Overview about the Redline Software ISA Server / TMG Toolkit

Abstract

In this article, I will show you how to use the Redline Software ISA Server / TMG Toolkit. I will give you a high-level overview about the most of the tools which comes with the Toolkit.

Let's begin

Redline Software released a free ISA Server / TMG Toolkit that extends the ISA Server capabilities by a several of different tools.

The ISA Server Toolkit contains several useful tools. I copied and pasted the overview of these tools from the Redline Software website. We will go into details by explaining most of these tools.

Config Viewer

Tool designed for the offline analysis of the Microsoft ISA Server (Forefront TMG) configuration.

Keywords Finder

Tool designed to analyze Microsoft ISA Server (Forefront TMG) log files in order to find out what keywords users enter in various search engines.

MDF Viewer

Tool designed to analyze and view Microsoft ISA Server (Forefront TMG) log files stored in the MDF format.

Pascal Script Studio

Tool designed to create, edit, run and debug administration scripts in the Pascal language.

Config Backup

Web filter for Microsoft ISA Server (Forefront TMG) designed to automatically back up the ISA Server (Forefront TMG) configuration.

Response Modifier

Web filter for Microsoft ISA Server (Forefront TMG) designed to automatically replace substrings on returned HTML pages.

Client Host Name Resolver

Web filter for Microsoft ISA Server (Forefront TMG) designed to automatically resolve client IP addresses into DNS computer names and to automatically add new items to the Computers list of the Microsoft ISA Server (Forefront TMG) console.

Client User Name Resolver

Web filter for Microsoft ISA Server (Forefront TMG) designed to automatically convert logins into complete usernames with the help of Active Directory.

URL Normalizer

Web filter for Microsoft ISA Server (Forefront TMG) designed to automatically convert the IP addresses of visited sites into their text representation.

Advanced Web Routing Rules

Web filter for Microsoft ISA Server (Forefront TMG) designed to redirect the outbound web traffic to various servers and upstream proxy servers depending on certain conditions.

SSL Decoder

Web filter for Microsoft ISA Server (Forefront TMG) allowing you to peek inside SSL Traffic.

Headers Modifier

Web filter for Microsoft ISA Server (Forefront TMG) that is used to automatically modify web request headers passing through ISA Server (Forefront TMG).

Download and installation

You can download the ISA Server Toolkit from the Redline Software website. As I wrote this article the latest version of the Toolkit is version number 1.3. After downloading the Toolkit, start the installation process and chose the tools that you want to install.

The ISA Server Toolkit distinguishes between standalone tools and Web filter applications as you can see in the following picture.
Stand Alone tools can run without directly integrating into the ISA Server architecture. On the other hand the Web filter applications integrate into the ISA Server configuration by extending the ISA Server functionality through a Web Filter.

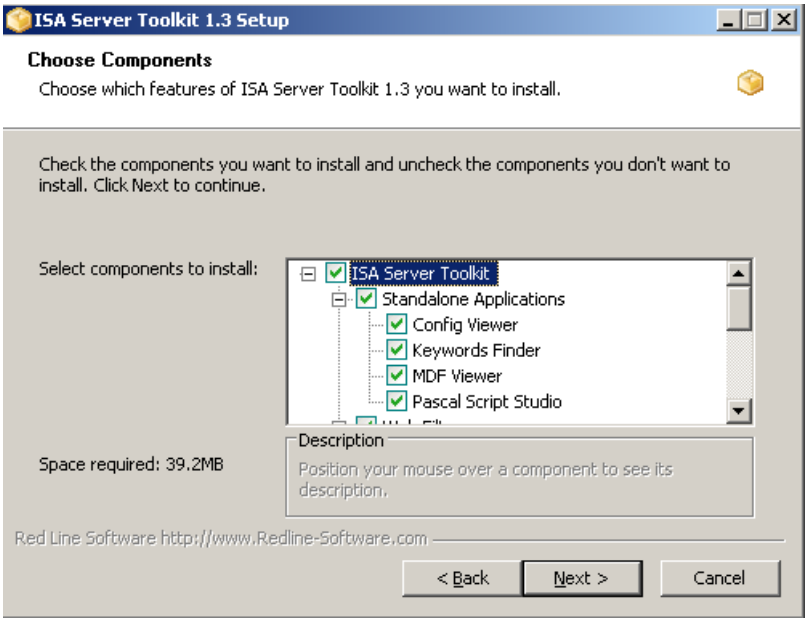


Figure 1: Select components to install

You can choose between different Setup Scenarios.

