ISA Server 2004 – Protokollierung - Von Marc Grote

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Übersicht Monitoring wurde eine Zusammenfassung aller Überwachungsfunktionen des ISA Server 2004 gegeben. Das vorliegende Kapitel beschreibt die Möglichkeit, die Protokollierungsfunktionen des ISA Server 2004 zu konfigurieren.

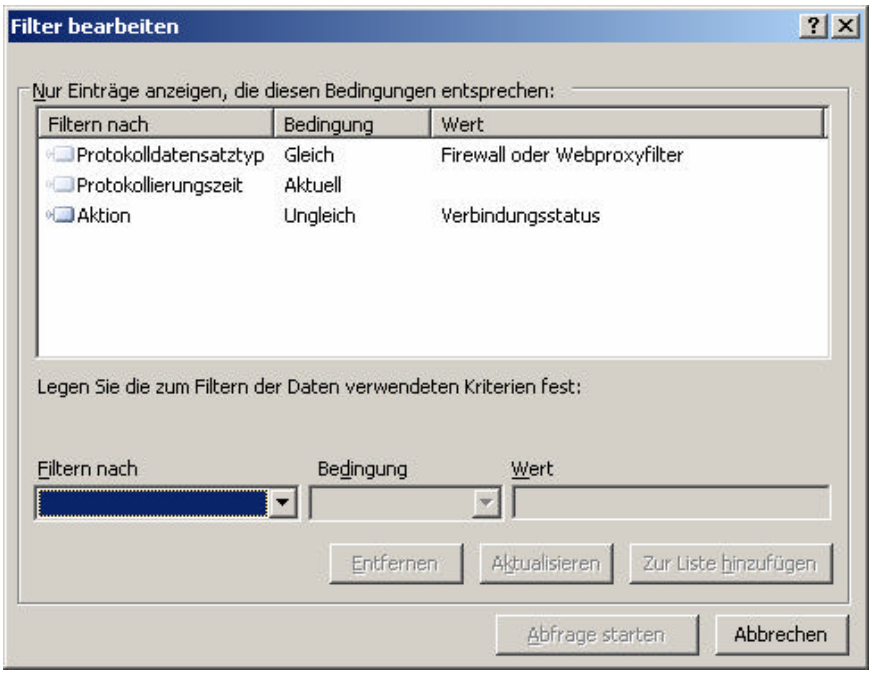
Einleitung

ISA Server 2004 protokolliert die Aktivität auf dem ISA Server-Computer. Diese Protokollierungen werden zum Erkennen von Sicherheitsverletzungen, zum Generieren von Berichten und zur Problembehandlung bei Netzwerkproblemen verwendet. Sie können festlegen, welche Informationen in den Protokollierungen in welchem der folgenden Formate gespeichert werden. Es stehen zur Auswahl:

