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

Explaining and configuring NIS (Network Inspection Service)

Abstract

In this article, I will show you how to configure the new Network Inspection functionality in 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.

A few month ago, Microsoft released Beta 2 from Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

NIS overview

Before we start explaining the NIS features in Microsoft Forefront Threat Management Gateway (TMG), we first have to explain what NIS is and on what protocols and techniques it is based on.

Defining NIS and IPS

TMG is a vulnerability based Intrusion Prevention System (IPS). An IPS should protect your internal network for known and unknown vulnerabilities. In the case of TMG directly on the edge of the internal network to the Internet. All network traffic must flow through TMG, so TMG is the first line of defense to protect against different vulnerabilities.
An IPS is defined at two level:

- System level
- Solution level

On the system level, IPS is an aggregation of multiple protection mechanisms.
On the solution level, IPS is applied on internal Host or at devices at the Edge, in this case on Microsoft Forefront TMG.

TMG NIS IPS features deals with blocking unknown and known attacks at the network level to fight against vulnerabilities.

TMG uses a signature based IPS. A signature based IPS protects your hosts against exploitation of found vulnerabilities. A signature based IPS is used to close the time window between an announcement of a vulnerability and the patch deployment of all possible vulnerable hosts. The practice tells us that an attacker can create an exploit faster than Administrators can deploy patches provided by the software developer. A signature can be released and deployed faster than patches, so Administrators have the time to deploy patches on all effected systems during they are protected through the TMG NIS feature.

Zero Day Vulnerability

An exploit that is available in short time to use a vulnerability of a system is called a zero day vulnerability. A typical protection against an zero day vulnerability consists of the following steps:

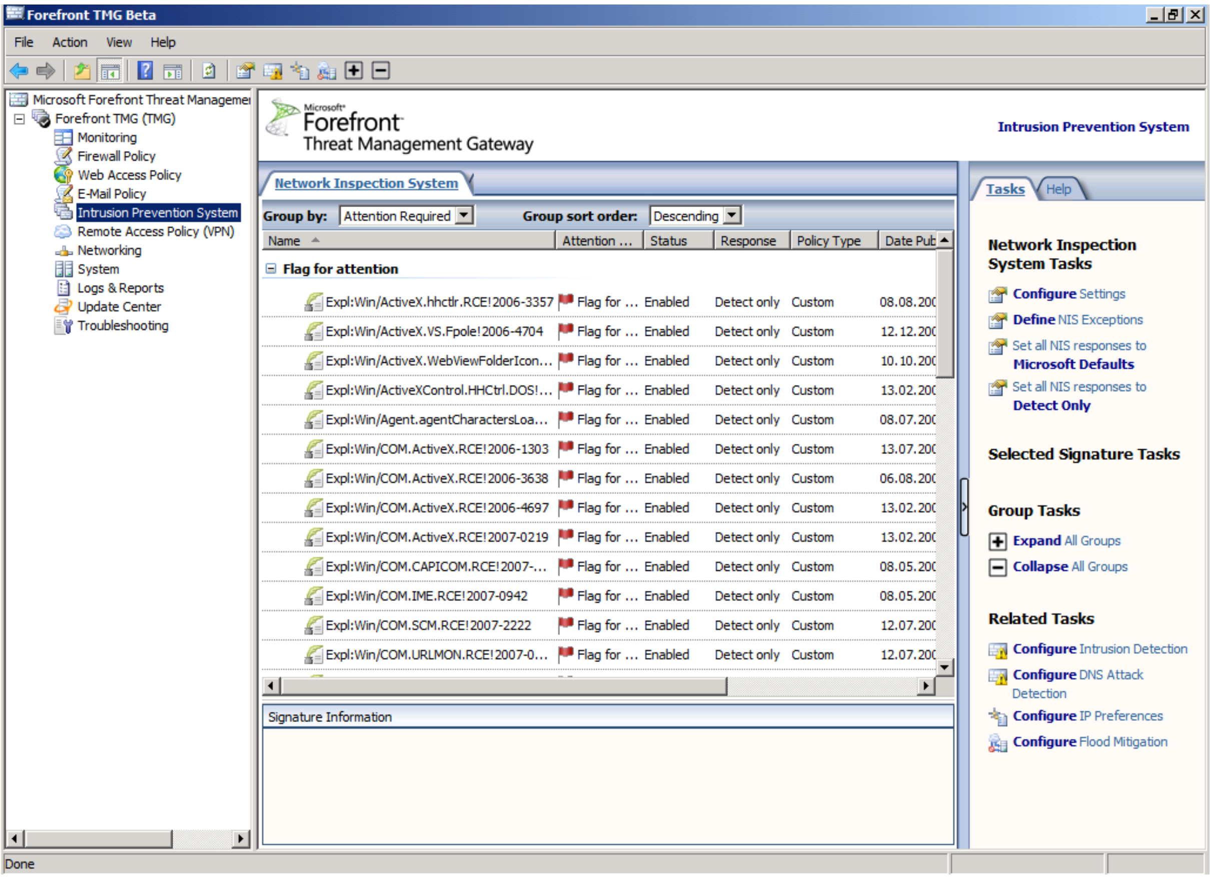
- A vulnerability is discovered
- The Microsoft Response Team (MRT) creates and tests the vulnerability signature
- The signature is released by Microsoft through a distribution service
- TMG uses this signature for the NIS protection feature
- All internal (unpatched) hosts behind TMG are now protected until an Patch is developed by Microsoft and rolled out through Windows Update, WSUS or other patch distribution systems.

