Configure ISA Server 2006 HTTP Filter

In this article we will provide you with a high level overview of the ISA Server 2006 HTTP Filter. We will also show you how to use the HTTP Filter to protect your local network from several types of attacks in Webserver Publishing environment, how to prevent people

This article is an overview of the ISA Server 2006 HTTP Filter and how to use the HTTP Filter to protect your local network.

In this article we will provide you with a high level overview of the ISA Server 2006 HTTP Filter. We will also show you how to use the HTTP Filter to protect your local network from a number of attacks in a Webserver Publishing environment, how to prevent users from using the Universal Firewall Bypass protocol (HTTP) to bypass the wall. fire. This type of looping is carried out for network traffic such as Microsoft Live Messenger, Yahoo Messenger or similar components that can use HTTP instead of their natural protocols. To fully understand the concept and technology of the HTTP protocol, you should refer here.

Now let's start with some Webfilter basics in ISA Server 2006.

What is Webfilter?

A Webfilter (ie Web filter) in ISA Server 2006 is a set of dynamic link libraries (DDLs) based on the IIS Internet Server Application Programming Interface (IIS ISAPI) model.

Webfilter in ISA Server 2006 is also loaded from Webproxy Filter. Every time you use Webfilter, all information will be sent to the Webproxy Filter. The Webproxy Filter is responsible for determining what type of event will be monitored. Every time these events appear, Webproxy Filter will be notified.

You will see in the illustration below the Add-in component of the HTTP Filter on ISA Server 2006.

Figure 1 : Add-in component supports HTTP filter in ISA Server 2006 HTTP

Webfilter function

Webfilter in ISA Server 2006 is responsible for performing the following tasks:

• Scan and edit HTTP requests.
• Analysis of network traffic.
• Scan and edit HTTP responses.
• Eliminate some specific HTTP responses.
• Encrypt and compress data.

There are also many other functions that are not very important, so we are not easy to list here.

Important :
The HTTP Filter in ISA Server 2006 has a number of specific rules, except for the maximum length set for the Header. The maximum length for Header (Maxium Header) follows all the rules in the firewall with HTTP protocol definitions like other components.

Noteworthy :
The HTTP Filter in ISA Server 2006 is also capable of filtering HTTPS traffic but only in case of comparison Web Servers using HTTPS Bridging. If you want to check that HTTPS is about to expire via ISA Server 2006 HTTP filters, you must use the software developed by the third party.