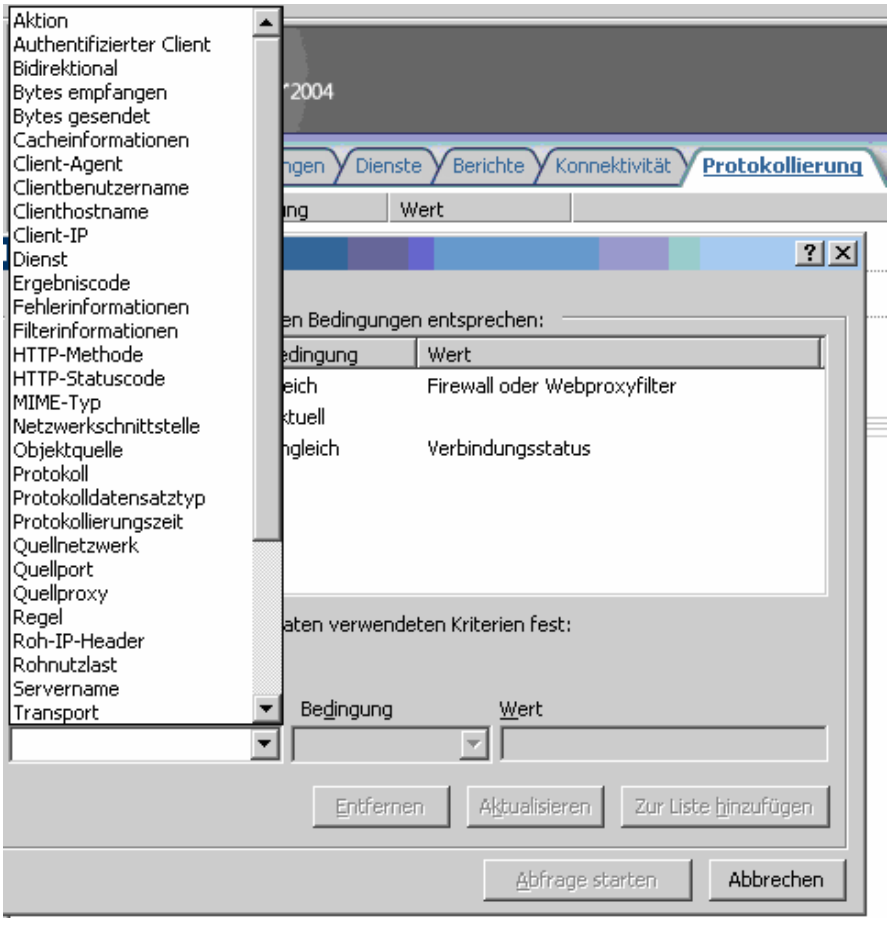
- Datei
- SQL
- MSDE

In der Protokollanzeige kann die Firewallprotokollierung und/oder die Webproxyprotokollierung angezeigt werden. Sie können die derzeit im Protokollrepository gespeicherten Onlineprotokollierungen anzeigen oder das Repository abfragen, um frühere Protokollierungen abzurufen. In beiden Modi können Sie Filter definieren, um die angezeigte Datenmenge zu begrenzen und übersichtlichere Auswertungen definieren zu können.

Der Standard Abfrage Filter filtert nach dem Protokolldatensatztyp = Firewall- oder Webproxyfilter, der Anzeige der Daten in Echtzeit und nach jedem Verbindungsstatus.

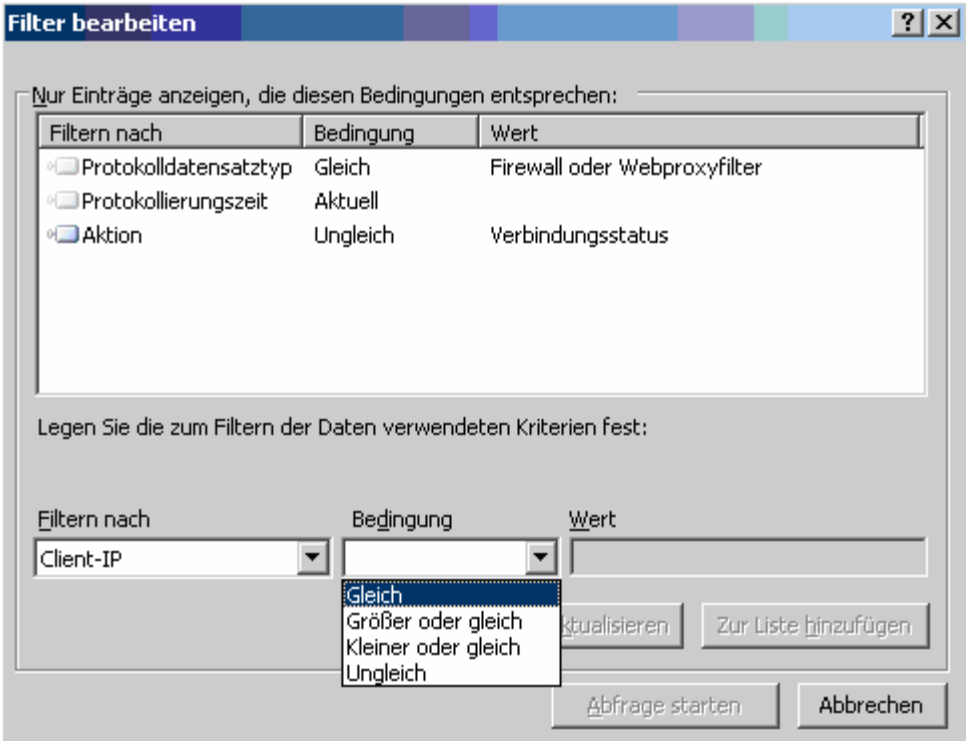


Sie können den Filter modifizieren, indem Sie im Standard-Filter unter *Filtern nach* den Filtertyp auswählen und dann anpassen.
Sie können auch einen eigenen Filter erstellen, indem Sie unter Filtern nach einen Filter auswählen. Es stehen zahlreiche Filtermöglichkeiten zur Verfügung. Eine Übersicht über die Filtermöglichkeiten zeigt das nächste Bild.