GAPA

To create signatures for a vulnerability, Microsoft is using the GAPA (Generic Application Protocol Analyzer) protocol. NIS in TMG is based on GAPA.
GAPA is a framework and a platform for safe and fast low level protocol parsing. GAPA which Microsoft has architected and prototyped. GAPA is using the GAPAL (Generic Application Protocol Analyzer Language) language. According to the Microsoft documentation, GAPA allows rapid creation of protocol analyzers, greatly reducing the time needed for development.

Network Inspection System walkthrough

NIS configuration in Forefront TMG is quite easy and requires only a view steps. In the following figure you can see the default signatures which comes with the Standard installation of TMG. It is possible to group the signatures to find specific signatures easier.



Forefront TMG Beta
File
Action
View
Help
Microsoft Forefront Threat Manageme
Forefront TMG (TMG)
Monitoring
Firewall Policy
Web Access Policy
E-Mail Policy
Intrusion Prevention System
Remote Access Policy (VPN)
Networking
System
Logs & Reports
Update Center
Troubleshooting
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
Related Tasks
Configure Intrusion Detection
Configure DNS Attack Detection
Configure IP Preferences
Configure Flood Mitigation
Signature Information
Done

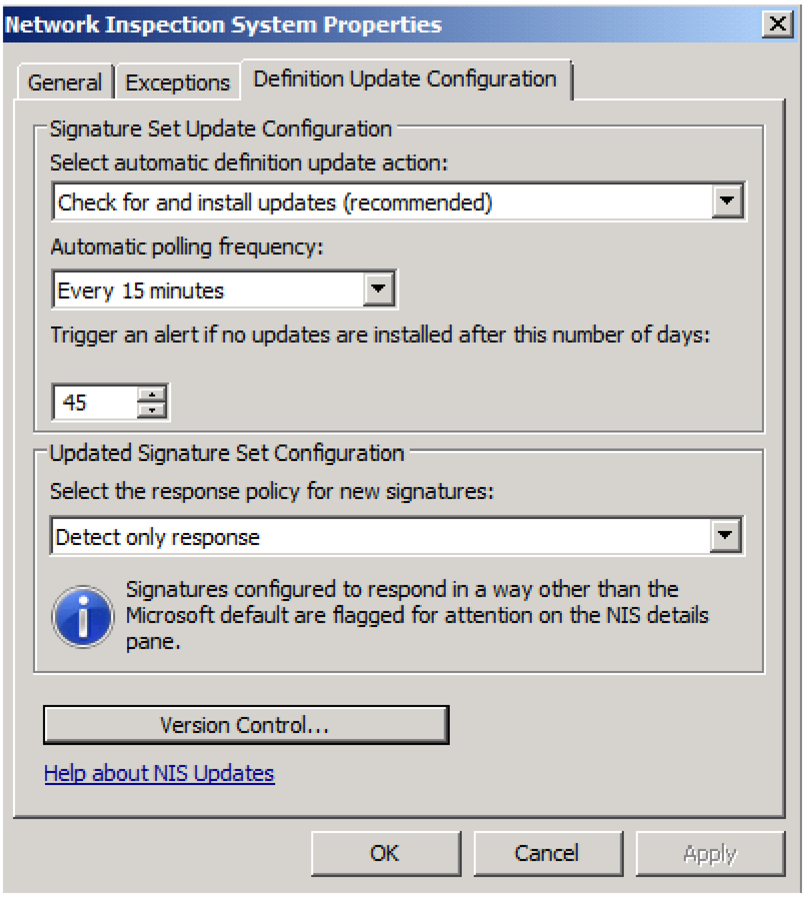
Group by: Attention Required

Group sort order: Descending

Name	Attention ...	Status	Response	Policy Type	Date Pub
Flag for attention					
Expl:Win/ActiveX.hhctlr.RCE!2006-3357	Flag for ...	Enabled	Detect only	Custom	08.08.200
Expl:Win/ActiveX.VS.Fpole!2006-4704	Flag for ...	Enabled	Detect only	Custom	12.12.200