Configure the HTTP Filter filter

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

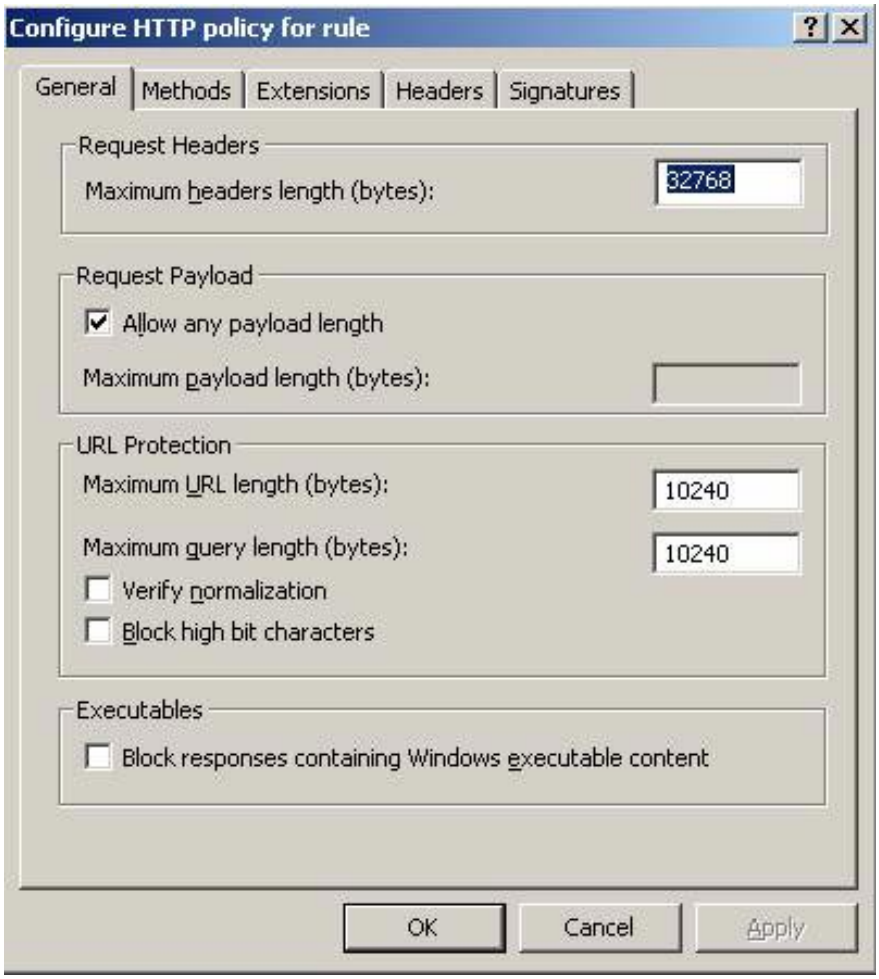

Figure 2 : General settings for ISA Server 2006 HTTP filters.

Request Header

Maximum Headers length (bytes) : is the maximum number of bytes for an HTTP request in the URL and HTTP Header until ISA Server removes the request.

Request Payload

Maximum payload length (bytes) : With this option you can limit the maximum number of bytes for users when sending requests such as HTTP POST in the Web Server environment.

URL-Protection

Maximum URL Length (Bytes) : The maximum length of a URL is allowed.

Maximum Query length (Bytes) : the maximum length of a URL in an HTTP request.

Verify normalization

You can select this check box to specify the URL path requirements containing uppercase characters after the

lowercase letters and will be replaced with lowercase letters. Normalization is the process of decoding encrypted URL requests. After decoding, the URL will be normal again to make sure that the program does not use the% character when coding the URL. If the HTTP Filter finds a different point in the URL after the second normalization, the requests will be removed.

Block High bit character

URL paths containing Double-byte Character (DBCS) or Latin1 will be removed if this setting is enabled. A normal trigger setting will remove languages ??that require more than 8 bits in the character display.

Executables

Remove responses that contain Windows executable content. This option eliminates the download and execution of executable content such as EXE files.

Next we will configure the allowed or removed HTTP methods.

Figure 3 : HTTP methods

In this example we are removing the HTTP POST command so no one can upload content to external websites.

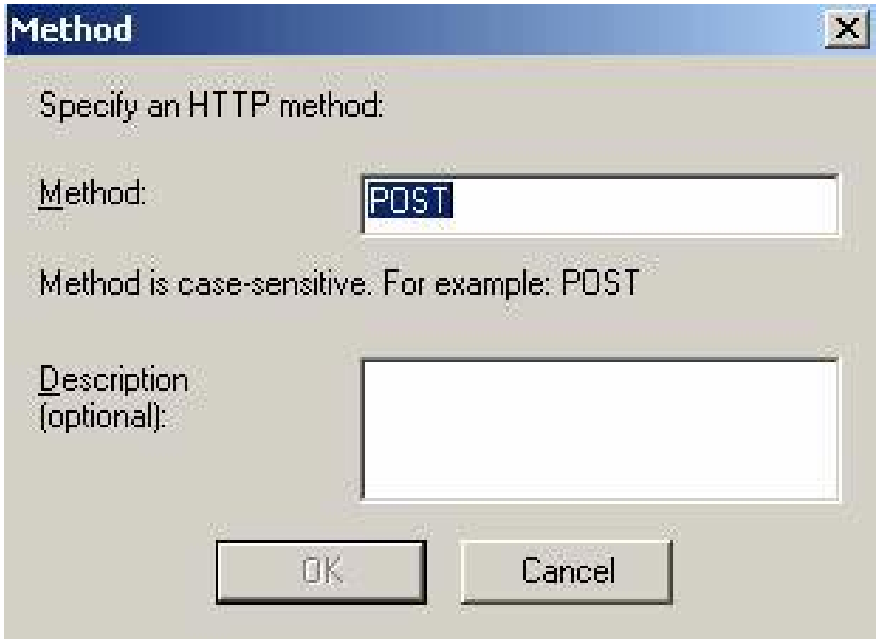

Figure 4

Remove executables

With this option you can remove or allow some specific file extensions in the Firewall (Firewall) rule.