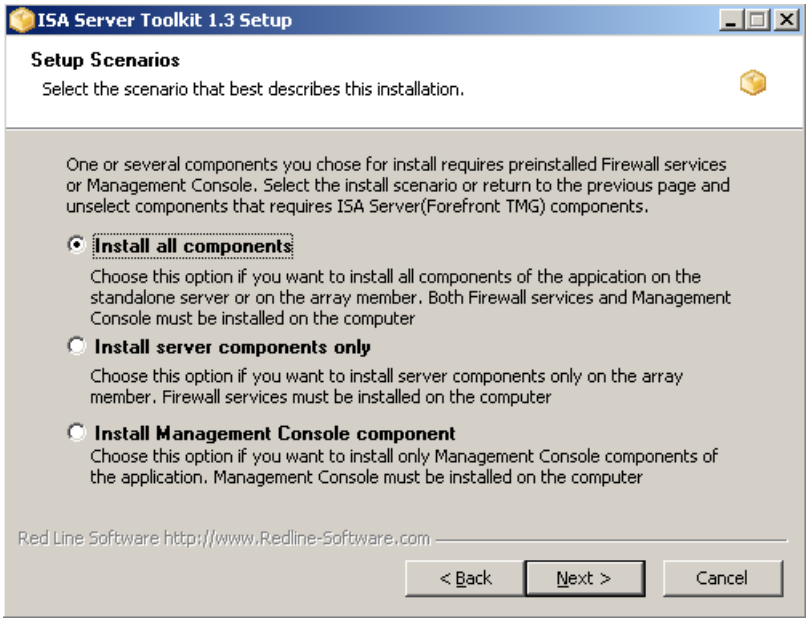


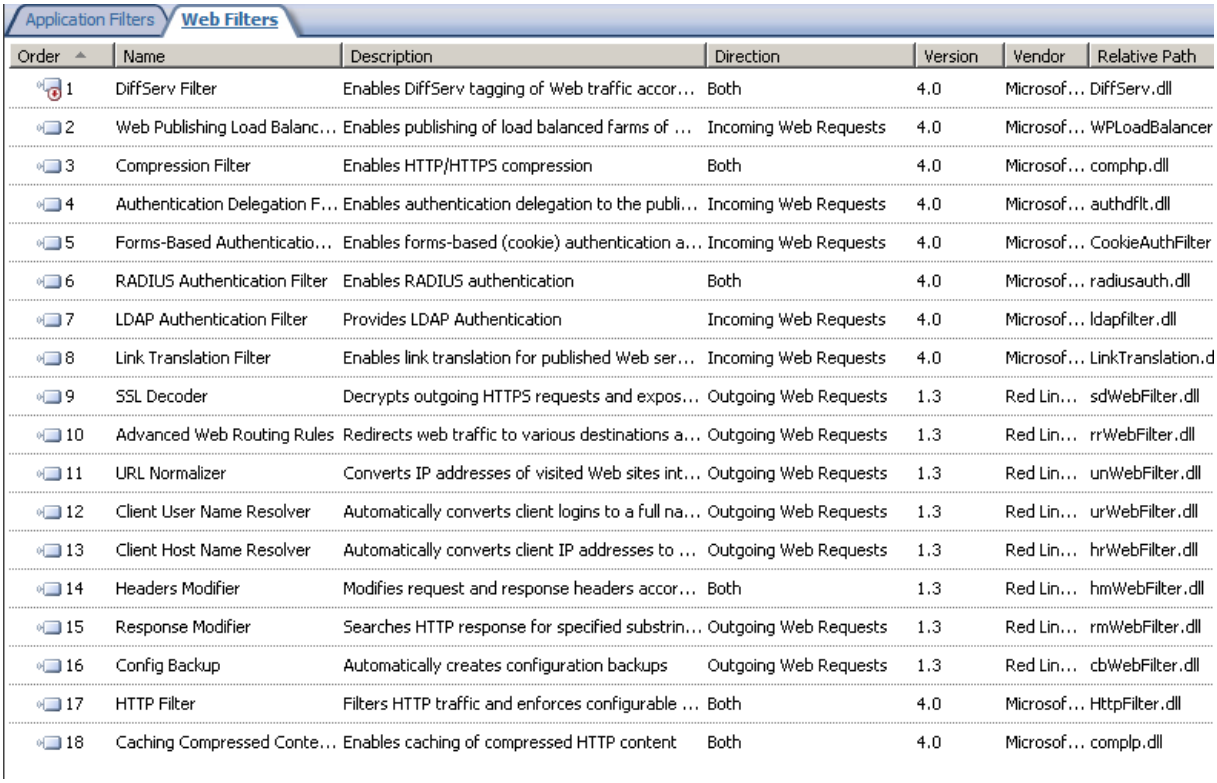
Figure 2: Setup scenarios – Chose the best Setup type

If you selected to install the Client Hostname Resolver tool during the initial setup, you must now specify an account with permission.

If you want to install one or more Web Filter from the ISA Server Toolkit, the Microsoft Firewall service must be restarted during the setup process. You have to confirm the restart of the process.

Specify the installation directory where all components should be installed.

After setup has successfully finished, you will find a number of installed Web Filters. You can easily find these Web Filters in the Vendor column.



Application Filters | Web Filters

Order	Name	Description	Direction	Version	Vendor	Relative Path
1	DiffServ Filter	Enables DiffServ tagging of Web traffic accor...	Both	4.0	Microsof...	DiffServ.dll
2	Web Publishing Load Balanc...	Enables publishing of load balanced farms of ...	Incoming Web Requests	4.0	Microsof...	WPLoadBalancer
3	Compression Filter	Enables HTTP/HTTPS compression	Both	4.0	Microsof...	comphp.dll
4	Authentication Delegation F...	Enables authentication delegation to the publi...	Incoming Web Requests	4.0	Microsof...	authdflt.dll
5	Forms-Based Authenticatio...	Enables forms-based (cookie) authentication a...	Incoming Web Requests	4.0	Microsof...	CookieAuthFilter
6	RADIUS Authentication Filter	Enables RADIUS authentication	Both	4.0	Microsof...	radiusauth.dll
7	LDAP Authentication Filter	Provides LDAP Authentication	Incoming Web Requests	4.0	Microsof...	ldapfilter.dll
8	Link Translation Filter	Enables link translation for published Web ser...	Incoming Web Requests	4.0	Microsof...	LinkTranslation.d
9	SSL Decoder	Decrypts outgoing HTTPS requests and expos...	Outgoing Web Requests	1.3	Red Lin...	sdWebFilter.dll
10	Advanced Web Routing Rules	Redirects web traffic to various destinations a...	Outgoing Web Requests	1.3	Red Lin...	rrWebFilter.dll
11	URL Normalizer	Converts IP addresses of visited Web sites int...	Outgoing Web Requests	1.3	Red Lin...	unWebFilter.dll
12	Client User Name Resolver	Automatically converts client logins to a full na...	Outgoing Web Requests	1.3	Red Lin...	urWebFilter.dll
13	Client Host Name Resolver	Automatically converts client IP addresses to ...	Outgoing Web Requests	1.3	Red Lin...	hrWebFilter.dll
14	Headers Modifier	Modifies request and response headers accor...	Both	1.3	Red Lin...	hmWebFilter.dll
15	Response Modifier	Searches HTTP response for specified substrin...	Outgoing Web Requests	1.3	Red Lin...	rmWebFilter.dll
16	Config Backup	Automatically creates configuration backups	Outgoing Web Requests	1.3	Red Lin...	cbWebFilter.dll
17	HTTP Filter	Filters HTTP traffic and enforces configurable ...	Both	4.0	Microsof...	HttpFilter.dll
18	Caching Compressed Conte...	Enables caching of compressed HTTP content	Both	4.0	Microsof...	complp.dll

Figure 3: Installed Web Filters from redline software

Some of the Web Filters are directly configurable, some Web Filters are not.

SSL Decoder

SSL Decoder is a utility that makes it possible to inspect outgoing HTTPS traffic by issuing certificates for each outgoing client request. SSL decoder acts a small Certificate Authority (CA) that issues certificates from this Root CA. It is possible to create your own Root CA and you can also chose the work scenario how SSL Decoder should work.
This is a nice feature because the current version of ISA Server has no outgoing HTTPS inspection capability, only incoming requests can be inspected via a HTTPS Bridging scenario in a reverse Proxy scenario.

