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

What's new in Forefront TMG Beta 2 – Part 2

Abstract

In this two part article series, I will show you the new and extended features of Microsoft Forefront Threat Management Gateway Beta 2.

Let's begin

First, keep in mind that the information in this article are based on a beta version of Microsoft Forefront TMG and are subject to change.

In this second article, I will show you some of the new features and how they work. Both articles should only give you some basic information about new and changed features in Microsoft Forefront TMG, so we would not go into details in this both articles.

Microsoft has divided the new feature into six sections:

- Control network policy access at the edge (Firewall)
- Protect users from web browsing threats (Web Client Protection)
- Protect users from E-mail threats (Email Protection)
- Protect desktops and servers from intrusion attempts (NIS)
- Enable users to remotely access corporate resources (VPN, Secure Web Publishing)
- Simplified management (Deployment)

Intrusion Prevention System

Microsoft Forefront TMG uses Network Inspection System (NIS), which is a part of the Intrusion Prevention System in TMG. NIS uses signatures of known vulnerabilities from the Microsoft Response Center to help detect and block malicious traffic, so TMG is the first line of defense when new Zero Day exploits are available and the Administrator doesn't have the time to patch all systems before the exploit reaches the internal network. TMG checks the network traffic for known and new exploits and TMG Administrators can configure the action, when exploits are detected.

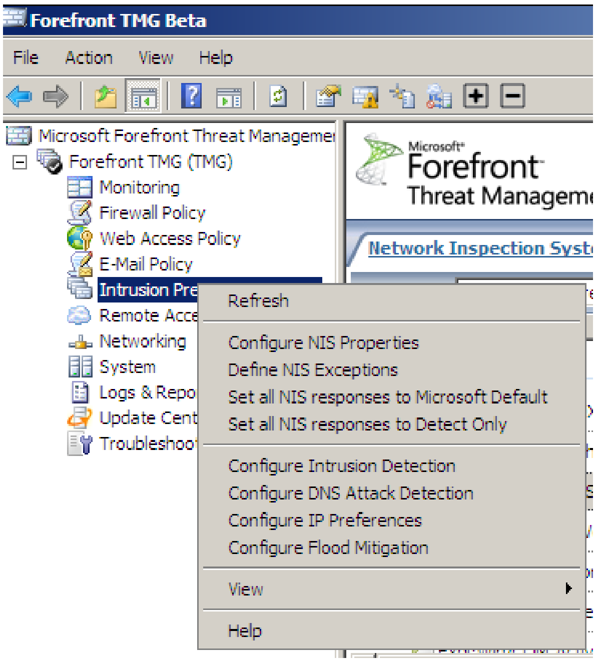
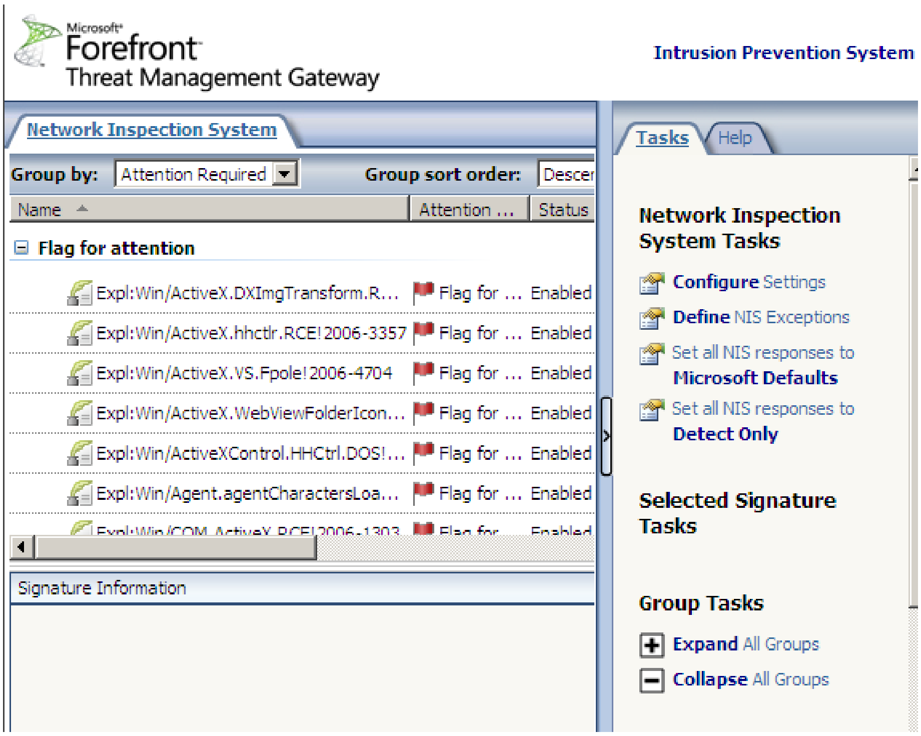


Figure 1: Network Inspection System settings

As a TMG Administrator, you can view and filter all NIS information in the TMG Management console and set the responses for all known exploits.