Expl:Win/ActiveX.WebViewFolderIcon...	Flag for ...	Enabled	Detect only	Custom	10.10.200
Expl:Win/ActiveXControl.HHCtrl.DOS!...	Flag for ...	Enabled	Detect only	Custom	13.02.200
Expl:Win/Agent.agentCharactersLoa...	Flag for ...	Enabled	Detect only	Custom	08.07.200
Expl:Win/COM.ActiveX.RCE!2006-1303	Flag for ...	Enabled	Detect only	Custom	13.07.200
Expl:Win/COM.ActiveX.RCE!2006-3638	Flag for ...	Enabled	Detect only	Custom	06.08.200
Expl:Win/COM.ActiveX.RCE!2006-4697	Flag for ...	Enabled	Detect only	Custom	13.02.200
Expl:Win/COM.ActiveX.RCE!2007-0219	Flag for ...	Enabled	Detect only	Custom	13.02.200
Expl:Win/COM.CAPICOM.RCE!2007-...	Flag for ...	Enabled	Detect only	Custom	08.05.200
Expl:Win/COM.IME.RCE!2007-0942	Flag for ...	Enabled	Detect only	Custom	08.05.200
Expl:Win/COM.SCM.RCE!2007-2222	Flag for ...	Enabled	Detect only	Custom	12.07.200
Expl:Win/COM.URLMON.RCE!2007-0...	Flag for ...	Enabled	Detect only	Custom	12.07.200

Figure 1: Intrusion Prevention System

As a first step you should configure default Network Inspection Settings. It is possible to define exceptions for the NIS scan and one of the most important configuration settings is to configure the NIS automatic definition update action. It is also possible to trigger an alert if update definitions are not installed in the last X number of days. The standard setting is 45 days. The default response for new applied signatures from Microsoft is Response only. It is possible to change the default response policy if you want to do that.


Network Inspection System Properties

Signature Set Update Configuration

Select automatic definition update action: Check for and install updates (recommended)