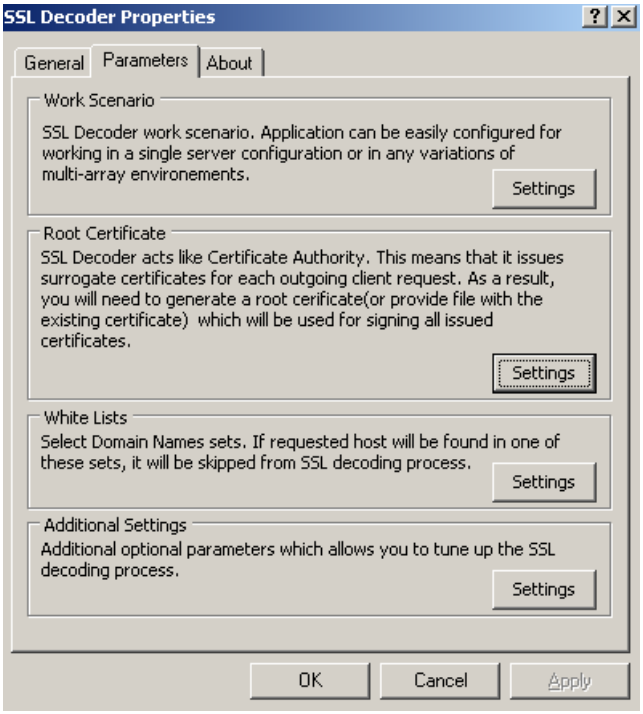


Figure 4: SSL Decoder configuration settings

As I said above, there are four different working scenarios how SSL Decoder should work.

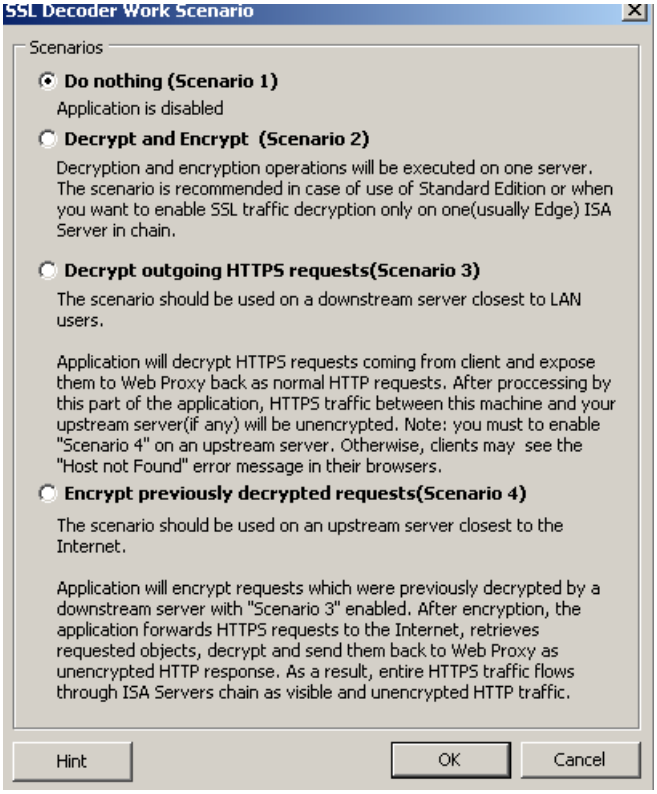


Figure 5: SSL Decoder scenarios

The additional settings tab allows the configuring of SSL Decoder logging. For a detailed installation instruction read this article: http://www.redline-software.com/eng/products/tk/components/ssl_decoder.php

Advanced Web Routing Rule

Advanced Web Routing extends the Web Chaining capabilities of ISA Server 2006, where traffic only could be forwarded to one destination without a chance to select, which traffic should be send to the Upstream Server. The Advanced Web Routing utility extends these features. It is now possible to specify some criteria for routing Web requests and it is also possible to specify different Web Routing destinations also based on several criteria's.

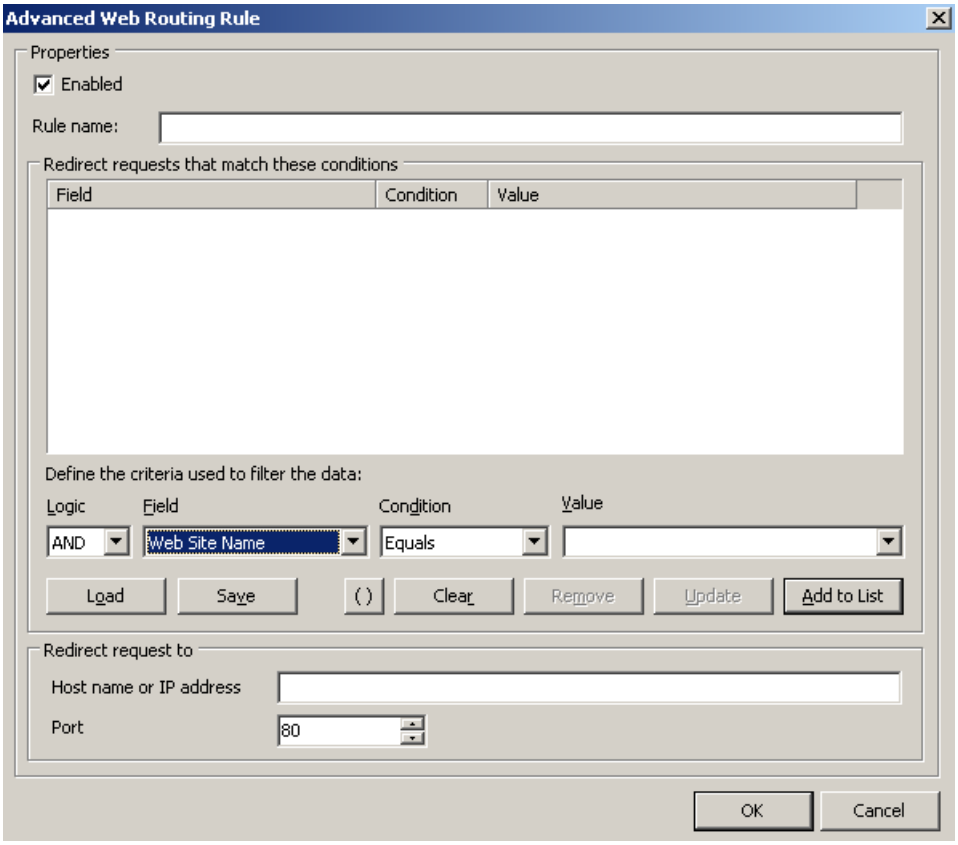


Figure 6: Advanced Web Routing Rule

Headers Modifier

The Headers Modifier tool allows ISA Server Administrators to search for specific HTTP Headers and provides different methods to add, modify, delete or to substitute HTTP Headers.

