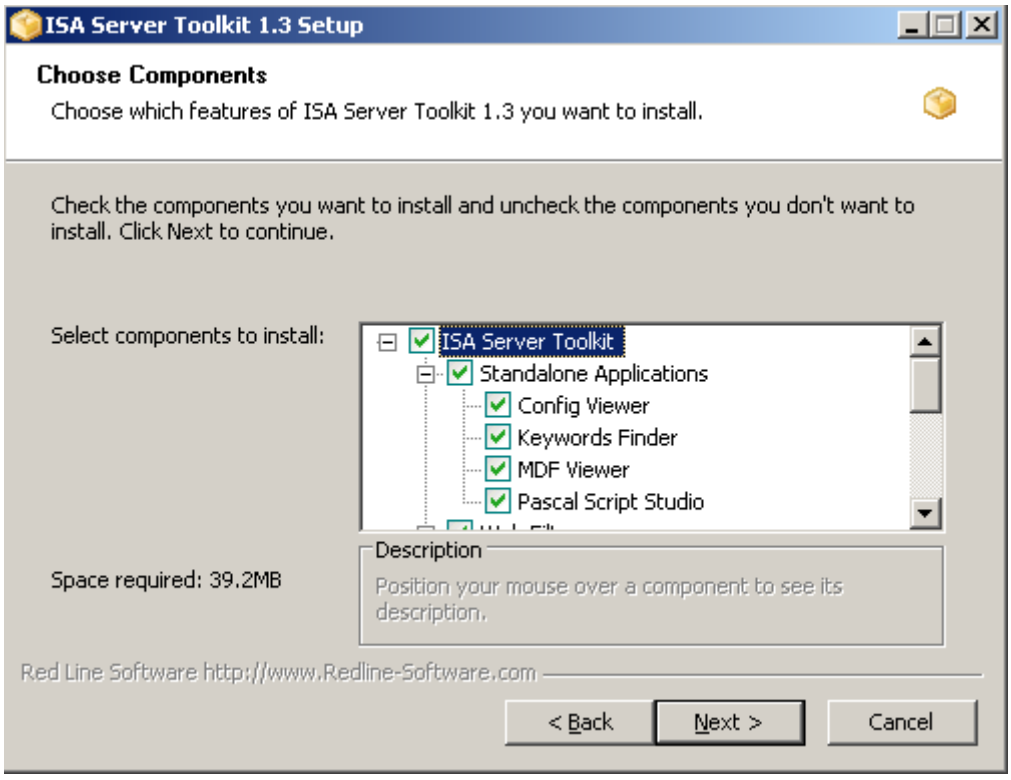
ISA Server Toolkit von Redline Software

Die Firma Redline Software stellt ein Toolkit fuer die erweiterte ISA Server Verwaltung zur Verfuegung.

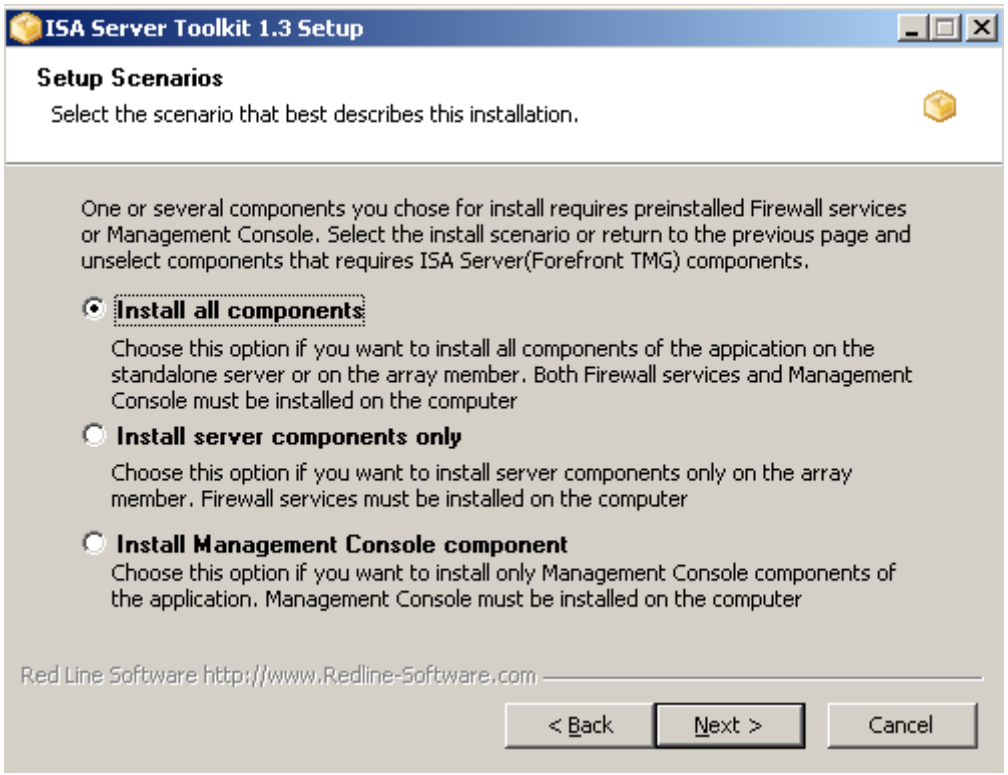
Das Toolkit kann kostenlos von der Webseite des Anbieters heruntergeladen werden.
http://www.redline-software.com/pub/tkSetup.exe

Installation

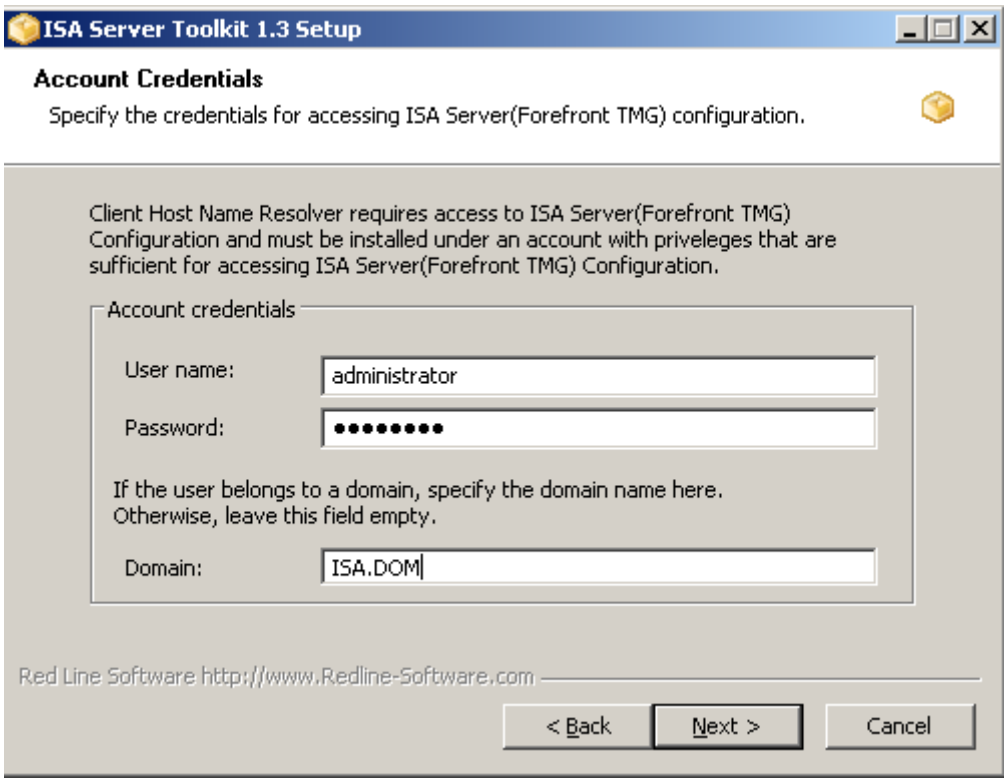
Was soll installiert werden?