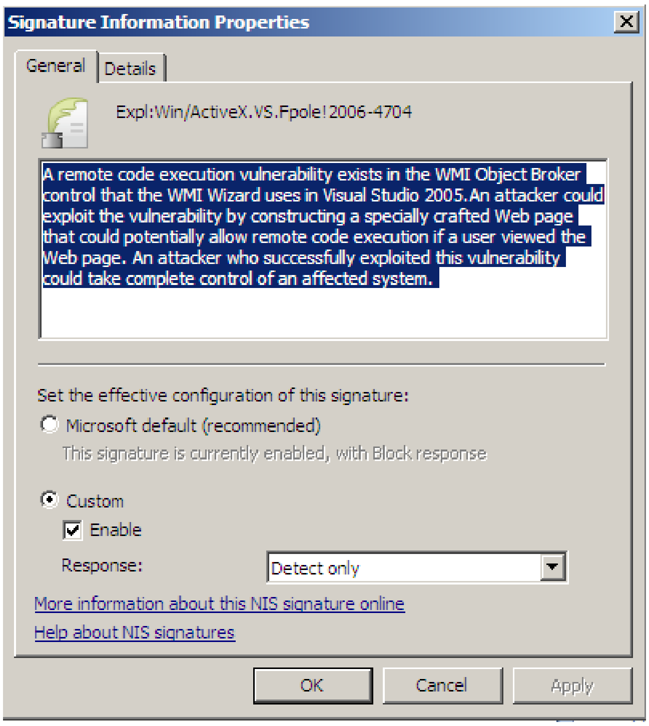

Microsoft Forefront Threat Management Gateway
Intrusion Prevention System
Network Inspection System
Tasks
Help
Network Inspection System Tasks
Configure Settings
Define NIS Exceptions
Set all NIS responses to Microsoft Defaults
Set all NIS responses to Detect Only
Selected Signature Tasks
Group Tasks
Expand All Groups
Collapse All Groups
Signature Information

Group by: Attention Required   Group sort order: Descer

Name	Attention ...	Status
Flag for attention		
Expl:Win/ActiveX.DXImgTransform.R...	Flag for ...	Enabled
Expl:Win/ActiveX.hhctlr.RCE!2006-3357	Flag for ...	Enabled
Expl:Win/ActiveX.VS.Fpole!2006-4704	Flag for ...	Enabled
Expl:Win/ActiveX.WebViewFolderIcon...	Flag for ...	Enabled
Expl:Win/ActiveXControl.HHCtrl.DOS!...	Flag for ...	Enabled
Expl:Win/Agent.agentCharactersLoa...	Flag for ...	Enabled
Expl:Win/COM.ActiveX.RCE!2006-1303	Flag for ...	Enabled

Figure 2: TMG exploit prevention

For every signature you can see a general and detailed description for more information.



Signature Information Properties

General | Details

Expl:Win/ActiveX.VS.Fpole!2006-4704

A remote code execution vulnerability exists in the WMI Object Broker control that the WMI Wizard uses in Visual Studio 2005.An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Set the effective configuration of this signature:

○ Microsoft default (recommended)

This signature is currently enabled, with Block response

● Custom

☑ Enable

Response: Detect only

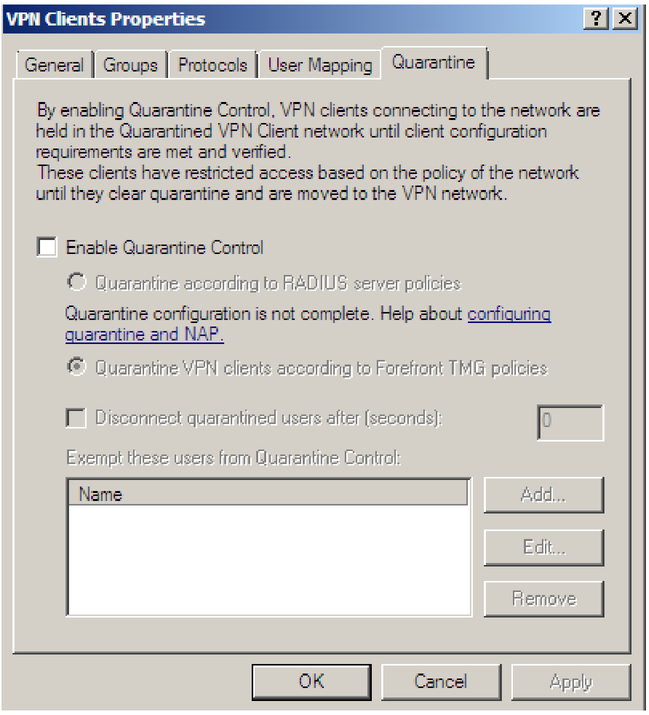
More information about this NIS signature online

Help about NIS signatures

Figure 3: Exploit description

VPN Quarantine

Microsoft Forefront TMG supports VPN Quarantine with the integration into the NAP (Network Access Prevention) feature of Windows Server 2008 and Windows Vista. NAP is integrated into the Windows Server 2008 NPS (Network Policy Server) and allows TMG and Windows Administrators to check VPN clients for compliance before the can connect to the internal LAN via VPN. Possible compliance checks are for example, a running virus scanner with current Antivirus signatures, an activated Windows Firewall, up to date installed Windows patches and many more. TMG VPN feature can be configured to integrate into NAP.



VPN Clients Properties

General | Groups | Protocols | User Mapping | Quarantine

By enabling Quarantine Control, VPN clients connecting to the network are held in the Quarantined VPN Client network until client configuration requirements are met and verified.
These clients have restricted access based on the policy of the network until they clear quarantine and are moved to the VPN network.

□ Enable Quarantine Control

○ Quarantine according to RADIUS server policies

Quarantine configuration is not complete. Help about configuring quarantine and NAP.