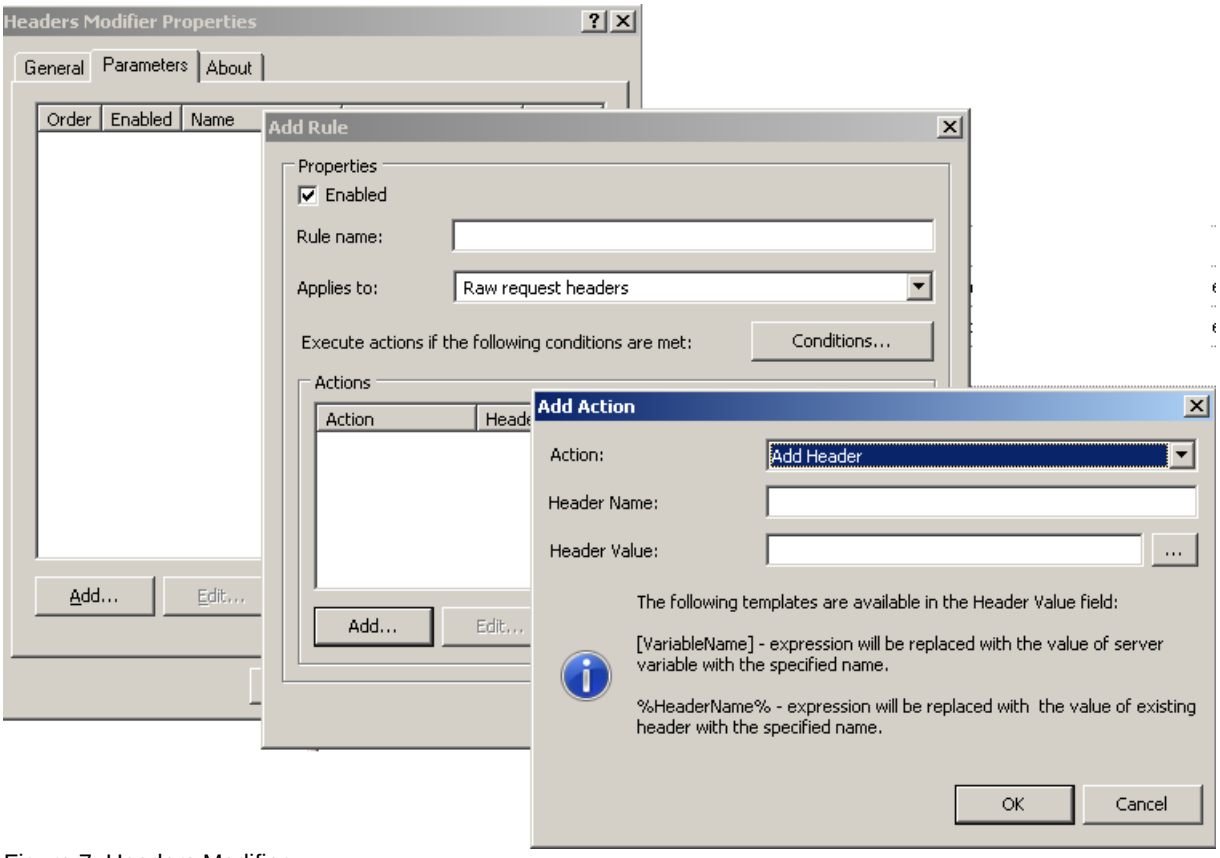


Figure 7: Headers Modifier

Response Modifier

Another helpful utility which allows you to search for specific strings inside a HTTP response and to replace these strings with a Replace string is the Response Modifier utility. For example, it is possible to enhance the virus security on computers; ISA Server Administrators can disable opening some HTML pages containing that dangerous content.

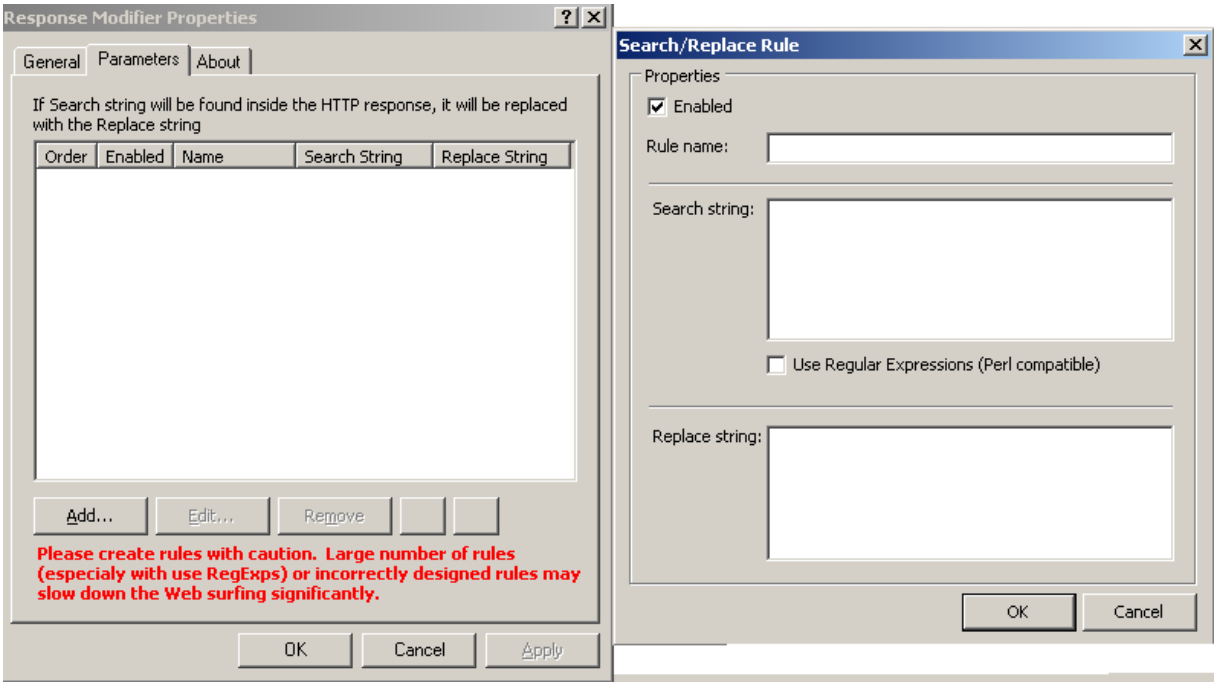


Figure 8: Advanced Web Routing Rule

Config Backup

Config Backup is my absolute favorite. Config Backup allows you to create a scheduled backup of the entire ISA Server configuration. Config Backup creates a normal XML export file like the Export process in the ISA Server Management console and schedules this process and it is possible to keep the last NN backup sets, which extends the available script from MSDN to create a scheduled backup which only backups the entire configuration and overwrites the existing backup file.

