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 use TMG network templates

Abstract

In this article I will show you how to use Microsoft Forefront TMG network templates, how to create additional networks and how to customize Forefront TMG network settings.

Let's begin

Forefront TMG uses the concept of multi networking. To define your network topology it is possible to create networks in Forefront TMG. After all necessary networks have been created; these networks must be brought in relationship between networks in form of network rules. Forefront TMG supports two types of network rules:

Route

A network rule from type *Route* establish a bidirectional network connection between two networks which routes the original IP addresses between these networks.

NAT

A network rule from type *NAT* (Network Address Translation) establishes a unidirectional network connection between two networks which masks IP addresses from the network segment with the IP address of the corresponding Forefront TMG network adapter.

After Networks and Network rules has been created, you must create Firewall rules to allow or deny network traffic between the connected networks.

Network templates

To ease the configuration of Forefront TMG, TMG provides network templates which allow the creation of typical Firewall scenarios. It is possible to change the network design after the initial installation. All you have to do is to launch the Getting Started Wizard in the TMG Management console. The following screenshot shows the Launch Getting Started Wizard location.

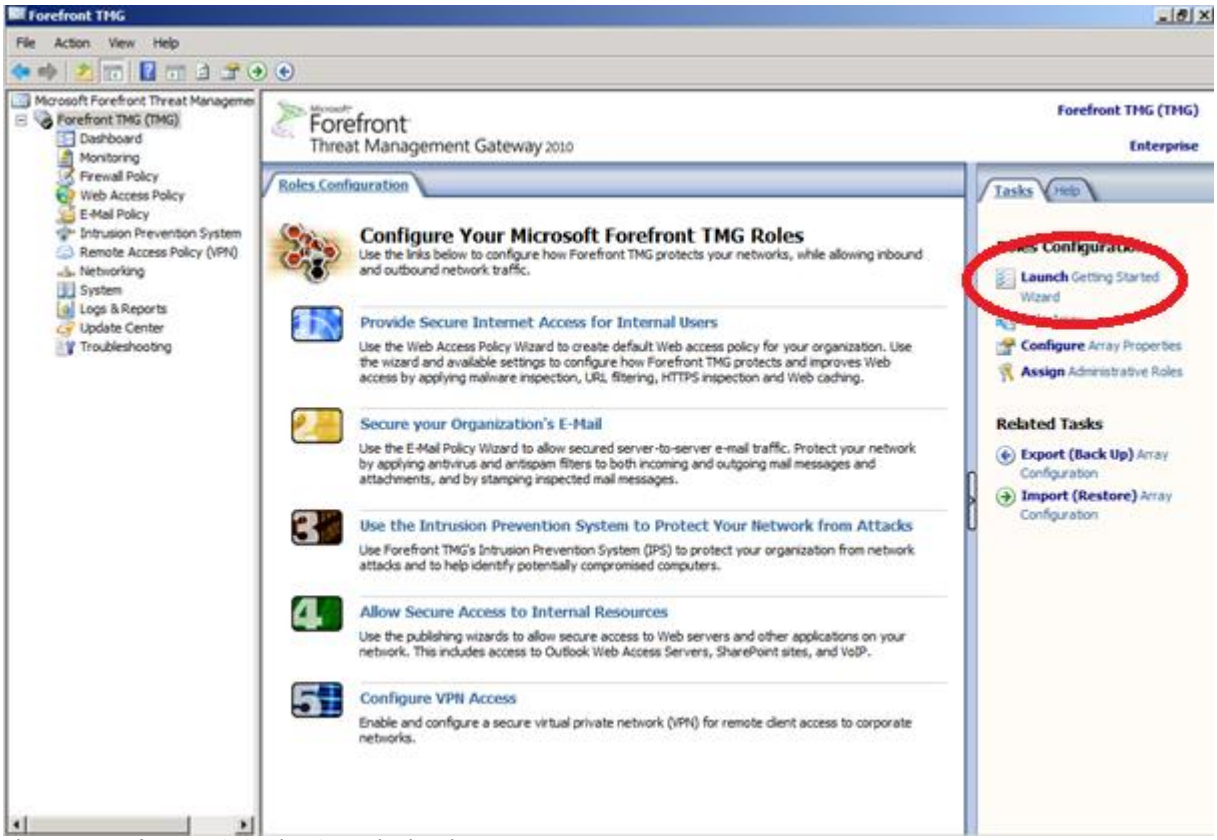

Figure 1: Forefront TMG Getting Started Wizard

Configure Network settings

The Launch Getting Started Wizard allows you to select the required network template. Forefront TMG comes with 4 network templates:

- Edge Firewall
- 3-Leg perimeter
- Back firewall
- Single network Adapter

Edge Firewall

The Edge Firewall template is the classic network template and connects the internal network to the Internet, protected by Forefront TMG. A typical Edge Firewall template requires a minimum of two network Adapters on the Forefront TMG Server.

