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

Microsoft Forefront UAG – Overview of Microsoft Forefront UAG

Abstract

In this article, I will show you how to install and configure some basic settings of Microsoft Forefront UAG. I will also show you how to create a new Portal to publish Exchange Server 2010 Outlook Web App, former known as Outlook Web Access (OWA).

Let's begin

First please note that I'm writing about the release candidate of UAG, so it might be possible that some information are changed in the RTM version of Microsoft Forefront UAG.

Microsoft Forefront UAG, currently available as an RC1 build is the successor of Microsoft Forefront IAG (Intelligent Application Gateway). With the help of UAG it is possible to extend the functionalities of Microsoft Forefront Threat Management Gateway 2010 (TMG). UAG allows the configuration of SSL VPN, the new Direct Access feature of Windows Server 2008 R2 and it also extends the basic webserver publishing features from Microsoft Forefront TMG. With IAG it is possible to create your own publishing portals called a trunk in UAG terms. One of the publishing capabilities of Forefront UAG is the publishing of Microsoft Exchange features like Outlook Web App, Outlook Anywhere but it is also possible to publish Microsoft SharePoint Server services to the Internet.

Key features of Forefront UAG

- Remote access
- Application intelligence
- Security and access control
- Frontend and Backend authentication

System requirements

Microsoft Forefront UAG has the following system requirements

Component	Requirement
Processor	2,66 Ghz or faster, Dual Core CPU
Memory	8 GB RAM or more recommended
Hard drive	30 GB

Table 1: Forefront UAG system requirements

Software and deployment requirements

Servers

Forefront UAG can be installed on computers running Windows Server 2008 R2 Standard or Windows Server 2008 R2 Enterprise X64 bit editions.

Arrays

If you want to deploy an array of multiple Forefront UAG servers, each server that will join the array must be installed as a domain member before beginning Forefront UAG installation.

Network adapters

Forefront UAG must be installed on a computer with at least two network adapters.

Other applications

The computer on which you are installing Forefront UAG should have a clean Windows Server 2008 installation, with no other applications installed on it.

Default installation

By default, Forefront Threat Management Gateway (TMG) is installed during Forefront UAG Setup.

Permissions

When installing Forefront UAG, you must have administrator permissions on the local server. You must also be a domain user in the domain to which the Forefront UAG server belongs.

Installation

After the RC version of UAG is downloaded, we can start the installation process. First review the Hardware and software requirements and check the deployment checklist.

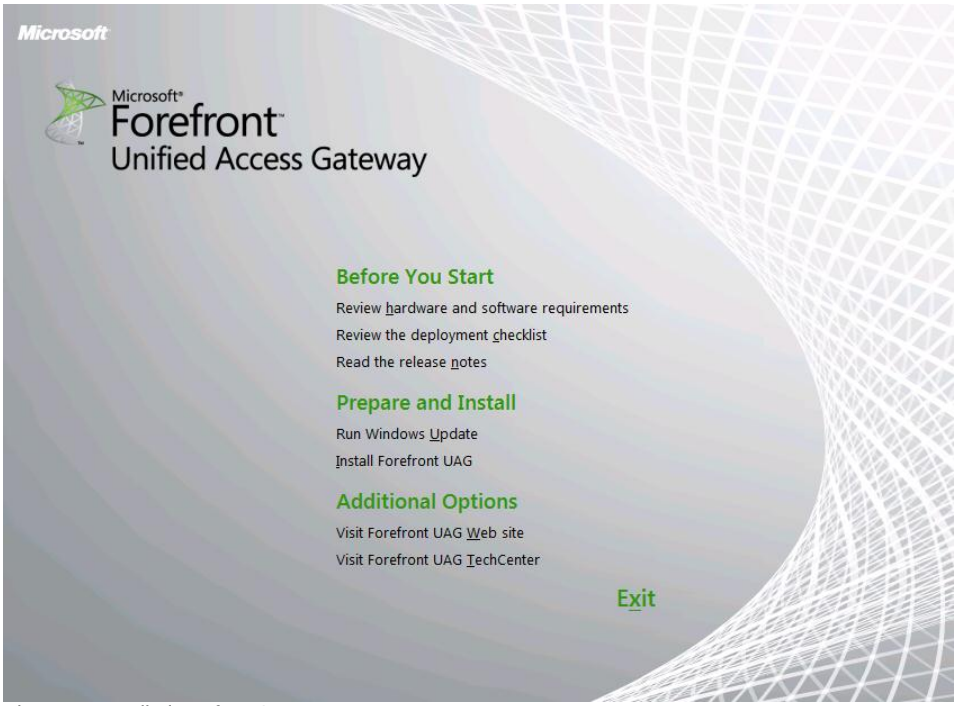

Figure 1: Installation of UAG

After the installation has finished you can launch the Getting Started Wizard from the UAG Management console. The Getting started wizard allows you some basic network configuration settings like UAG network card settings and the UAG Server topology. Forefront UAG can be installed as a standalone Server or in an UAG array to provide high availability and better performance.