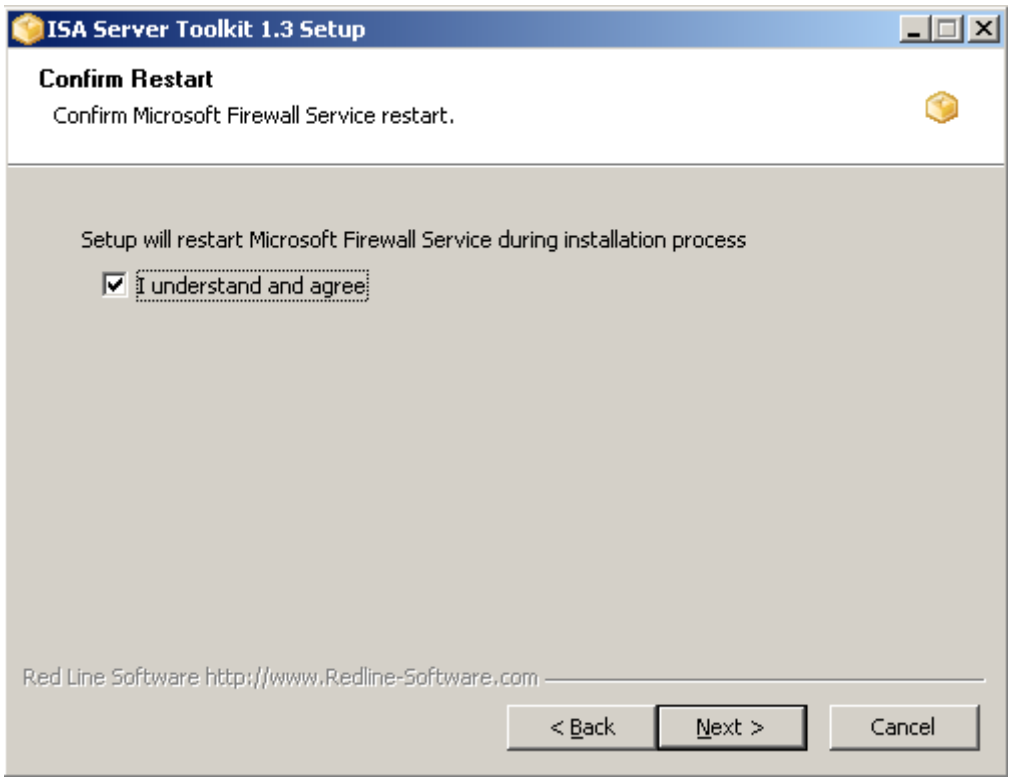
Das ISA Server Toolkit benoetigt natuerlich einige Komponenten von ISA Server ☺



Fuer das Tool „Client Hostname Resolver“ muss ein Account angegeben werden, welcher fuer die User Aufloesung zustaendig ist.

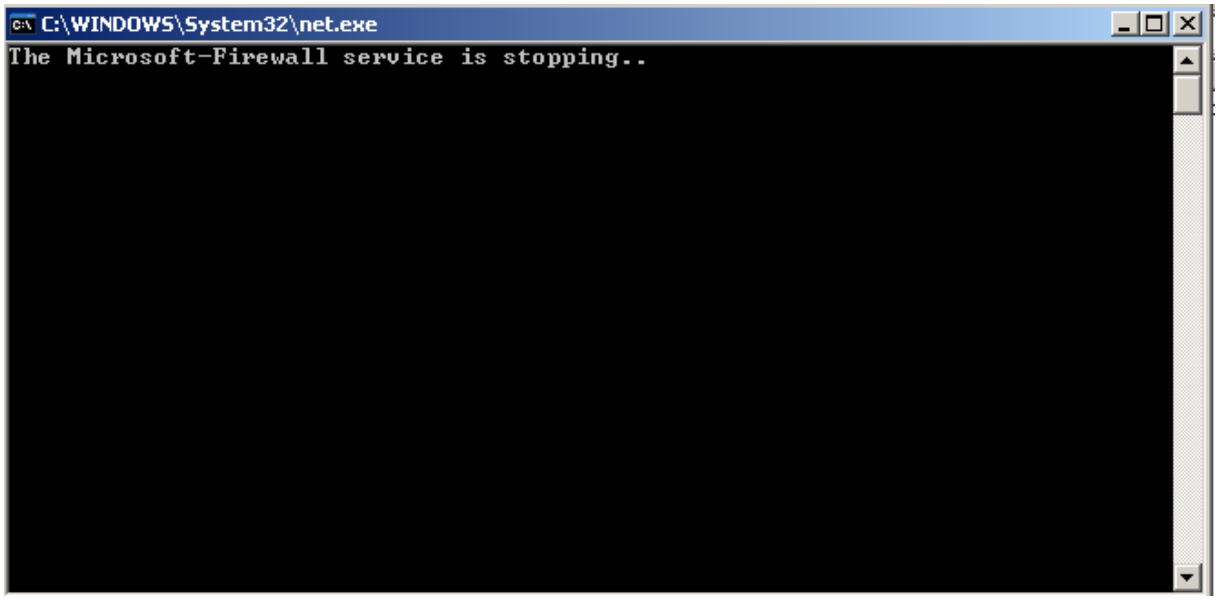


Nett, ich muss zustimmen, dass der ISA Server Firewall Dienst waehrend der Installation neu gestartet wird.

