
Configuring the Forefront TMG HTTP Filter

Abstract

In this article I will show you how to configure and use the HTTP Filter of Forefront TMG to filter HTTP traffic in Firewall policy rules.

Let's begin

A simple Firewall only allows or denies access for the HTTP protocol based on source and destination IP addresses and doesn't looks deeper into the HTTP protocol to filter HTTP traffic. The HTTP protocol is often called the Universal Firewall Bypass protocol because many Firewall admins allows users from the internal network to access to the outside for the HTTP protocol. The HTTP protocol can bes used by applications to encapsulate their specific protocols into the HTTP or HTTPS protocol. Some examples for those applications are Outlook Anywhere, the Remote Desktop Gateway service and applications like Skype, Windows Live Messenger and many more which encapsulates their native protocols into the HTTP/HTTPS protocol, which allows the traffic to bypass the Firewall. With Forefront TMG it is possible to filter HTTP traffic with the HTTP filter for incoming and outgoing access and when you use the new HTTPS inspection feature of Forefront TMG you can also filter outgoing HTTPS traffic. Incoming HTTPS traffic can be filtered by Forefront TMG in Webserver publishing scenarios where the HTTPS bridging feature of Forefront TMG is used.

Let's start with some basics about the Web filters in Forefront TMG.

What is a Web filter?

A Web filter in Forefront TMG is a set of Dynamic Link Libraries (DLLs) which are based on the IIS ISAPI (Internet Server Application Programming Interface) Model
A Web filter in Forefront TMG will be loaded from the Webproxy Filter. If the Webfilter is loaded all information's will be forwarded to the Webproxy Filter. The Webproxy Filter is responsible to determine which type of events should be monitored.
Every time such events occurs the Webproxy Filter will be notified.

The following figure shows the HTTP Filter Add in of Forefront TMG.