● Quarantine VPN clients according to Forefront TMG policies

□ Disconnect quarantined users after (seconds): 0

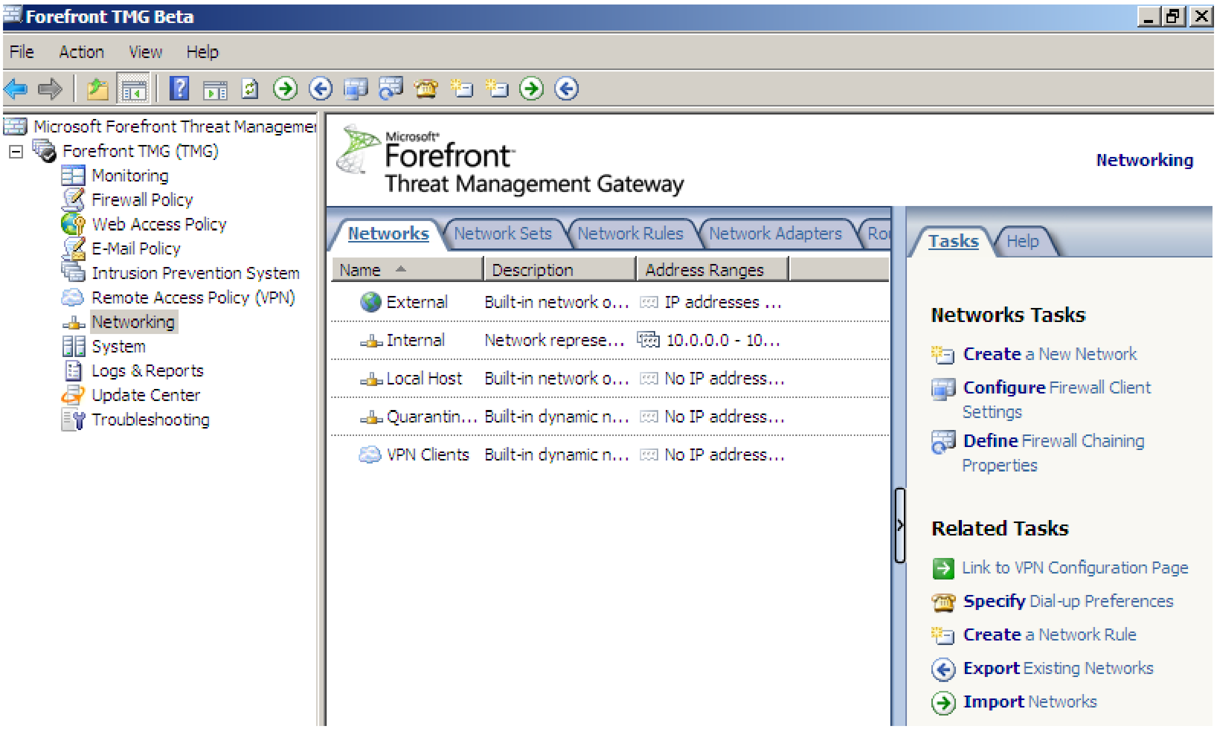
Exempt these users from Quarantine Control:

Name

Figure 4: VPN Quarantine

Multi network support

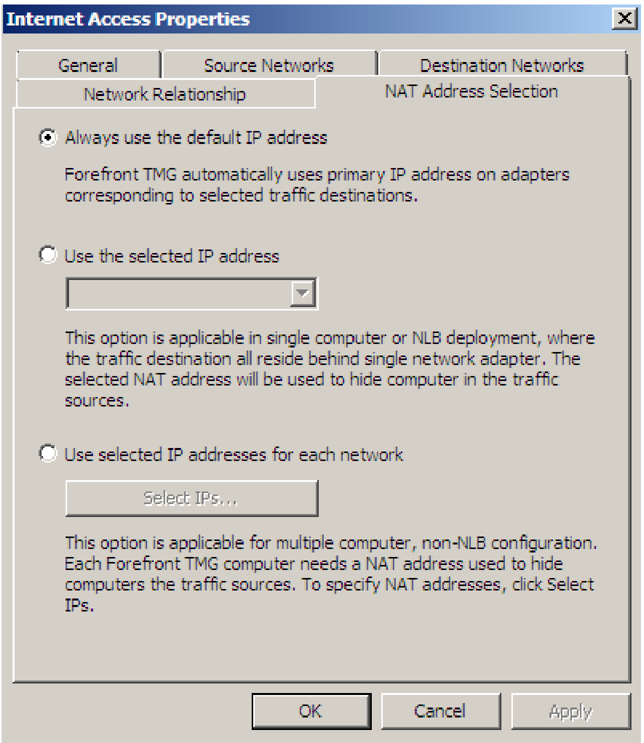
Like ISA Server 2006, TMG provides Multi networking support which is very similar to ISA Server 2006 with one exception that TMG now supports a granular NAT configuration based on TMG networks.



Name	Description	Address Ranges
External	Built-in network o...	IP addresses ...
Internal	Network represe...	10.0.0.0 - 10...
Local Host	Built-in network o...	No IP address...
Quarantin...	Built-in dynamic n...	No IP address...
VPN Clients	Built-in dynamic n...	No IP address...

Figure 5: TMG network definition

Now it is possible to use selected IP addresses for outgoing requests as you can see in the following picture.



● Always use the default IP address

Forefront TMG automatically uses primary IP address on adapters corresponding to selected traffic destinations.

○ Use the selected IP address

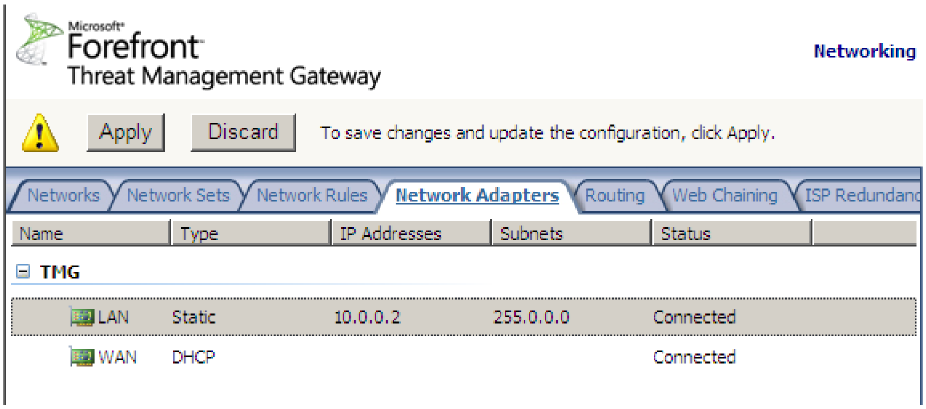
This option is applicable in single computer or NLB deployment, where the traffic destination all reside behind single network adapter. The selected NAT address will be used to hide computer in the traffic sources.

○ Use selected IP addresses for each network

This option is applicable for multiple computer, non-NLB configuration. Each Forefront TMG computer needs a NAT address used to hide computers the traffic sources. To specify NAT addresses, click Select IPs.