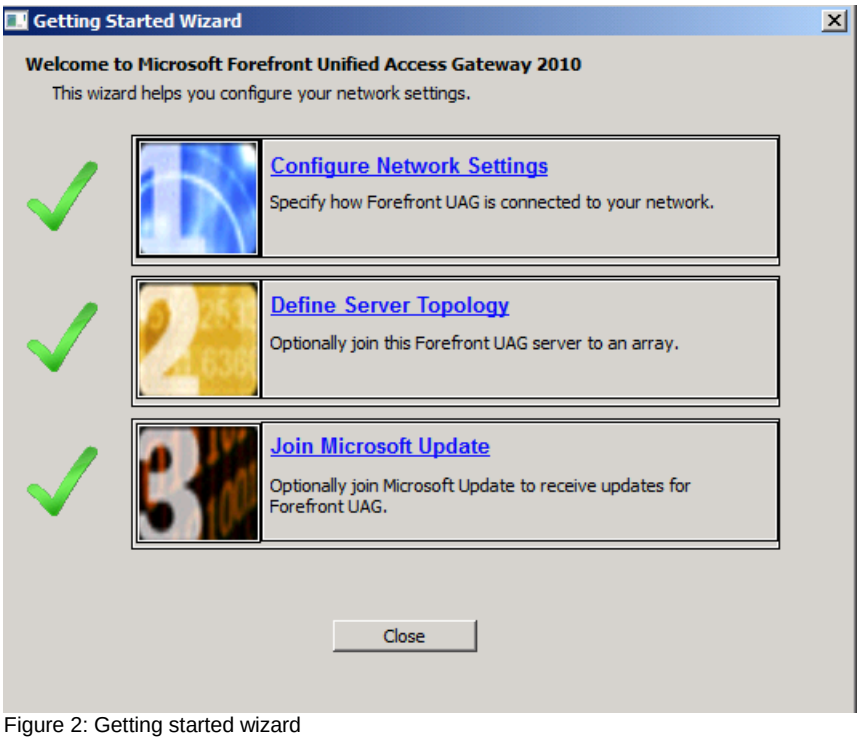

Figure 2: Getting started wizard

The define Network Adapter settings is important to tell UAG which network cards connects to the Internal (Trusted) network and which network card connects to the External (Untrusted) network.

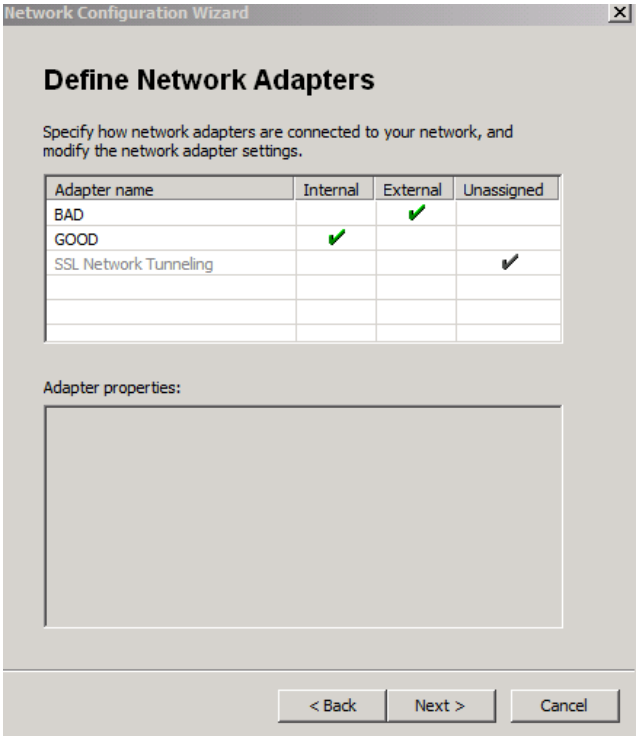

Figure 3: Define network adapters

After the Getting started wizard has finished, it is possible to more advanced settings before creating a new trunk but first let's have a look at the installed services during the Forefront UAG setup.

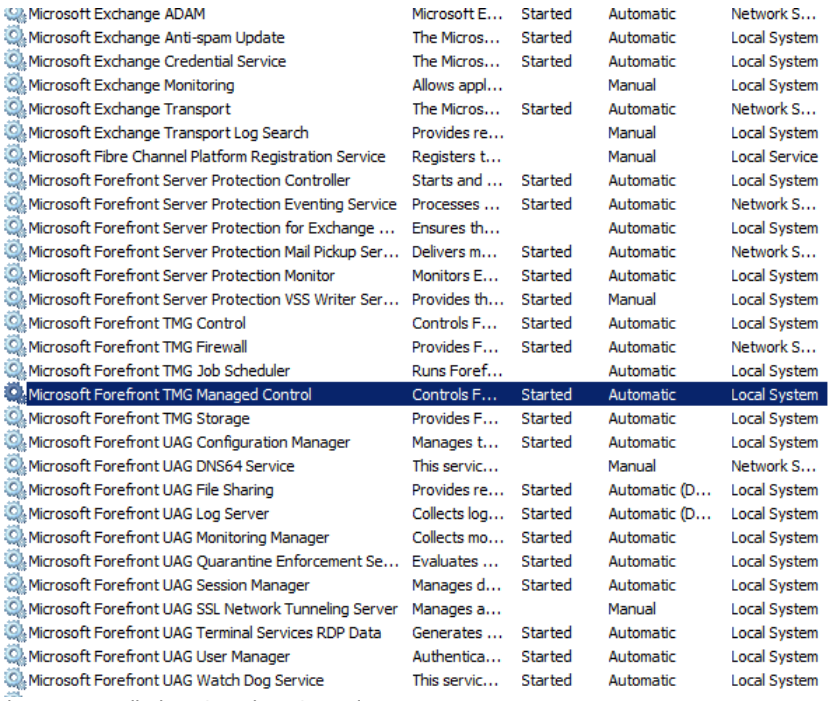

Figure 4: Installed UAG and TMG services

Forefront UAG Gateway Activation Monitor

Forefront UAG now provides an Activation Monitor that shows configuration activation activity. This feature is useful to monitor the status of UAG array members