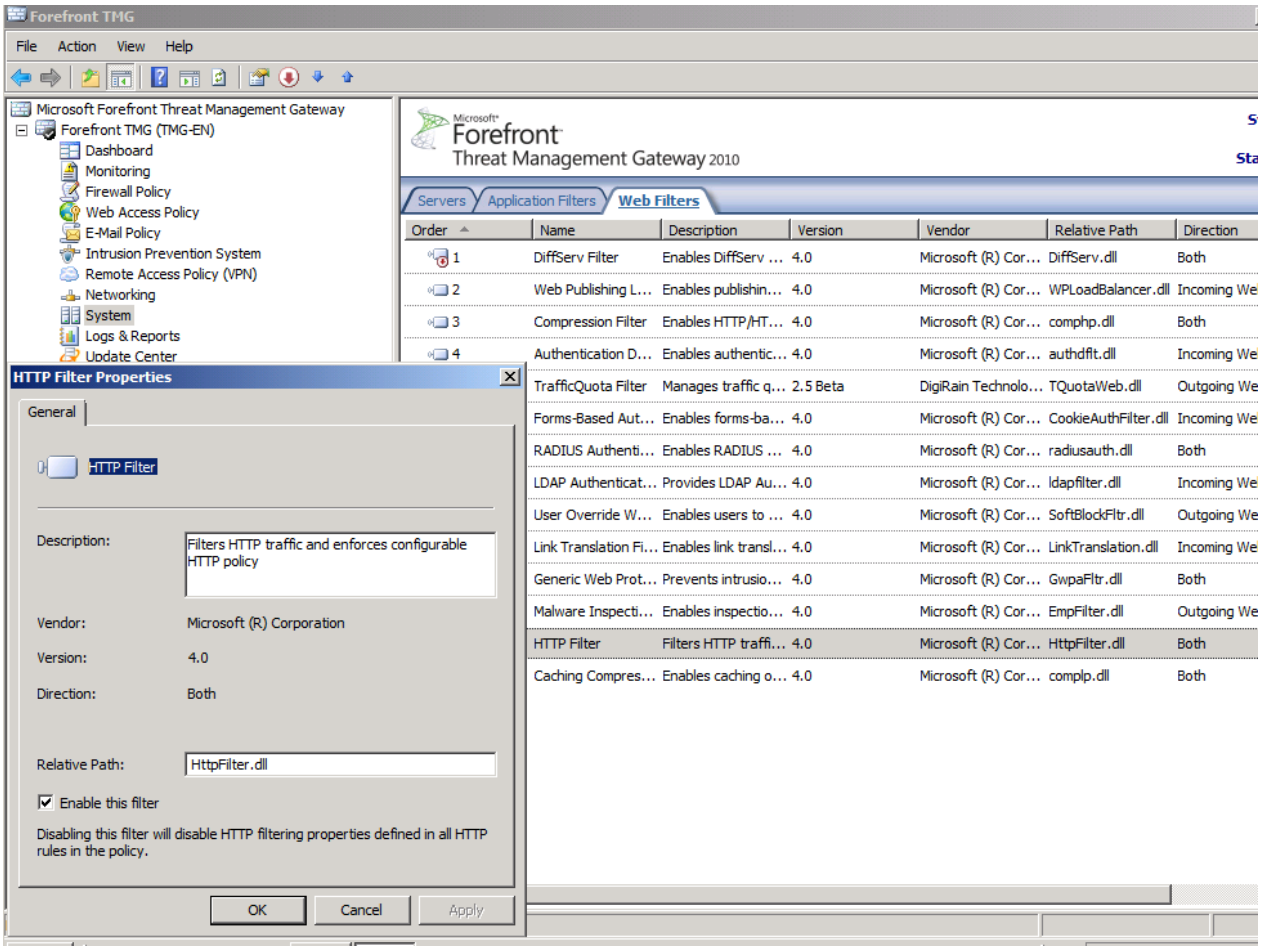

Figure 1: Forefront TMG HTTP filter Add in

Web filter functionality

The Web filter in Forefront TMG is responsible for the following tasks:

- Scanning and modifying HTTP requests
- Analyzing and protocol network traffic
- Scanning and modifying HTTP responses
- Blocking of specific HTTP responses
- Data encryption and compression

and many more.

Important:

The HTTP Filter in Forefront TMG is rule specific except the Maximum Header length setting. The Maximum Header length in Forefront TMG is the same for all Firewall rules with HTTP protocol definitions.

Attention:

The HTTP Filter in Forefront TMG is also capable to filter HTTPS traffic used in reverse web server publishing scenarios where HTTPS Bridging is used and for

outgoing HTTPS requests when the HTTPS inspection feature of Forefront TMG is activated.

HTTP Filter configuration

If you want to start configuring the HTTP filter, right click a rule that contains a HTTP protocol definition and select *Configure HTTP* from the context menu.

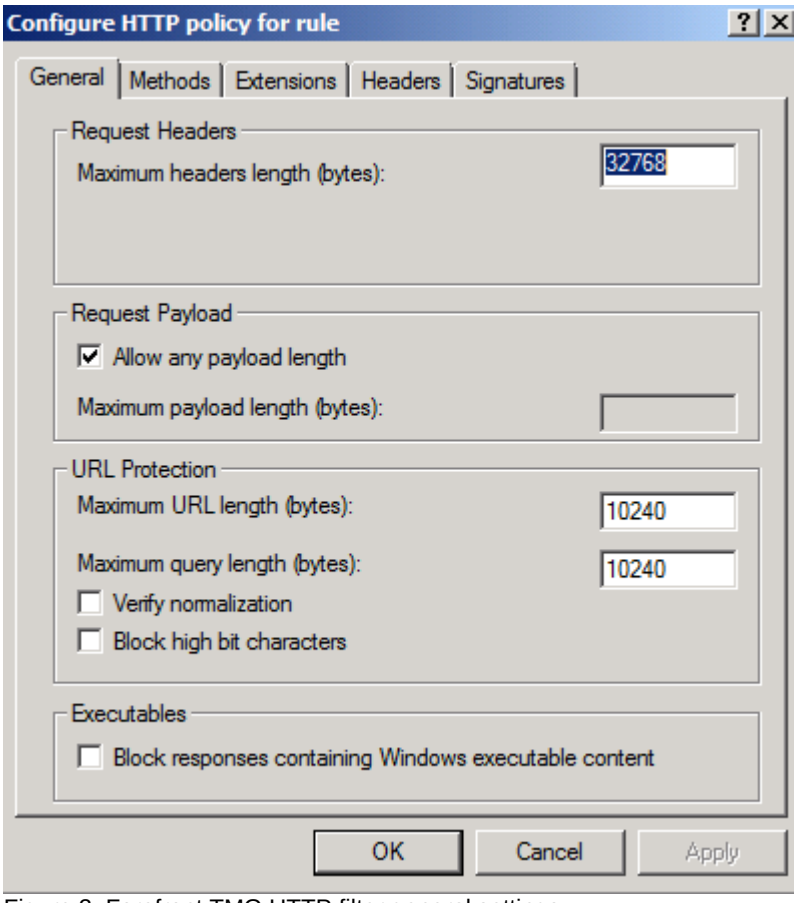

Figure 2: Forefront TMG HTTP filter general settings

On the General tab of the HTTP filter it is possible to configure the following settings:

Request Header:

Maximum Headers length (bytes):

The maximum Header length specifies the maximum number of bytes in the URL and HTTP Header for a HTTP request until Forefront TMG blocks the request.