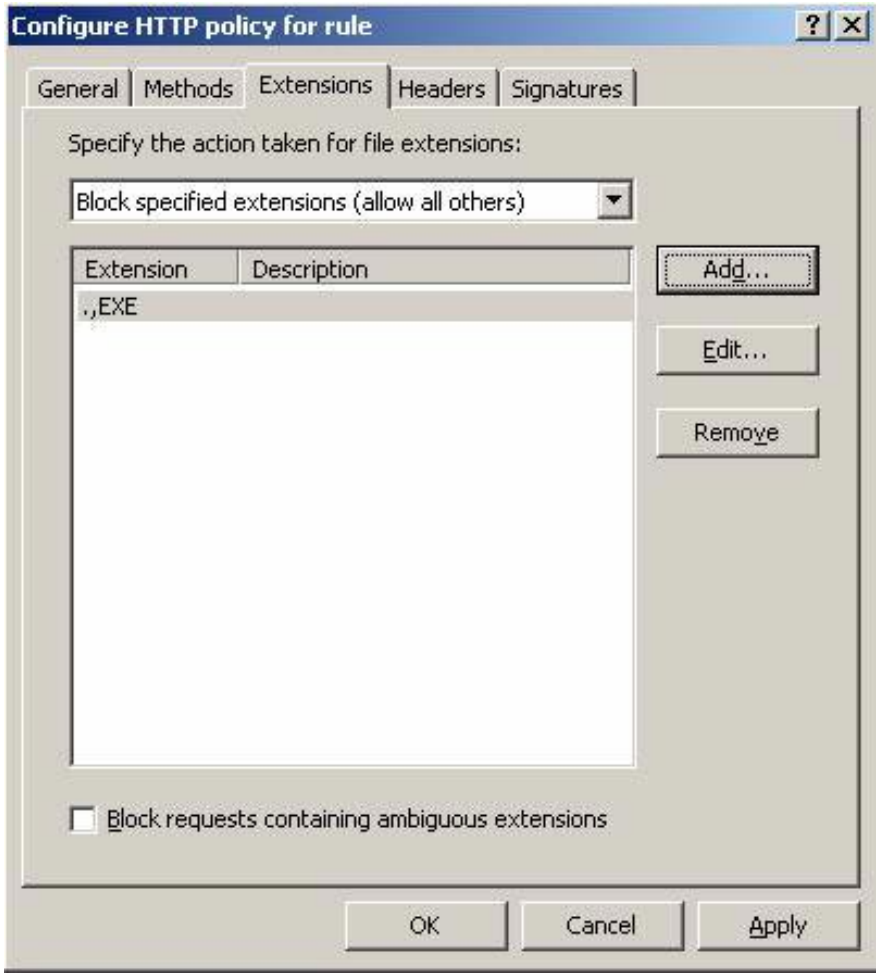

Figure 5 : Use ISA Server 2006 to remove some file extensions

Remove requests that contain vague extension names

This option instructs the HTTP filter to remove all extended file names ISA Server 2006 cannot be identified.

In this example we will remove access to the .EXE file extension name.

