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

Microsoft Forefront TMG – How to configure Forefront TMG as a DirectAccess Server

Abstract

In this article I will show you how to configure Forefront TMG as a DirectAccess Server.

Let's begin

First, this article will only show the required steps to prepare Forefront TMG as a DirectAccess Server. The DirectAccess configuration is out of scope in this article and will be covered in several other articles in the Internet. You will find some helpful links at the end of this article.

As a first important step you have to understand is that Forefront TMG doesn't accept any IPv6 traffic or allow it to pass through it, so we must first modify this behavior BEFORE Forefront TMG gets installed to allow the following traffic:

- Inbound authenticated IPv6 traffic (using IPSec). This also includes the IPSec initiation traffic.
- Inbound and outbound IPv6 transition technologies (6to4, Teredo, IP-HTTPS and ISATAP).
- Native IPv6 from the Forefront TMG machine.

In addition, Forefront TMG integrates with the IPSec Denial of Service Protection (DoSP) component of Windows DirectAccess to ensure that only IPSec traffic is allowed through it.

Important:

For this reason, it is really important to install and configure Windows Server 2008 R2 DirectAccess before installing Forefront TMG.

First, we have to install the Windows Server 2008 R2 DirectAccess Management console as shown in the following screenshot.

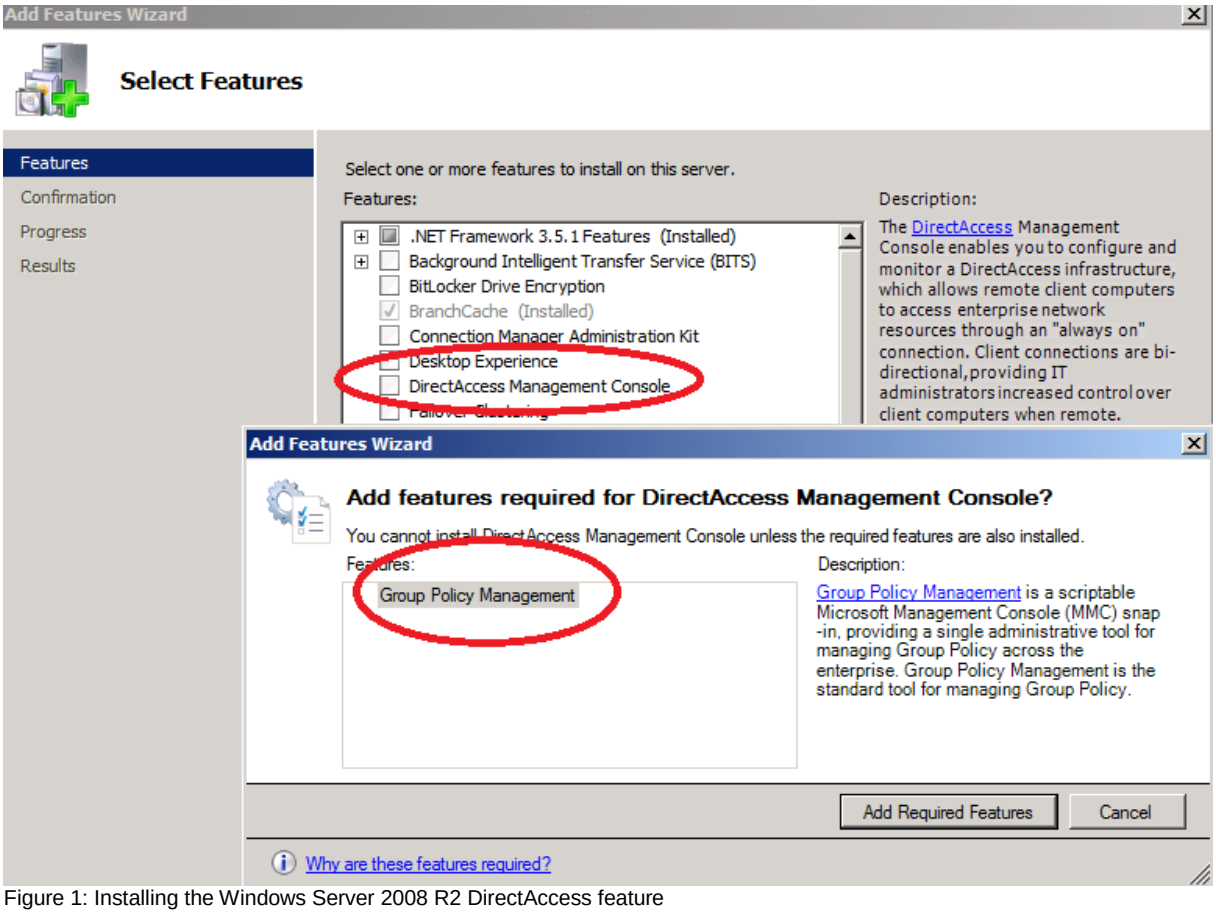

Figure 1: Installing the Windows Server 2008 R2 DirectAccess feature

After the Windows Server 2008 R2 DirectAccess Management console has been installed, start the console and configure DirectAcces and test the entire functionality before you install Forefront TMG.

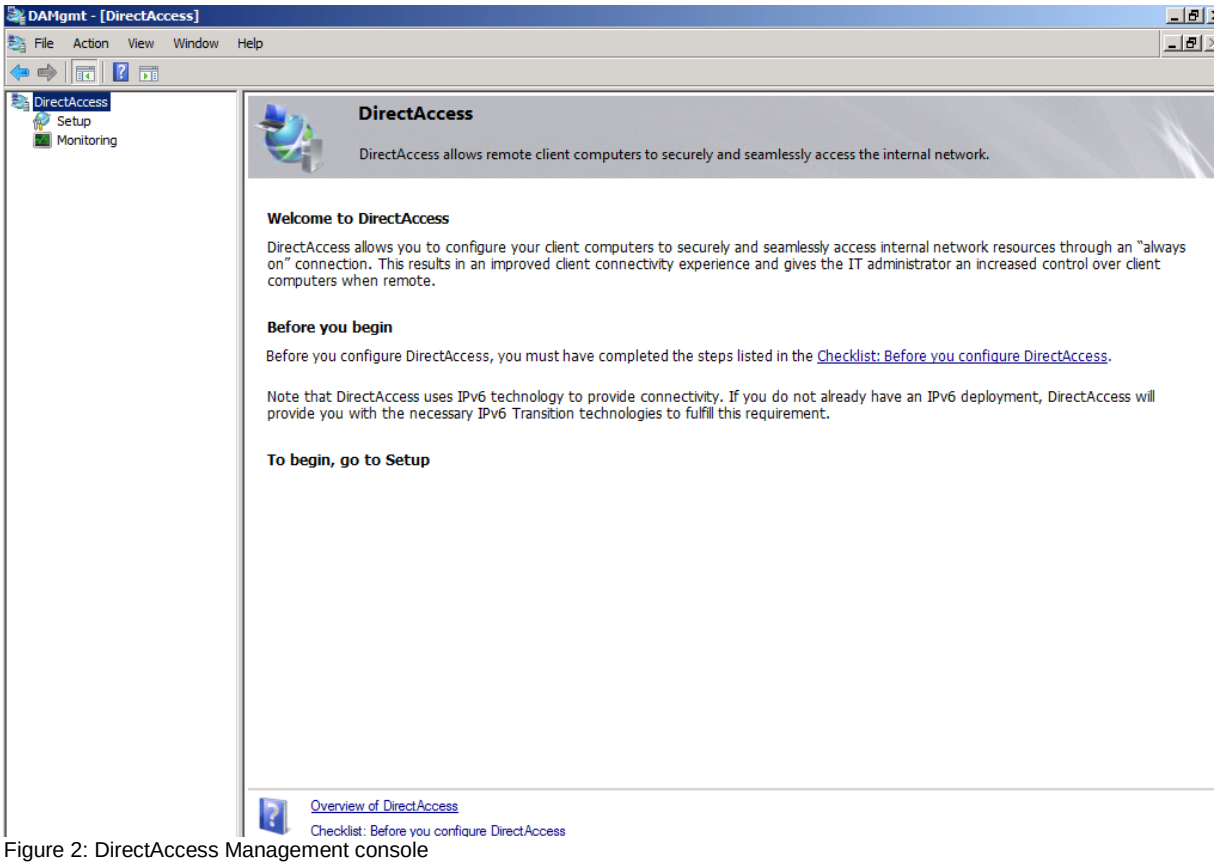

Figure 2: DirectAccess Management console

After you verified the successful DirectAccess installation and configuration, we have to modify the Registry with a new Registry key before installing Forefront TMG. This Registry key prevents Forefront TMG to disable the Ipv6 protocol support during the Forefront TMG installation.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RAT\Stingray\Debug\ISACTRL]
"CTRL_SKIP_DISABLE_IPV6_PROTOCOLS"=dword:00000001