Request Payload:

Maximum payload length (bytes):

With this option it is possible to restrict the maximum length in bytes a user can send via a HTTP POST in a Web server publishing scenario.

URL Protection:

Maximum URL Length (Bytes): The maximum length of an allowed URL
Maximum Query length (Bytes): The maximum length of an URL in the HTTP request

Verify normalization

You can select this checkbox to specify that requests with URLs containing escaped characters after normalization will be blocked. Normalization is the process where URL coded requests will be decoded. After decoding the URL the URL will be normalized again to be sure that no process is using the % character to encode a URL. If the HTTP Filter finds a difference in the URL after the second normalization the requests will be rejected.

Block high bit characters

URLs that contain Double Byte Character (DBCS) or Latin1 will be blocked if this setting is active. An active setting regulary blocks languages that require more than eight bit to display all language specific characters.

Executables

Block responses containing Windows executable content

This option blocks the download and executing of executable content like EXE files.

As a next step we should configure the allowed or blocked HTTP methods

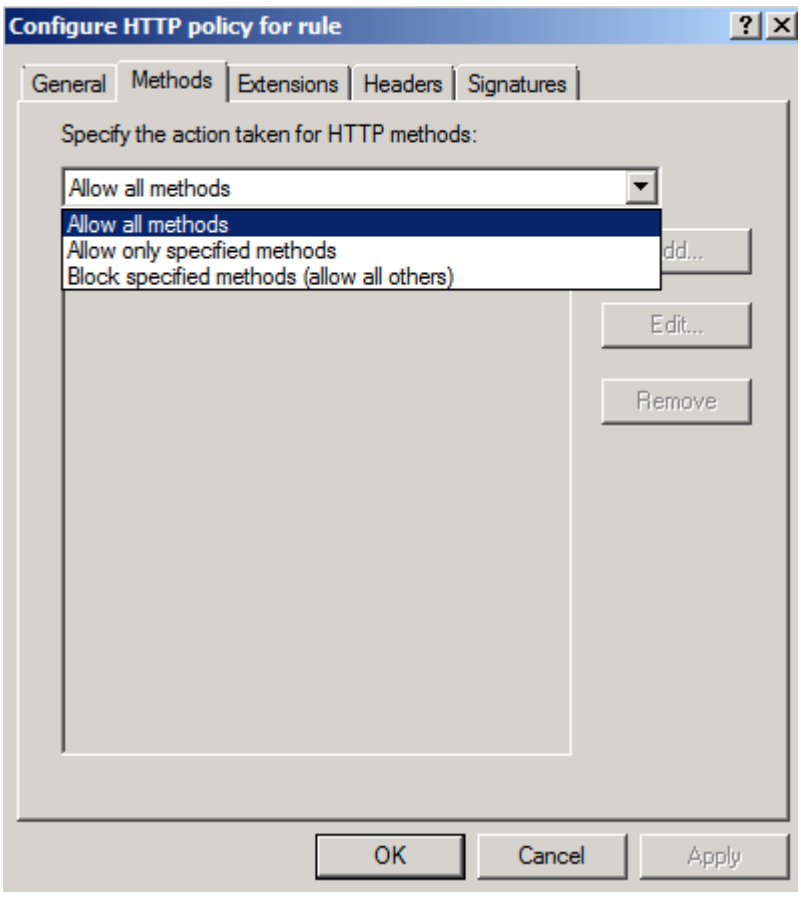

Figure 3: HTTP Methods

In this example we are blocking the HTTP POST command so that nobody can upload content on external websites.