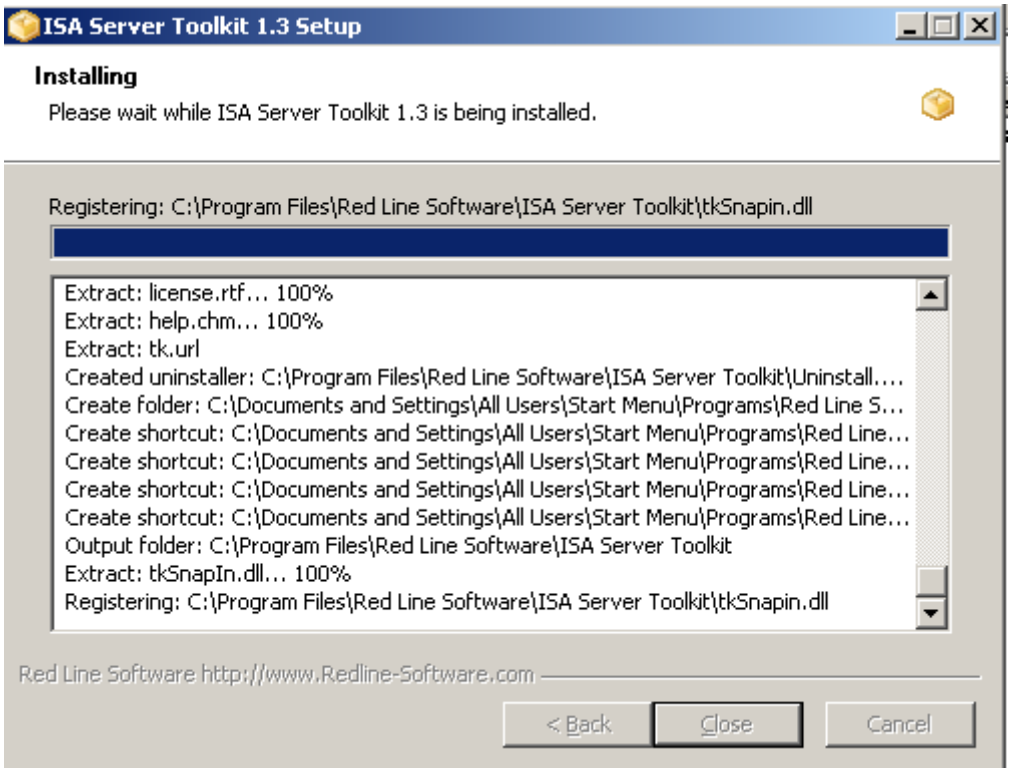


Installationspfad angeben

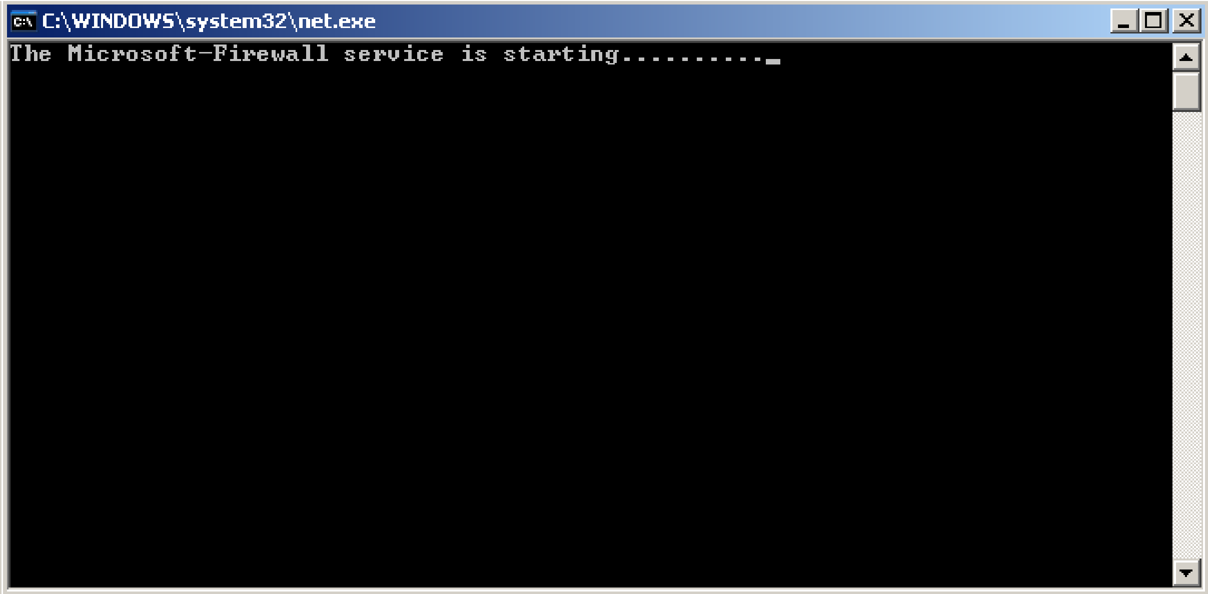
Firewalldienst stoppt



.. und ab gehts



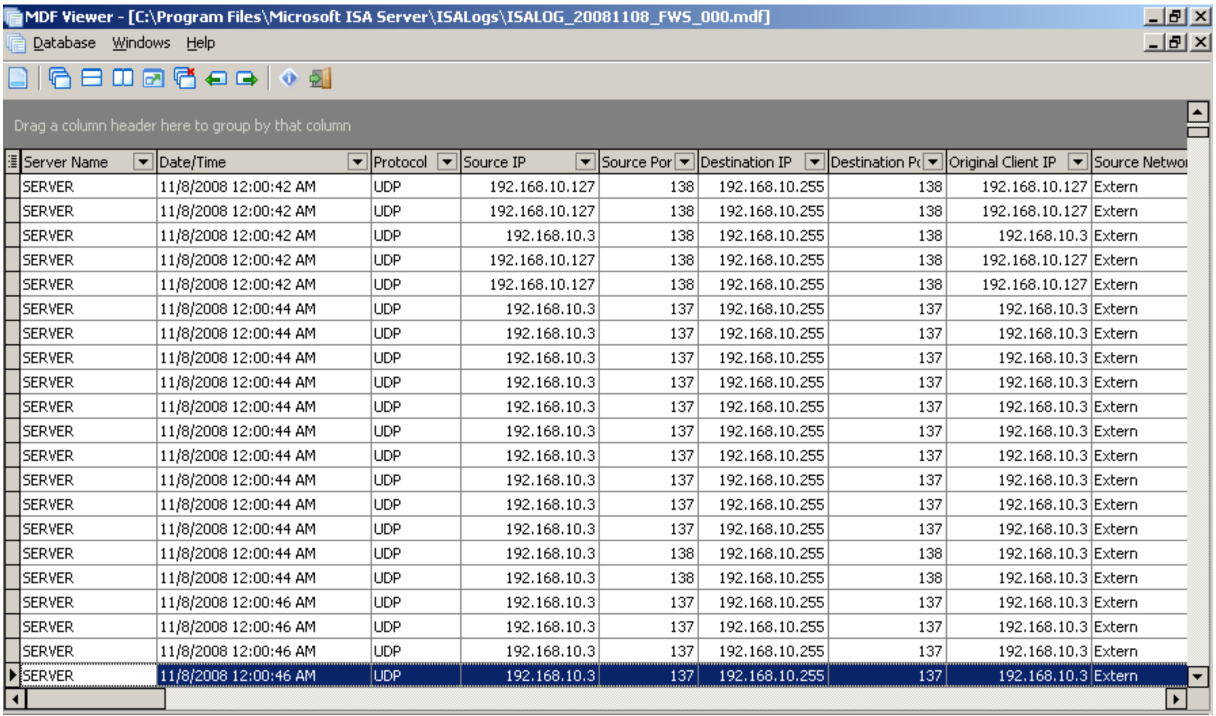
Es geht wieder bergauf …



Die Tools

MDF Viewer

.. dient zum angucken der ISA Webproxy und Firewall-Logdateien

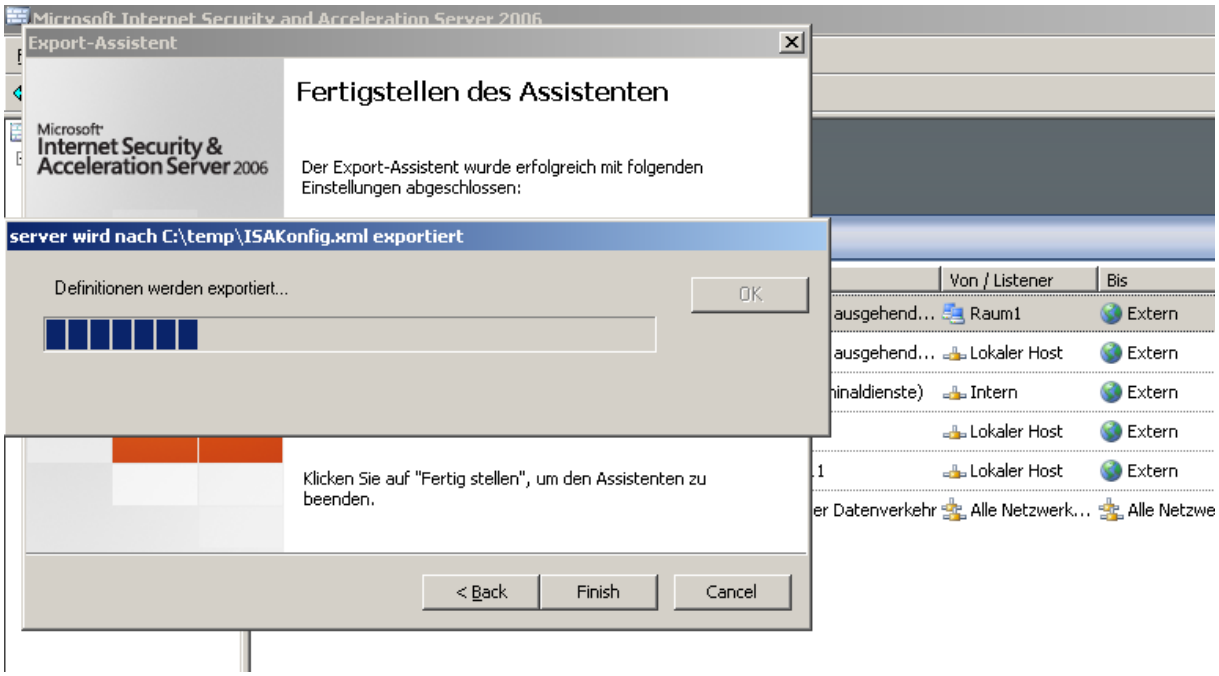


Server Name	Date/Time	Protocol	Source IP	Source Por	Destination IP	Destination P(	Original Client IP	Source Netwo
SERVER	11/8/2008 12:00:42 AM	UDP	192.168.10.127	138	192.168.10.255	138	192.168.10.127	Extern
SERVER	11/8/2008 12:00:42 AM	UDP	192.168.10.127	138	192.168.10.255	138	192.168.10.127	Extern
SERVER	11/8/2008 12:00:42 AM	UDP	192.168.10.3	138	192.168.10.255	138	192.168.10.3	Extern
SERVER	11/8/2008 12:00:42 AM	UDP	192.168.10.127	138	192.168.10.255	138	192.168.10.127	Extern
SERVER	11/8/2008 12:00:42 AM	UDP	192.168.10.127	138	192.168.10.255	138	192.168.10.127	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	138	192.168.10.255	138	192.168.10.3	Extern
SERVER	11/8/2008 12:00:44 AM	UDP	192.168.10.3	138	192.168.10.255	138	192.168.10.3	Extern
SERVER	11/8/2008 12:00:46 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:46 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:46 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern
SERVER	11/8/2008 12:00:46 AM	UDP	192.168.10.3	137	192.168.10.255	137	192.168.10.3	Extern