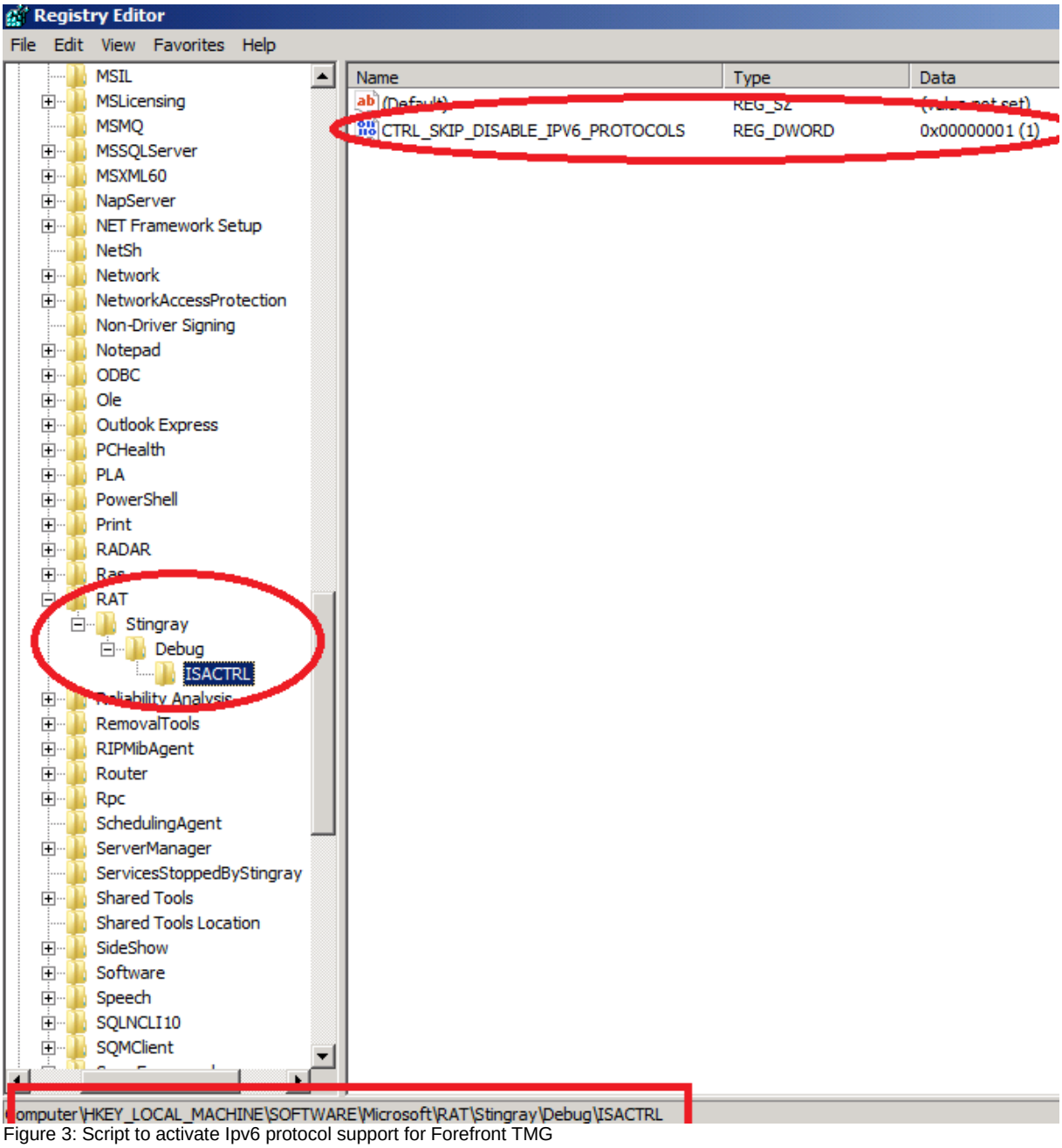

Figure 3: Script to activate Ipv6 protocol support for Forefront TMG

After the Registry has been modified successful install Forefront TMG in the way you install every Forefront TMG Server. After Forefront TMG has been installed, we have to modify the Forefront TMG configuration storage with a script which enables Ipv6 support for Forefront TMG. Copy the following lines into an empty Notepad file and save it with the .VBS extension.

```
set o = createobject("fpc.root")
set arr = o.Arrays.Item(1)
set policy = arr.ArrayPolicy
set IPV6Settings = policy.IPv6Settings
IPV6Settings.DirectAccessEnabled = vbTrue
arr.save
