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

Overview about the Microsoft Reputation Service (MRS), Microsoft Malware Protection Center (MMPC) and other techniques

Abstract

In this article I will give you an overview about the Microsoft Reputation Service (MRS) and how it is used by Microsoft Forefront TMG and other Microsoft products. We will also cover techniques like Microsoft Spynet and the Microsoft Telemetry service, the Microsoft Malware Protection Center and GAPA (Generic Application Programming Application) and GAPAL.

Let's begin

- To protect against new threats and the dynamically changing landscape of new threats, starting with Forefront TMG, Microsoft has developed some new dynamically services which should protect against Malware, exploits and something more. Forefront TMG comes with the following new technologies which should protect the internal network:
  NIS (Network Inspection System)
  Dynamic URL filtering
- Outgoing Malware inspection
- Outgoing HTTPS inspection

NIS, URL filtering and the Malware inspection in Forefront TMG uses signature based services (NIS, Malware) or a dynamic URL filtering database in the cloud (URL filtering). Some of these services use MRS, the Microsoft Reputation Service and also the Microsoft Telemetry Service (Spynet) and definition files from the Microsoft Malware Protection Center (MMPC). In this article I will explain most of these technologies.

Microsoft Reputation Service (MRS) and TMG URL filtering

Microsoft Forefront TMG has a new functionality called dynamic URL filtering. Forefront TMG administrators are able to allow or deny access for URLs based on a dynamic URL filtering database, hosted in Microsoft datacentres in the cloud. Forefront TMG evaluates the requested URL from a user and checks this URL against a local MRS (URL cache) or online against the MRS database in the cloud.

The following screenshot will give you an overview about the dynamic URL filtering process in Forefront TMG.

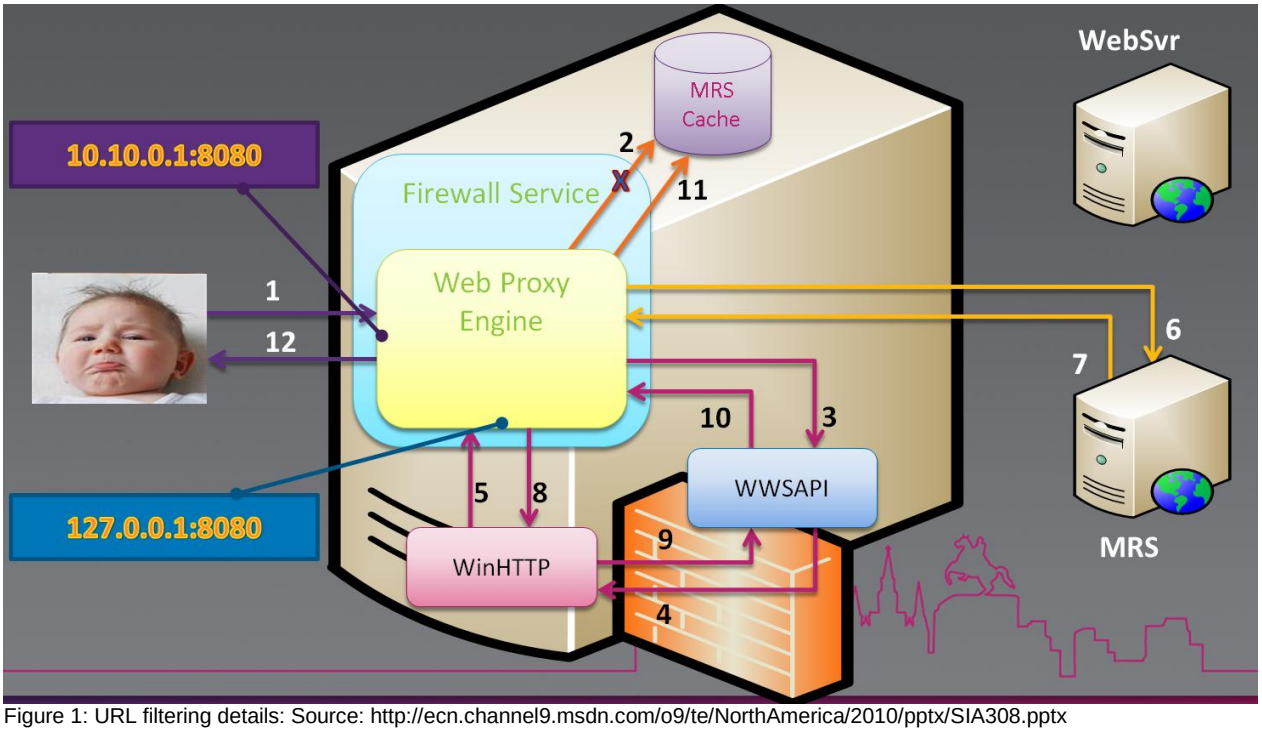

Figure 1: URL filtering details: Source: http://ecn.channel9.msdn.com/o9/te/NorthAmerica/2010/pptx/SIA308.pptx