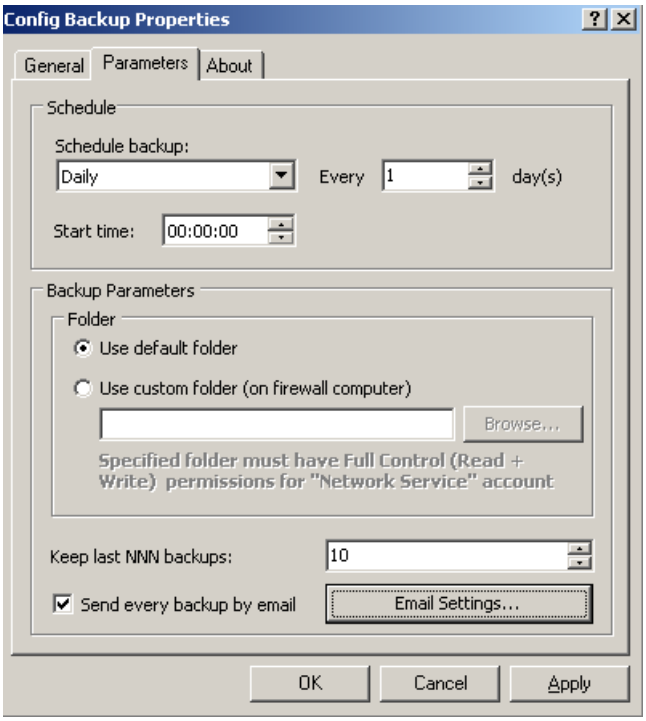


Figure 9: Redline Toolkit Config Backup settings

Config Backup allows using a custom folder to store the ISA Server backup files. The network service account must have Read and Write access permissions to the network share and for the folder.

Config Viewer

Config Viewer is a tool which can be used to open an exported ISA Server configuration (XML file) for offline viewing the configuration of your ISA Server. This tool is very helpful because it is possible to open different configurations to see the difference between these configurations. As an ISA Server Consultant the tool is helpful for documentation purposes of ISA Server implementations at customer side.

Please note: Another very helpful ISA config viewer utility is the ISAInfo tool from Jim Harrision. You can download the tool at Jim's website at http://www.isatools.org/tools/isainfo.zip.

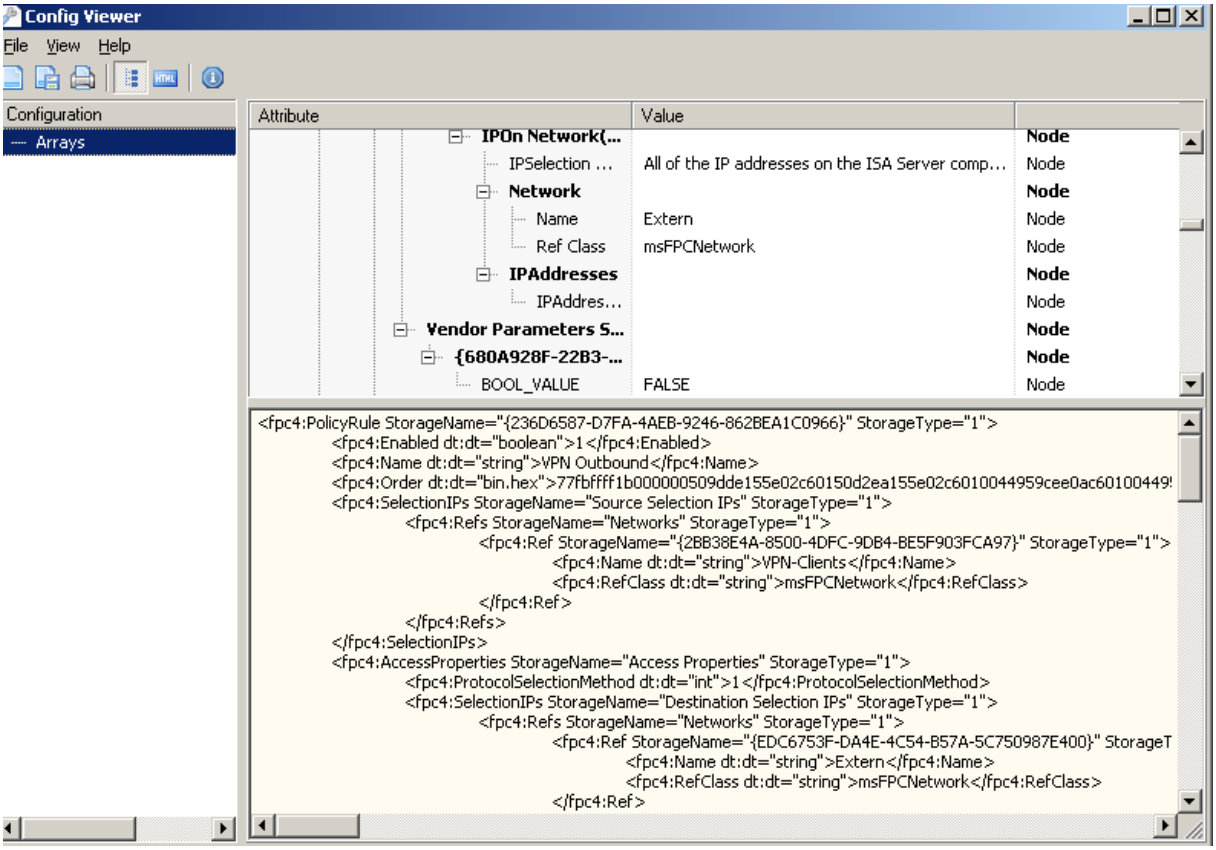
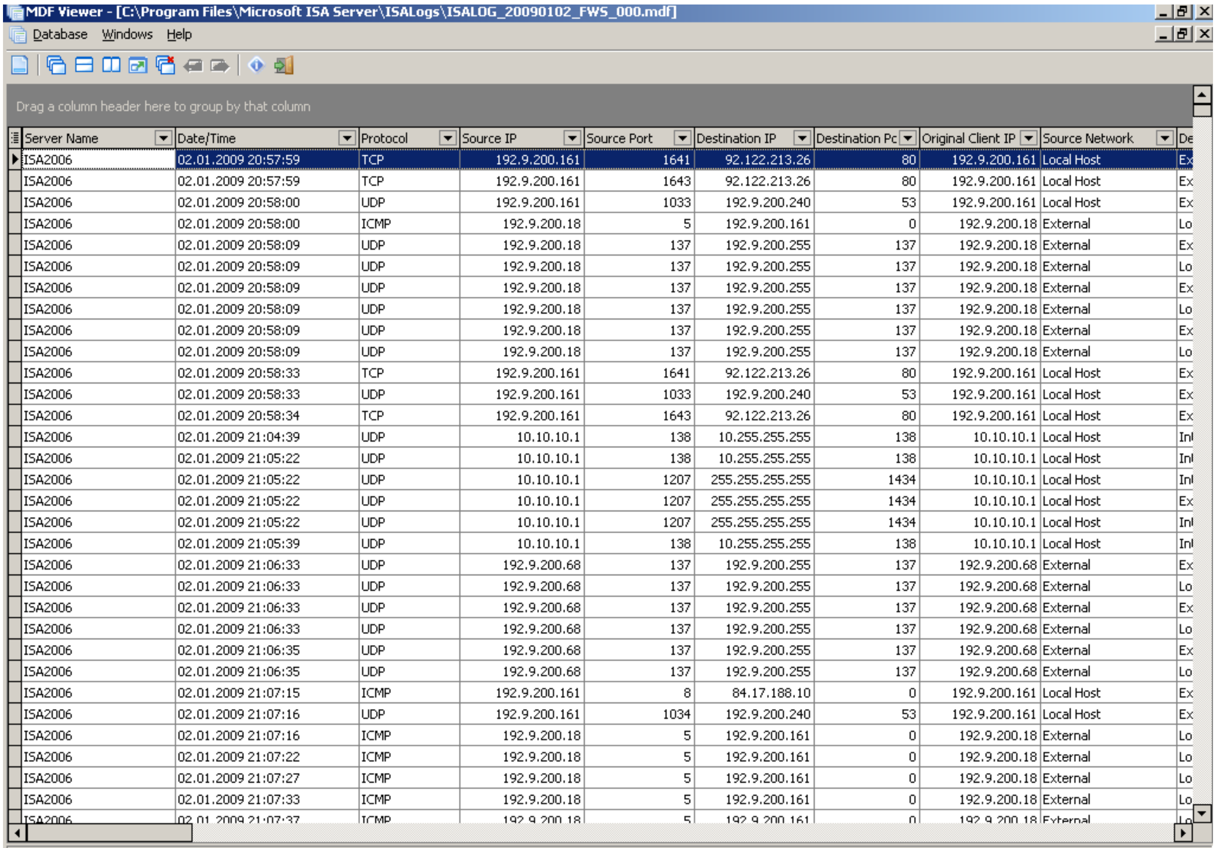