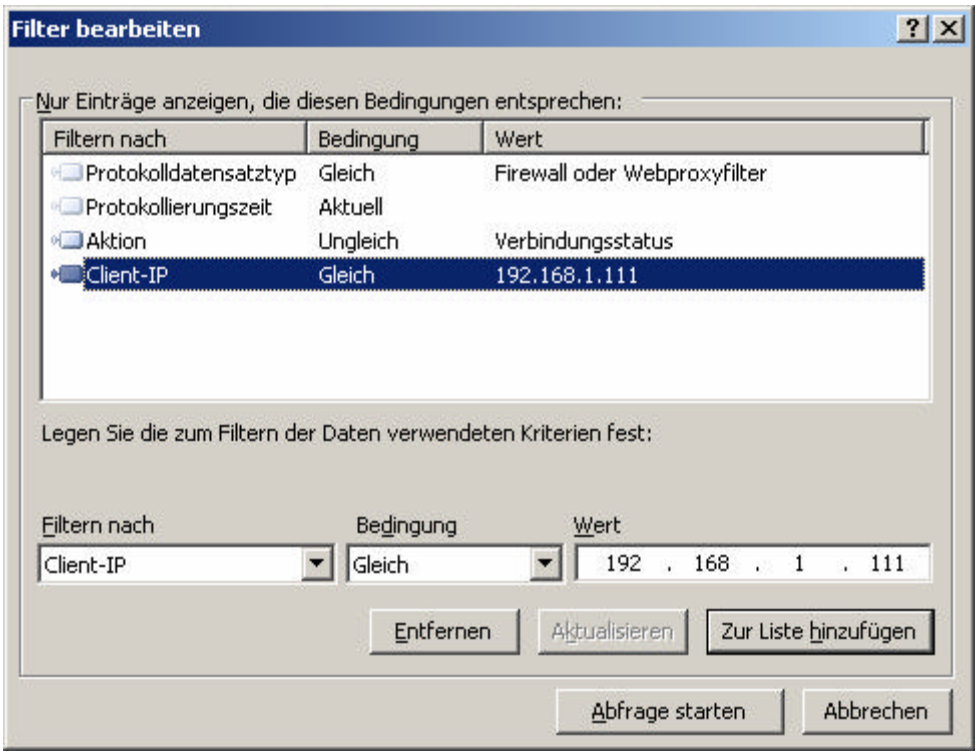


Nachdem Sie einen Filtertyp ausgewählt haben (in diesem Beispiel Client-IP) können Sie noch eine Bedingung zur Filterung hinzufügen.

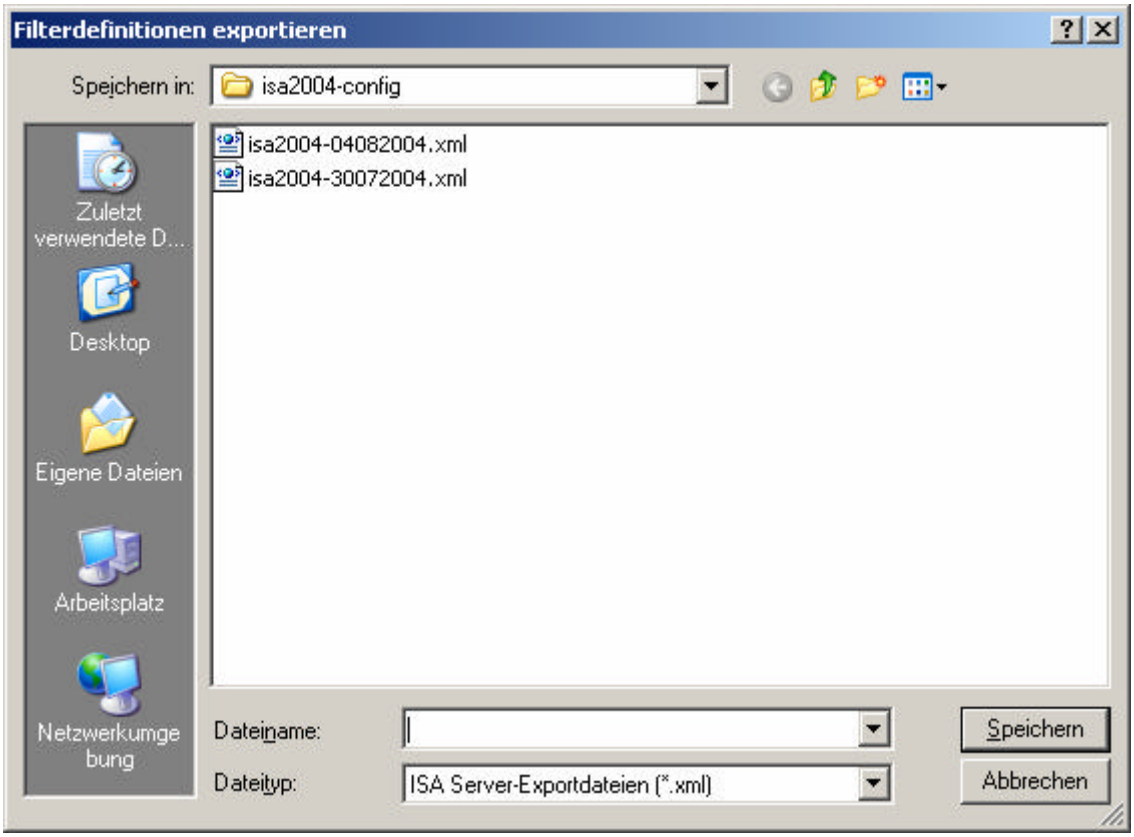
Achtung: Die zur Verfügung stehenden Filter Bedingungen sind immer abhängig von der Filterart (Filtern nach). In diesem Beispiel ist die Filterart Client-IP und für diese Filterart stehen die Bedingungen *Gleich, Größer oder gleich*, *kleiner oder gleich* und *Ungleich* zur Verfügung.