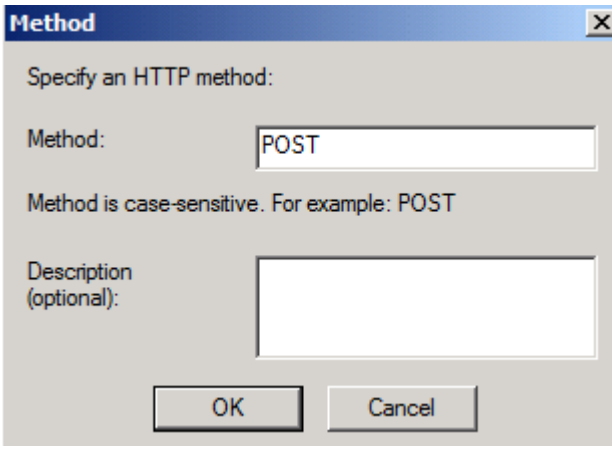

Figure 4: Block the HTTP POST method

Block executables

With this option it is possible to block or allow some specific file extensions in the specific firewall rule.

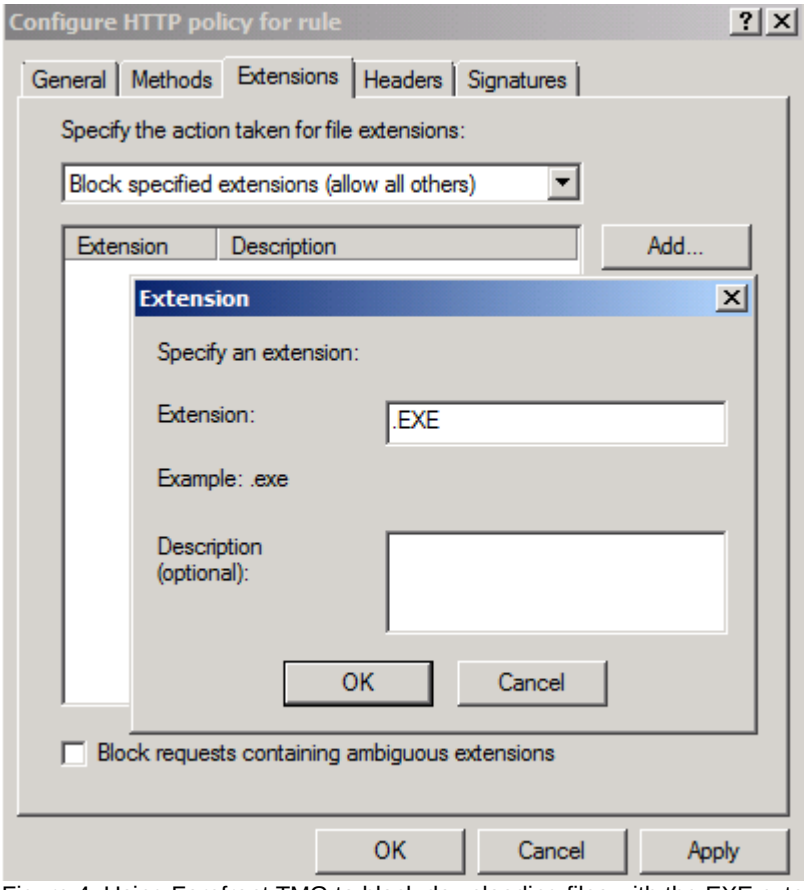

Figure 4: Using Forefront TMG to block downloading files with the EXE extension

Block requests containing ambiguous extensions

This option instructs the HTTP filter to block all file extensions which Forefront TMG cannot determine.

In this example we are blocking access to the .EXE file extension.

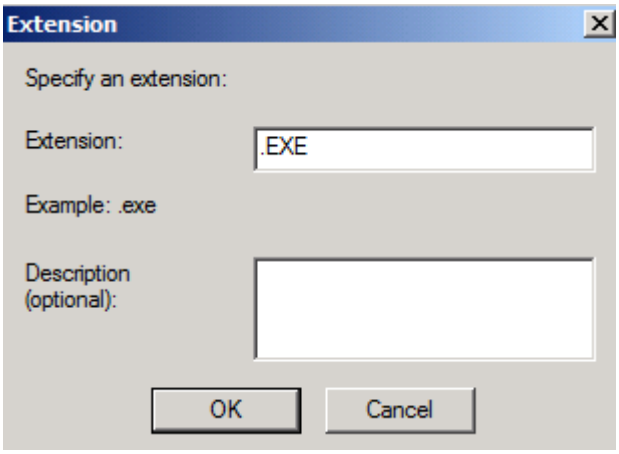

Figure 5: Blocking the .EXE file extension

HTTP Header handling

When a webclient sends requests to a web server or the web server is answering queries the first part of an answer is a HTTP request or a HTTP response. After the HTTP request or HTTP response, the client or Server sends a HTTP Header. The request Header field allows the client to send additional information to the server. HTTP Header contains information about the Browser, operating system information, and authorization details and more, the client Header uses the attribute User-Agent which determines which application is responsible for the request.