Figure 6: Network Address Translation based on TMG networks

Microsoft Forefront TMG Administrator can now configure the properties of the network cards from the Windows Server within the TMG console.

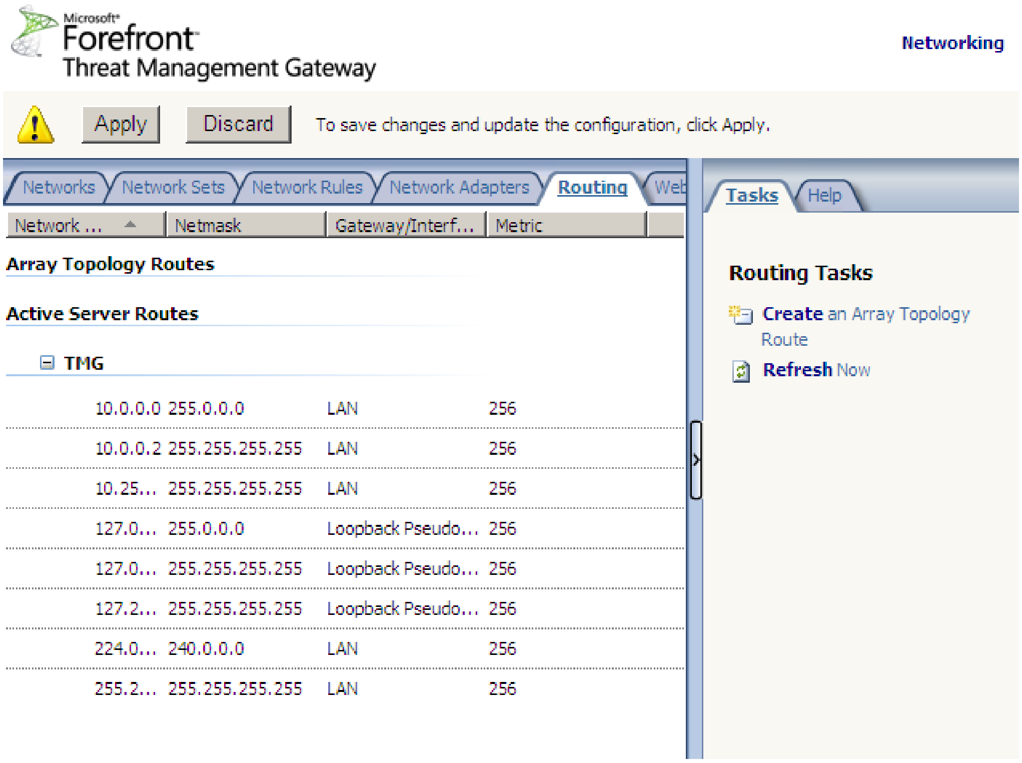


To save changes and update the configuration, click Apply.

Name	Type	IP Addresses	Subnets	Status
⊟ TMG				
LAN	Static	10.0.0.2	255.0.0.0	Connected
WAN	DHCP			Connected

Figure 7: Network Adapter configuration in TMG

It is also possible to view and configure the Server Routing table within the TMG console.



To save changes and update the configuration, click Apply.

Network ...	Netmask	Gateway/Interf...	Metric
Array Topology Routes			
Active Server Routes			
⊟ **TMG**			
10.0.0.0	255.0.0.0	LAN	256
10.0.0.2	255.255.255.255	LAN	256
10.25...	255.255.255.255	LAN	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
224.0...	240.0.0.0	LAN	256
255.2...	255.255.255.255	LAN	256

Routing Tasks

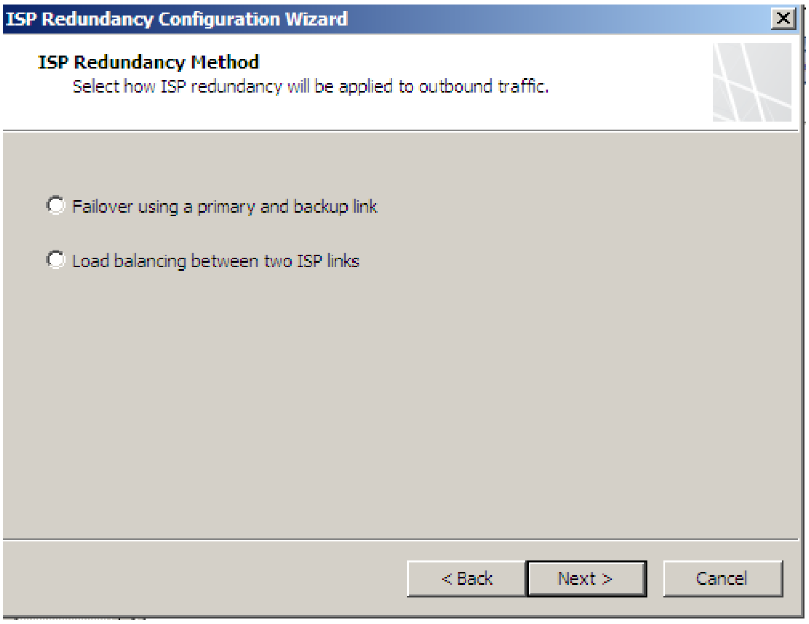
Create an Array Topology Route

Refresh Now

Figure 8: TMG routing configuration

ISP Redundancy

A long requested feature from many ISA customers is now reality. Microsoft Forefront TMG now supports ISP redundancy to provide Failover support between two Internet connections or Load Balancing between two ISP. This feature was previously provided by Rainfinity, but the product was discontinued.