Figure 10: Config Viewer

MDF Viewer

If your ISA Server logs network traffic into the MSDE (Microsoft SQL Server Desktop engine), and that is the default setting in ISA Server setup, ISA Server logs into database file. With the help of the MDF Viewer it is possible to have a view into this log files.



Server Name	Date/Time	Protocol	Source IP	Source Port	Destination IP	Destination Pc	Original Client IP	Source Network	De
ISA2006	02.01.2009 20:57:59	TCP	192.9.200.161	1641	92.122.213.26	80	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 20:57:59	TCP	192.9.200.161	1643	92.122.213.26	80	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 20:58:00	UDP	192.9.200.161	1033	192.9.200.240	53	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 20:58:00	ICMP	192.9.200.18	5	192.9.200.161	0	192.9.200.18	External	Lo
ISA2006	02.01.2009 20:58:09	UDP	192.9.200.18	137	192.9.200.255	137	192.9.200.18	External	Ex
ISA2006	02.01.2009 20:58:09	UDP	192.9.200.18	137	192.9.200.255	137	192.9.200.18	External	Lo
ISA2006	02.01.2009 20:58:09	UDP	192.9.200.18	137	192.9.200.255	137	192.9.200.18	External	Ex
ISA2006	02.01.2009 20:58:09	UDP	192.9.200.18	137	192.9.200.255	137	192.9.200.18	External	Lo
ISA2006	02.01.2009 20:58:09	UDP	192.9.200.18	137	192.9.200.255	137	192.9.200.18	External	Ex
ISA2006	02.01.2009 20:58:09	UDP	192.9.200.18	137	192.9.200.255	137	192.9.200.18	External	Lo
ISA2006	02.01.2009 20:58:33	TCP	192.9.200.161	1641	92.122.213.26	80	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 20:58:33	UDP	192.9.200.161	1033	192.9.200.240	53	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 20:58:34	TCP	192.9.200.161	1643	92.122.213.26	80	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 21:04:39	UDP	10.10.10.1	138	10.255.255.255	138	10.10.10.1	Local Host	In
ISA2006	02.01.2009 21:05:22	UDP	10.10.10.1	138	10.255.255.255	138	10.10.10.1	Local Host	In
ISA2006	02.01.2009 21:05:22	UDP	10.10.10.1	1207	255.255.255.255	1434	10.10.10.1	Local Host	In
ISA2006	02.01.2009 21:05:22	UDP	10.10.10.1	1207	255.255.255.255	1434	10.10.10.1	Local Host	Ex
ISA2006	02.01.2009 21:05:22	UDP	10.10.10.1	1207	255.255.255.255	1434	10.10.10.1	Local Host	In
ISA2006	02.01.2009 21:05:39	UDP	10.10.10.1	138	10.255.255.255	138	10.10.10.1	Local Host	In
ISA2006	02.01.2009 21:06:33	UDP	192.9.200.68	137	192.9.200.255	137	192.9.200.68	External	Ex
ISA2006	02.01.2009 21:06:33	UDP	192.9.200.68	137	192.9.200.255	137	192.9.200.68	External	Lo
ISA2006	02.01.2009 21:06:33	UDP	192.9.200.68	137	192.9.200.255	137	192.9.200.68	External	Ex
ISA2006	02.01.2009 21:06:33	UDP	192.9.200.68	137	192.9.200.255	137	192.9.200.68	External	Lo
ISA2006	02.01.2009 21:06:35	UDP	192.9.200.68	137	192.9.200.255	137	192.9.200.68	External	Ex
ISA2006	02.01.2009 21:06:35	UDP	192.9.200.68	137	192.9.200.255	137	192.9.200.68	External	Lo
ISA2006	02.01.2009 21:07:15	ICMP	192.9.200.161	8	84.17.188.10	0	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 21:07:16	UDP	192.9.200.161	1034	192.9.200.240	53	192.9.200.161	Local Host	Ex
ISA2006	02.01.2009 21:07:16	ICMP	192.9.200.18	5	192.9.200.161	0	192.9.200.18	External	Lo
ISA2006	02.01.2009 21:07:22	ICMP	192.9.200.18	5	192.9.200.161	0	192.9.200.18	External	Lo
ISA2006	02.01.2009 21:07:27	ICMP	192.9.200.18	5	192.9.200.161	0	192.9.200.18	External	Lo
ISA2006	02.01.2009 21:07:33	ICMP	192.9.200.18	5	192.9.200.161	0	192.9.200.18	External	Lo
ISA2006	02.01.2009 21:07:37	ICMP	192.9.200.18	5	192.9.200.161	0	192.9.200.18	External	Lo

Figure 11: MDF Viewer

Keywords Finder

The keywords Finder tool allows ISA Administrators to find keywords in the ISA Server MSDE log files. It is possible to search for several of ISA objects like IP addresses, MAC addresses and many more.