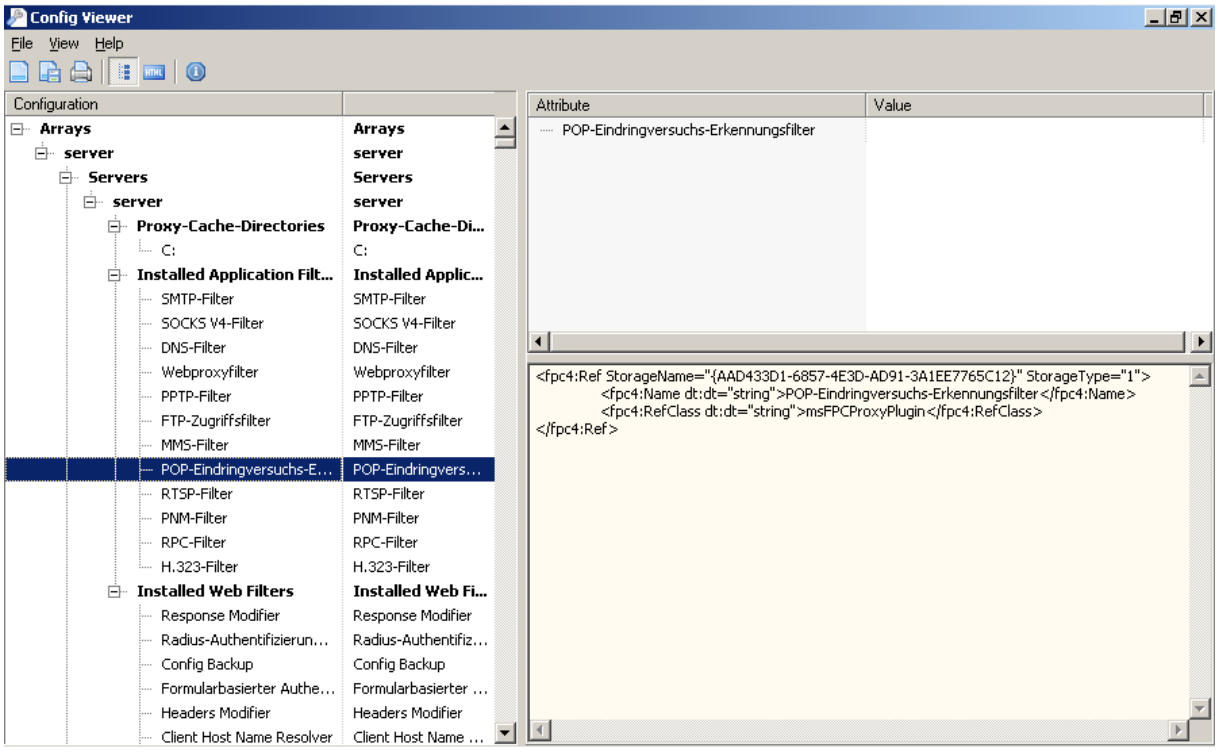
Config Viewer

.. Offline angucken einer ISA Server Konfiguration. Absolut genial fuer Consultants wie mir, die im Jahr bis zu einem Dutzend oder mehr Firewall Installationen vornehmen.

1) ISA Export erstellen



2) Im Config Viewer importieren und geniessen



Neue Webfilter

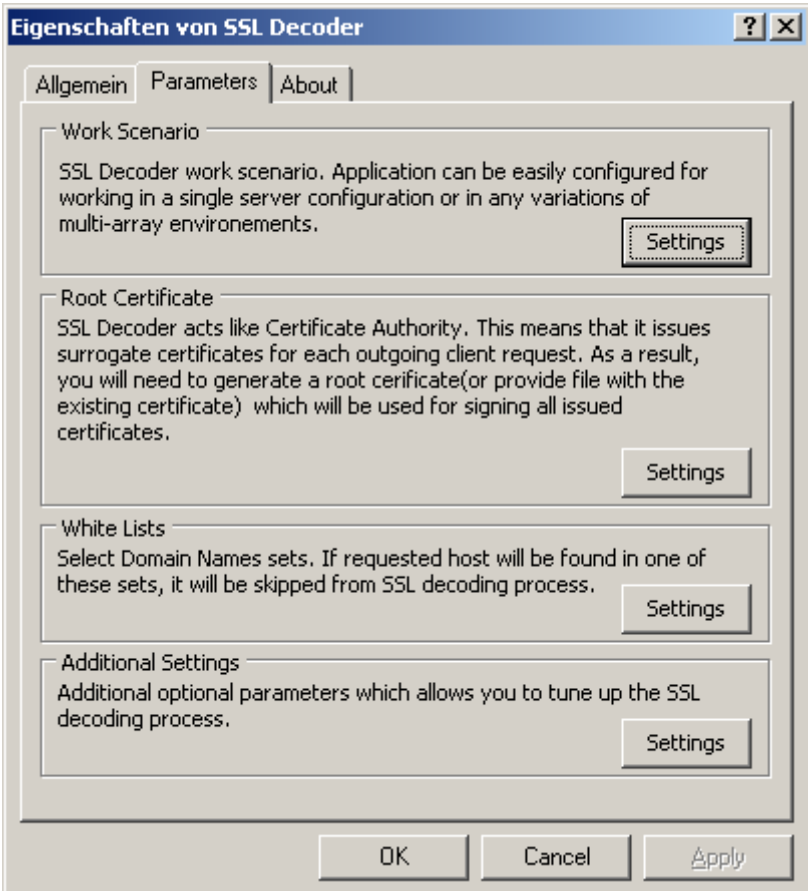
Die ISA Toolbox installierte eine Reihen von zusaetzlichen Webfiltern in ISA Server (deswegen muss der Firewalldienst auch neu gestartet werden).

Zu den Webfiltern gehoeren:

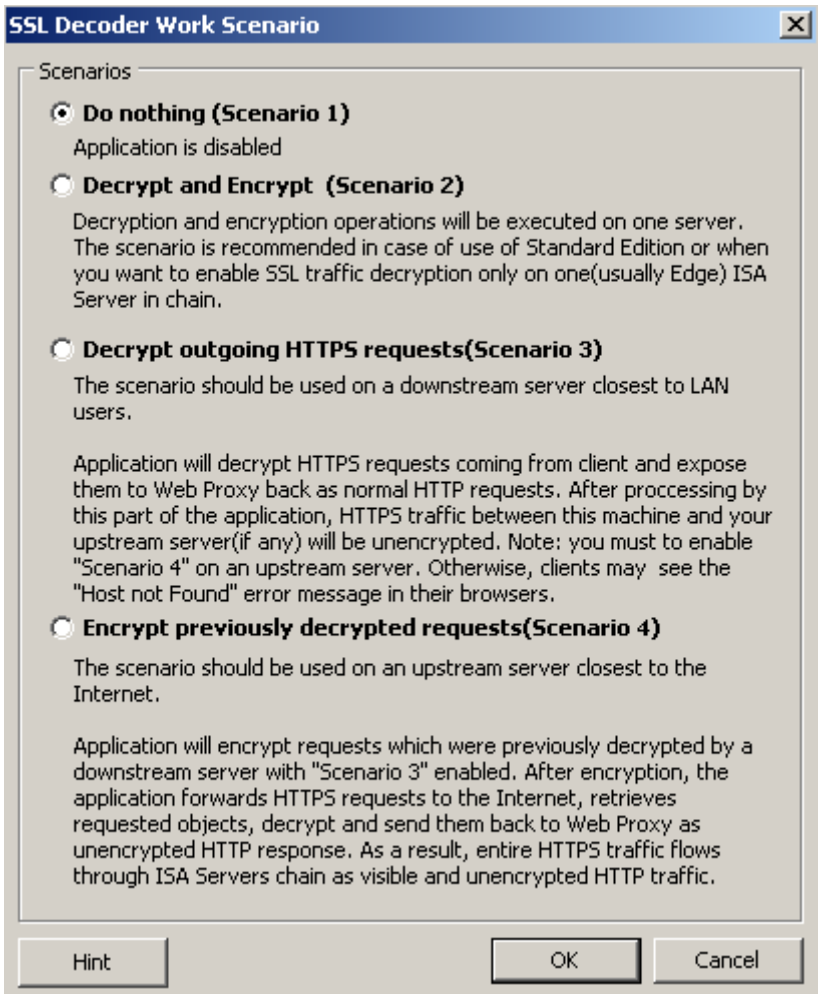
8	Linkübersetzungsfilter	Aktiviert die Linkübersetzung für veröffentlichte Webserver.	Eingehende Webanforde...
9	SSL Decoder	Decrypts outgoing HTTPS requests and exposes them to Web Proxy as normal HTTP traffic	Ausgehende Webanford...
10	Advanced Web Routing Rules	Redirects web traffic to various destinations according to well configurable routing rules	Ausgehende Webanford...
11	URL Normalizer	Converts IP addresses of visited Web sites into their text representation	Ausgehende Webanford...
12	Client User Name Resolver	Automatically converts client logins to a full names using Active Directory	Ausgehende Webanford...
13	Client Host Name Resolver	Automatically converts client IP addresses to host names	Ausgehende Webanford...
14	Headers Modifier	Modifies request and response headers according to well configurable rules	Beide
15	Response Modifier	Searches HTTP response for specified substrings and replaces them with another ones	Ausgehende Webanford...
16	Config Backup	Automatically creates configuration backups	Ausgehende Webanford...