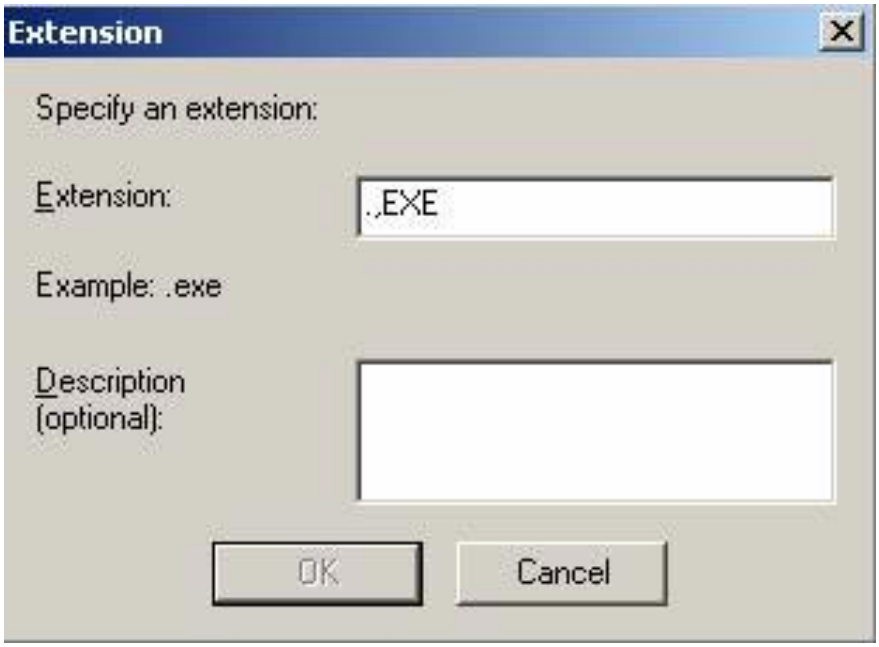

Figure 6 : Removing the extension file name .EXE

HTTP Header control

When a Web Client sends a request to the Web Server or the Web Server responds to the request, the first part of the answer is an HTTP request or HTTP response. After the HTTP request or HTTP response, Client or Server sends HTTP Header. The Request Header field allows the Client to send additional information to the Server. HTTP Header contains information about browsers, operating systems and licensing details . The client Header uses the User-Agent distribution to determine which application is responsible for executing the request.

With the help of the HTTP Filter, you can remove certain HTTP Headers if you want.

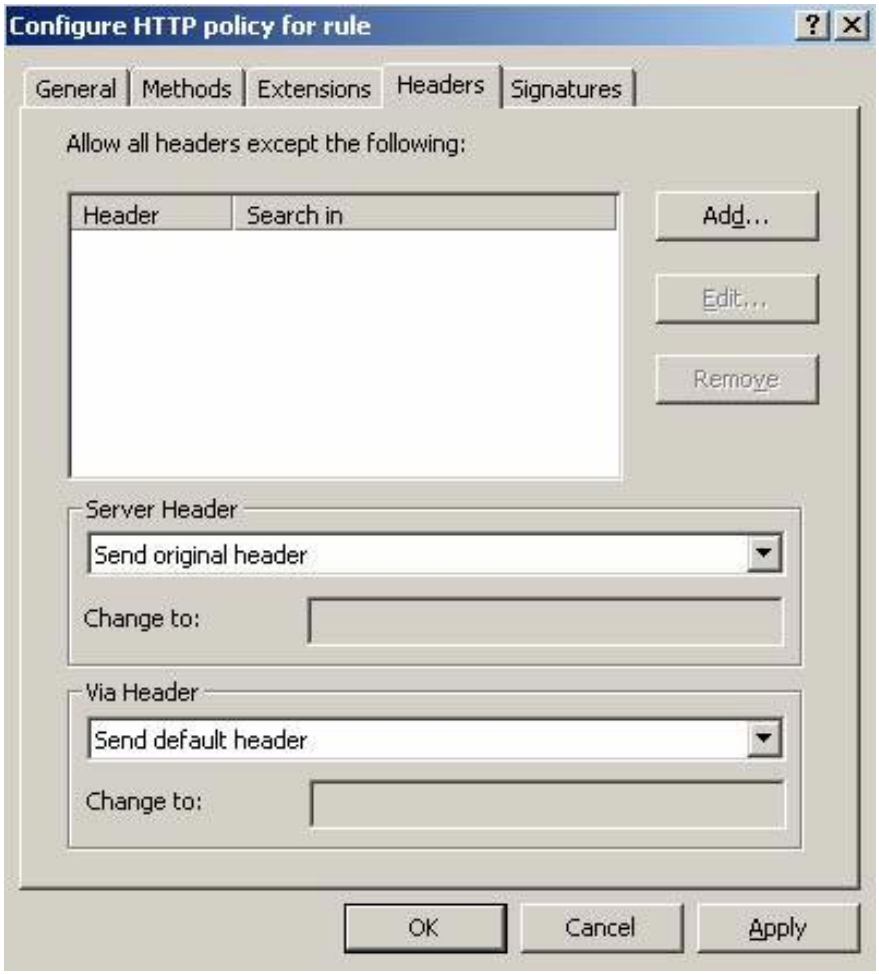

Figure 7 : Header section of the HTTP Filter filter.