3-Leg Perimeter

The 3-Leg Perimeter Firewall is a Forefront TMG Server with three or more network adapters. One network adapter connects the internal network, one network adapter connects to the external network, and one network adapter connects to the DMZ (Demilitarized Zone), also called Perimeter Network. The Perimeter network contains services, which should be accessible from the Internet but also been protected by Forefront TMG. Typical services in a DMZ are Web Servers, DNS Servers or WLAN networks. A 3-Leg Perimeter Firewall is also

often called the “Poor Man’s Firewall”, because it is not a “true” DMZ. A true DMZ is the zone between two recommended different Firewall brands.

Back firewall

The Back Firewall template can be used by Forefront TMG Administrator, when forefront TMG is placed behind a Front Firewall. The Back firewall protects the internal network from access from the DMZ and the external network and it controls the network traffic which is allowed from DMZ hosts and from the Front Firewall.

Please note: Forefront TMG has no built in Front Firewall network template

Single Network Adapter

The Single Network Adapter template has some limitations, because a Forefront TMG server with only one network interface cannot be used as a real Firewall, so many services are not available. Only the following features are available:

- Forward Web Proxy requests that use HTTP, Secure HTTP (HTTPS), or File Transfer Protocol (FTP) for downloads
- Cache Web content for use by clients on the corporate network
- Web publishing to help protect published Web or FTP servers
- Microsoft Outlook Web Access, ActiveSync, and remote procedure call (RPC) over HTTP publishing (also called Outlook Anywhere in Exchange Server 2007 and above)