```

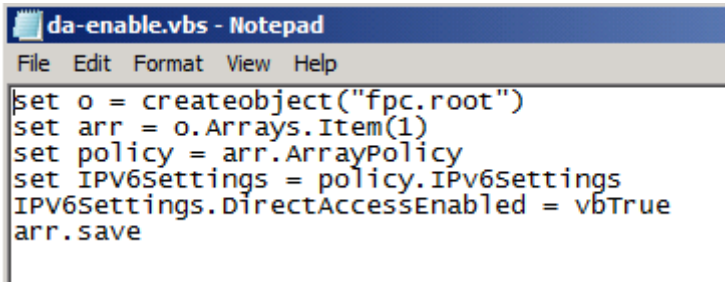

Figure 4: Save the script with the .VBS extension

Save the script with the .VBS extension and run it from an elevated command line with the following command:

Cscript DA-Enable.VBS

Due to the Forefront TMG configuration change it takes some time until the configuration has been successfully synchronized. You can see the configuration state in the Forefront TMG Management console as shown in the following screenshot.

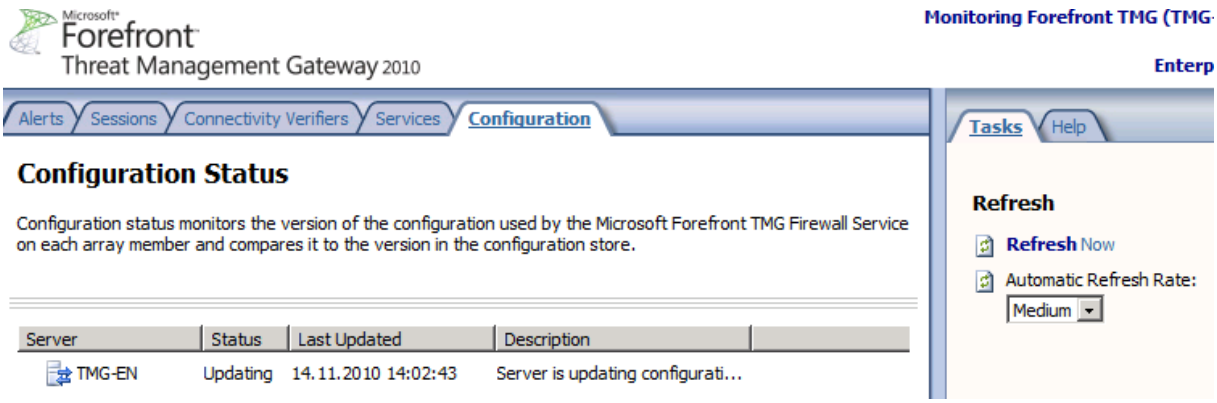

Figure 5: Wait for Forefront TMG Storage synchronization

The script creates four new System Policy rules to allow Ipv6 traffic for DirectAccess.