Automatic polling frequency: Every 15 minutes

Trigger an alert if no updates are installed after this number of days: 45

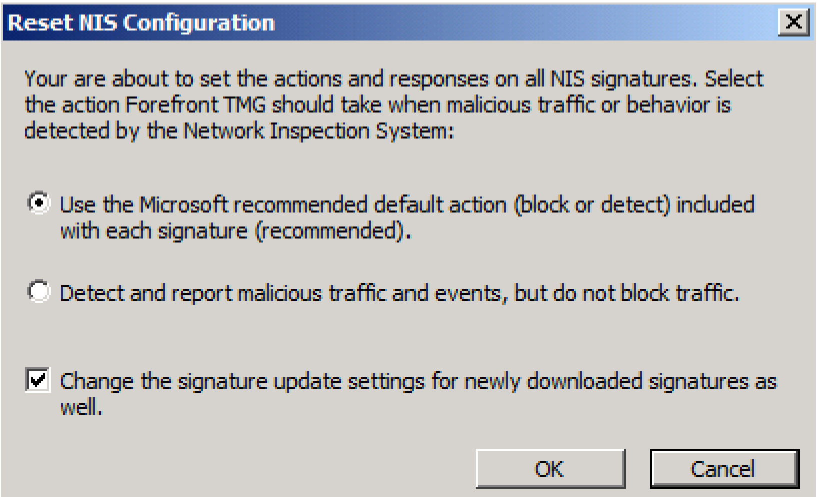
Updated Signature Set Configuration

Select the response policy for new signatures: Detect only response

Signatures configured to respond in a way other than the Microsoft default are flagged for attention on the NIS details pane.

Figure 2: Definition Update Configuration

In the NIS task pane it is possible to reset the NIS configuration actions and response on all NIS signatures. The default action is to block or only detect the vulnerable network traffic based on the signature setting as you can see in the following figure.


Reset NIS Configuration

Your are about to set the actions and responses on all NIS signatures. Select the action Forefront TMG should take when malicious traffic or behavior is detected by the Network Inspection System:

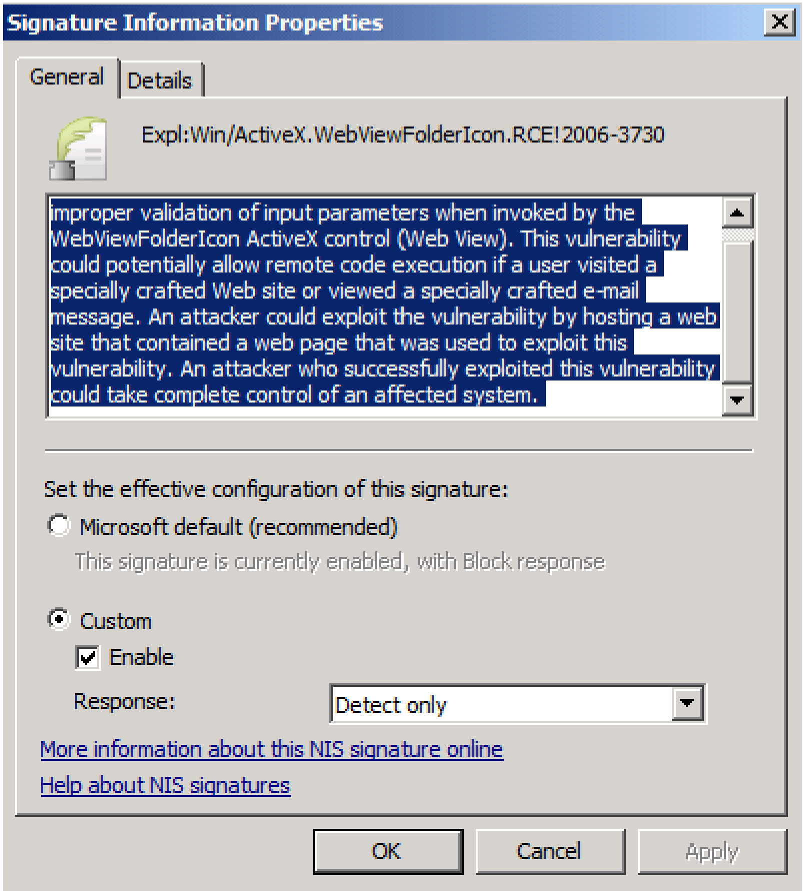
● Use the Microsoft recommended default action (block or detect) included with each signature (recommended).

○ Detect and report malicious traffic and events, but do not block traffic.

☑ Change the signature update settings for newly downloaded signatures as well.

Figure 3: Reset NIS Configuration

For every signature it is possible to get more information about the vulnerability. It is also possible to set the default action for this signature to Detect or block the network traffic.