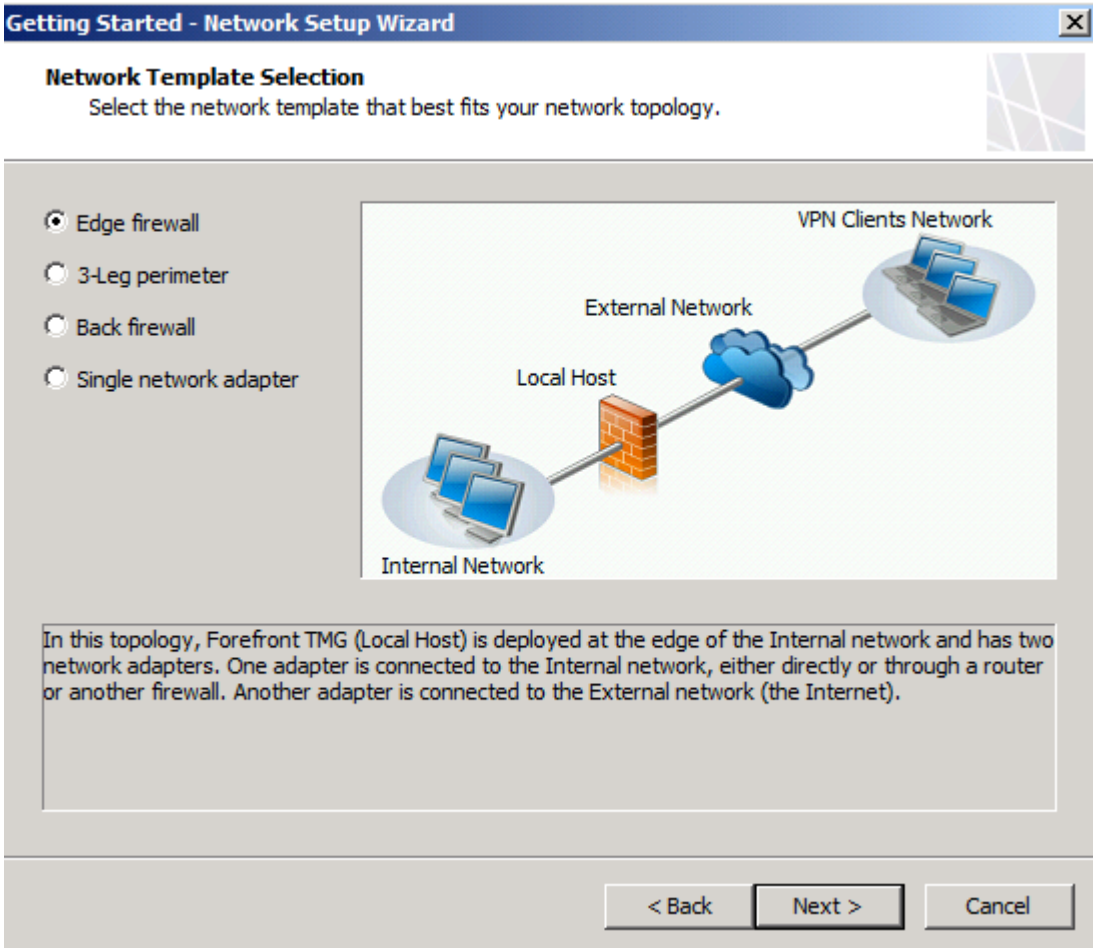

Figure 1: Network Template selection

As a next step select the network adapters which should be used for this network template. For this example I used the Edge Firewall template so you have to choose which network adapter connects to the LAN and which network adapter connects to the external (untrusted) network.

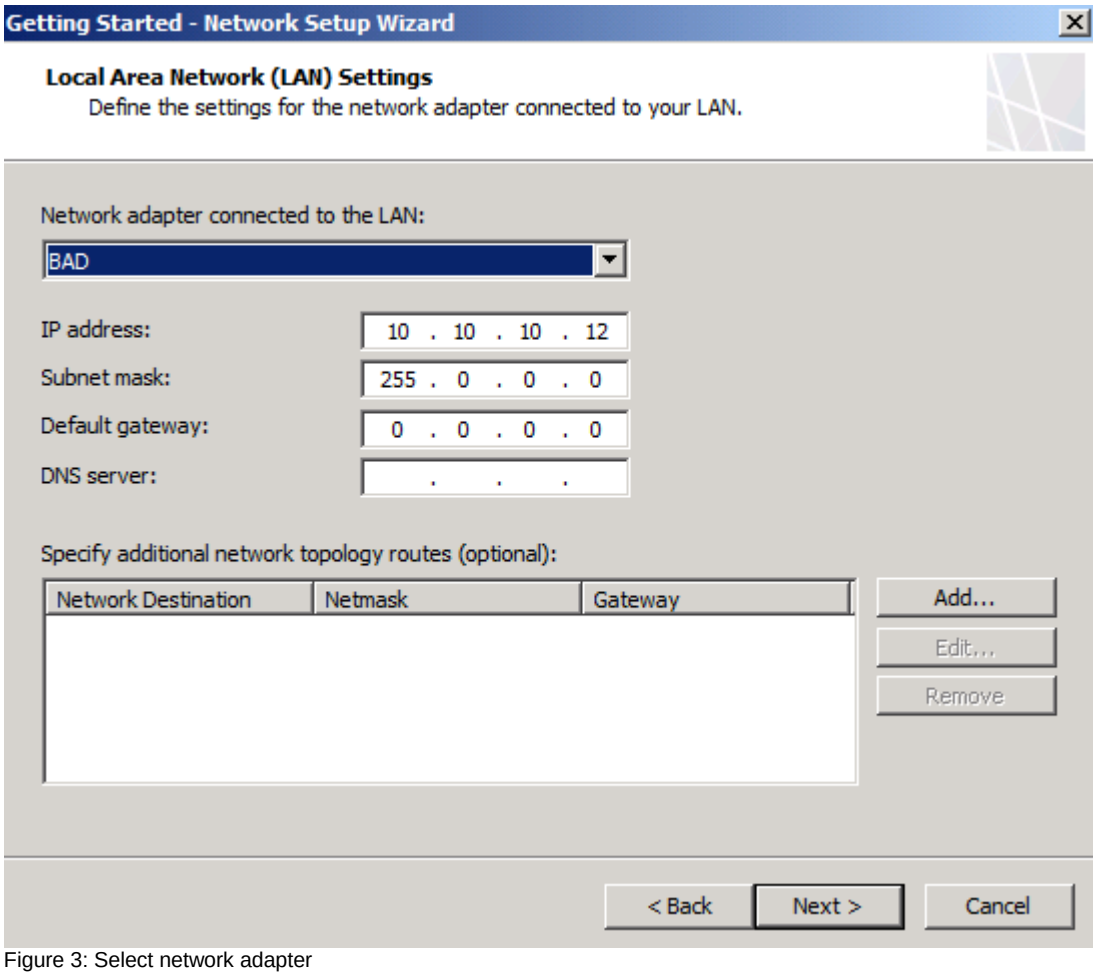

Figure 3: Select network adapter

In Forefront TMG it is now possible to specify additional network routes with the UI. You don't have to use the Route add command from the command line. The following screenshot shows the default networks created by the Microsoft Forefront TMG installation. Only the Internal network has the option to configure the IP address ranges.

