UAG)

Forefront UAG placement

Because of the several limitations you must plan where to implement Forefront UAG in your network environment. Possible placements are:

- Forefront UAG in a DMZ (Perimeter) scenario with a Front- and Back firewall in place
- Forefront UAG as a parallel placement with your existing Firewall

Depending on your decision you have to open several Firewall ports for correct communication with Forefront UAG. You will find more information about these deployments here.

Conclusion

In this article I gave you a detailed comparison between the Forefront TMG and Forefront UAG features and we also discussed the support boundaries of Forefront

UAG and the unsupported Forefront TMG configurations. I hope that this article gave you some helpful information to decide which version is the right for your deployment.

Related links

About the Forefront TMG editions
http://technet.microsoft.com/en-us/library/ee207137.aspx
System requirements for Forefront TMG
http://technet.microsoft.com/en-us/library/dd896981.aspx
Forefront TMG unsupported configurations
http://technet.microsoft.com/de-de/library/ee796231.aspx
System requirements for Forefront UAG servers
http://technet.microsoft.com/en-us/library/dd903051.aspx
Forefront UAG support boundaries
http://technet.microsoft.com/en-us/library/ee522953.aspx
Forefront UAG – Frequently Asked Questions
http://www.microsoft.com/forefront/unified-access-gateway/en/us/faq.aspx
Comparing Forefront TMG with ISA Server 2006
http://www.microsoft.com/forefront/threat-management-gateway/en/us/features.aspx#Compare
Forefront UAG placement
http://technet.microsoft.com/en-us/library/ee809089.aspx