when activation occurs on the array manager. Activation Monitor is available from the Forefront UAG options in the Start menu.

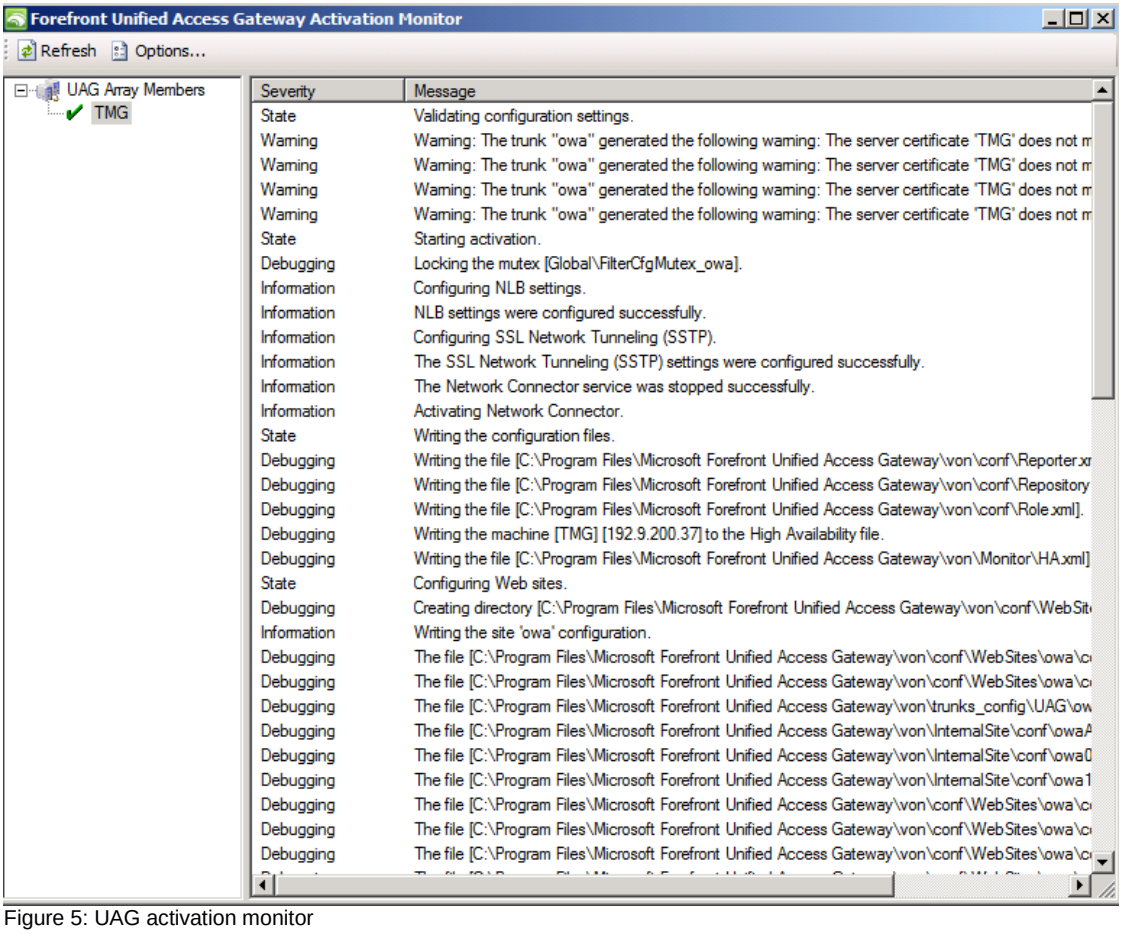

Figure 5: UAG activation monitor

Microsoft Forefront UAG configuration console

The UAG configuration console allows the configuration of default settings and the creation of new trunks. The console access is divided into three nodes called

- HTTP connection
- HTTPS connection
- DirectAccess

The HTTP and HTTPS connection node is used to create new trunks (aka publishing rules in TMG) to publish services like Outlook Web App in Exchange Server 2010 or many other applications.
The DirectAccess node is used to create Microsoft Windows Server 2008 DirectAccess trunks.