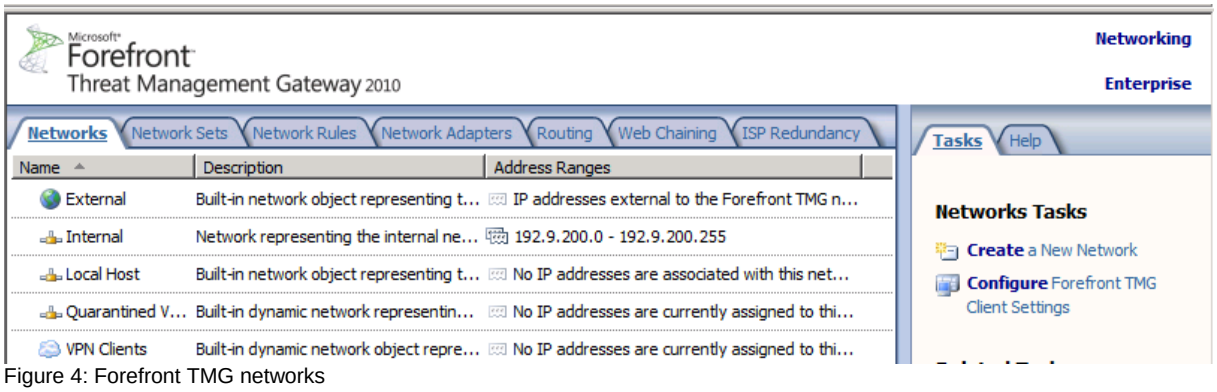

Figure 4: Forefront TMG networks

Forefront TMG comes with some built in network rules which defines the network relationship between the networks.

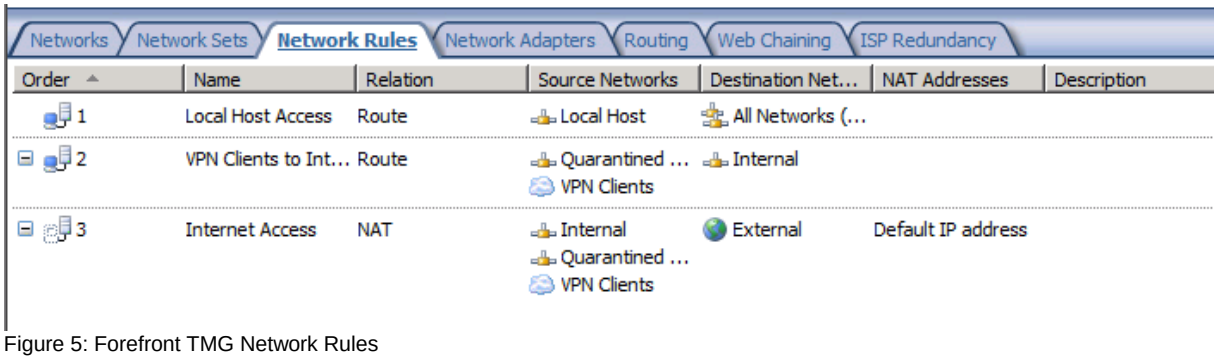

Figure 5: Forefront TMG Network Rules

Also new in Microsoft Forefront TMG is the built in capability to define some basic network adapter settings like IP addresses, Default Gateways and more.