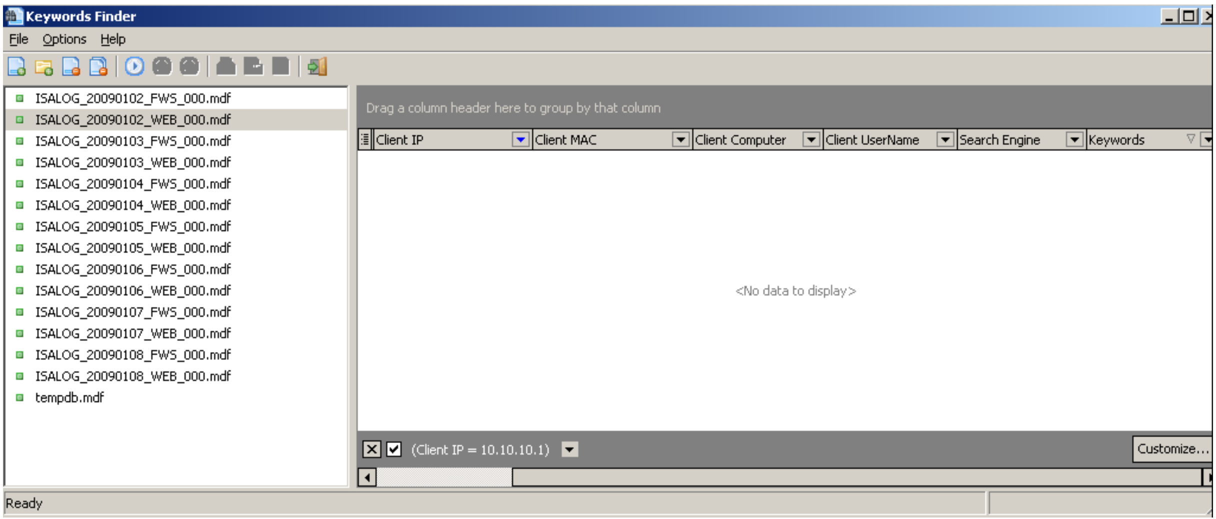


Figure 12: Keywords Finder

The ISA Server Toolkit integrates into the ISA Server MMC and on the General tab it is possible to backup and restore the ISA Server Toolkit configuration.

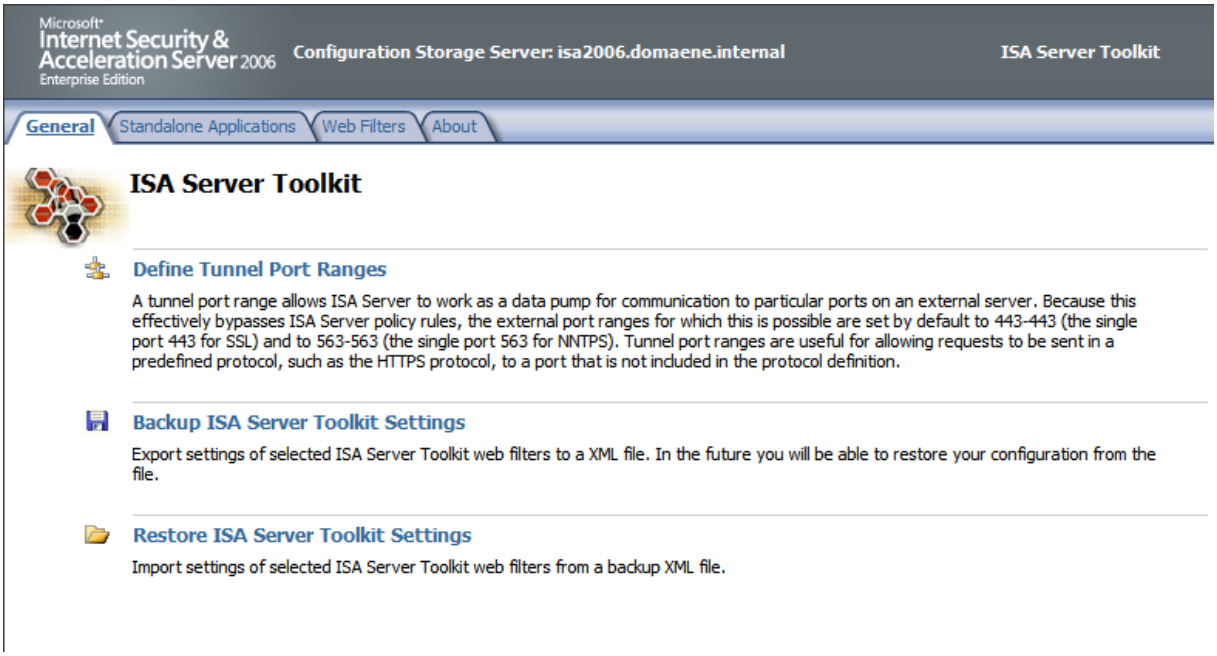


Figure 13: Toolkit Backup and Restore

In the ISA MMC you will find a new tab under the ISA Server Toolkit node with an overview about all Web Filters and Standalone Applications provided by the ISA Server Toolkit.