URL categories

Microsoft divided the dynamic URL database into categories. These categories can be used in Forefront TMG to allow or deny access for users.

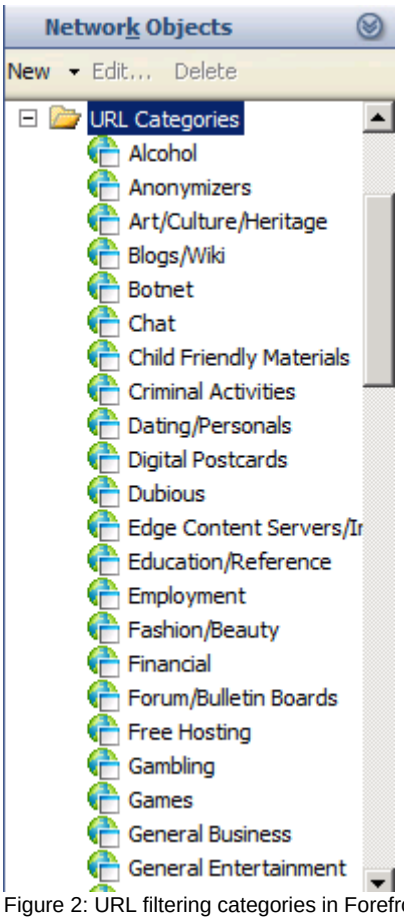

Figure 2: URL filtering categories in Forefront TMG

URL category query

Some URLs are associated to multiple categories, for example http://www.web.de is categorized as Portal Sites, Search Engines and Technical Information. URL Filtering in Forefront TMG is based on a single category per URL, so Forefront TMG need to choose one of these categories as the primary URL category. Forefront TMG uses a pre-defined category precedence list. Forefront TMG has a category precedence list, where categories are ordered by importance. Microsoft has hardcoded this precedence list and you cannot change the URL precedence.
When Forefront TMG receives a URL request, it first checks the URL category from the local MRS cache. If the URL has multiple associated categories, Forefront TMG applies category precedence rules based on the precedence list. The URL category with the highest precedence is used by Forefront TMG.

To see to which URL category a URL belongs, you can use the URL category query in the Forefront TMG Management Console (MMC) or the MRS website of Microsoft.