Signature Information Properties

Expl:Win/ActiveX.WebViewFolderIcon.RCE!2006-3730

improper validation of input parameters when invoked by the WebViewFolderIcon ActiveX control (Web View). This vulnerability could potentially allow remote code execution if a user visited a specially crafted Web site or viewed a specially crafted e-mail message. An attacker could exploit the vulnerability by hosting a web site that contained a web page that was used to exploit this vulnerability. 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

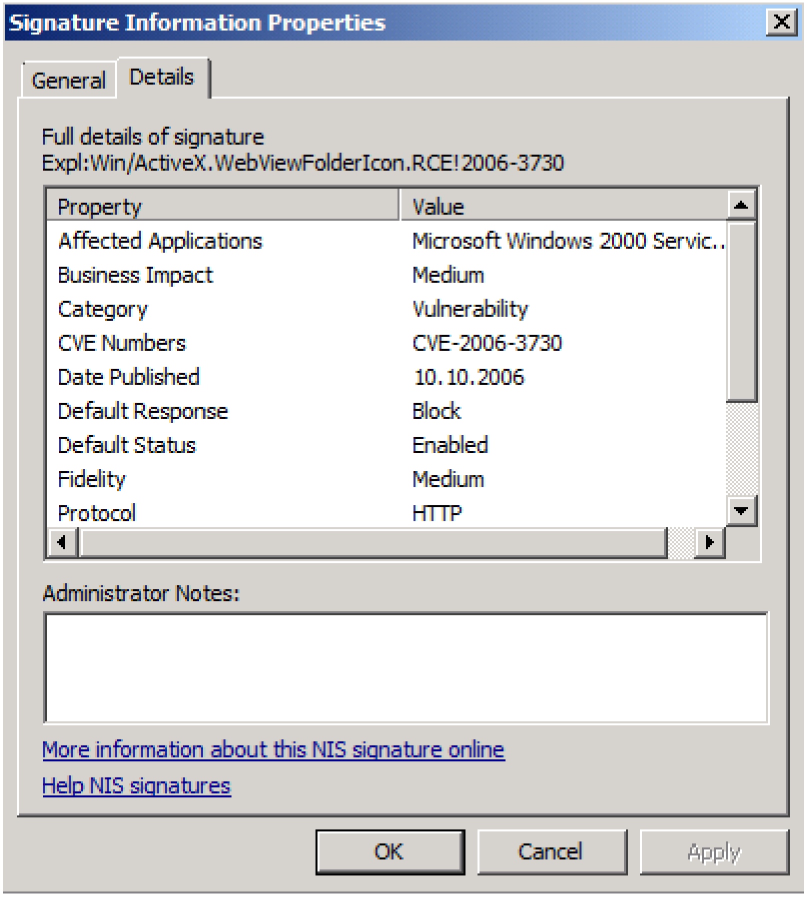
☑ Enable

Response: Detect only

More information about this NIS signature online
Help about NIS signatures
OK
Cancel
Apply

Figure 4: Signature Information Properties

If you want to get more information about the signature, click the Details tab and you will find more helpful information. For every signature, Microsoft also published a CVE number for which you will find more information about the functionality and dangerous of the vulnerability. You will find more information about the specific threat on the Microsoft security bulletin website.



Full details of signature
Expl:Win/ActiveX.WebViewFolderIcon.RCE!2006-3730

Property	Value
Affected Applications	Microsoft Windows 2000 Servic..
Business Impact	Medium
Category	Vulnerability
CVE Numbers	CVE-2006-3730
Date Published	10.10.2006
Default Response	Block
Default Status	Enabled
Fidelity	Medium
Protocol	HTTP

Administrator Notes:

More information about this NIS signature online

Help NIS signatures

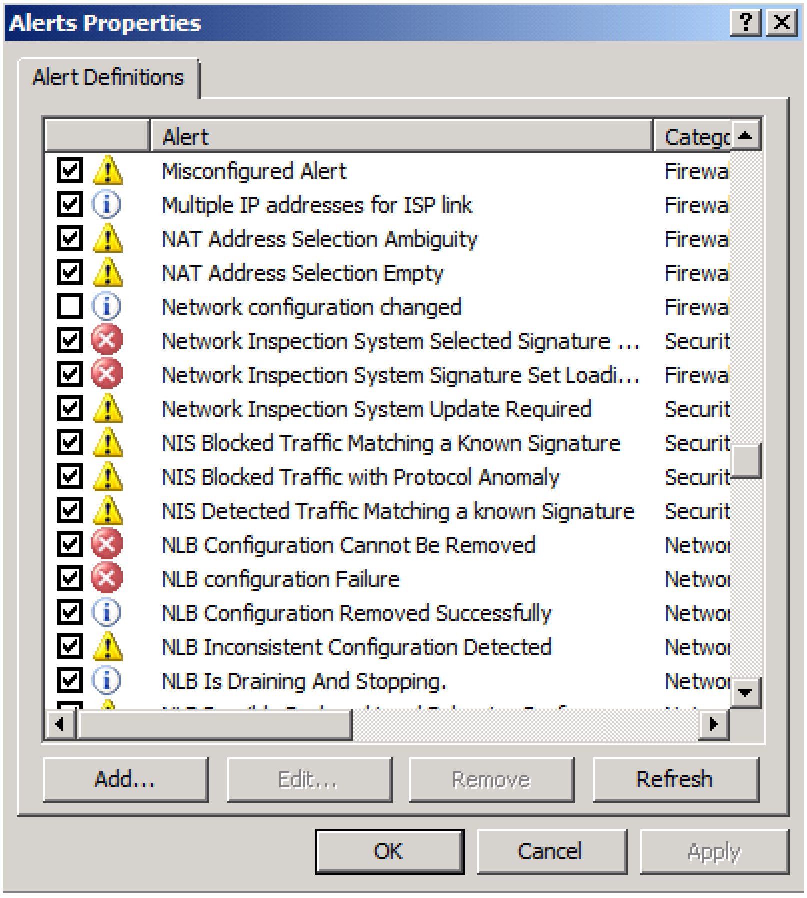
Figure 5: Signature Information Properties - Details

How to test the NIS functionality

One way to test the NIS functionality is to open a test signature in your web browser and to see if the NIS protection in TMG is working as expected. TMG comes with a test signature. Enter the following URL in your web browser to test NIS: http://www.contoso.com/testNIS.aspx?testValue=1!2@34$5%6^[%7BNIS-test-URL%7D}1!2@34$5%6^. If NIS is working, the attempt to open the website should be blocked by TMG with an TMG generated message.

TMG alert settings

If the NIS component detected or blocked network traffic because a matching signature was found in the network traffic, a default alert action is configured in the TMG alert section which creates an entry in the Event Log of the TMG server. Other alert actions like a program execution or stopping a service is possible.



		Alert	Catego
☑	⚠	Misconfigured Alert	Firewa
☑	ⓘ	Multiple IP addresses for ISP link	Firewa
☑	⚠	NAT Address Selection Ambiguity	Firewa
☑	⚠	NAT Address Selection Empty	Firewa
□	ⓘ	Network configuration changed	Firewa
☑	⊗	Network Inspection System Selected Signature ...	Securit
☑	⊗	Network Inspection System Signature Set Loadi...	Firewa
☑	⚠	Network Inspection System Update Required	Securit
☑	⚠	NIS Blocked Traffic Matching a Known Signature	Securit
☑	⚠	NIS Blocked Traffic with Protocol Anomaly	Securit
☑	⚠	NIS Detected Traffic Matching a known Signature	Securit
☑	⊗	NLB Configuration Cannot Be Removed	Networ
☑	⊗	NLB configuration Failure	Networ
☑	ⓘ	NLB Configuration Removed Successfully	Networ
☑	⚠	NLB Inconsistent Configuration Detected	Networ
☑	ⓘ	NLB Is Draining And Stopping.	Networ

Figure 6: NIS alert definitions

Conclusion

In this article, I gave you an overview about the Microsoft Forefront Threat Management Gateway NIS features. I also tried to show you the configuration of the NIS functionality and how Administrators can protect its networks against different vulnerabilities. The NIS functionality is a great weapon for TMG Administrators to fight against different network intrusion attempts.

Related links

Overview of GAPA and GAPAL
http://research.microsoft.com/apps/pubs/default.aspx?id=70223
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
What's new in Forefront TMG Beta 2 (Part 1)
http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html
Installing and configuring Microsoft Forefront TMG Beta 2
http://www.isaserver.org/tutorials/Installing-configuring-Microsoft-Forefront-TMG-Beta2.html
Microsoft Security Bulletin Search
http://www.microsoft.com/technet/security/current.aspx