The settings in the Server Header field give the administrator the ability to control the removal of HTTP Headers or edit HTTP Headers in replies and some other settings.

In the example below we use the HTTP Header component in ISA Server 2006 to remove Kazaa, the information is on the Request Header.

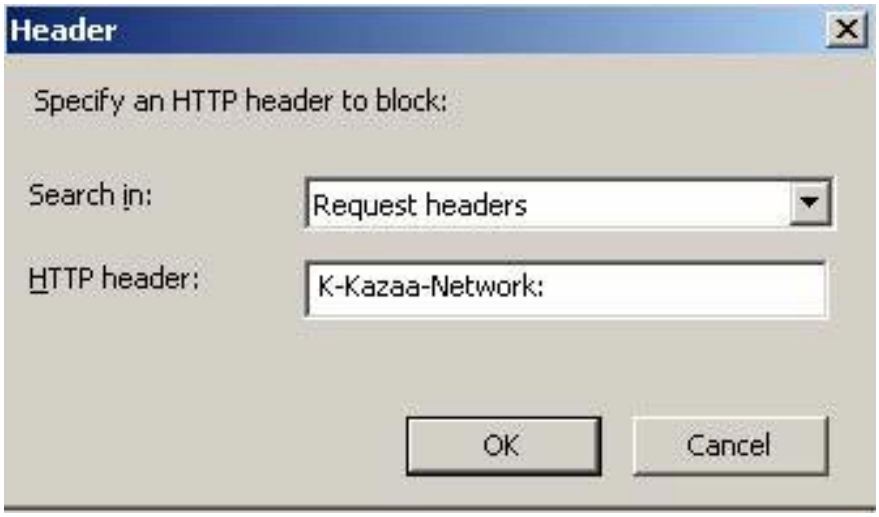

Figure 8 : Eliminate Kazaa

Symbols in HTTP Filter

An HTTP symbol may exist in the HTTP body or the header. You can use HTTP symbols to deny execution on specific applications. To find a specific HTTP symbol, you must know which signature is used for which application. Some documents on the Internet can help you get more information about HTTP symbols, but you can also use network sniffer to identify these symbols. I will show you how to use the network sniffer below.

Important :
Filtering HTTP symbols in ISA Server 2006 can only be performed when requests and responses are UTF-8 encoded.