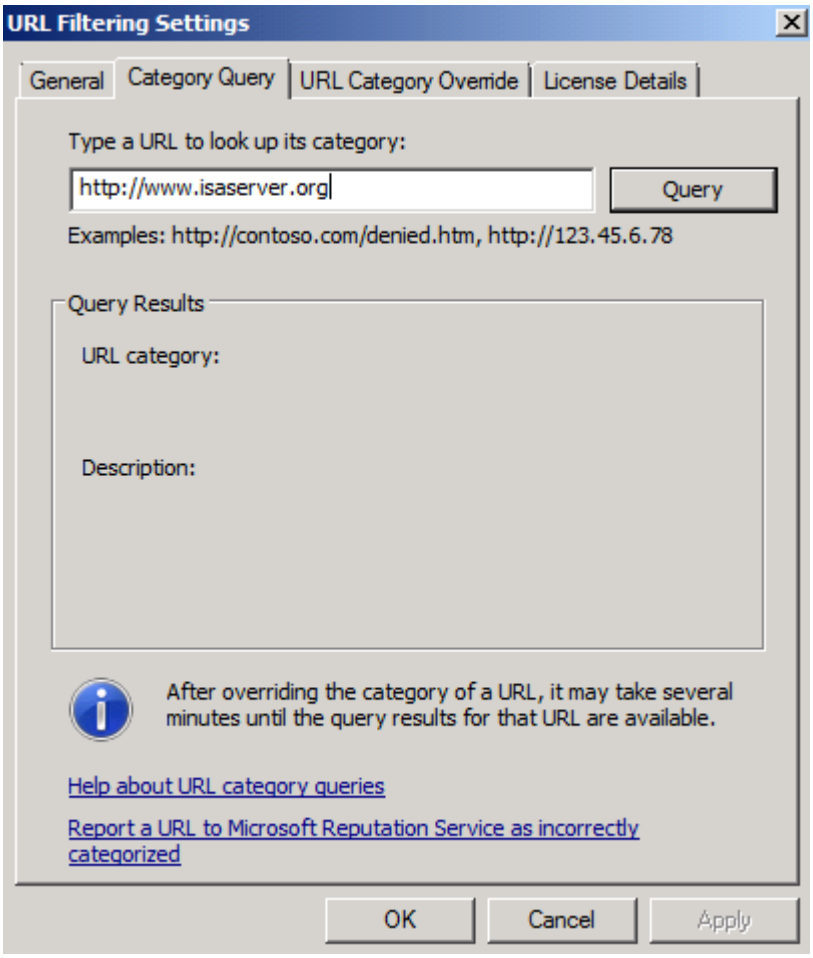

Figure 3: URL category query

The other way to query for URL categories is to use the Microsoft Reputation Services website, as shown in the following screenshot.

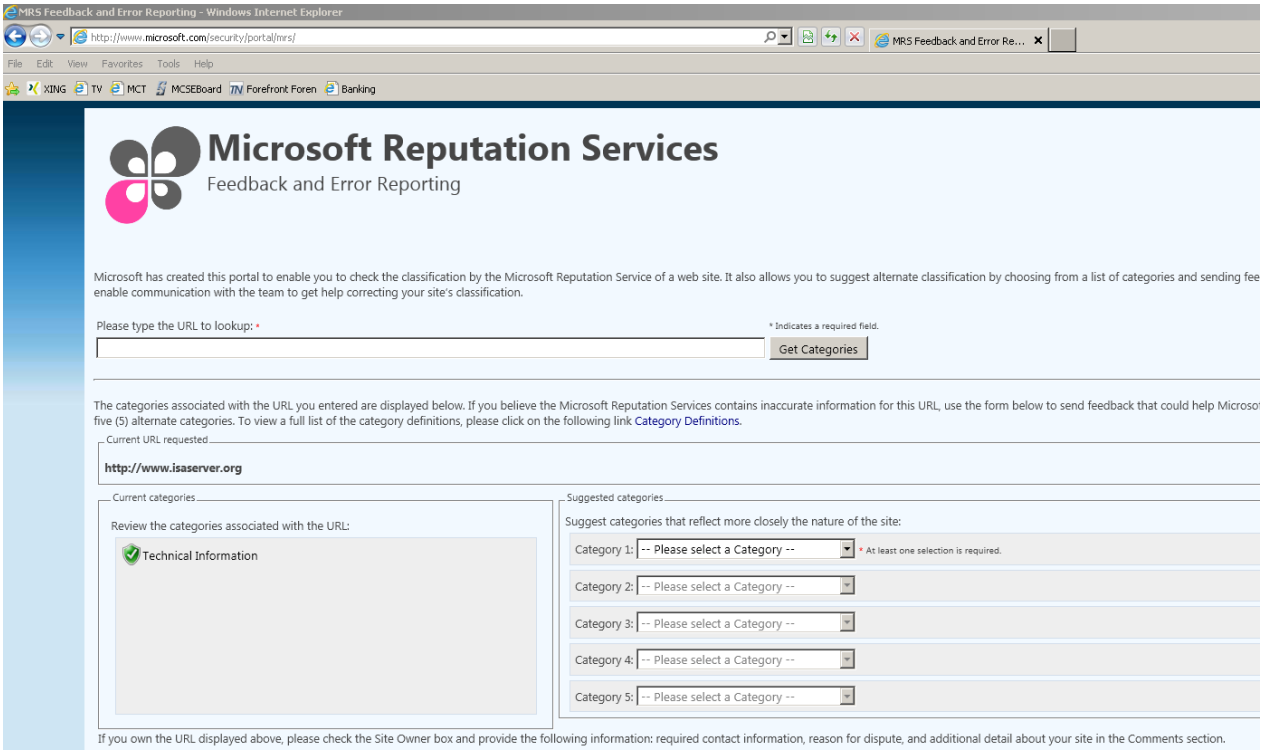

Figure 4:Microsoft Reputation Services (MRS)

The MRS website can also be used to suggest other URL categories if you are the owner of the website and in your opinion other URL categories better reflect the nature of the website.