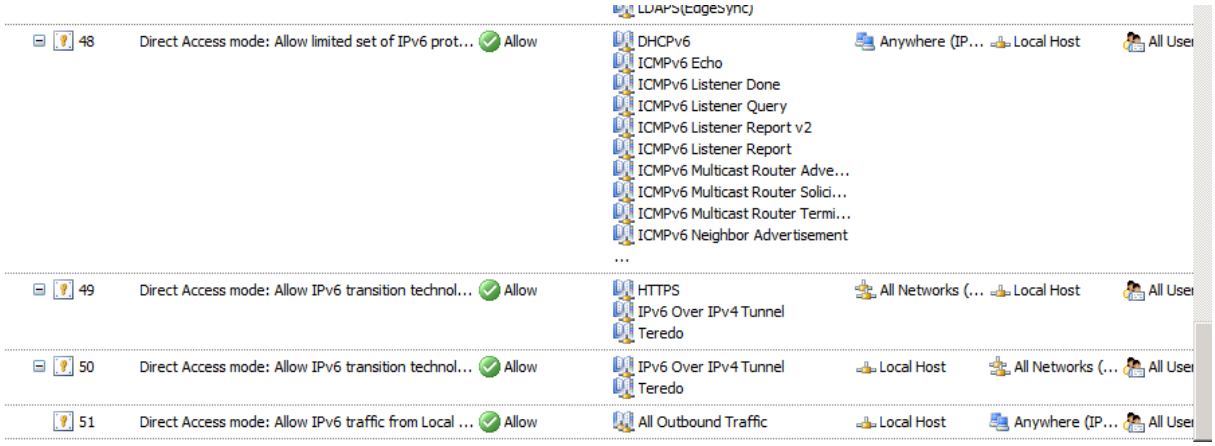

Figure 6: Some new Forefront TMG System Policies

Where is the “Act as a Direct Access server” button in Forefront TMG?

Forefront TMG Beta and RC had an Ipv6 tab in the IP preferences section in the Forefront TMG console to configure Forefront TMG as a DirectAccess Server as shown in the following screenshot.

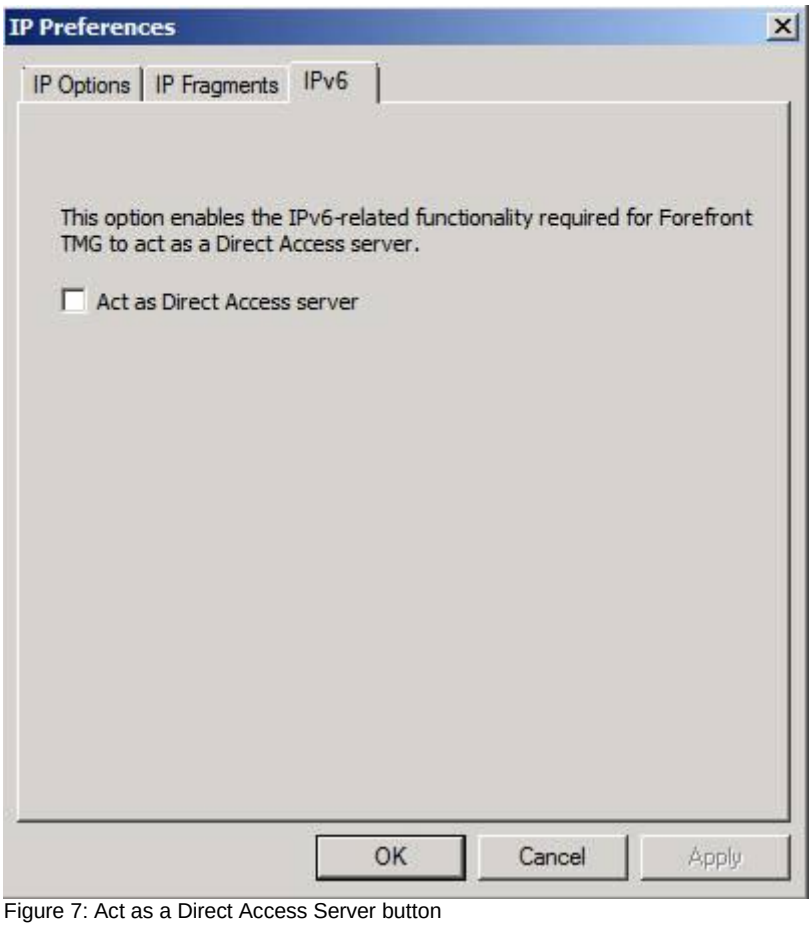

Figure 7: Act as a Direct Access Server button

After Forefront TMG has been RTM, I’ve never seen this Ipv6 tab again, so my assumption is, that it was removed from the Forefront TMG Management console, and DirectAccess works without this DirectAccess button ☺