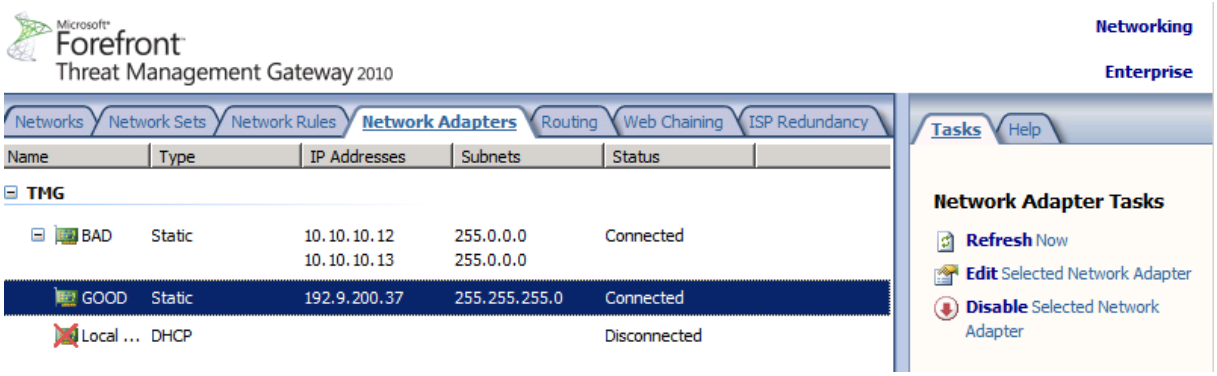

Figure 6: Forefront TMG Network Adapters

The following screenshot shows the configuration options for the TMG network adapters.

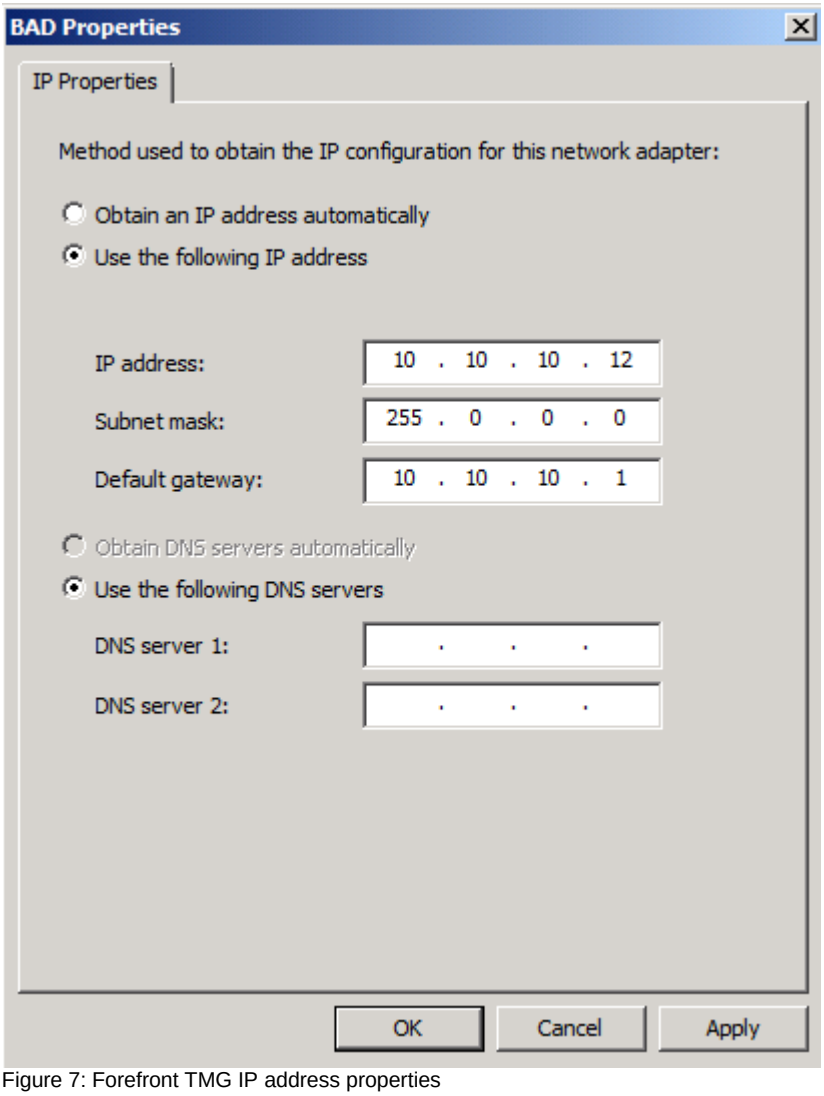

Figure 7: Forefront TMG IP address properties

With Forefront TMG it is now possible to create new network routes with the TMG Management console.