Microsoft Telemetry Reporting Service

Microsoft Forefront TMG has a new functionality called Malware Inspection, which inspects outgoing HTTP and HTTPS traffic (when Forefront TMG HTTPS inspection is used), against Malware. With the help of the Update Center integrated in Forefront TMG, Forefront TMG downloads Antimalware definition signatures from Microsoft Servers and checks the network traffic against these signatures.

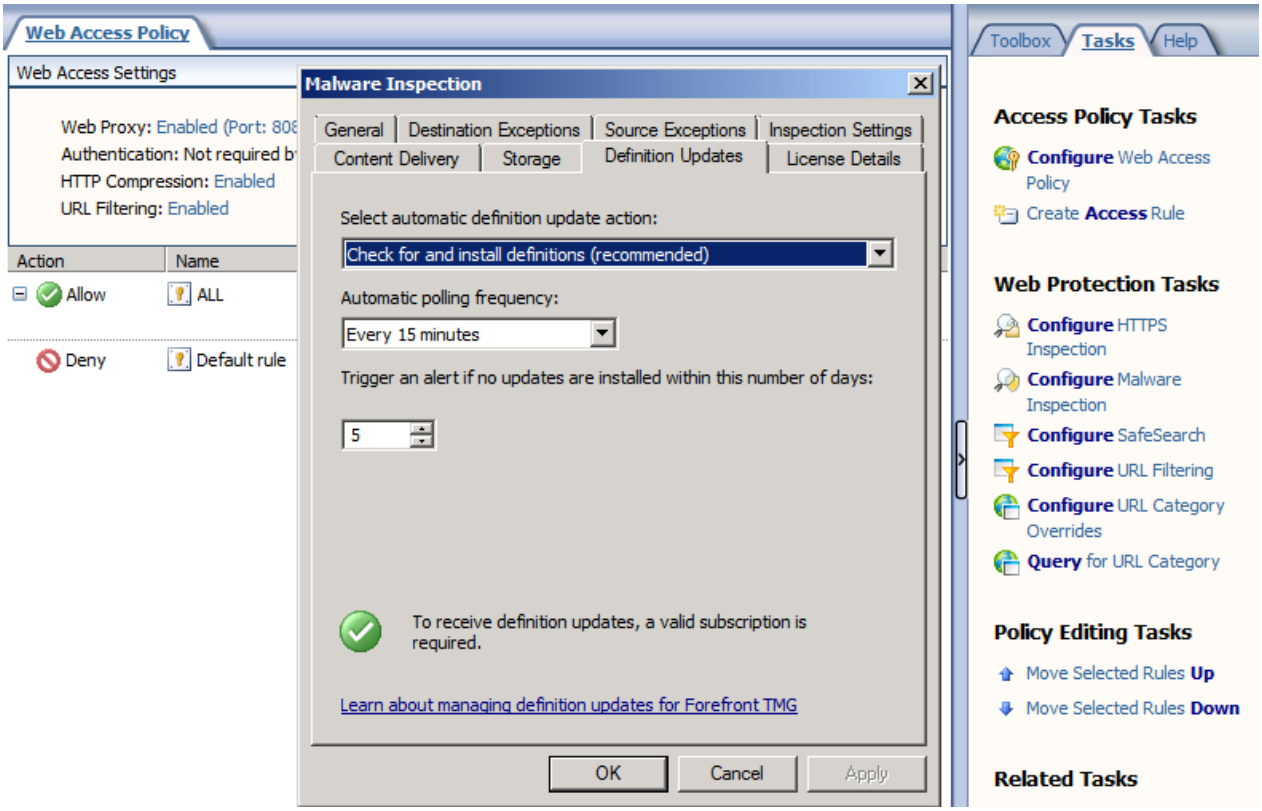

Figure 5: Malware inspection in Forefront TMG

Microsoft Forefront TMG and other products like Forefront Endpoint Protection can automatically submit information about discovered Malware during Malware inspection to the Microsoft Response Center. The Telemetry reports include the source of the Malware, the threat level defined by Microsoft, and the action that was taken by the Antimalware software (for example: Quarantine, delete). The report (when advanced membership is used) can also include traffic samples and complete URLs. The Microsoft Response Center uses this information to create new Antimalware definition files and to provide additional information how to protect against this threat. The Microsoft Telemetry service has to possible settings:

- Basic membership
- Advanced membership

Basic membership

When the Basic membership has been selected, the reports about Malware inspection results include the source of the Malware, the Malware threat level, and the action that was taken.