SSL Decoder

Ausgehende HTTPS Inspection. ISA terminiert in einem Forward Proxy Szenario die HTTPS Verbindung und ersetzt diese durch eine HTTP-Verbindung, inspiziert den Traffic und leitet die Anfrage dann erneut verschluesselt weiter.

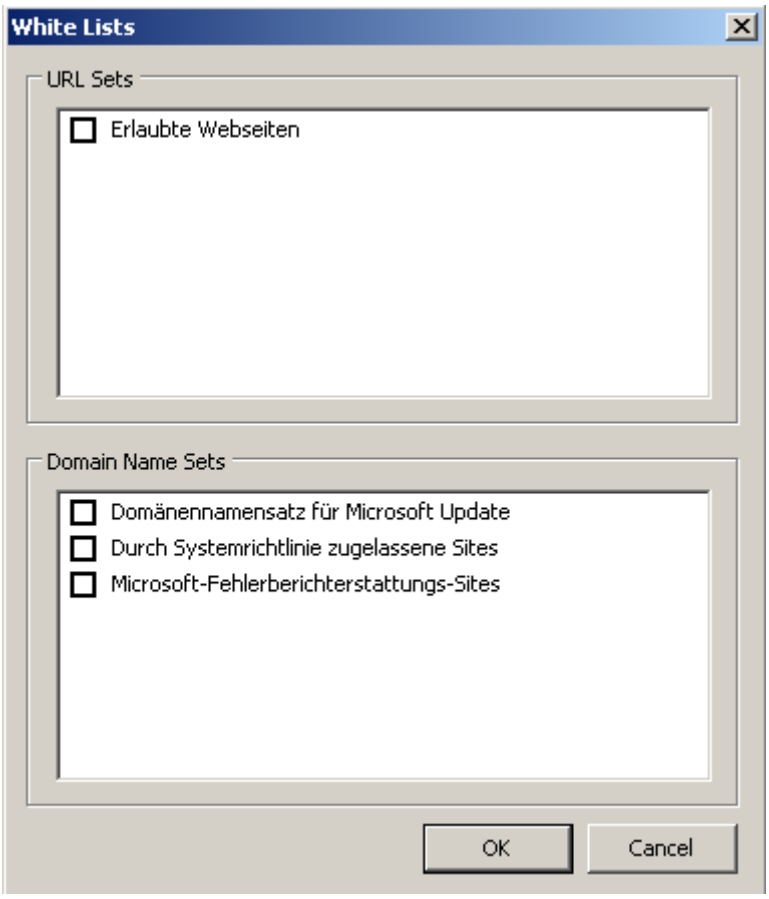


Verschiedene Moeglichkeiten

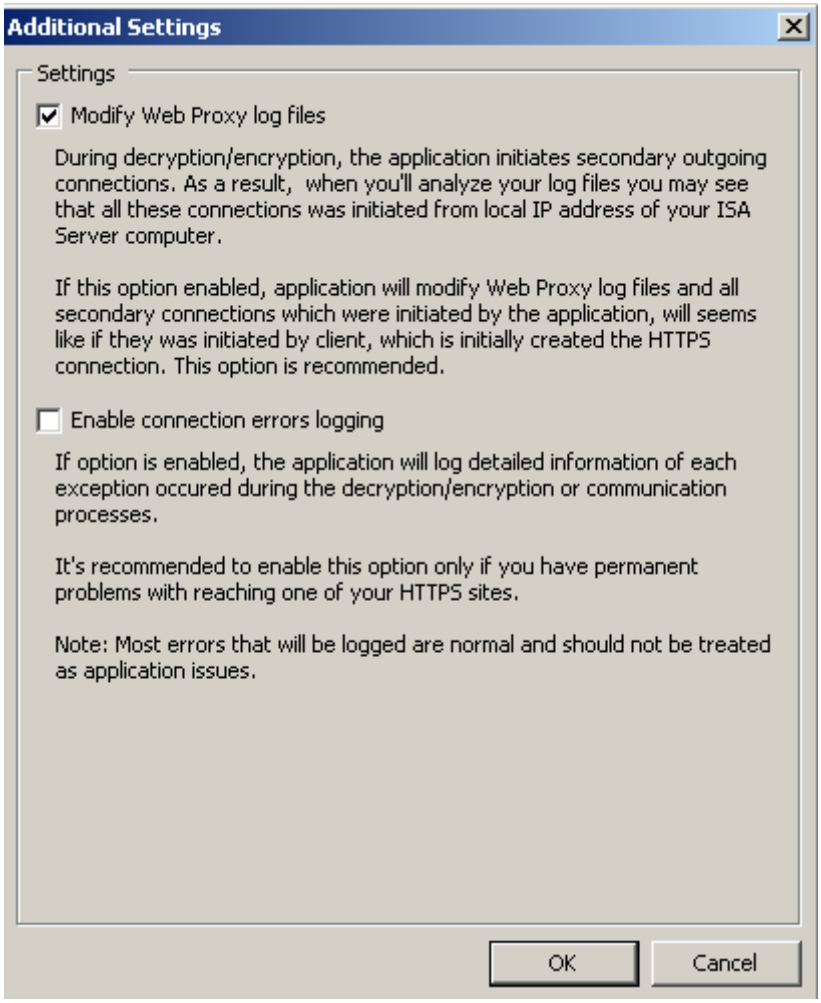