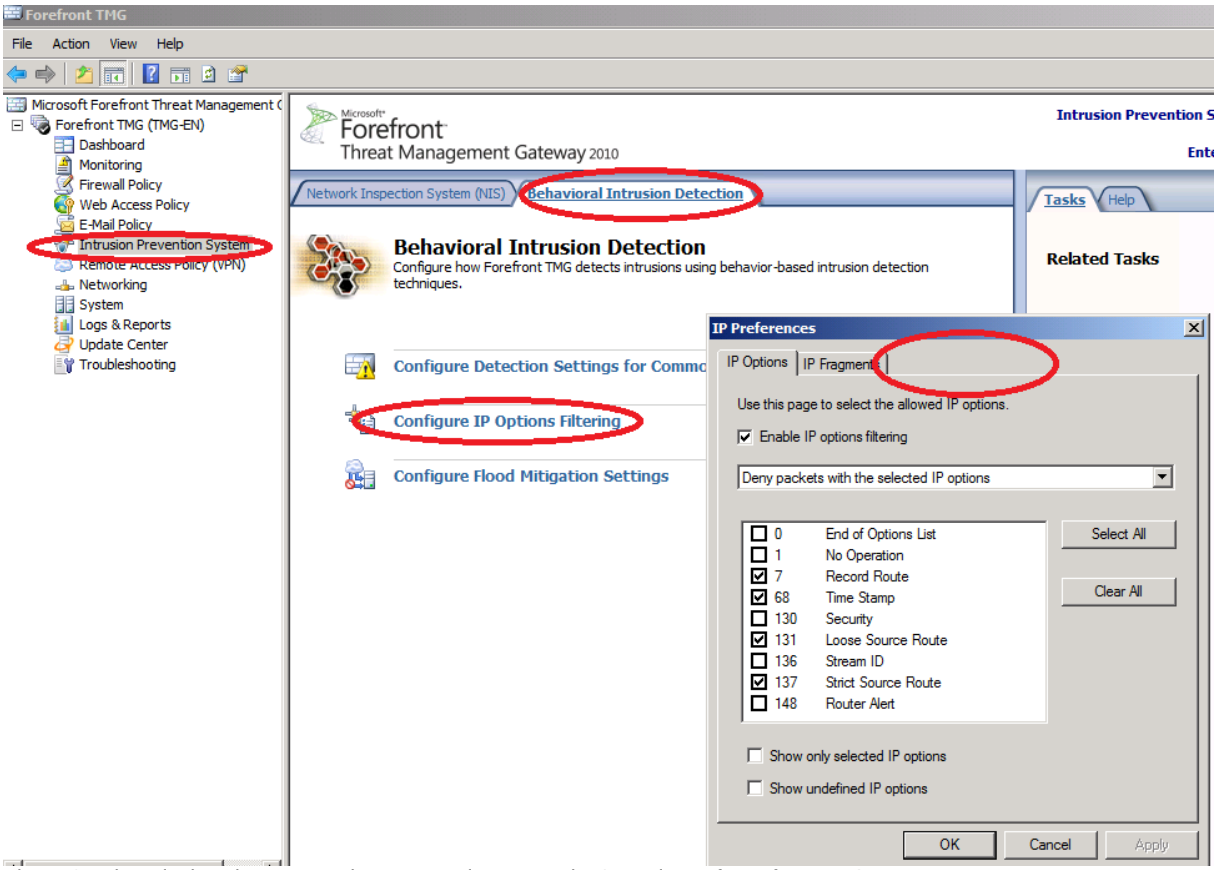

Figure 8: Where is the DirectAccess button seen in Beta and RC versions of Forefront TMG

Hide IPv6 Log entries

Forefront TMG has the option to Hide IPv6 traffic from the Real-time monitoring tab. Because Forefront TMG has no full support for IPv6 it might be an option for you as a Forefront TMG administrator to hide the entries to have a clearer view in the TMG logging.