With the help of the HTTP filter it is possible to block specific HTTP Header.

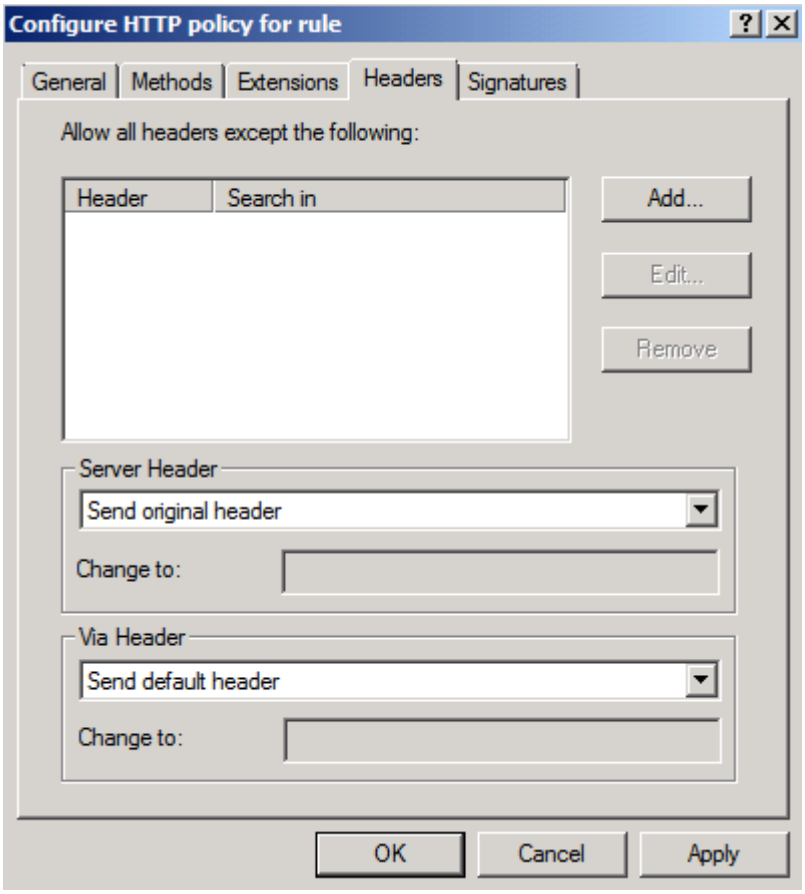

Figure 6: HTTP filter Header section

The settings in the Server Header field give Administrators the control to remove the HTTP header from the response or to modify the HTTP Header in the response and some more settings.

In the following example we are using the HTTP Header feature in Forefront TMG to block Kazaa which information resides in the request header.

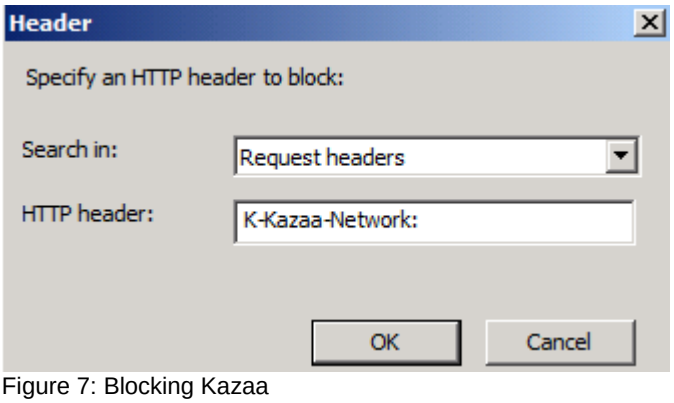

Figure 7: Blocking Kazaa

HTTP Filter signatures

An HTTP signature can exist in the HTTP body or HTTP header. You can use HTTP signatures to deny the execution from specific applications. To find a specific HTTP signature you must know which signature the application is using. There are some documents on the Internet that can give you some information about specific HTTP

signature but it is also possible to use a network sniffer to determine HTTP signatures. I will show you how to use a network sniffer later in this article.

Important:

Filtering HTTP signatures in Forefront TMG only works when the requests and responses are UTF-8 coded.