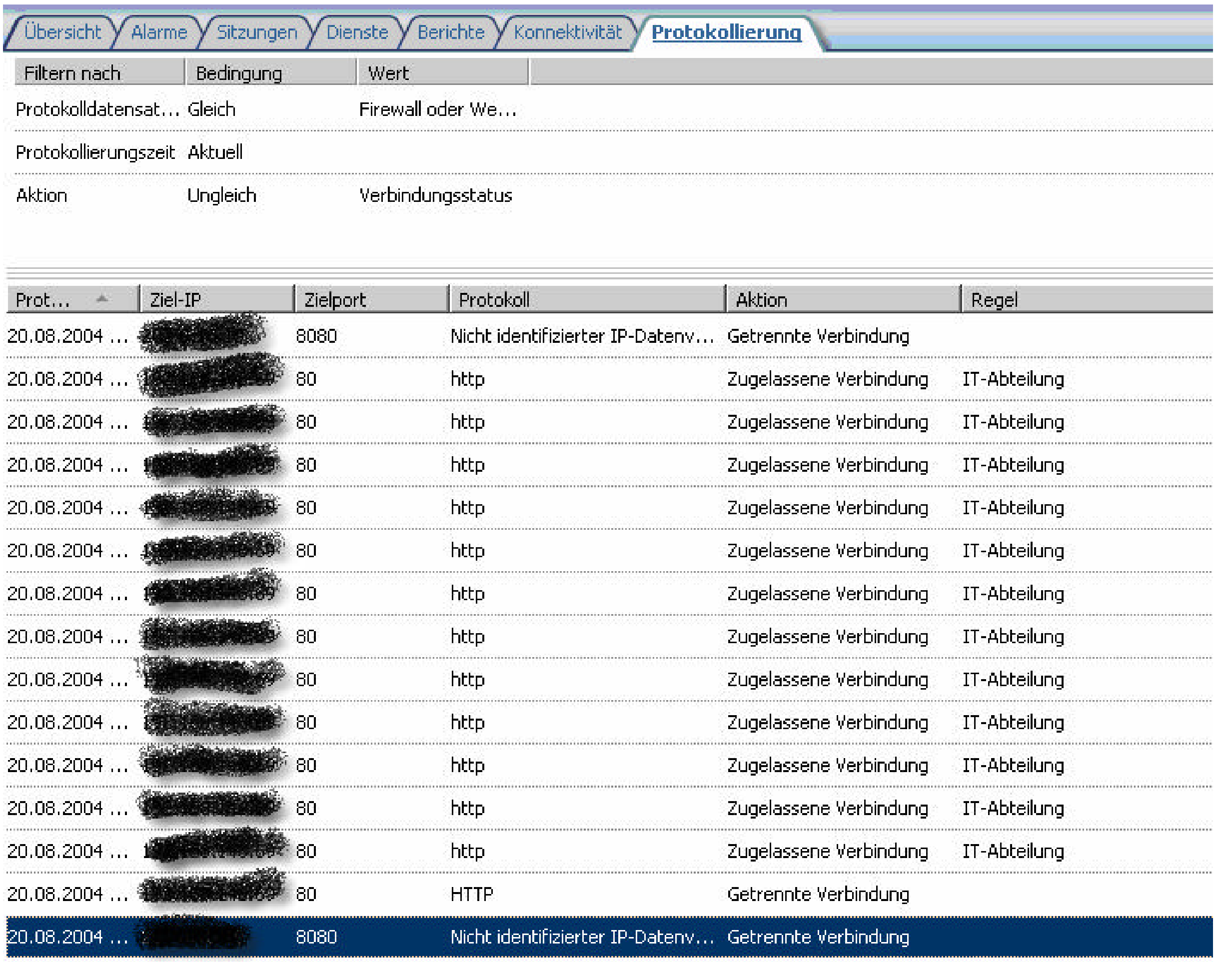
Als *Wert* wurde in diesem Beispiel die IP-Adresse 192.168.1.111 eingegeben. Zum Abschluss müssen Sie noch auf *Zur Liste hinzufügen* klicken, damit der neue Filter zur Filterbedingung hinzugefügt wird und auf *Abfrage starten* klicken.