ISP Redundancy Method

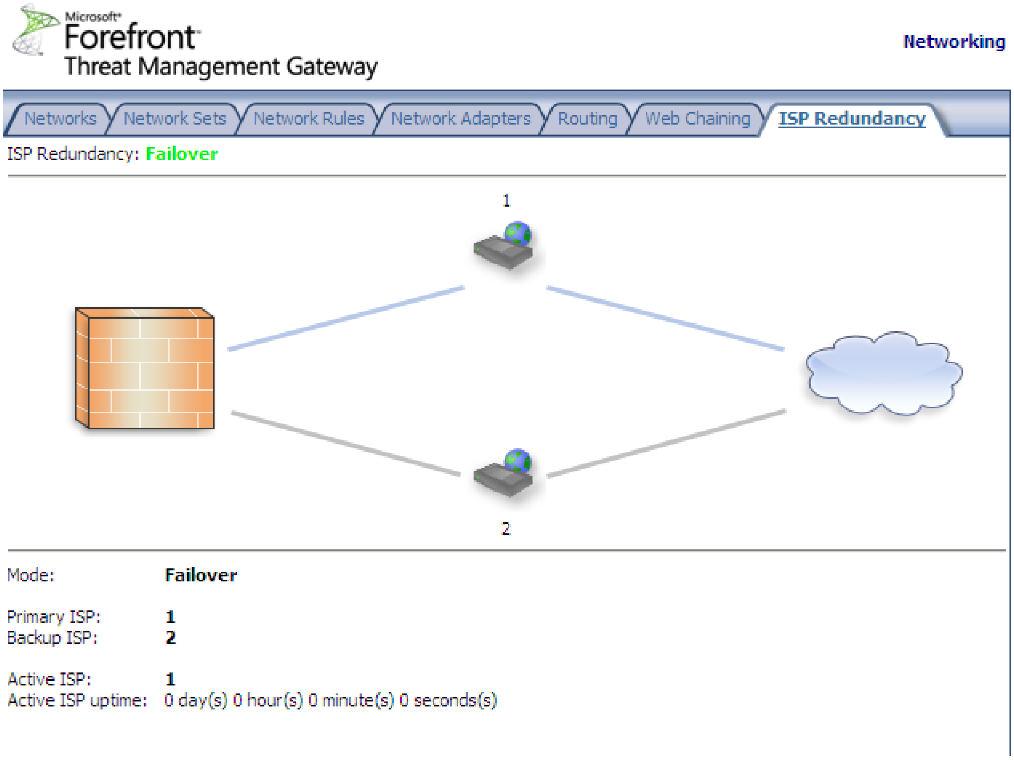
Select how ISP redundancy will be applied to outbound traffic.

○ Failover using a primary and backup link

○ Load balancing between two ISP links

Figure 9: ISP Redundancy methods

ISP Failover redundancy has a graphical user interface (GUI) to see what happened.



ISP Redundancy: Failover

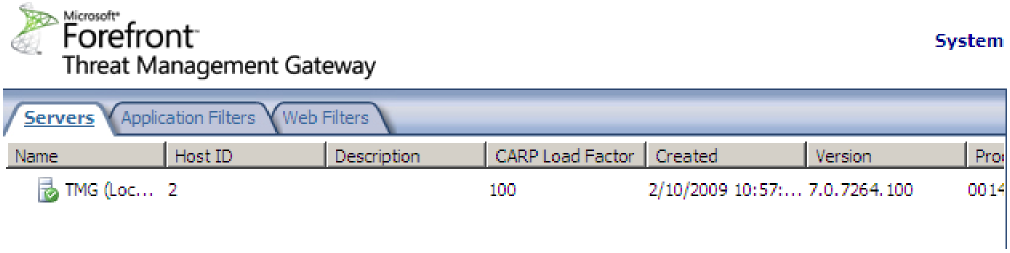
Mode: Failover

Primary ISP: 1
Backup ISP: 2

Active ISP: 1
Active ISP uptime: 0 day(s) 0 hour(s) 0 minute(s) 0 seconds(s)

Figure 10: ISP Failover Redundancy GUI

TMG, like ISA Server 2006 Enterprise has the feature to view the status of each TMG Server in an array.

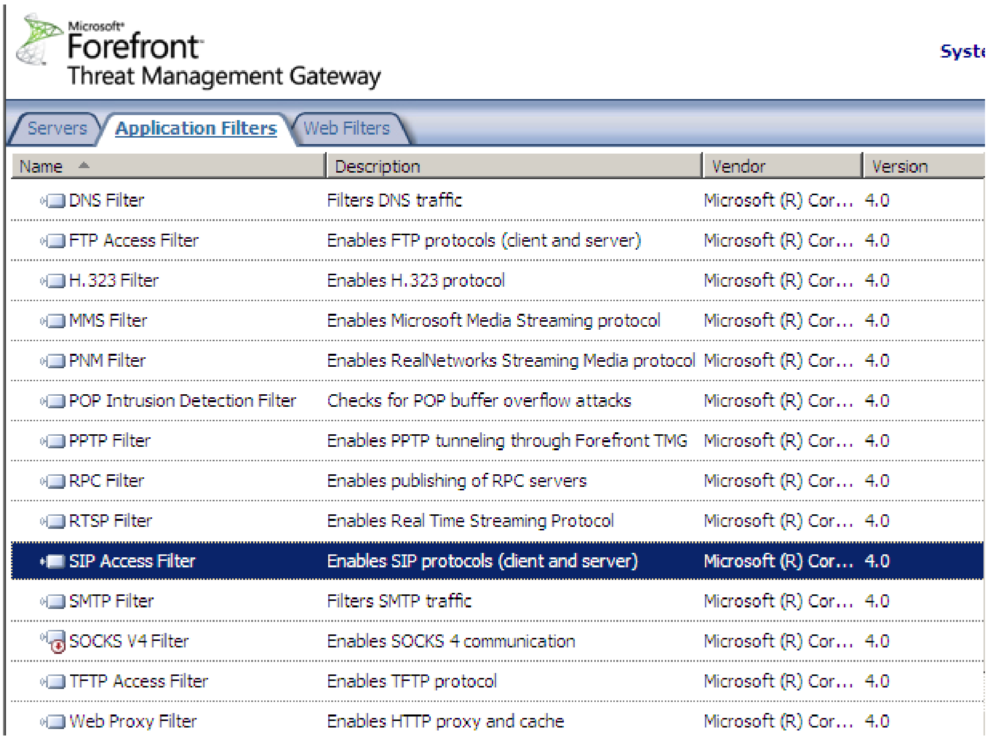


Name	Host ID	Description	CARP Load Factor	Created	Version	Pro
TMG (Loc…	2		100	2/10/2009 10:57:…	7.0.7264.100	0014