Advanced Membership

When the advanced membership has been selected each report also includes a traffic sample and the complete URL requested. Because the art and amount of information submitted to Microsoft can contain sensitive data, you should carefully read the privacy statement.

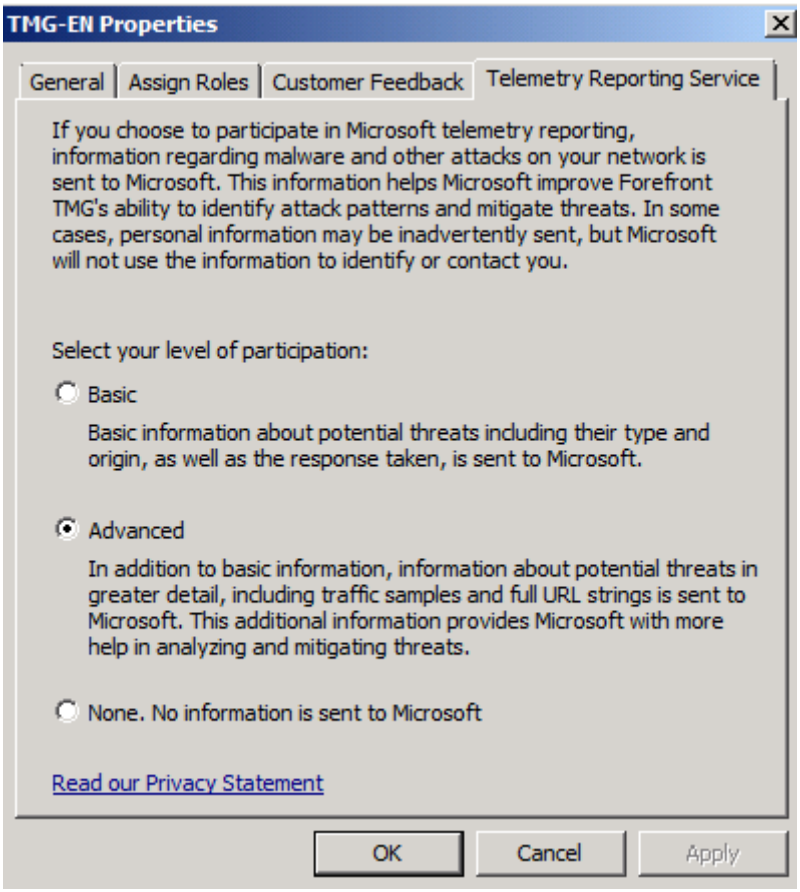

Figure 6: Forefront TMG Telemetry Reporting Service

Forefront TMG is not the only Microsoft product which can be used with the Telemetry service. The following screenshot shows the Telemetry service settings of Forefront Endpoint Protection 2010.