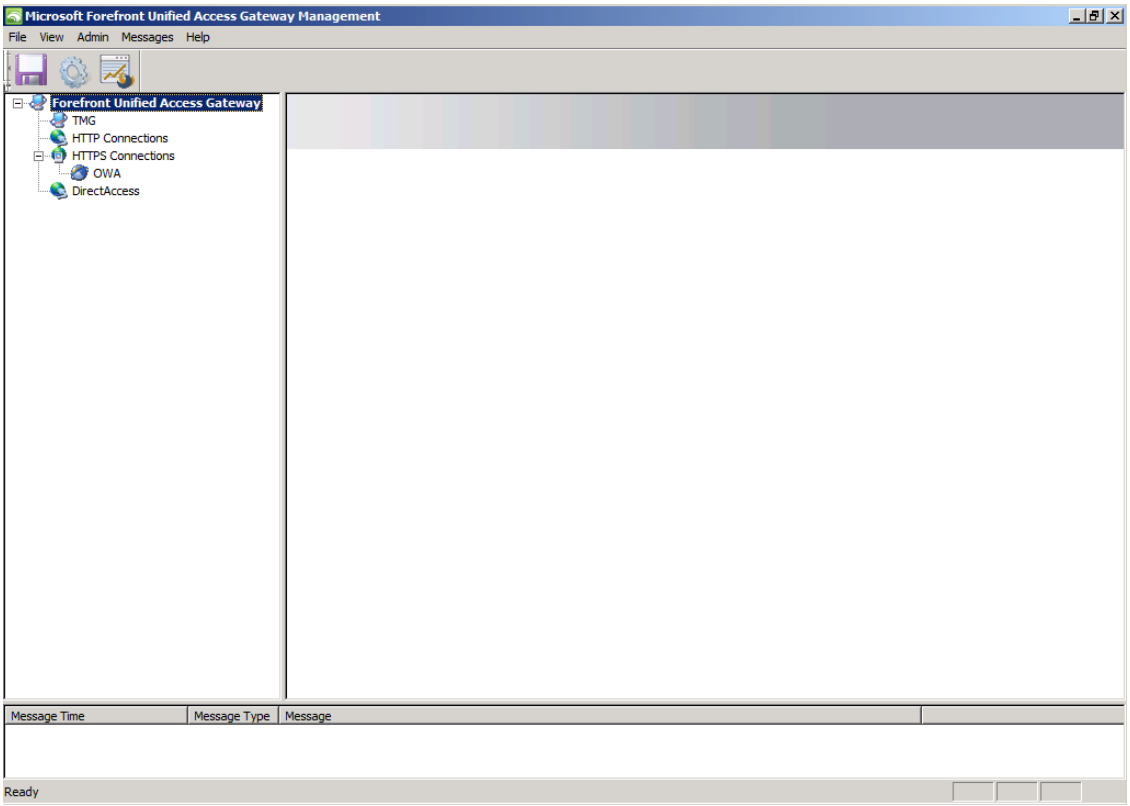

Figure 6: UAG GUI

To configure some default settings which can be used later for creating trunks, you can use the Admin settings. At this point it is possible to configure things like Authentication and Authorization Servers, Network Policy Servers (NPS), Load Balancing settings and many more. The settings you change here, or the objects created in this UI can be used when you create new trunks.

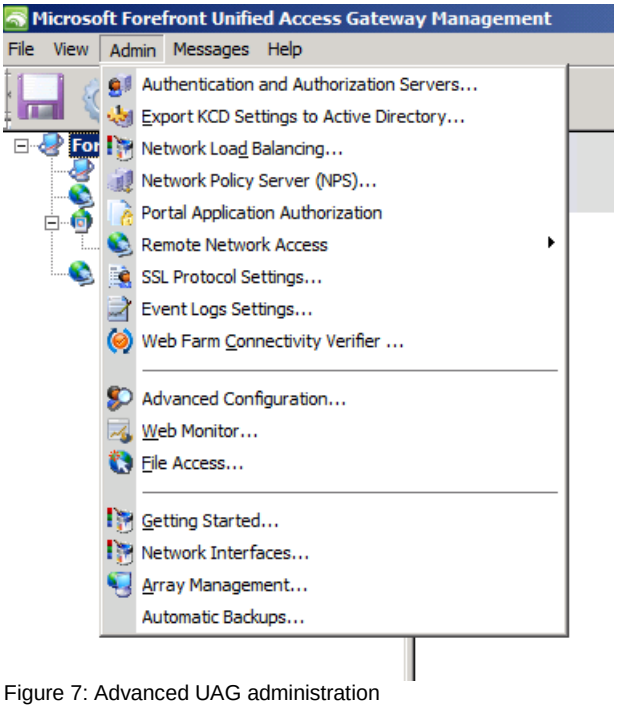

Figure 7: Advanced UAG administration

As you can see in the following screenshot, UAG supports many directory services like Netscape LDAP Server, Novell Directory services and a lot of more Directories.