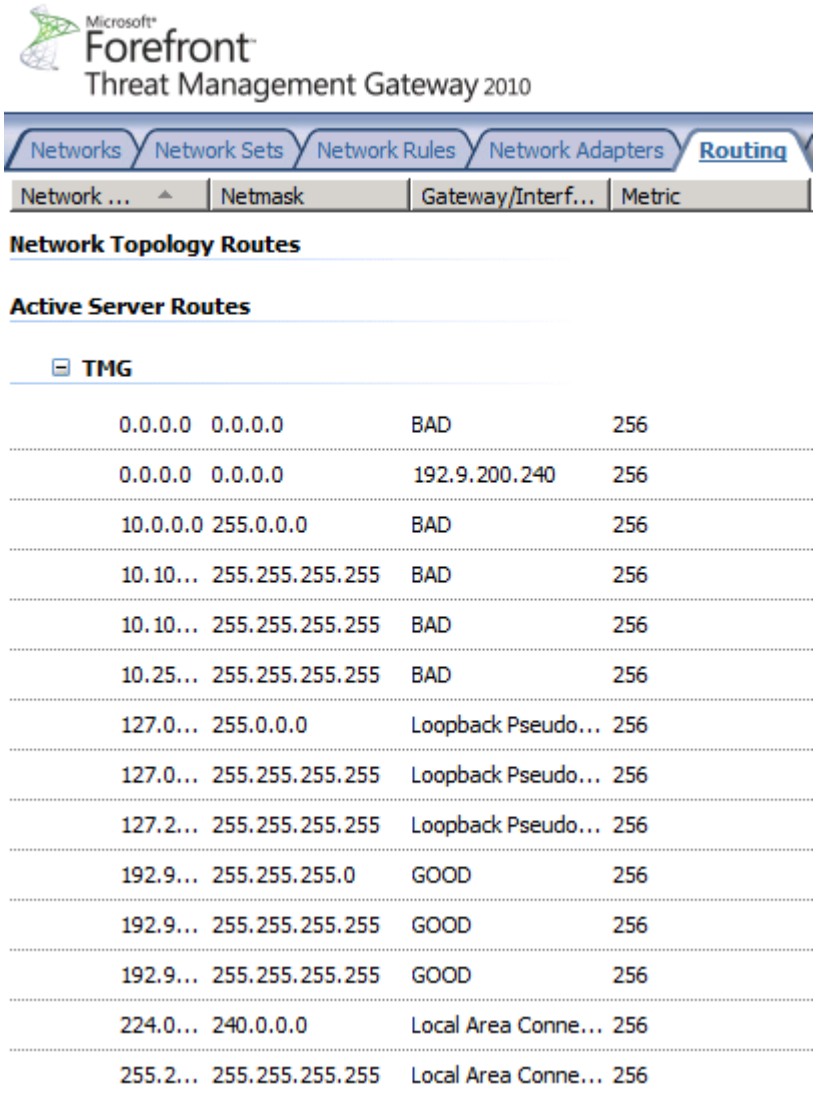

Figure 8: Forefront TMG Network routes

The following screenshot shows an example of the new Network Topology route creation dialog box.

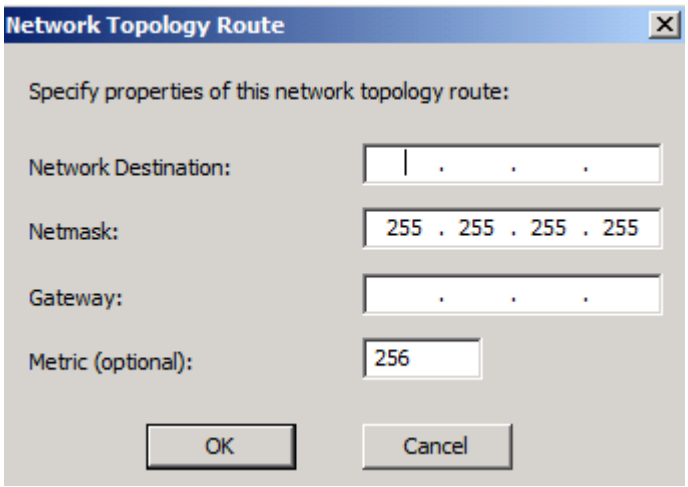

Figure 9: Forefront TMG – Create new Network Topology route

New networks in TMG

It is possible to create additional networks in Forefront TMG. Forefront TMG comes with a built in wizard to create new networks.