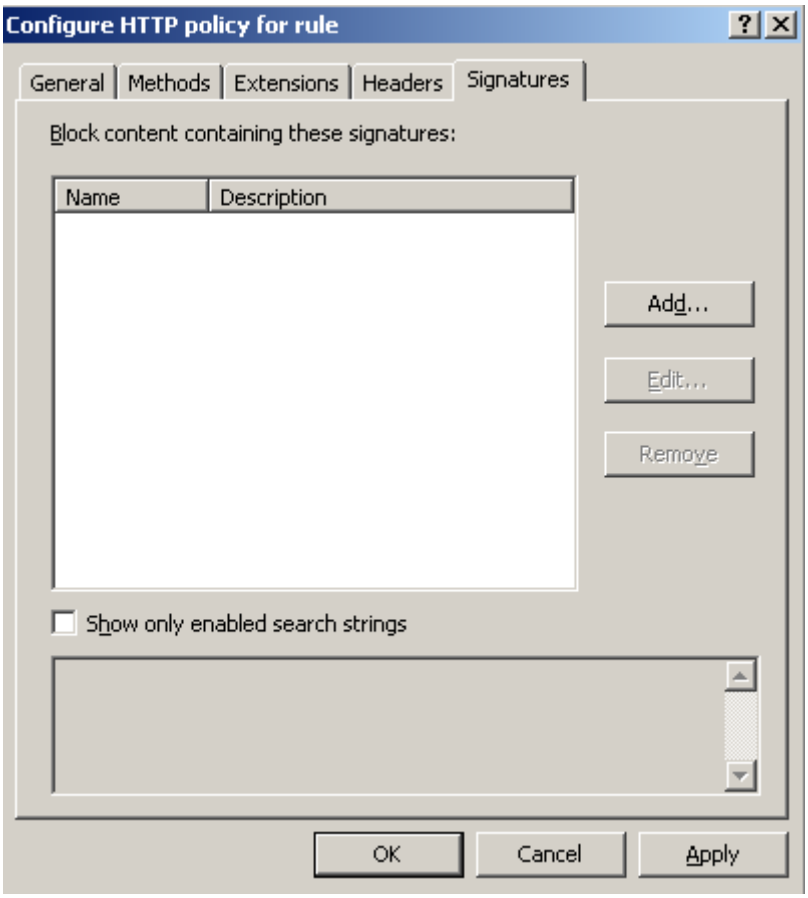

Figure 8: Blocking HTTP signatures

In the following example we are blocking the access for the Windows Live Messenger protocol.

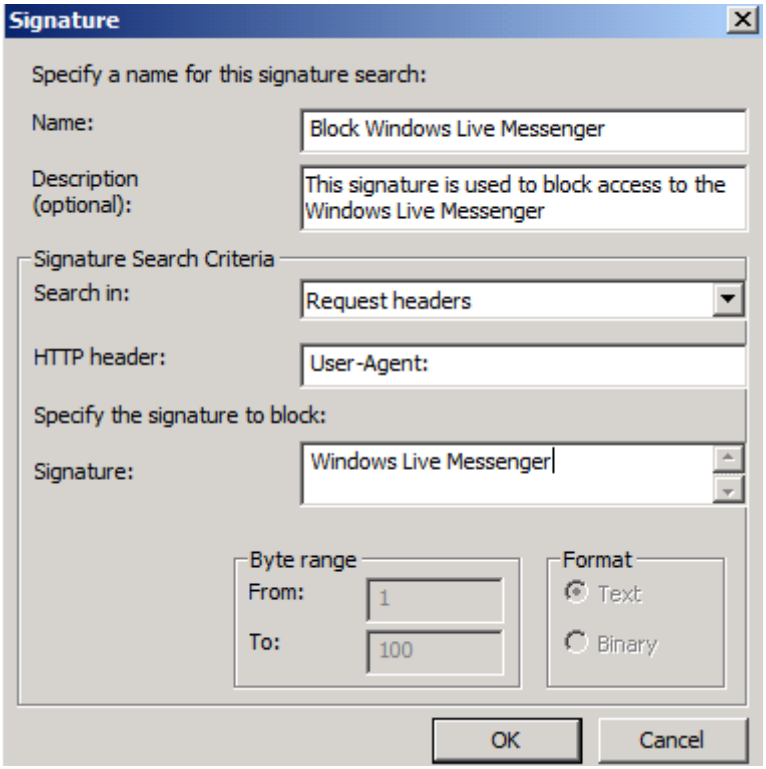

Figure 9: Windows Live Messenger Block

If you want to know more about application signatures click here.