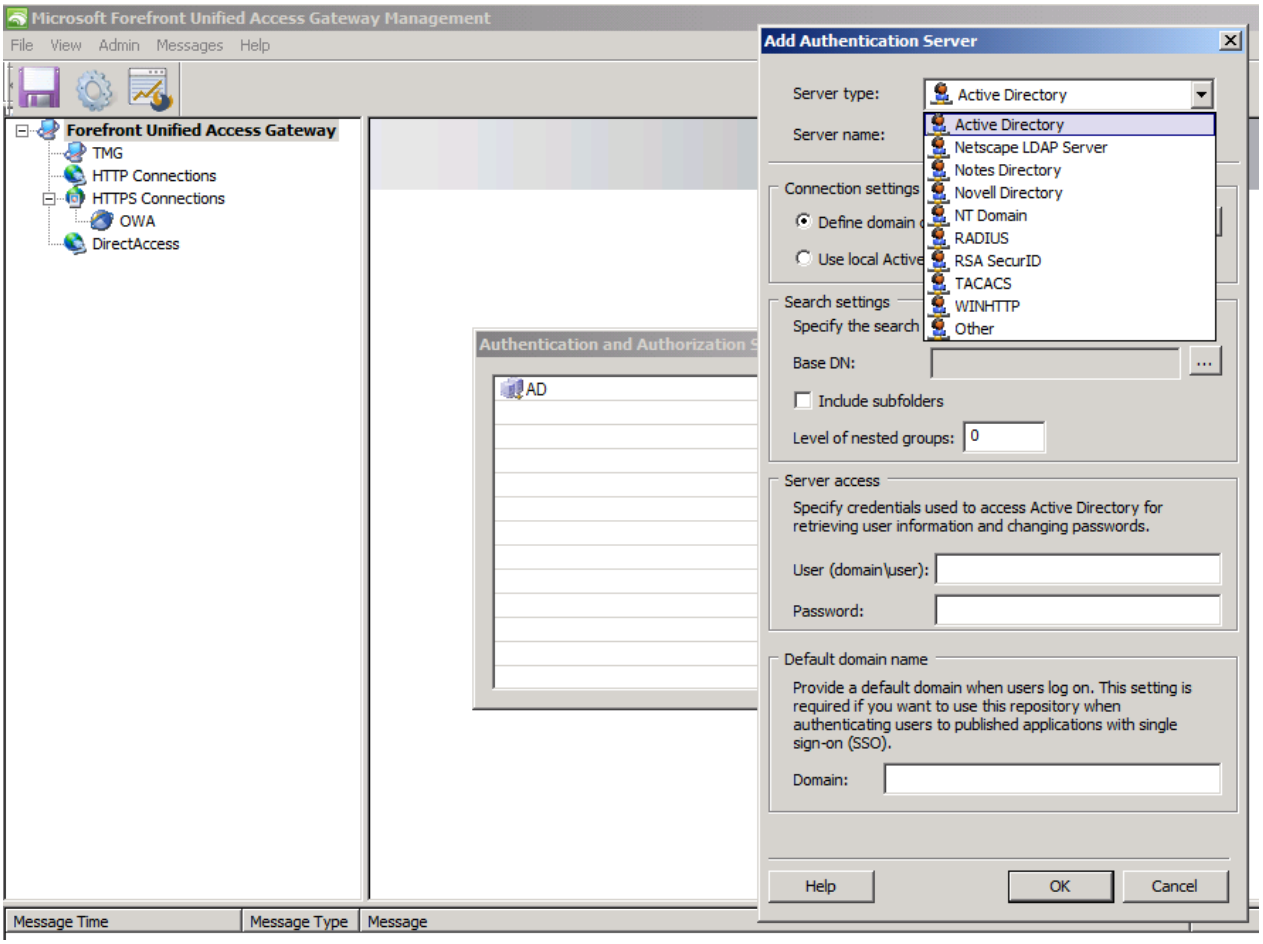

Figure 8: UAG authentication and authorization settings

Network Load Balancing settings

UAG provides its own Network Load Balancing configuration which is really easy to configure. Like the Integrated Network Load Balancing in Microsoft Forefront TMG, UAGs NLB sits on top of the NLB features of the underlying operating system.

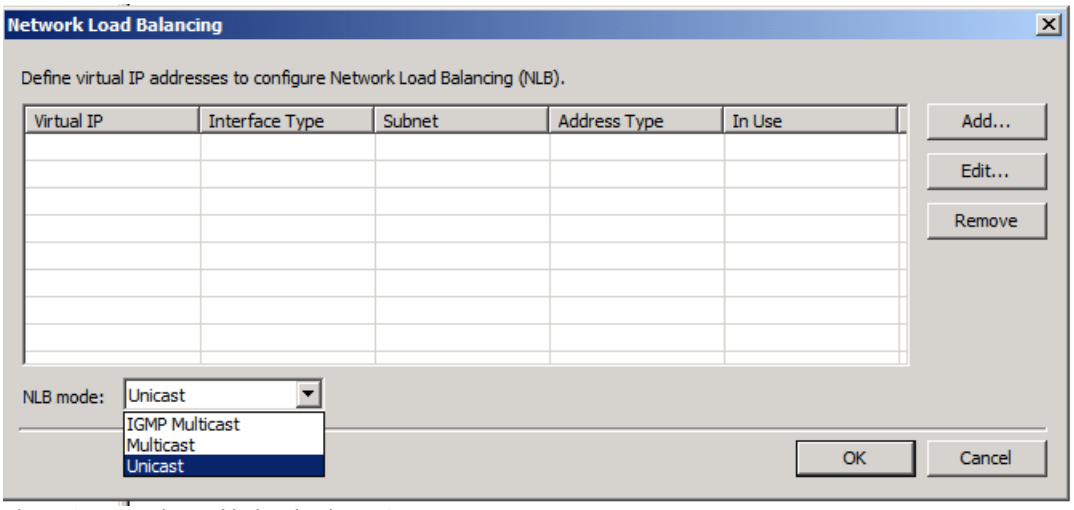

Figure 9: Network Load balancing in UAG

Portal publishing

For the examples in this article, I created a new Exchange Server 2010 Outlook Web App (known as OWA in previous versions of Exchange Server) portal. The wizard does a lot of work and eases the creation of a new portal so I will only show you the results of the Wizard, so let's have a look at the Portal settings, created with the wizard. The first page gives you an overview about the basic Portal settings like the Public host name, the IP address and used HTTPS port.