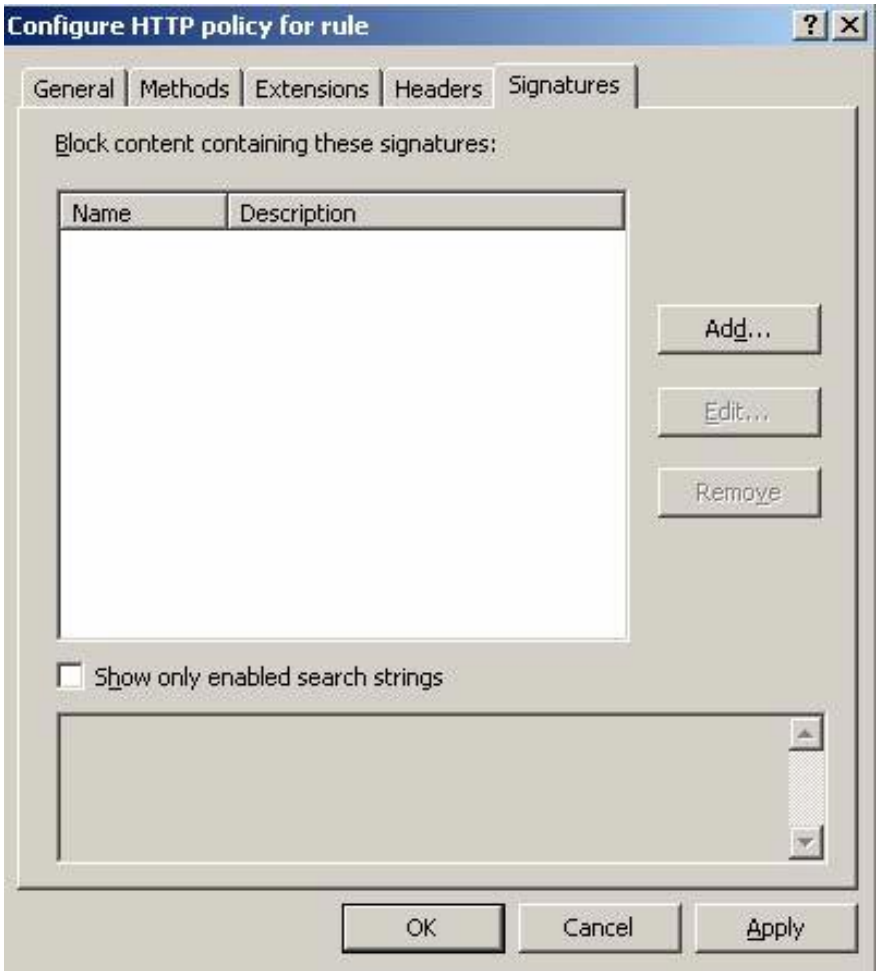

Figure 9 : Removing HTTP symbols

In the example below we will remove access to the Windows Live Messenger protocol.

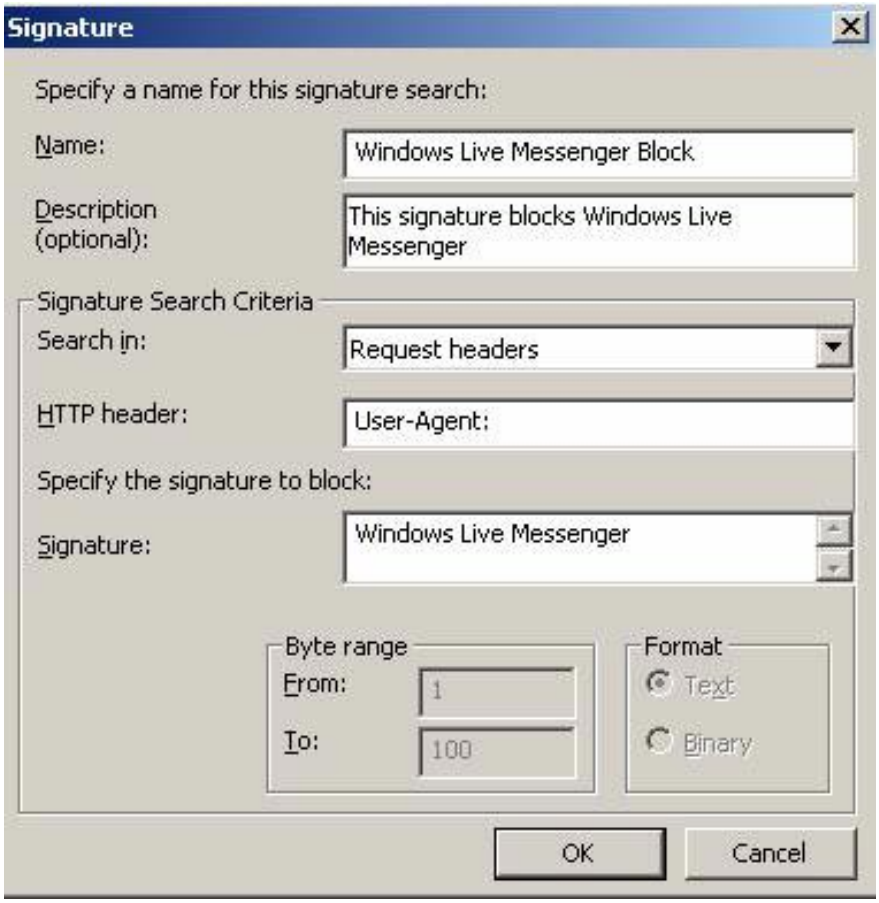

Figure 10 : Remove Windows Live Messenger

If you want to know more about application signs, please click here.

Important :
ISA Server 2006 only checks the first 100 bytes in the request and response body. You can increase the maximum number of bytes but this will make some Server implementations less effective.

