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.

E Forefront TMG								ļ
File Action View He	elp							
🗢 🔿 🖄 🖬 🛛	🗊 🖻 🔮 🖲 🐐 🔹							
Microsoft Forefront The	reat Management Gateway IG-EN)	Forefre	ont					5
Monitoring		Threat N	lanagement Ga	teway 2010				Sta
Firewall Policy	.t	Servers Applic	ation Filters	Filters				
E-Mail Policy	ысу	Order 🔺	Name	Description	Version	Vendor	Relative Path	Direction
Thrusion Preve	ention System	ି 🐻 1	DiffServ Filter	Enables DiffServ	4.0	Microsoft (R) Cor	DiffServ.dll	Both
Remote Access Apple Networking	s Policy (VPN)	• = 2	Web Publishing L	Enables publishin	4.0	Microsoft (R) Cor	WPLoadBalancer.dll	Incoming We
System		viii 3	Compression Filter	Enables HTTP/HT	4.0	Microsoft (R) Cor	comphp.dll	Both
Update Center	S	o 4	Authentication D	Enables authentic	4.0	Microsoft (R) Cor	authdflt.dll	Incoming We
HTTP Filter Properties		×	TrafficQuota Filter	Manages traffic q	2.5 Beta	DigiRain Technolo	TQuotaWeb.dll	Outgoing We
General			Forms-Based Aut	Enables forms-ba	4.0	Microsoft (R) Cor	CookieAuthFilter.dll	Incoming We
			RADIUS Authenti	Enables RADIUS	4.0	Microsoft (R) Cor	radiusauth.dll	Both
0 HTTP Filter			LDAP Authenticat	Provides LDAP Au	4.0	Microsoft (R) Cor	ldapfilter.dll	Incoming We
			User Override W	Enables users to	4.0	Microsoft (R) Cor	SoftBlockFltr.dll	Outgoing We
Description:	Filters HTTP traffic and enforces of	onfigurable	Link Translation Fi	Enables link transl	4.0	Microsoft (R) Cor	LinkTranslation.dll	Incoming We
	HTTP policy		Generic Web Prot	Prevents intrusio	4.0	Microsoft (R) Cor	GwpaFltr.dll	Both
Vandari	Microsoft (P) Corporation		Malware Inspecti	Enables inspectio	4.0	Microsoft (R) Cor	EmpFilter.dll	Outgoing We
venuor.			HTTP Filter	Filters HTTP traffi	4.0	Microsoft (R) Cor	HttpFilter.dll	Both
Version:	4.0		Caching Compres	Enables caching o	4.0	Microsoft (R) Cor	complp.dll	Both
Direction:	Both							
Relative Path:	HttpFilter.dll							
Enable this filter								
Disabling this filter will a rules in the policy.	disable HTTP filtering properties defi	ned in all HTTP						
	OK Cancel	Apply						
I			1					

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.

Configure HTTP policy for rule	? ×
General Methods Extensions Headers Signatures	
Request Headers Maximum headers length (bytes):	32768
Request Payload	
Allow any payload length	
Maximum payload length (bytes):	
URL Protection	
Maximum URL length (bytes):	10240
Maximum query length (bytes):	10240
Verify normalization	
Block high bit characters	
Executables	
Block responses containing Windows executable of	content
OK Cancel	Apply

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

Configure	HTTP pol	icy for ru	e				?	×
General	Methods	Extension	s Headers	Signatures				
Specif	fy the action	n taken for	HTTP method:	S:				
Allow	all methods	3				-		
Allow Allow Block	all methods only specifi specified n	ed method nethods (al	s low all others)			dd Edit		
						Remove		
,								
		[ок	Cancel		App	y	

Figure 3: HTTP Methods

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

Method	<u>×</u>
Specify an HTTP m	nethod:
Method:	POST
Method is case-sen	sitive. For example: POST
Description (optional):	
	OK Cancel

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.

Configure HTTP policy for rule					?)
General M	lethods	Extensions	Headers	Signatures	
Specify th	he action	n taken for fil	e extension:	s:	
Block sp	ecified	extensions (a	llow all othe	rs) 💌	
Extensi	on	Description			Add
	Extensi	on			×
	Specify	/ an extension	n:		
	Extensi	ion:	.EXE		
	Example: .exe				
	Descrip (option	otion al):	Г		
			ок	Cancel	
E Block	reques	ts containing	ambiguous	extensions	
			ок	Cancel	Apply

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.

Extension		x
Specify an extension:		
Extension:	.EXE	-
Example: .exe		
Description (optional):		
ОК	Cancel	

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.

Configure HTTP policy for rule	? ×
General Methods Extensions Headers Signatures	
Allow all headers except the following:	
Header Search in	Add
	Edit
	Remove
- Server Header	
Send original header	-
Change to:	
Via Header	
Send default header	•
Change to:	
OK Cancel	Apply

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.

Header		X
Specify an HTTP he	eader to block:	
Search in:	Request headers	•
HTTP header:	K-Kazaa-Network:	
	OK	Cancel

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.

Configure HTTP po	onfigure HTTP policy for rule			
General Method:	s Extensions Headers	Signatures		
<u>B</u> lock content co	ntaining these signatures:			
Name	Description			
			Ad <u>d</u>	
			<u>E</u> dit,	
			Remo <u>v</u> e	
l □ S <u>h</u> ow only e	nabled search strings			
			<u> </u>	
			_	
	ОК	Cancel	Apply	

Figure 8: Blocking HTTP signatures

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

Signature		X
Specify a name for th	is signature search:	
Name:	Block Windows	Live Messenger
Description (optional):	This signature i Windows Live N	s used to block access to the lessenger
Signature Search Crit	eria	
Search in:	Request heade	ers 💌
HTTP header:	User-Agent:	
Specify the signature	to block:	
Signature:	Windows Live I	Messenger
	Byte range	Format
	From: 1	🖲 Text
	To: 100	C Binary
		OK Cancel

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

X Network Access Message: The page cannot be displayed
Explanation: There is a problem with the page you are trying to reach and it cannot be displayed.
Try the following:
 Refresh page: Search for the page again by clicking the Refresh button. The timeout may have occurred due to Internet conception
 Check spelling: Check that you typed the Web page address correctly. The address may have been mistyped.
 Access from a link: If there is a link to the page you are looking for, try accessing the page from that link.
If you are still not able to view the requested page, try contacting your administrator or Helpdesk.
 Technical Information (for support personnel) Error Code: 500 Internal Server Error. The request was rejected by the HTTP filter. Contact your Forefront TMG administrator. (12217) IP Address: 192.9.200.123 Date: 29.01.2011 14:59:42 [GMT] Server: TMG-EN.trainer.intern Source: web filter

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 <u>Wireshark</u> (former Ethereal).

```
ProtocolVersion: HTTP/1.1
ProtocolVersion: HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
UserAgent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: www.it-training-grote.de
Connection: Keep-Alive
HeaderEnd: CRLF
```

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 <u>SDK</u> 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/commonapplicationsig natures.mspx More about the HTTP protocol HTTP://www.ietf.org/rfc/rfc2616.txt