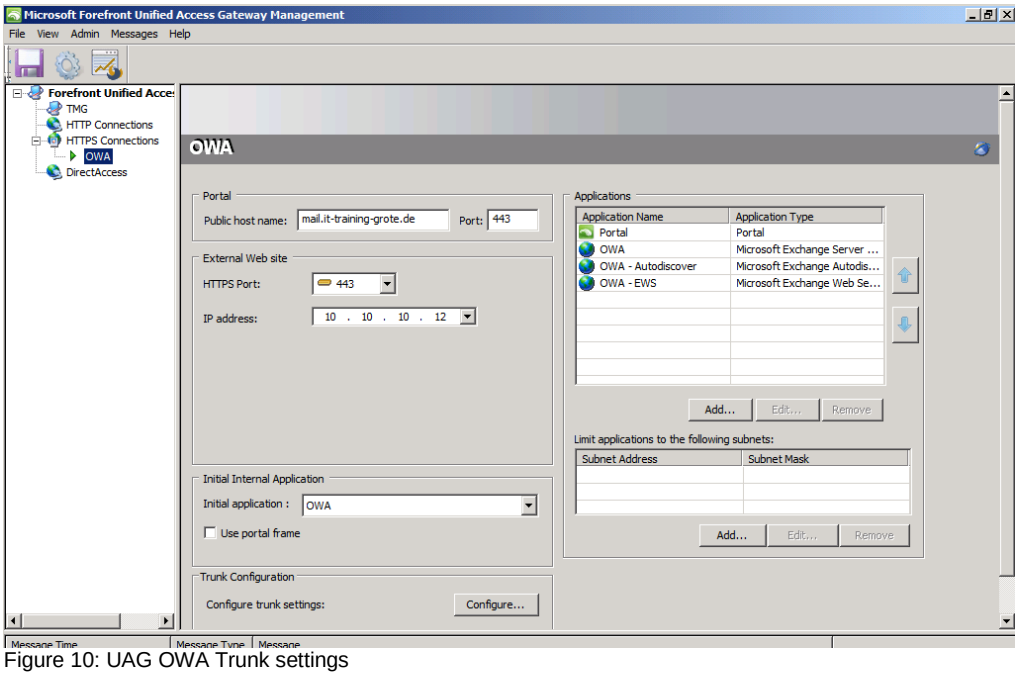

Figure 10: UAG OWA Trunk settings

If you click *Configure* in the Trunk configuration settings, you will see the power of Microsoft Forefront UAG. The trunk configuration settings allows you to configure so many settings more than Microsoft Forefront TMG, so that you have all the options to provide a more detailed configuration of nearly any setting regarding the configuration of Outlook Web App used in this scenario. For example it is possible to configure the maximum number of concurrent connections to the Outlook Web App Server. It is possible to configure detailed URL inspection and URL set configuration. In the *Application Customization* tab it is possible to customize the Portal experience for Endusers.