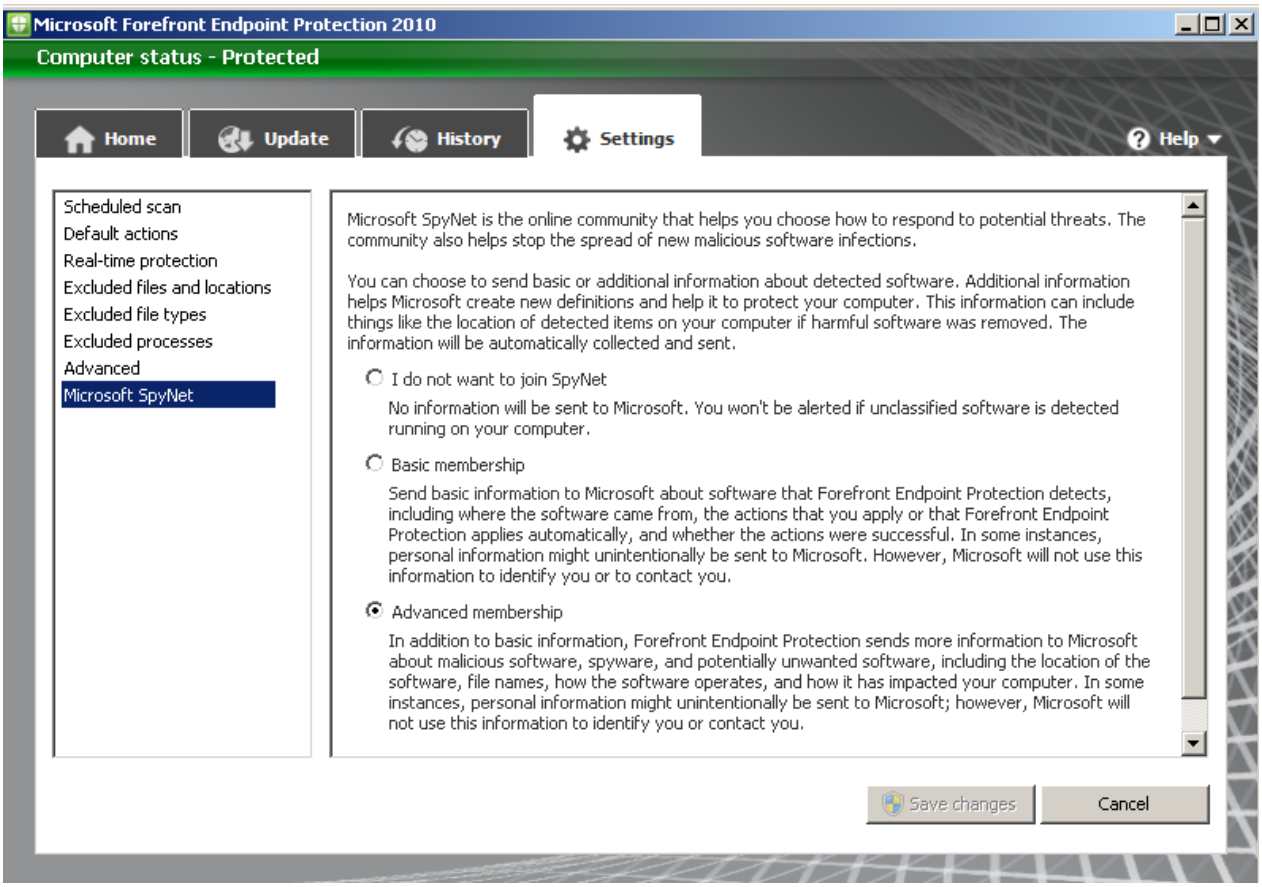

Figure 7: Forefront Endpoint Protection Telemetry Reporting Service

Microsoft Malware Protection Center (MMPC)

The Microsoft Malware Protection Center (MMPC) is your starting point to get informed about all aspects of Antimalware. The MMPC will give you the latest information about Malware and you will get a better understanding about how Malware works. It is possible to subscribe to an RSS feed to stay up to date about the latest Malware. It is also possible to download the latest definitions for Microsoft Forefront Endpoint Protection 2010 (FEP), Microsoft Forefront Client Security (FCS), Microsoft Forefront Security for Exchange (FPE), Microsoft Forefront Security for SharePoint (FSSP), Microsoft Forefront Security for Office Communication Server (FSOCS), Microsoft Security Essentials and Windows Intune if you don’t want to use the automatic update process of these products. The MMPC also gives you the possibility to submit a Malware sample to Microsoft, so that Microsoft engineers can analyse the Malware to create a new Antimalware definition update for their Antimalware products.

Figure 8: Microsoft Malware Protection Center (MMPC)

GAPA and GAPAL used by the Network Inspection System (NIS) in Forefront TMG

Forefront TMG is a vulnerability-based Intrusion Prevention System (IPS). An IPS should protect your internal network from known and unknown vulnerabilities if TMG is being used directly on the edge of the internal network on the Internet. All network traffic must flow through TMG, so Forefront TMG is the first line of defence to protect against different vulnerabilities.

An IPS is defined at two levels:

- 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 block un/known attacks at the network level to fight against vulnerabilities.

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

To create signatures for vulnerability, Microsoft uses the GAPA (Generic Application Protocol Analyzer) protocol. NIS in Forefront TMG is based on GAPA.

GAPA is a framework and platform for safe and fast low-level protocol parsing. GAPA has been architected and prototyped by Microsoft. GAPA uses GAPAL (Generic Application Protocol Analyzer Language). According to Microsoft's documentation, GAPA allows rapid creation of protocol analyzers, greatly reducing the time needed for development. You can read more about GAPA here.