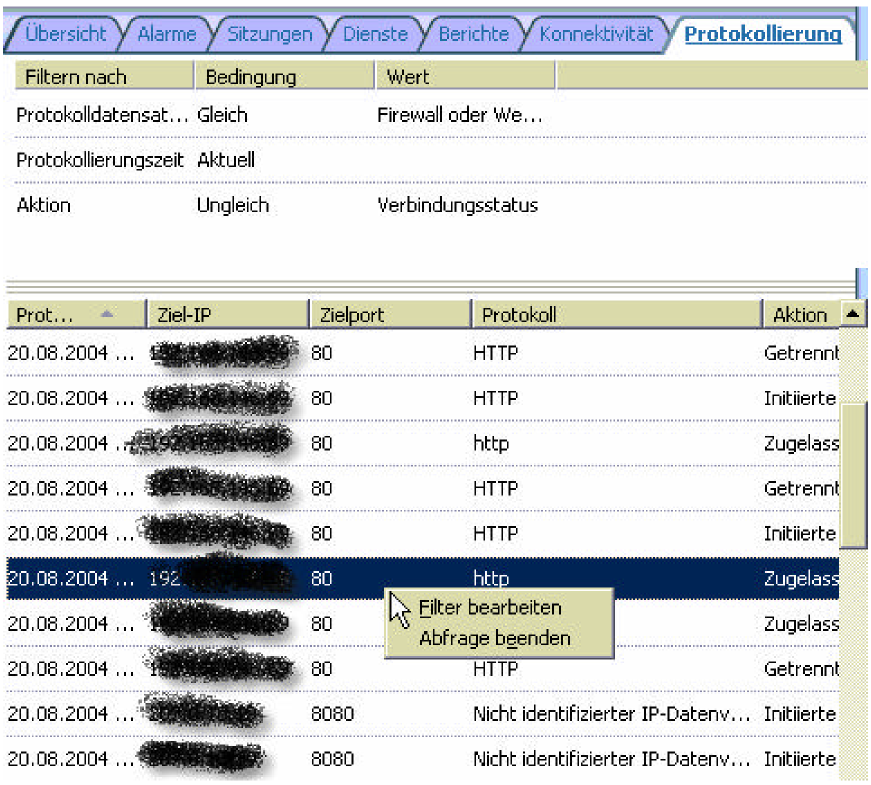
Einmal definierte Filteroptionen können exportiert und auch wieder importiert werden. Dieses Feature ist sehr hilfreich, weil sich der Administrator damit eine Sammlung an Filterdefinitionen erstellen kann, welche in einem bestimmten Verzeichnis gespeichert werden und dann bei Bedarf importiert werden können.
Somit stehen dem Administrator fertige Vorlagen zur Verfügung mit welchem er die Protokolldaten filtern kann.



