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.

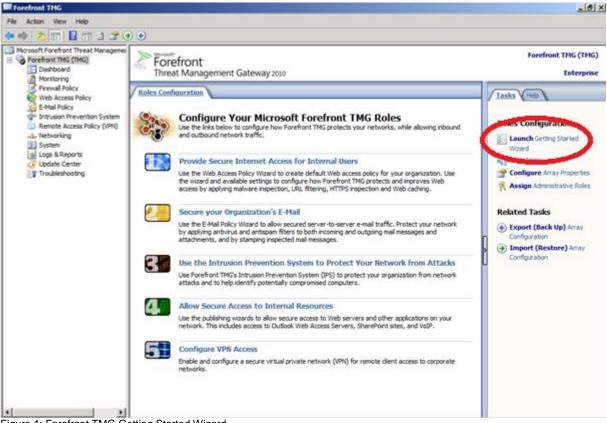


Figure 1: Forefront TMG Getting Started Wizard

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)

Getting Started - Network Setu	p Wizard	×
Network Template Selection Select the network template	that best fits your network topology.	\mathbb{R}
network adapters. One adapter i	VPN Clients Network External Network Local Host Internal Network	nd has two
		1
	< Back Next >	Cancel

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.

Getting Started - Network Setup Wizard		×
Local Area Network (LAN) Settings Define the settings for the network adapte	r connected to your LAN.	
Network adapter connected to the LAN:		
IP address: 10 . 10 Subnet mask: 255 . 0 Default gateway: 0 . 0 DNS server: .		
Specify additional network topology routes (opt Network Destination Netmask	ional): Gateway	Add
		Edit Remove
1	< Back Next >	Cancel

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.

Forefront Threat Man	t agement Gateway 201	10	Networking Enterprise
Networks Networ	k Sets Network Rules	Vetwork Adapters Routing Web Chaining ISP Redundancy	Tasks Help
🎯 External	Built-in network object rep	resenting t 🖾 IP addresses external to the Forefront TMG n	Networks Tasks
👍 Internal	Network representing the i	internal ne 🛞 192.9.200.0 - 192.9.200.255	Treate a New Network
👍 Local Host	Built-in network object rep	resenting t 📨 No IP addresses are associated with this net	Configure Forefront TMG
👍 Quarantined V	. Built-in dynamic network re	presentin 🖾 No IP addresses are currently assigned to thi	Client Settings
S VPN Clients		oject repre 🖾 No IP addresses are currently assigned to thi	

Figure 4: Forefront TMG networks

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

Networks	Network Sets	Rules Net	twork Adapters Routing	Web Chaining	ISP Redundancy	
Order 🔺	Name	Relation	Source Networks	Destination Net	NAT Addresses	Description
_] 1	Local Host Access	Route	👍 Local Host	🛓 All Networks (
2 🗐 📃 🖬	VPN Clients to Int	Route	👍 Quarantined line VPN Clients	👍 Internal		
⊟ ⊖ <mark>,</mark> 3	Internet Access	NAT	uternal use Quarantined S VPN Clients	🎯 External	Default IP address	

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.

Forefree Threat N	O nt 1anagement Ga	teway 2010			Networking Enterprise
Networks Netw	work Sets Network	Rules Network A	dapters Routing	Web Chaining VISP Redundancy	Tasks Help
Name	Туре	IP Addresses	Subnets	Status	
🗆 TMG					Network Adapter Tasks
🖃 过 BAD	Static	10.10.10.12 10.10.10.13	255.0.0.0 255.0.0.0	Connected	Refresh Now Edit Selected Network Adapter
🕎 GOOD	Static	192.9.200.37	255.255.255.0	Connected	Disable Selected Network
💢 Local	DHCP			Disconnected	Adapter