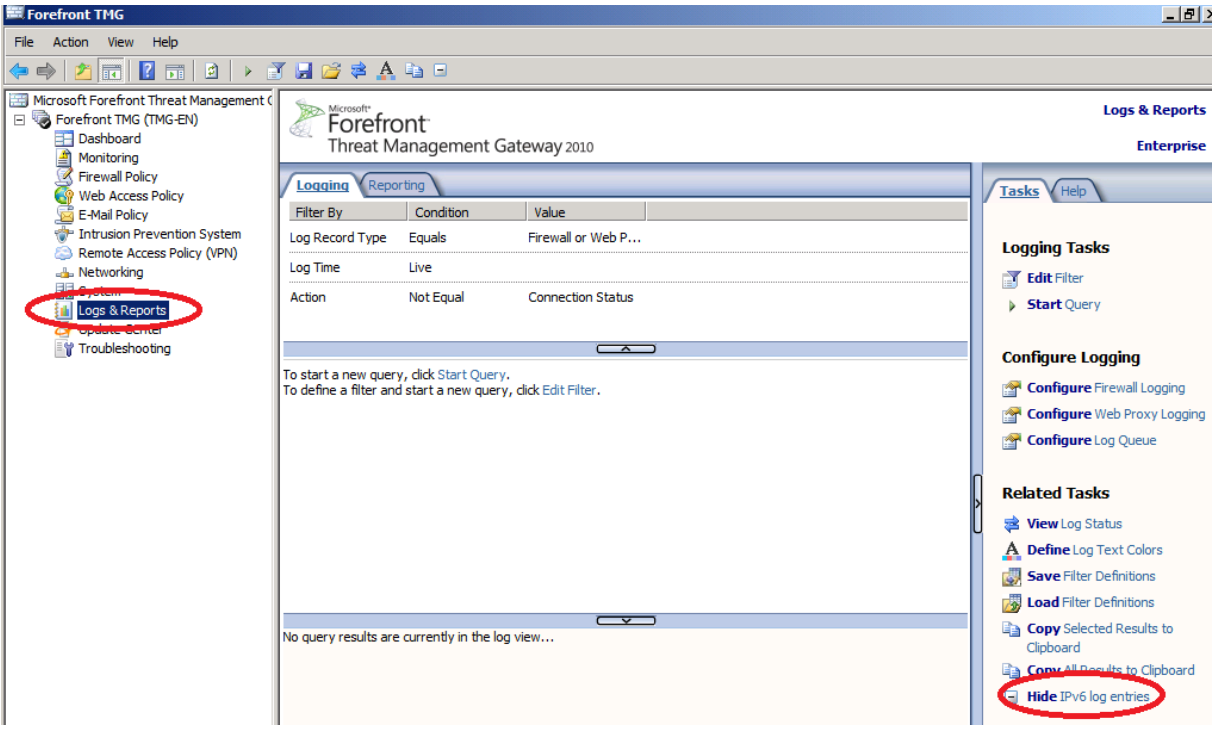

Figure 9: Hide Ipv6 log entries

If you want to have more functionality and flexibility you can use Forefront UAG for your DirectAccess scenario. Using Forefront UAG has the following advantages:

- Scalability (up to 8 Forefront UAG Server joined into an Array)
- High availability (with Windows Server 2008 R2 NLB)
- Access to corporate legacy servers over IPv4
- Easier configuration, deployment, and management
- Forefront UAG installs Forefront TMG on each node during Setup
- Alternative remote access solution for non-domain joined machines

Conclusion

In this article I gave you some information about how to configure Forefront TMG as a DirectAccess Server. In my opinion using Forefront TMG as a DirectAccess Server is good choice when you don't want to have High Availability and you don't need the advanced feature of Forefront UAG like Portal access and advanced Endpoint Security Policies.

Related links

Configure Forefront TMG as a DirectAccess Server
http://blogs.technet.com/b/isablog/archive/2009/09/23/forefront-tmg-and-windows-7-directaccess.aspx
Forefront TMG and Ipv6:
http://technet.microsoft.com/en-us/library/cc487898.aspx
Windows Server 2008 R2 DirectAccess Overview
http://www.microsoft.com/downloads/en/details.aspx?familyid=d8eb248b-8bf7-4798-a1d1-04d37f2e013c&displaylang=en