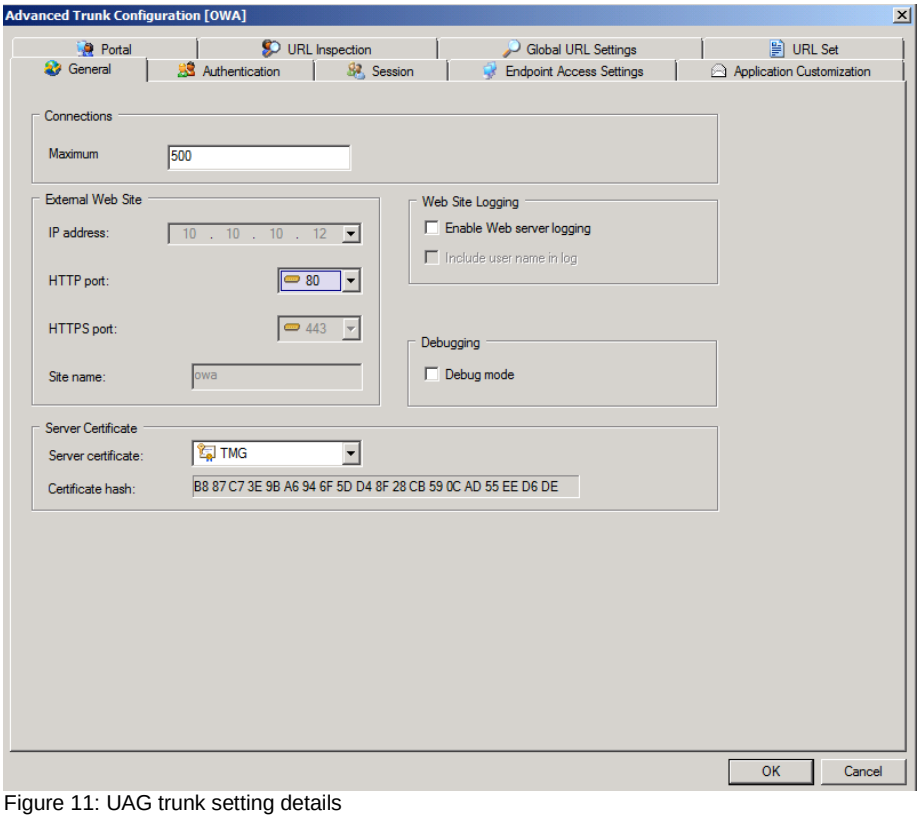

Figure 11: UAG trunk setting details

One of the most powerful feature in Forefront UAG in my opinion are the Endpoint Access settings which allows you to select specific policies from a long list of policies which allows more granular access to the portal for example for specific operating systems or specific application features. It is possible to create your own policies and expressions in Forefront UAG. UAG compares the policies against a client which wants to access the portal and gives the client access to the portal based on these policies.

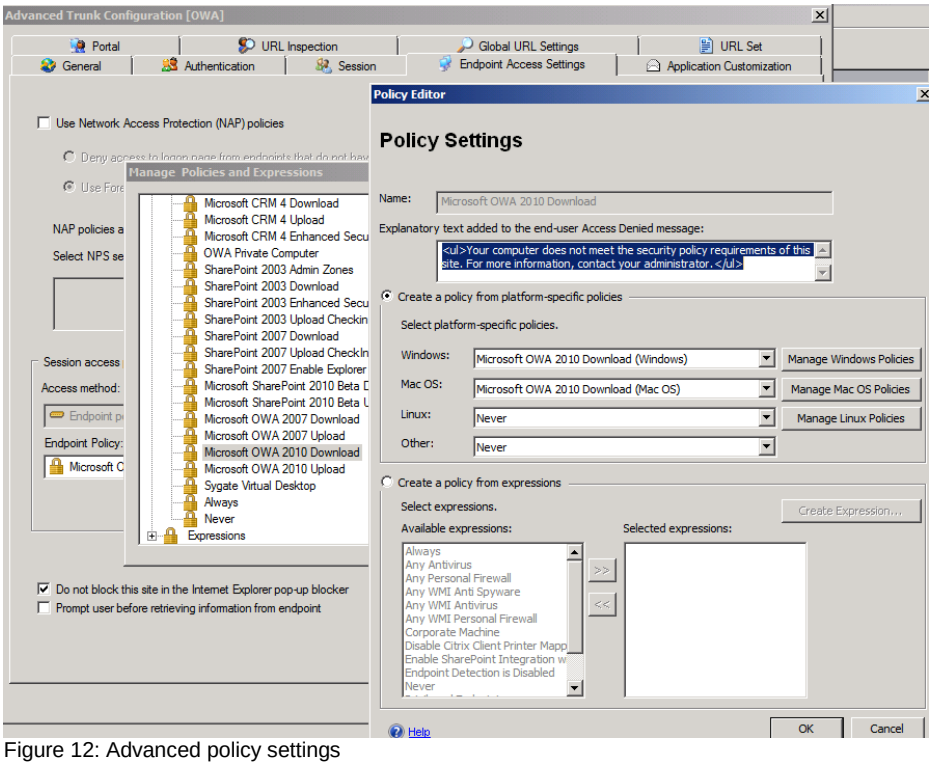

Figure 12: Advanced policy settings

After the creation of the new portal trunk is finished, the settings made by UAG are stored in the TMG configuration storage. You can see this storage configuration in the UAG Activation monitor. As you can see in the following screenshot, the configuration of the Portal trunk in UAG results in some new Firewall Policy rules in Microsoft Forefront TMG.