Figure 11: Server settings and CARP load factor

Application and Web Filter

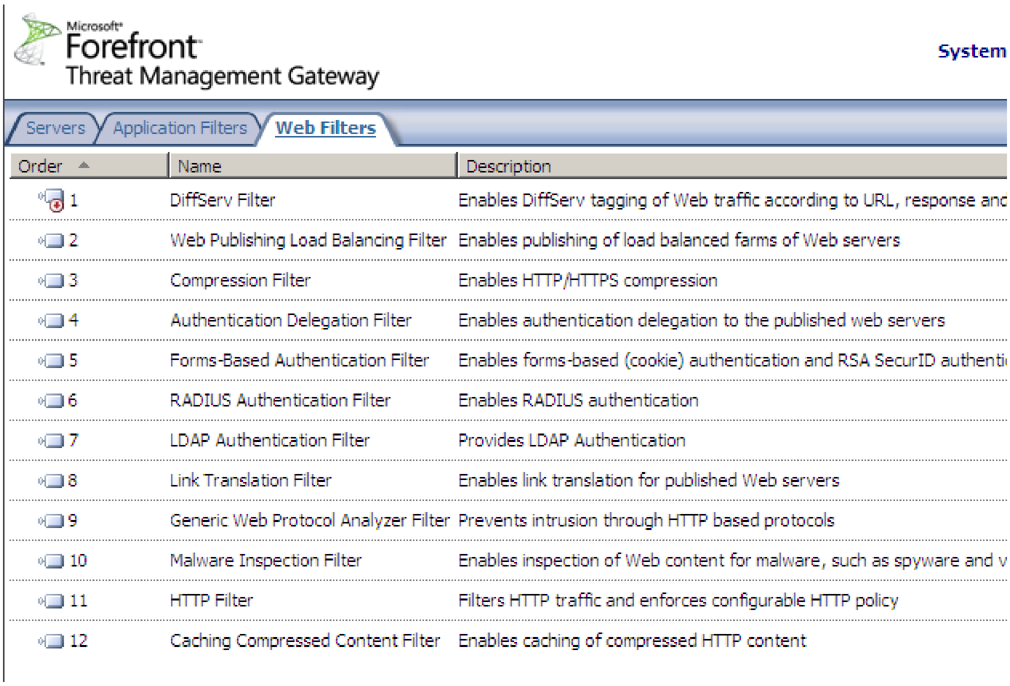
Microsoft Forefront TMG ships with some new Application and Web Filters. The new Application filters in TMG Beta 2 are the SIP filter for VOIP (Voice over IP) support and the TFTP access filter.



Name	Description	Vendor	Version
DNS Filter	Filters DNS traffic	Microsoft (R) Cor...	4.0
FTP Access Filter	Enables FTP protocols (client and server)	Microsoft (R) Cor...	4.0
H.323 Filter	Enables H.323 protocol	Microsoft (R) Cor...	4.0
MMS Filter	Enables Microsoft Media Streaming protocol	Microsoft (R) Cor...	4.0
PNM Filter	Enables RealNetworks Streaming Media protocol	Microsoft (R) Cor...	4.0
POP Intrusion Detection Filter	Checks for POP buffer overflow attacks	Microsoft (R) Cor...	4.0
PPTP Filter	Enables PPTP tunneling through Forefront TMG	Microsoft (R) Cor...	4.0
RPC Filter	Enables publishing of RPC servers	Microsoft (R) Cor...	4.0
RTSP Filter	Enables Real Time Streaming Protocol	Microsoft (R) Cor...	4.0
SIP Access Filter	Enables SIP protocols (client and server)	Microsoft (R) Cor...	4.0
SMTP Filter	Filters SMTP traffic	Microsoft (R) Cor...	4.0
SOCKS V4 Filter	Enables SOCKS 4 communication	Microsoft (R) Cor...	4.0
TFTP Access Filter	Enables TFTP protocol	Microsoft (R) Cor...	4.0
Web Proxy Filter	Enables HTTP proxy and cache	Microsoft (R) Cor...	4.0

Figure 12: Microsoft Forefront TMG Application filter

New Web Filters in TMG are the Malware Inspection Filter and the Generic Web Protocol Analyzer filter which are both used for the Intrusion Prevention feature in Microsoft Forefront TMG.



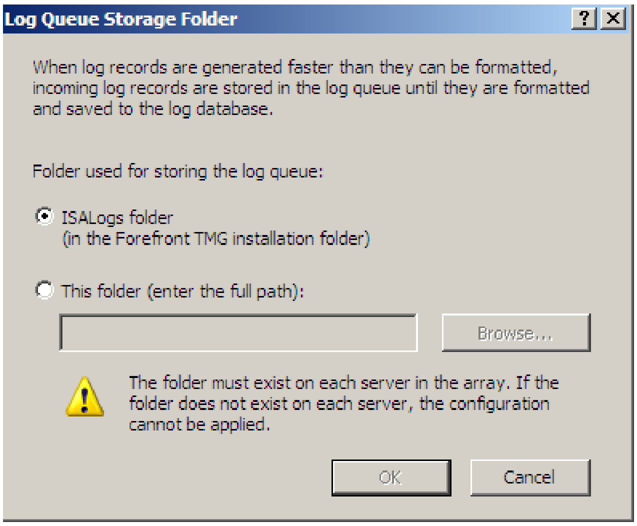
Order	Name	Description
1	DiffServ Filter	Enables DiffServ tagging of Web traffic according to URL, response anc
2	Web Publishing Load Balancing Filter	Enables publishing of load balanced farms of Web servers
3	Compression Filter	Enables HTTP/HTTPS compression
4	Authentication Delegation Filter	Enables authentication delegation to the published web servers
5	Forms-Based Authentication Filter	Enables forms-based (cookie) authentication and RSA SecurID authenti
6	RADIUS Authentication Filter	Enables RADIUS authentication
7	LDAP Authentication Filter	Provides LDAP Authentication
8	Link Translation Filter	Enables link translation for published Web servers
9	Generic Web Protocol Analyzer Filter	Prevents intrusion through HTTP based protocols
10	Malware Inspection Filter	Enables inspection of Web content for malware, such as spyware and v
11	HTTP Filter	Filters HTTP traffic and enforces configurable HTTP policy
12	Caching Compressed Content Filter	Enables caching of compressed HTTP content