Figure 6: Forefront TMG Network Adapters

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

BAD Properties								×
IP Properties								
Method used to obtain the IP co	onfigura	atic	n fo	r th	is ne	etw	ork ad	apter:
Obtain an IP address autom	atically							
• Use the following IP address								
IP address:	10		10		10		12	
IP duuress;								
Subnet mask:	255	•	0	•	0	•	0	
Default gateway:	10		10		10		1	
C								
C Obtain DNS servers automa								
Use the following DNS serve	rs							
DNS server 1:		·		•		•		
DNS server 2:								
	,							
	OK		٦		Car	nce		Apply

Figure 7: Forefront TMG IP address properties

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



Networks	Netw	ork Sets	Network F	Rules	Network Ada	pters	Routing
Network		Netmas	k	Gate	way/Interf	Metric	

Network Topology Routes

Active Server Routes

🖃 TMG			
0.0.0.0	0.0.0.0	BAD	256
0.0.0.0	0.0.0.0	192.9.200.240	256
10.0.0.0	255.0.0.0	BAD	256
10.10	255.255.255.255	BAD	256
10.10	255.255.255.255	BAD	256
10.25	255.255.255.255	BAD	256
127.0	255.0.0.0	Loopback Pseudo	256
127.0	255.255.255.255	Loopback Pseudo	256
127.2	255.255.255.255	Loopback Pseudo	256
192.9	255.255.255.0	GOOD	256
192.9	255.255.255.255	GOOD	256
192.9	255.255.255.255	GOOD	256
224.0	240.0.0.0	Local Area Conne	256
255.2	255.255.255.255	Local Area Conne	256

Figure 8: Forefront TMG Network routes

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

Network Topology Route	×							
Specify properties of this network topology route:								
Network Destination:								
Netmask:	255 . 255 . 255 . 255							
Gateway:								
Metric (optional):	256							
OK	Cancel							

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.

New Network Wizard		×
	Welcome to the New Network Wizard	
	This wizard helps you create a new network. Networks specify one or more ranges of IP addresses as a network object that can be used in rules.	
	Network name:	
	To continue, click Next.	
	< Back Next > Canc	el

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

New Network Wizard	×
Network Type Specify the type of network you are defining.	\mathbb{R}^{+}
C Internal Network	
Internal networks contain client computers that Forefront TMG will protect.	
Perimeter Network	
A Perimeter network usually contains servers that are published to the Internet. less trusted than internal networks.	It will usually be
© VPN Site-To-Site Network	
A VPN site-to-site network represents a network in a remote site, connected thre link.	ough a VPN
C External Network	
An external network represents an untrusted network, such as the Internet. Fore a default external network.	efront TMG has
< Back Next >	Cancel

Figure 11: Forefront TMG – Specify Network type

Specify the IP address ranges for the new network.

Nev	w Network Wizard			3	×
	Network Addresses Specify the IP addre	ess ranges to include in this	network.	\mathcal{A}	
	Address ranges:				
	Start Address	End Address		Add Adapter	
	192.168.0.0	192.168.255.255		E dit	
				Remove	
				Add Private	
				Add Range	
	1				
			< Back	Next > Cancel	

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.

Networks Network Sets Network Rules Network Adapters Routing Web Chaining ISP Redundancy			Tasks Help
ame 🔺	Description	Address Ranges	
🎯 External	Built-in network object representing t	🖾 IP addresses external to the Forefront TMG n	Networks Tasks Create a New Network Configure Forefront TMG Client Settings
👍 Internal	Network representing the internal ne	〒 192.9.200.0 - 192.9.200.255	
🖦 Local Host	Built-in network object representing t	🖾 No IP addresses are associated with this net	
👍 Quarantined V	Built-in dynamic network representin	🖾 No IP addresses are currently assigned to thi	
log VPN Clients	Built-in dynamic network object repre	📖 No IP addresses are currently assigned to thi	Related Tasks
			 Enable Network Load Balancing Integration Link to VPN Configuration Page
			Specify Dial-up Preferences
			Create a Network Rule

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