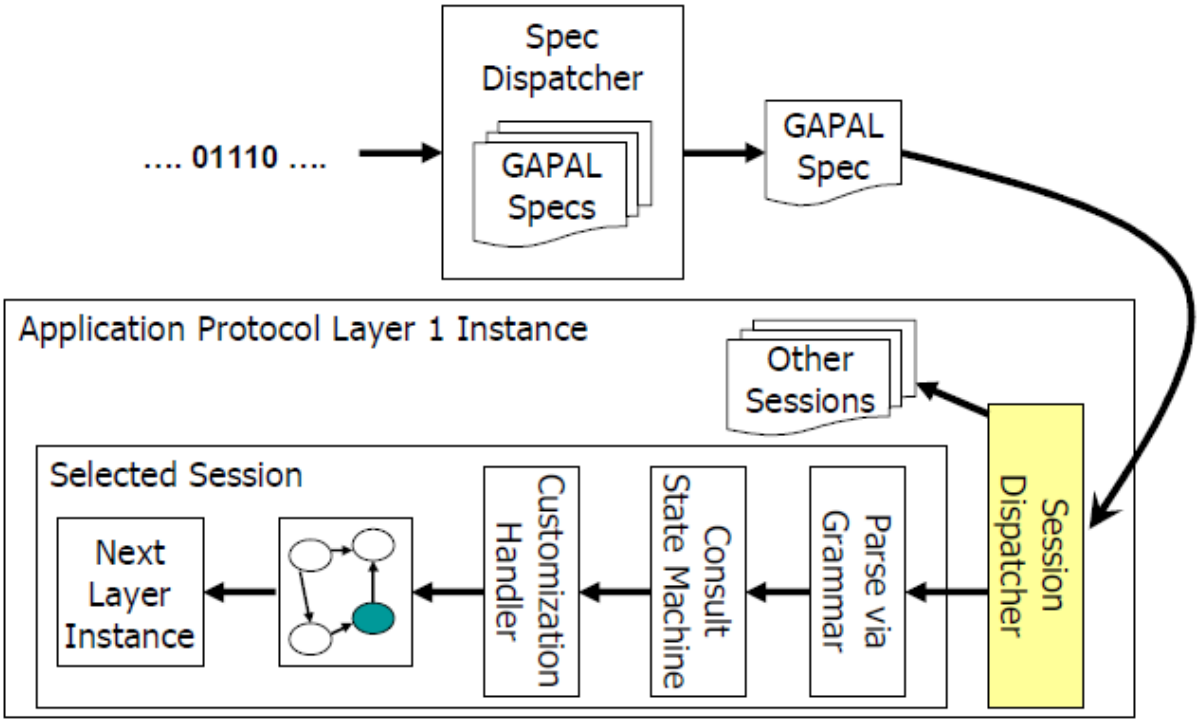

Figure 9: GAPA System architecture - Source: http://research.microsoft.com/pubs/70223/tr-2005-133.pdf

Conclusion

I hope that my article gave you a better understanding how the technologies like MRS, the Microsoft Telemetry service, and the MMPC work together to provide a better protection for your networks with the help of Microsoft Forefront TMG.

Related links

Microsoft Spynet
http://windows.microsoft.com/en-US/windows-vista/Join-the-Microsoft-SpyNet-community
Microsoft Reputation Service
http://www.microsoft.com/security/portal/mrs/
Microsoft Malware Protection Center
http://www.microsoft.com/security/portal/
Forefront TMG URL category precedence
http://blogs.technet.com/b/isablog/archive/2010/08/03/tmg-url-filtering-category-precedence.aspx
Forefront TMG – Categories for URL Filtering
http://blogs.technet.com/b/isablog/archive/2010/01/03/categories-for-url-filtering.aspx
Planning for URL Filtering
http://technet.microsoft.com/en-us/library/ee207145.aspx
GAPA and GAPAL
http://research.microsoft.com/apps/pubs/default.aspx?id=70223
MRS Categories
http://www.microsoft.com/security/portal/mrs/categories/MRS_Categories.en-us.htm
Explaining and configuring NIS (Network Inspection Service)
http://www.isaserver.org/tutorials/Explaining-configuring-NIS-Network-Inspection-Service.html