Root CA Zertifikat erstellen

Konfigurieren von Whitelisten

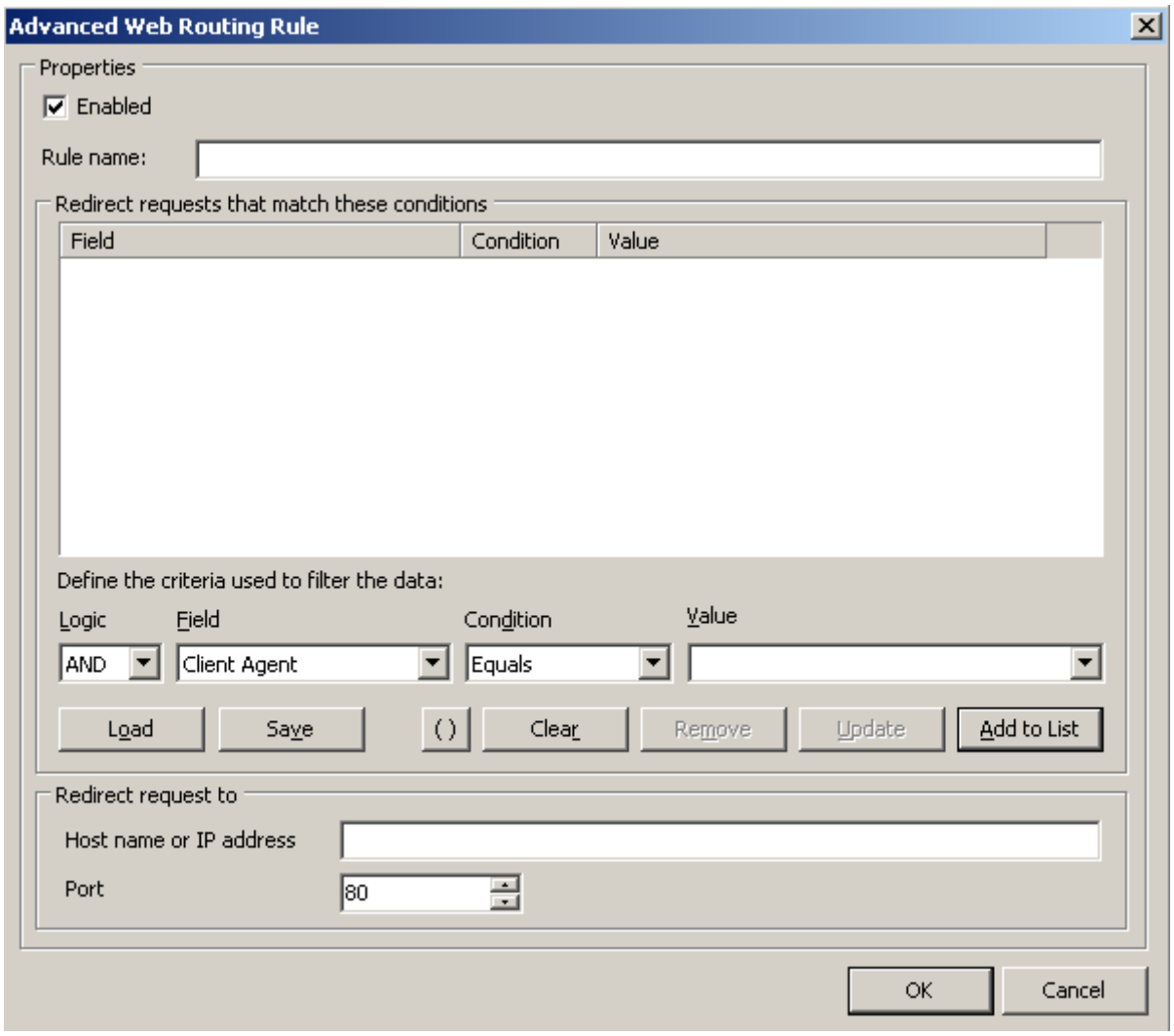


Modifikation des Logfile Verhaltens



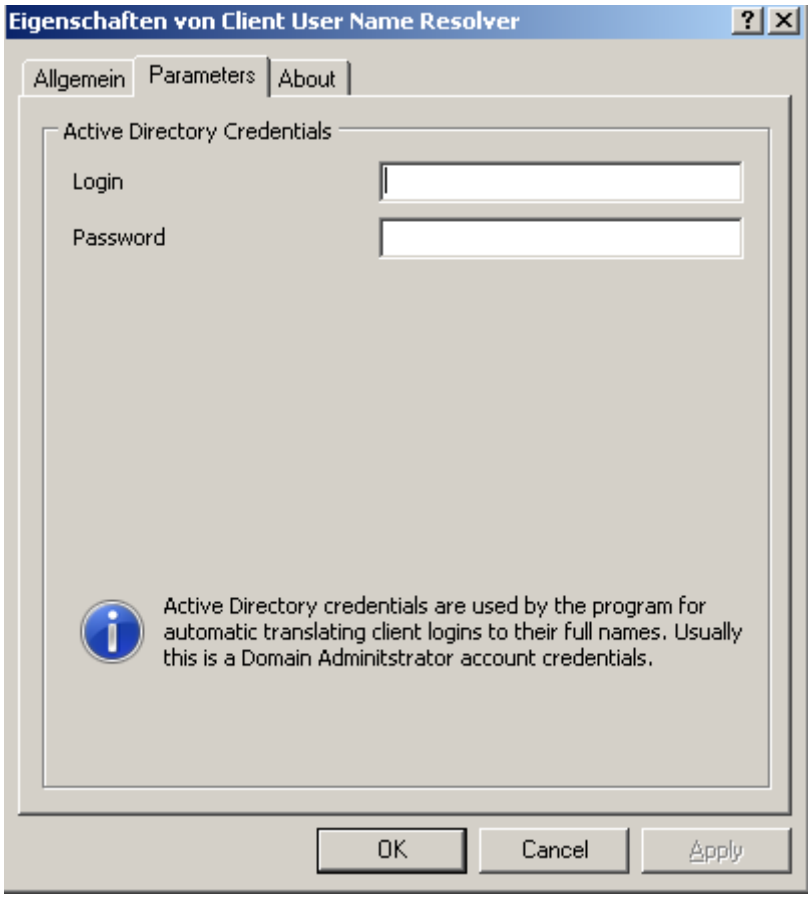
Advanced Web Routing Rule

Genial: Anfragen basierend anhand bestimmter Kriterien zu unterschiedlichsten Hosts weiterleiten.