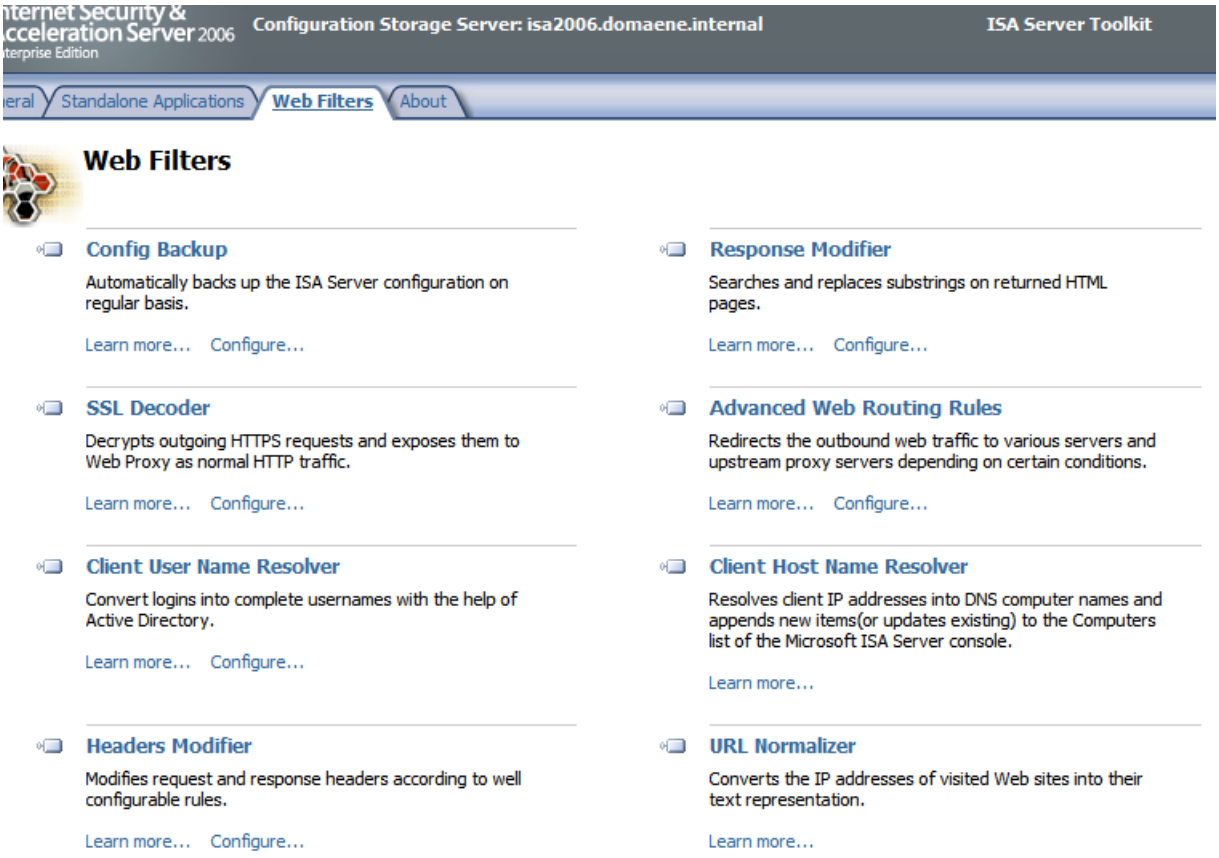


Figure 14: Overview about Web Filters

Tunnel Port Range Editor

The ISA Server Toolkit also contains an ISA Server Tunnel Port Range Editor, like the well known Tunnel Port Range editor from www.isatools.org. With the help of this tool it is possible to change the ports or port range for SSL traffic which typically used Port 443 or 563 for NNTPS.

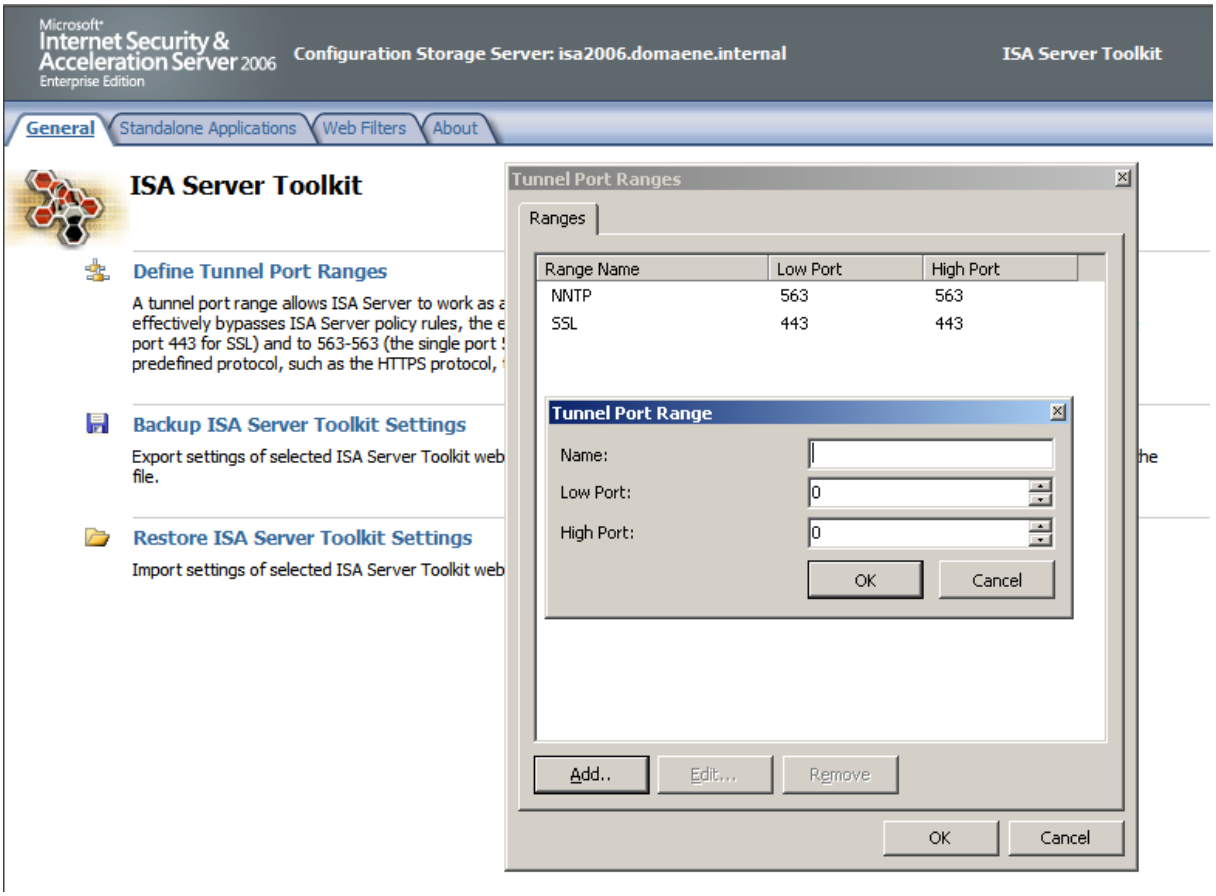


Figure 15: ISA Toolkit Tunnel Port Editor

Conclusion

In this article, I tried to give you an overview about the ISA Server / TMG Toolkit. The ISA Server Toolkit is in my opinion a wonderful addition and extension to the ISA Server product and a must have for every ISA Server Administrator. My personally favorite is the integrated filter for automating the ISA Server backup.

Related links

Redline ISA Server / TMG Toolkit 1.3
http://www.redline-software.com/ger/download/