Figure 13: Microsoft Forefront TMG Web filter

LLQ – Large Logging Queue

LLQ (Large Logging Queue) is a new feature in Microsoft Forefront TMG which helps reduce the number of times when TMG enters Firewall lockdown mode due to logging failures. Large Logging Queue is a local queue directory on your TMG Server

which is used to save TMG log entries when TMG cannot log into the log destination – by default the SQL Server Express edition.
LLQ has two main components that run in the Kernel mode from TMG (FWENG.SYS) and the User mode (Dispatcher). The process in user mode only reads data from hard disk while the Kernel mode process Fweng writes to the hard disk.



When log records are generated faster than they can be formatted, incoming log records are stored in the log queue until they are formatted and saved to the log database.

Folder used for storing the log queue:

● ISALogs folder
(in the Forefront TMG installation folder)

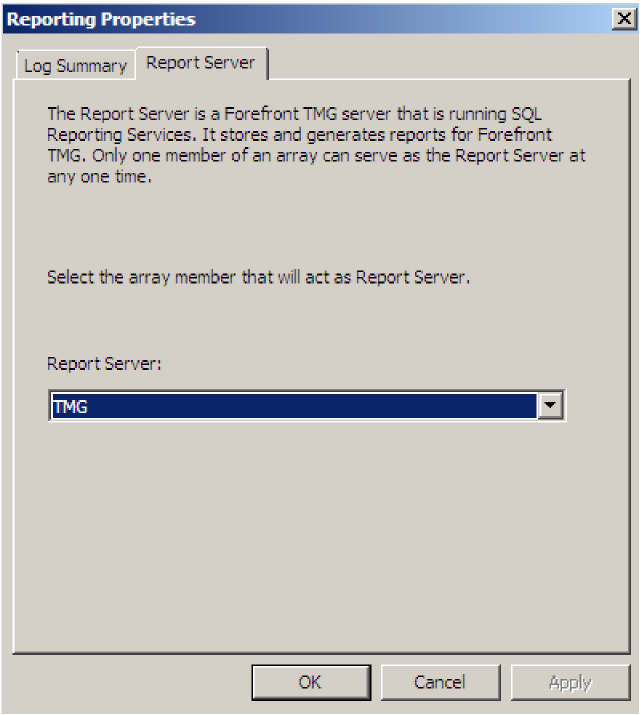
○ This folder (enter the full path):

The folder must exist on each server in the array. If the folder does not exist on each server, the configuration cannot be applied.

Figure 14: TMG Log queue feature

SQL Reporting

Microsoft Forefront TMG installs a local SQL Server 2005 Express which uses SQL Reporting services.



The Report Server is a Forefront TMG server that is running SQL Reporting Services. It stores and generates reports for Forefront TMG. Only one member of an array can serve as the Report Server at any one time.

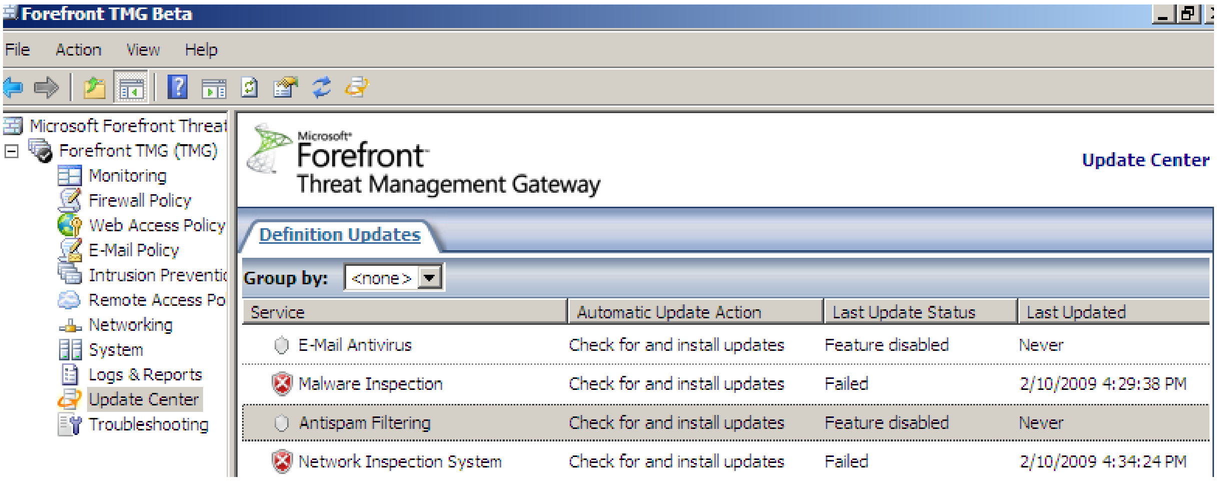
Select the array member that will act as Report Server.