Figure 10: Forefront TMG – New network name

New networks can be created for different areas. For example it is possible to create a new network for an additional DMZ on Microsoft Forefront TMG

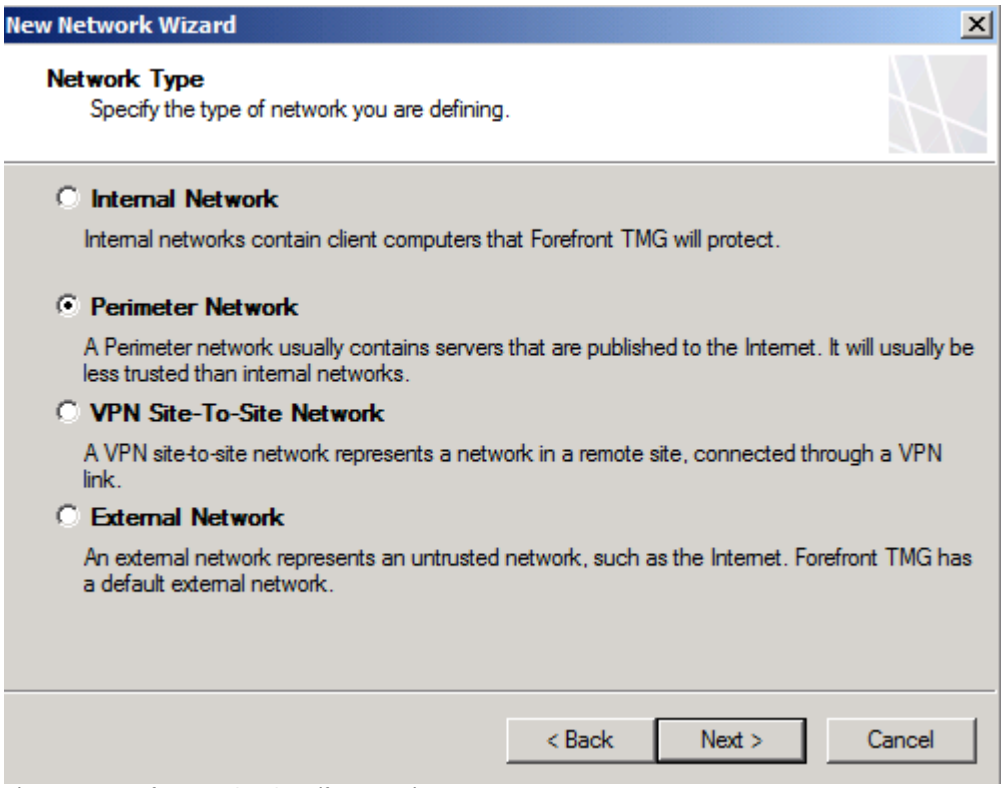

Figure 11: Forefront TMG – Specify Network type

Specify the IP address ranges for the new network.