Important:

Forefront TMG inspects only the first 100 Bytes of the request and response body. It is possible to expand the maximum number of bytes but this could result in some server performance degradation.

HTTP error message if the HTTP filter blocks some content

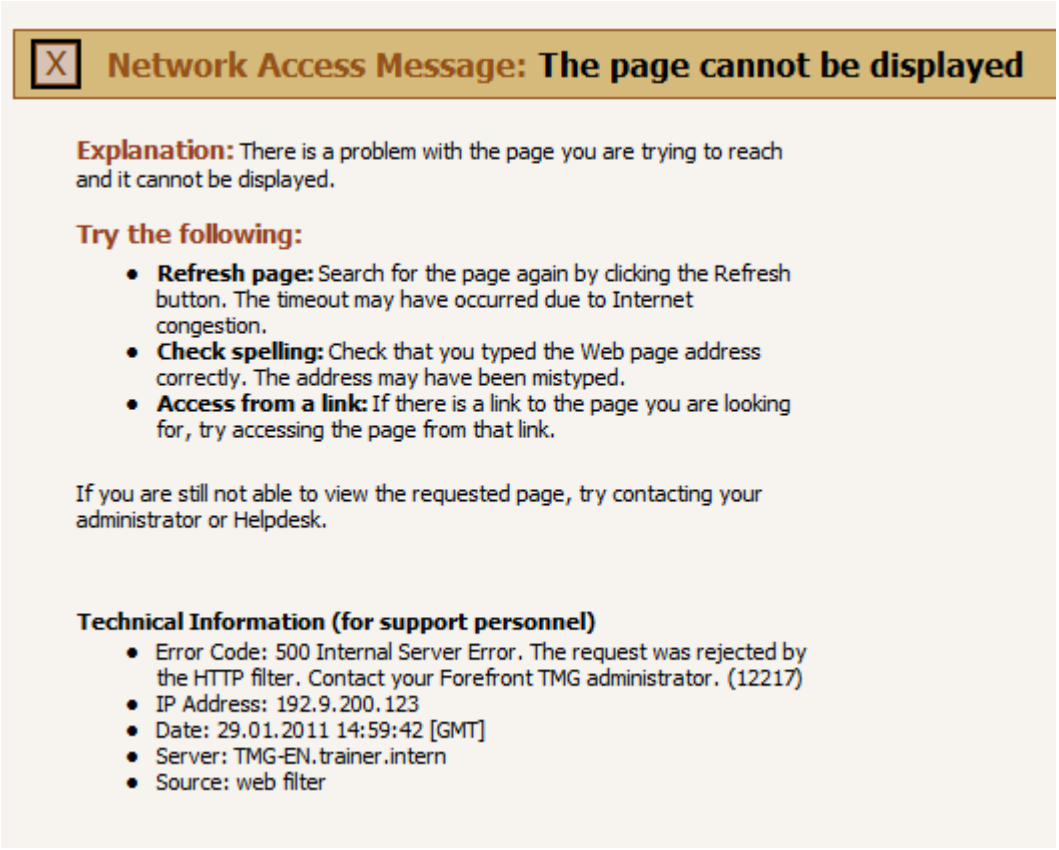

Figure 10: HTTP Filter access message

How to discover specific HTTP Header

To determine HTTP signatures that are unknown to you, it is possible to use a network sniffer like Microsoft Network Monitor (Netmon) 3.4 to trace the HTTP network traffic.

The following figure shows a sample network trace output from Microsoft Netmon 3.4, but you can use any other Network monitor like Wireshark (former Ethereal).

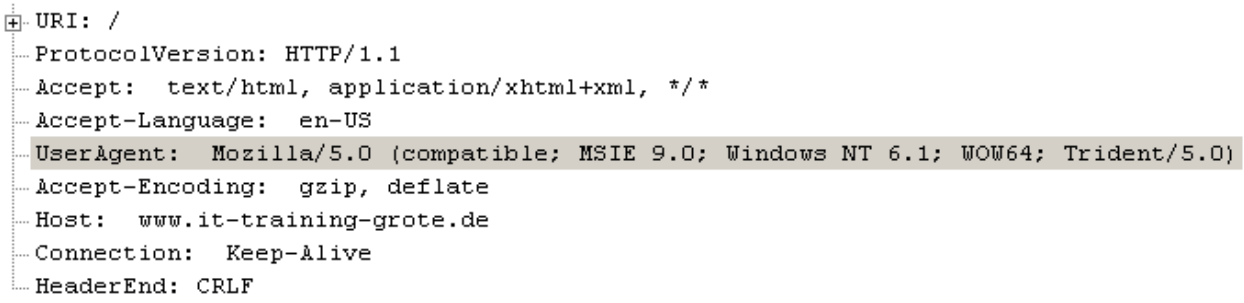

Figure 11: Netmon HTTP trace

This example shows User-Agent (Mozilla/5.0) and the signature (MSIE 9.0).