Report Server: TMG

Figure 15: SQL Reporting services

Update Center

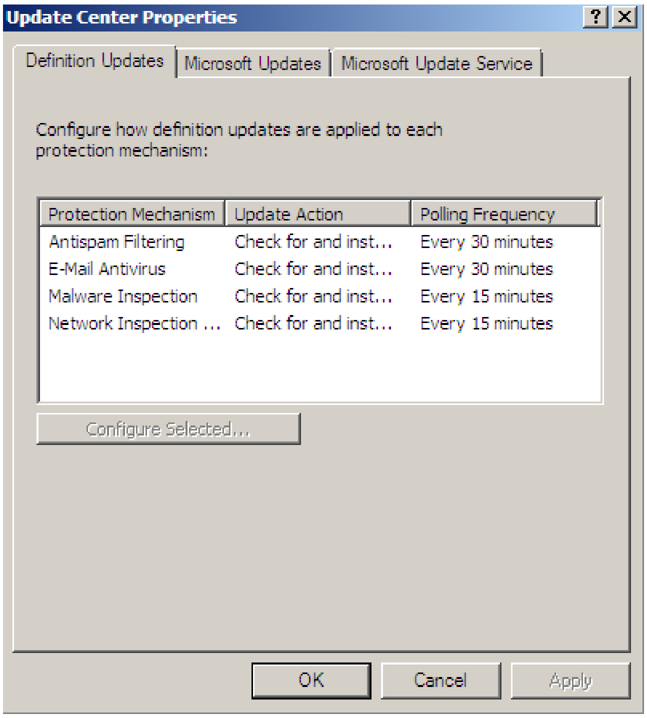
Microsoft Forefront TMG requires up to date signatures for several features like Anti malware protection, Antivirus support, NIS signatures and something more, so the central Update Center gives TMG administrator a tool to configure update settings and a quick view to see if all feature have the last updates.



Service	Automatic Update Action	Last Update Status	Last Updated
E-Mail Antivirus	Check for and install updates	Feature disabled	Never
Malware Inspection	Check for and install updates	Failed	2/10/2009 4:29:38 PM
Antispam Filtering	Check for and install updates	Feature disabled	Never
Network Inspection System	Check for and install updates	Failed	2/10/2009 4:34:24 PM

Figure 16: Update Center

It is possible to configure the update intervals for every protection mechanism.

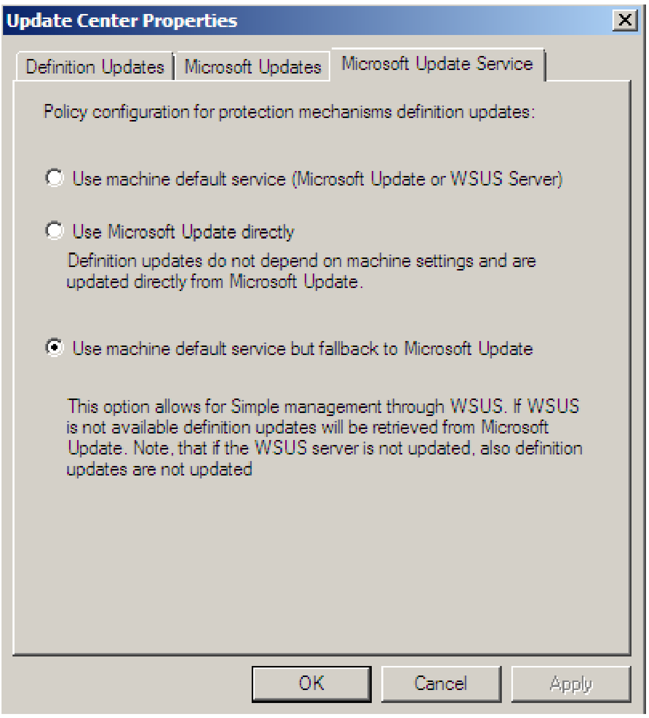


Configure how definition updates are applied to each protection mechanism:

Protection Mechanism	Update Action	Polling Frequency
Antispam Filtering	Check for and inst...	Every 30 minutes
E-Mail Antivirus	Check for and inst...	Every 30 minutes
Malware Inspection	Check for and inst...	Every 15 minutes
Network Inspection ...	Check for and inst...	Every 15 minutes

Figure 17: Configure TMG update settings

To keep the Windows configuration on TMG up to date, the Microsoft Update Service settings use WSUS settings by default and fails back to Microsoft Update settings when the WSUS Server is not reachable.



Policy configuration for protection mechanisms definition updates:

○ Use machine default service (Microsoft Update or WSUS Server)

○ Use Microsoft Update directly
Definition updates do not depend on machine settings and are updated directly from Microsoft Update.

● Use machine default service but fallback to Microsoft Update

This option allows for Simple management through WSUS. If WSUS is not available definition updates will be retrieved from Microsoft Update. Note, that if the WSUS server is not updated, also definition updates are not updated

Figure 18: Microsoft Update Service settings

Conclusion

In this second part of this article, I tried to give you a high level overview about the new features and functionalities in Microsoft Forefront TMG. There are an l lot of new funny things and some functionality has been extended but there are also many not changed feature, so it should be possible to get familiar with the new Microsoft Firewall without learning from the beginning.

Related links

Forefront Threat Management Gateway Beta 2
http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&DisplayLang=en
Forefront TMG Beta 2 is Released
http://blogs.technet.com/isablog/archive/2009/02/06/forefront-tmg-beta-2-is-released.aspx
Forefront TMG MBE Frequently Asked Questions
http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-mbe-faq.aspx
How to install the Forefront Threat Management Gateway (Forefront TMG) Beta 1
http://www.isaserver.org/tutorials/Installing-Forefront-Threat-Management-Gateway-Forefront-TMG-Beta1.html
How to configure the Microsoft Forefront TMG Firewall Lockdown Mode and the new TMG Log queue feature (LLQ).
http://www.isaserver.org/tutorials/Explaining-Microsoft-Forefront-TMG-Firewall-Lockdown-Mode.html
Keeping High Availability with Forefront TMG's ISP Redundancy Feature
http://blogs.technet.com/isablog/archive/2009/02/16/keeping-high-availability-with-forefront-tmg-s-isp-redundancy-feature.aspx