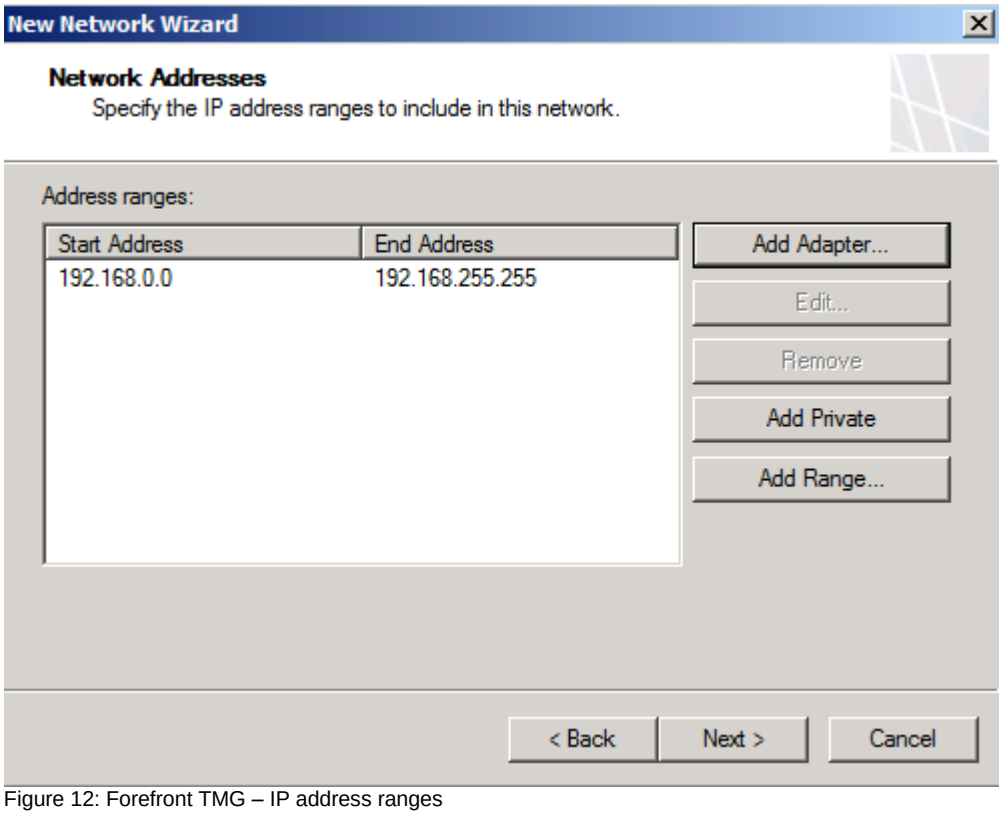

Figure 12: Forefront TMG – IP address ranges

After the new network has been created, you must associate the new network with an existing network rule or it is possible to create a new network rule relationship from type Route or NAT.

Exporting and importing network definitions

It is possible to export the Forefront TMG networks and network settings to an XML file with the built in import and export capabilities of Forefront TMG.

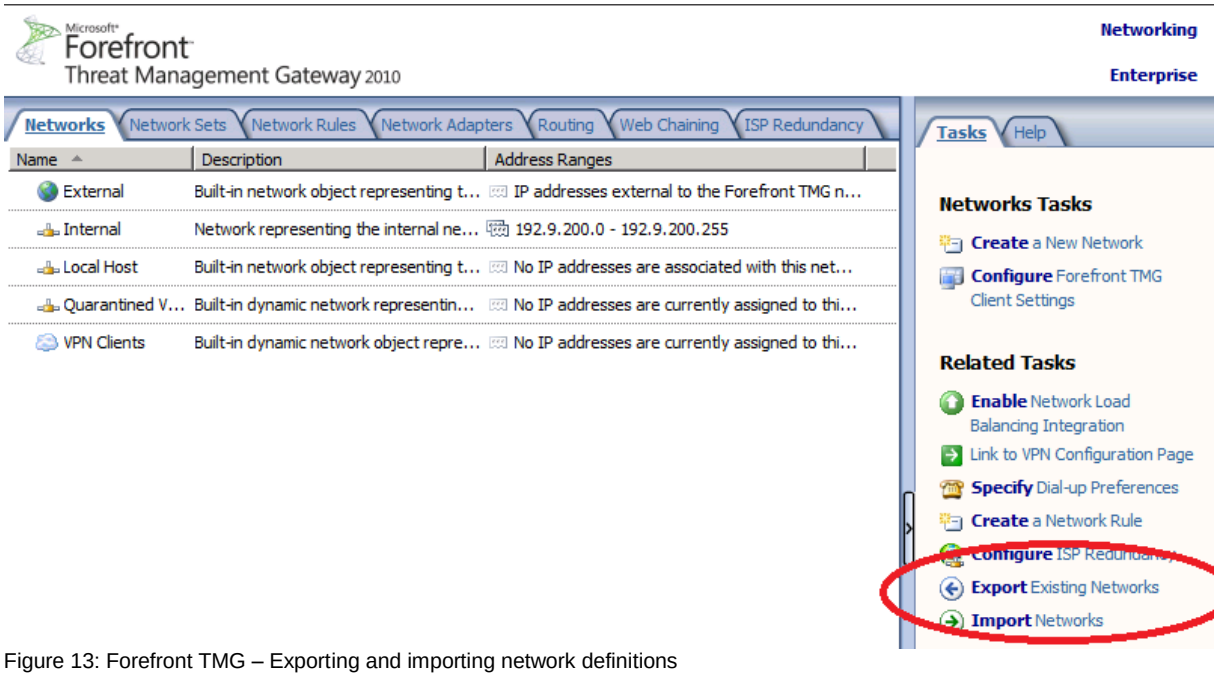

Figure 13: Forefront TMG – Exporting and importing network definitions

Conclusion

In this article, I tried to give you an overview about how to use networks, network templates and network rules in Forefront TMG to create your network topology with TMG. As you have seen in this article it is very easy to create your network topology with the help of network templates. Forefront TMG has some helpful enhancements related to the network configuration. It is a nice feature that it is now possible for TMG administrators to create network routes with the TMG Management console and that it is possible to configure some basic IP address settings with the TMG console. Most of the other settings remained unchanged compared to Microsoft ISA Server 2006.

Related links

How to use the ISA Server 2006 Network Templates
http://www.isaserver.org/tutorials/ISA-Server-2006-Network-Templates.html