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

Support boundaries for Forefront UAG

Abstract

In this article I will write about Forefront UAG support boundaries. I will explain which configurations are supported and which not and I will also show ways to configure the underlying Forefront TMG Server for special configurations without affecting the Forefront UAG functionality.

Let's begin

If you install Forefront UAG, Forefront TMG will also be installed as the underlying Firewall to protect the local system. Changes in the Forefront UAG MMC will be distributed to the Forefront TMG Server. For example if you create a new portal trunk and applications in the trunk, Forefront TMG Firewall policies will be created. This combination is important because there are some pitfalls if you try to modify the TMG configuration directly, but more about this later.

The first support boundary is Forefront UAG and Forefront UAG DirectAccess:
You can use Forefront UAG as a publishing server, creating trunks to publish applications for access by remote clients directly, or via a Forefront UAG portal. In addition, you can deploy Forefront UAG as a DirectAccess server but you must be aware of the following:

- A single Forefront UAG server can be configured as both a Forefront UAG publishing server, and as a Forefront UAG DirectAccess server.
- An array can consist of Forefront UAG servers that act as both remote access publishing servers, and as Forefront UAG DirectAccess servers.
- You cannot publish the legacy Network Connector application when Forefront UAG is configured as a DirectAccess server.

Forefront UAG / TMG networking

Many customers asked my in the past about the supported number of Network adapters in Forefront UAG. The Microsoft statement is as follows:

- Forefront UAG supports configuration of two networks – internal and external. Connecting to different switches for network redundancy is supported, providing that both are defined as part of the internal or external network.
- Using Forefront TMG running on the Forefront UAG server to provide multiple network routing is not supported.
- Deployment with a single network adapter is not supported.

If you want to implement Forefront UAG as a DirectAccess Server, Forefront UAG allows the following IPv6 traffic:

- Inbound authenticated IPv6 traffic (using IPsec).
- Native IPv6 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 UAG customization

Forefront UAG provides a wide range of customization settings, with the following support guidelines:

- CSS provides a commercially reasonable effort to customers in making custom changes to SRA, AppWrap, and FormLogin.xml, to resolve problems in publishing out-of-the box supported applications
- CSS provides a commercially reasonable effort to deliver samples to customers for SRA, AppWrap and FormLogin.xml for applications
- CSS will provide commercially reasonable effort to provide samples for general Forefront UAG product functionality that is documented in the Forefront UAG Microsoft TechNet Library. For example, features such as access policy detection, language customization, custom reporting events, portal page customization, and login page user interface customization.
- All other customizations are not supported by CSS.

Forefront TMG running on Forefront UAG

As mentioned in the beginning of this article Forefront TMG is installing during the Forefront UAG setup. 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 the Forefront UAG server.
- Forefront UAG uses Forefront TMG infrastructure and functionality in some deployment and monitoring scenarios.

It is possible to configure Forefront TMG running on Forefront UAG using the Forefront TMG MMC but Forefront TMG is intended for use of the Forefront UAG infrastructure only.

Not supported Forefront TMG configurations:

- Forefront TMG is installed automatically during Forefront UAG Setup, and removed automatically if Forefront UAG is uninstalled. Installing and uninstalling only Forefront TMG is not supported.
- Forefront TMG as a forward proxy for outbound Internet access.
- Forefront TMG application publishing, except for the publishing scenarios listed in the Supported Forefront TMG configurations section that follows.
- Forefront TMG as a site-to-site VPN.
- Forefront TMG as an intrusion protection system.
- Forefront TMG as a network perimeter firewall. Forefront TMG running on Forefront UAG is only intended to protect the Forefront UAG local host server.
- Publishing Forefront TMG via Forefront UAG.

You should read this limitations carefully. In the past I had some customers which configured Forefront TMG on the UAG Server like a Standalone Forefront TMG Server which resulted in some problems with the Forefront UAG configuration.

Supported Forefront TMG configurations:

You can use Forefront TMG running on the Forefront UAG server with the following:

- Creating Firewall Policy rules using the Forefront TMG MMC for the purpose of limiting users, groups, and networks for granular access when deploying Forefront UAG for VPN remote network access

Important: If you create Firewall policy rules in the TMG MMC, make sure that you place the rules before or after the "Anchor" Firewall policy rules, created by Forefront UAG.

- Monitoring with the Forefront TMG MMC.
- Limiting users, groups, sources and destinations on Forefront TMG system policy rules, with the purpose of enabling access to corporate servers and remote management to and from the Forefront UAG local host server.
- You can publish the following applications via Forefront TMG:
  - Exchange SMTP/SMTPS
  - Exchange POP3/POP3S
  - Exchange IMAP/IMAPS
  - Office Communications Server (OCS)—Only Communicator Web Access should be published using Forefront UAG. Other OCS features should be published using the Forefront TMG MMC running on the Forefront UAG server

Conclusion

In this article I tried to explain the supported and unsupported configurations with Forefront UAG in combination with Forefront TMG. In general you should do most of the Forefront UAG configuration through the Forefront UAG MMC to avoid configuration problems. For some special configurations it is allowed to use the Forefront TMG MMC but you should be careful by using the TMG MMC.

Related links

Support boundaries with Forefront UAG
http://technet.microsoft.com/en-us/library/ee522953.aspx