HTTPFILTERCONFIG.VBS

You can use HTTPFILTERCONFIG.VBS from the directory C:\Program Files<x86>\Microsoft Forefront TMG Tools\SDK\Samples\Admin from the Forefront TMG SDK to import and export HTTP-Filter configurations.

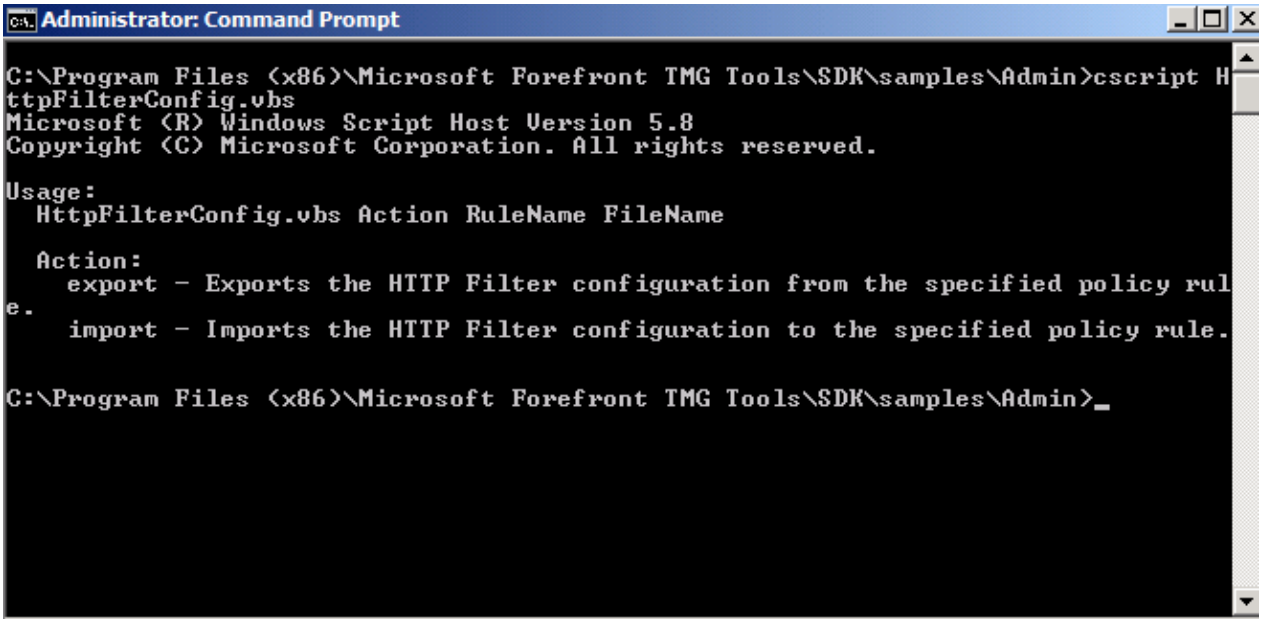

Figure 12: HTTPFILTERCONFIG.VBS from the Forefront TMG SDK

Conclusion

In this article I tried to show you how the Forefront TMG HTTP filter works. The HTTP filter in Forefront TMG is a great tool to block some dangerous content to protect against malicious code or Trojans and worms. You can also use the HTTP filter to block specific HTTP signatures, Blocking these signatures helps administrator to block some type of applications like Windows Live Messenger that can be tunnelled through HTTP if the associated standard protocol for the application is blocked through firewall restrictions.

Related Links

ISA Server 2006 HTTP filter
http://www.isaserver.org/tutorials/Configuring-ISA-Server-2006-HTTP-Filter.html
Forefront TMG SDK
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8809cfda-2ee1-4e67-b993-6f9a20e08607&displaylang=en
Common Application signatures
HTTP://www.microsoft.com/technet/prodtechnol/isa/2004/plan/commonapplicationsignatures.mspx
More about the HTTP protocol
HTTP://www.ietf.org/rfc/rfc2616.txt