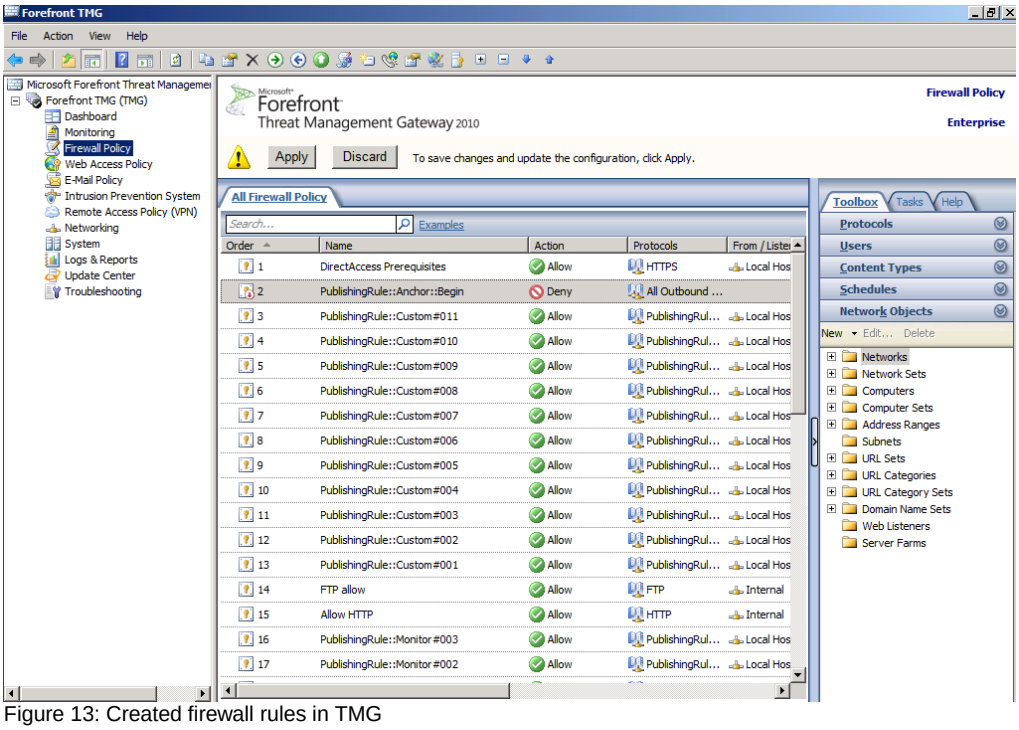

Figure 13: Created firewall rules in TMG

DirectAccess

As the last step in our short UAG overview article lets have a look at the DirectAccess capabilities of Forefront UAG. As some of you know, the DirectAccess configuration windows in UAG looks similar to the DirectAccess Management console in Windows Server 2008 R2 so it should be easy to configure DirectAccess in UAG for Administrators which are experienced configuring DirectAccess in Windows Server 2008 R2.

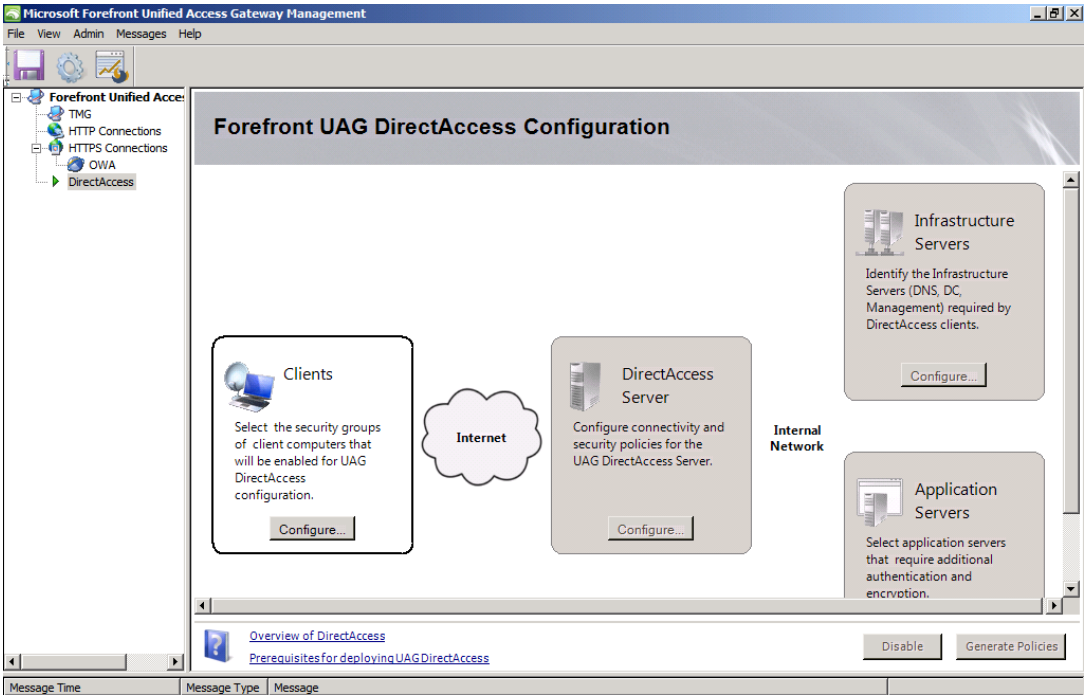

Figure 14: UAG Direct Access configuration dialog box

Conclusion

In this article, I gave you an overview about the installation and configuration process of the new Microsoft Forefront UAG product. As a basic example I highlighted the steps that are required to publish the Microsoft Exchange Server 2010 Outlook Web App feature (former known as Outlook Web Access (OWA)). Microsoft Forefront UAG has many new and enhanced features to securely publish Microsoft services and products from other vendors. This article can only provide an overview about the powerful UAG. If you are interested to learn more about Forefront UAG let me know, it could be possible to write more articles about UAG in the future on www.isaserver.org.

Related links

Microsoft Forefront UAG overview
http://www.microsoft.com/forefront/edgesecurity/iag/en/us/UAG-Beta.aspx
Microsoft Forefront UAG supported configurations with TMG
http://technet.microsoft.com/en-us/library/ee522953.aspx#BKMK_SupportedConfig
Microsoft Forefront UAG – FAQ
http://www.microsoft.com/forefront/prodinfo/roadmap/uag-faq.mspx
Microsoft Forefront UAG RC download on Connect
https://connect.microsoft.com/
Forefront Unified Access Gateway Beta System Requirements
http://www.microsoft.com/forefront/edgesecurity/iag/en/us/UAG-system-requirements.aspx