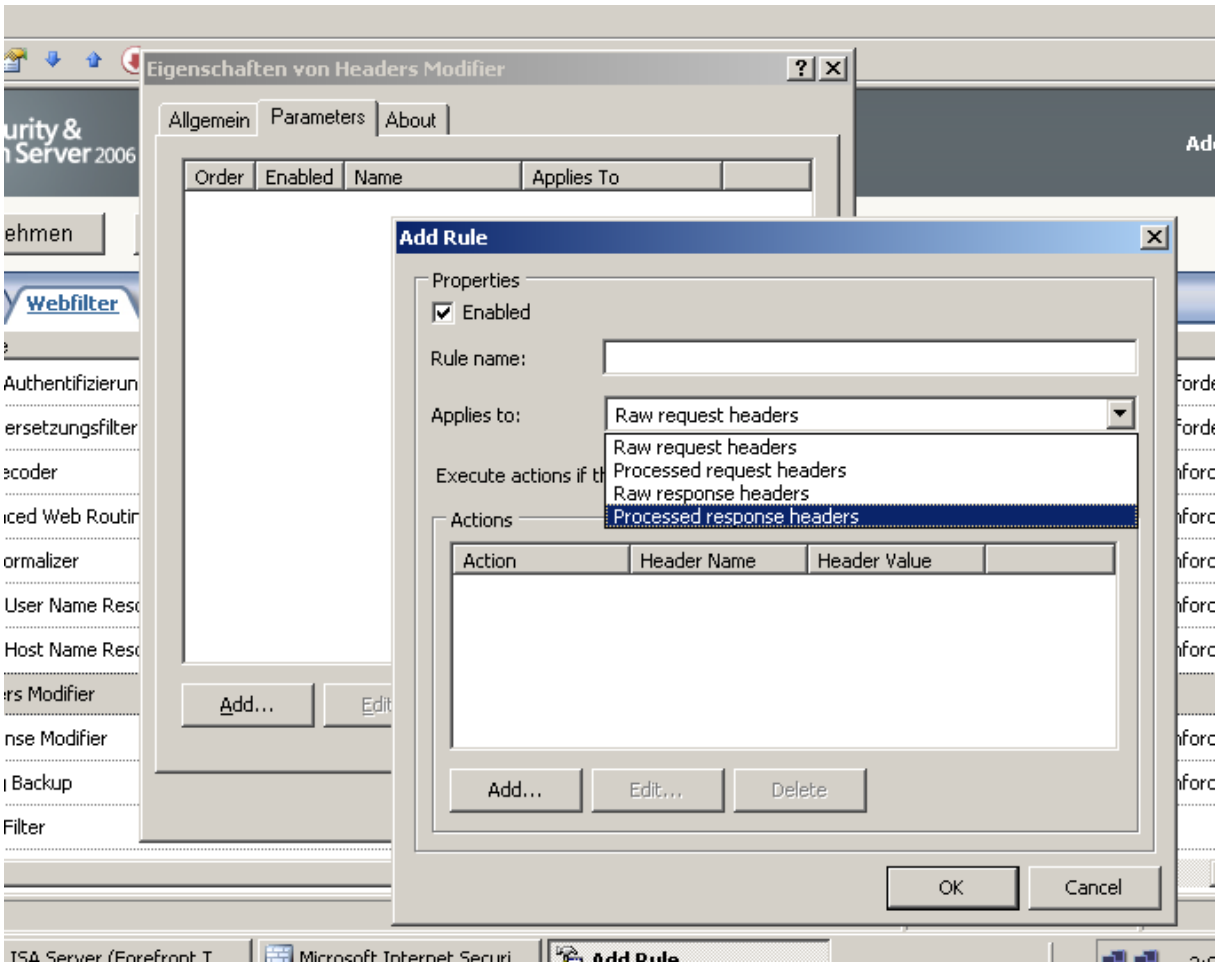
Client User Name Resolver

Konvertiert Firewall Client Logins zu Active Directory Benutzernamen fuer eine bessere Uebersicht. Habe ich noch nicht getestet, klingt aber einfach und sinnvoll ☺



Header Modifier

Kann automatisiert HTTP Header modifizieren. Braucht man nur in speziellen Szenarien?! – Erst mal ungetestet.

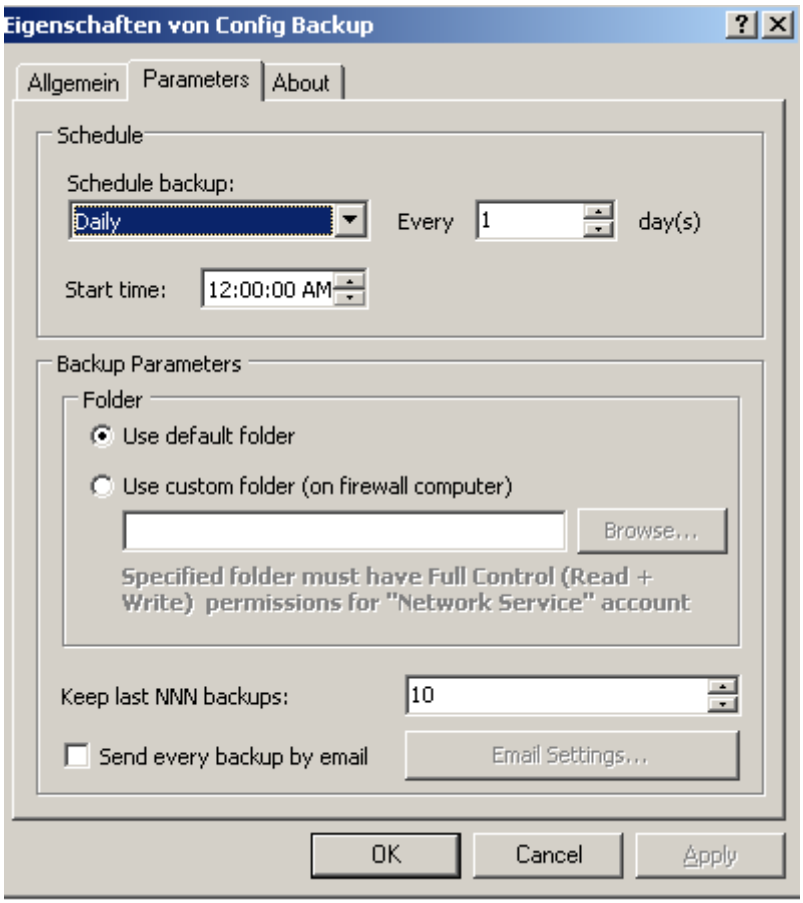


Mein Liebling

Config Backup

Klar kann man auch das VB Script nehmen und per Taskplaner ausfuehren, welches wir im ISA 2006 Handbuch beschreiben, aber diese Loesung finde ich auch sehr elegant und sie funktioniert auch!

Und das geniale hier: Man kann festlegen, wieviele Backup Sets behalten werden. Bei „unserem“ Script wird die alte Backup-Datei immer ueberschrieben.


Eigenschaften von Config Backup
Allgemein
Parameters
About
Schedule
Schedule backup:
Daily
Every
1
day(s)
Start time:
12:00:00 AM
Backup Parameters
Folder
Use default folder
Use custom folder (on firewall computer)
Browse...
Specified folder must have Full Control (Read + Write) permissions for "Network Service" account
Keep last NNN backups:
10
Send every backup by email
Email Settings...
OK
Cancel
Apply