HTTP error message if HTTP Filter removes content

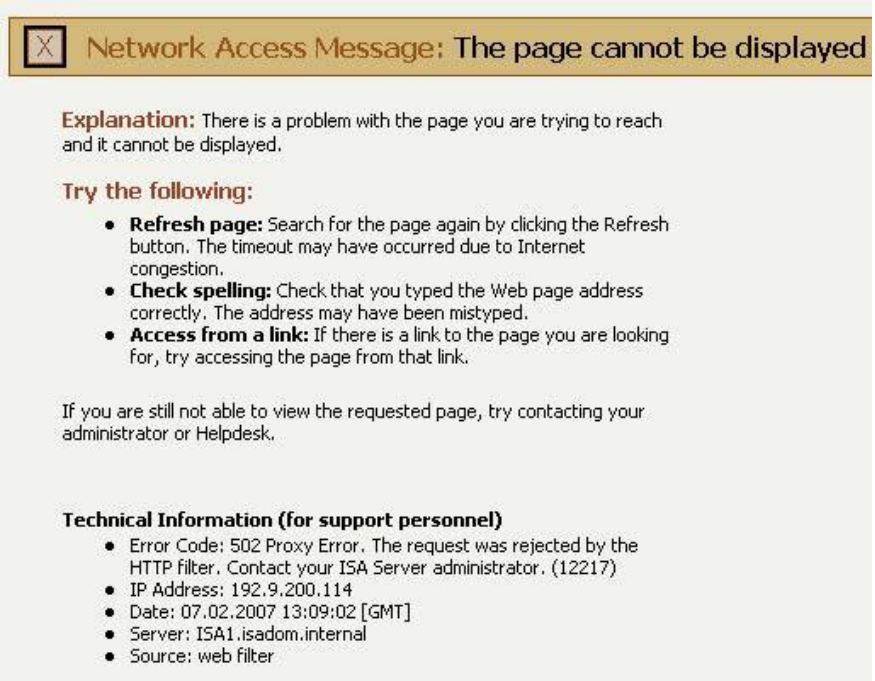

Figure 11 : Notice of HTTP Filter access

Find out how specific HTTP Headers are

To find unknown HTTP symbols, you can use a network sniffer like Windows Netmon 3.0 to detect HTTP network traffic.

The illustration below shows a sample network pattern detection on Microsoft Netmon 2.0, but you can use any other network monitoring program such as Wireshark (formerly Ethereal).

Figure 12 : Detecting Netmon HTTP

This example provides a type request (GET), requires HTTP Header (HTTP / 1.1) User-Agent (Mozilla / 4.0) and a symbol (MSIE 6.0).

HTTPFILTERCONFIG.VBS

You can use HTTPFILTERCONFIG.VBS from directory C: PROGRAMMEMICROSOFT ISA SERVER 2006 SDKSDKSAMPLESADMIN on the ISA Server 2006 SDK to import and export HTTP-Filter configurations.

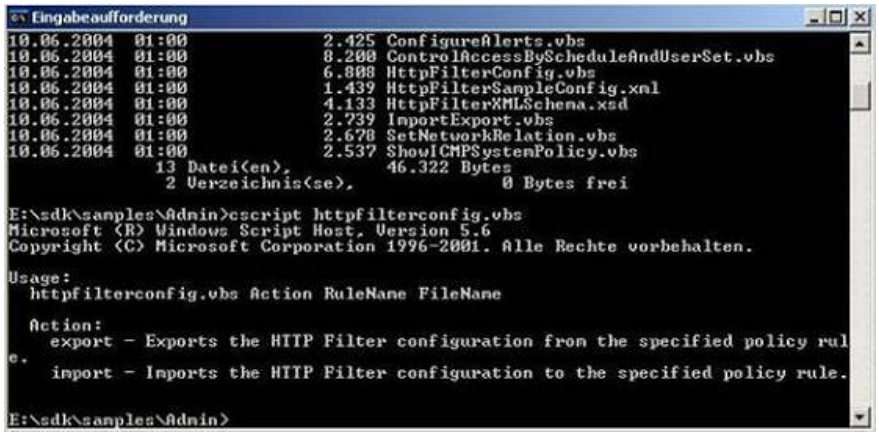

Figure 13 : HTTPFILTERCONFIG.VBS on the ISA 2006 SDK

Conclude

In this article we learned how the ISA Server 2006 HTTP filter works. The HTTP Filter in ISA Server 2006 is a great tool to remove some dangerous content to protect against malicious code. or Trojan, worm. You can also use the HTTP Filter to remove specific HTTP symbols. Removing these symbols will help administrators restrict certain types of applications such as Windows Live Messenger. These types of applications are created from HTTP if the protocol is normally removed by restrictive portions of the firewall.