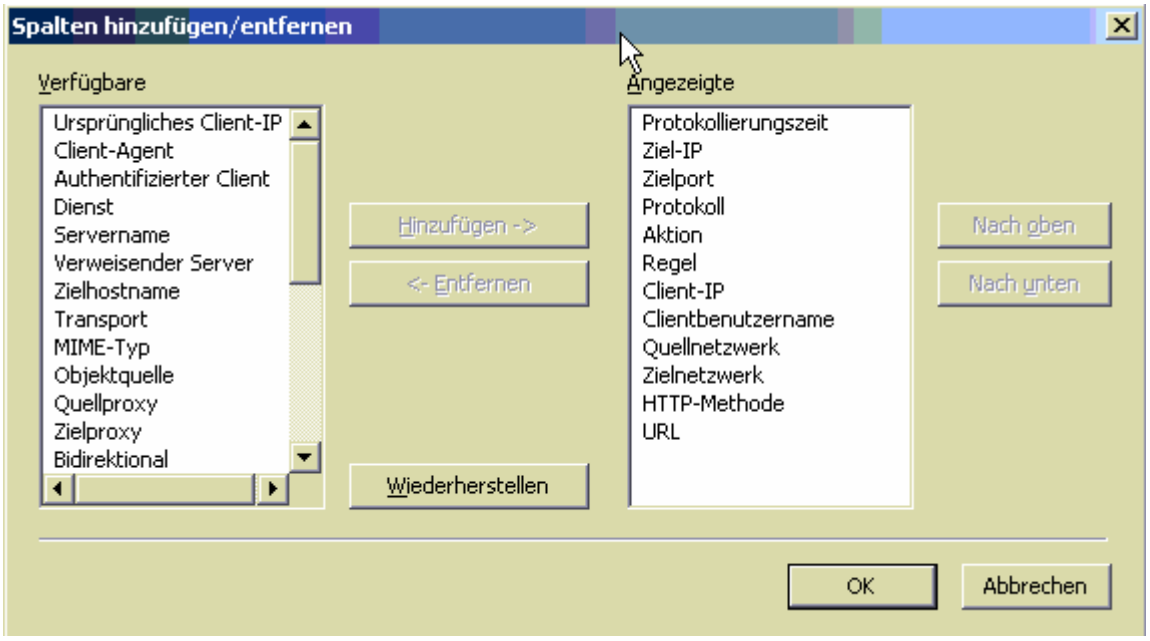
Der ISA Server 2004 zeigt jetzt in „Echtzeit“ die Protokolldaten, basierend auf Ihrer Filterdefinition an.



Mit einem Rechtsklick mit der Maus im Protokollfenster können Sie die *aktuelle Abfrage beenden* oder den *Filter bearbeiten*.



Sie können dem Protokollfenster zusätzliche Spalten Hinzufügen/Entfernen, sowie den Ursprungszustand *Wiederherstellen*.

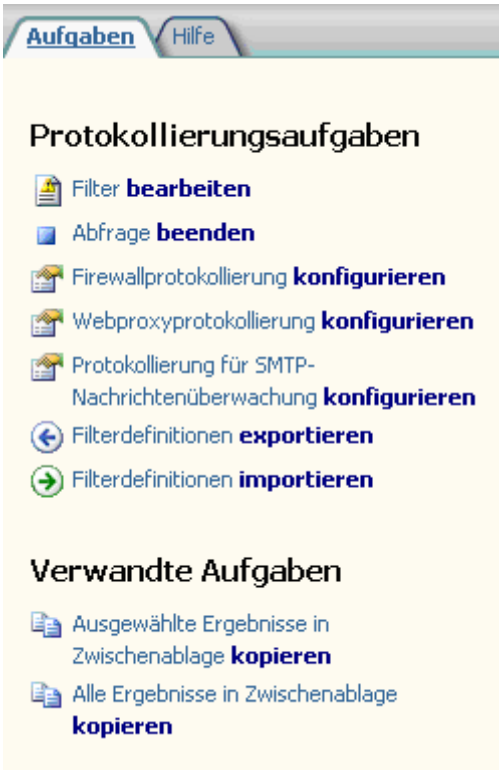


Nachdem wir uns um die Anzeige der Protokolldaten und deren Filterung gekümmert haben, gehen wir jetzt zur Konfiguration der Protokollierung über.

Der ISA Server 2004 bietet die Möglichkeit eine …

- Firewallprotokollierung
- Webproxyprotokollierung und
- SMTP Nachrichtenüberwachungsprotokollierung

einzurichten.



Folgende Protokollspeicherformate stehen zur Verfügung:

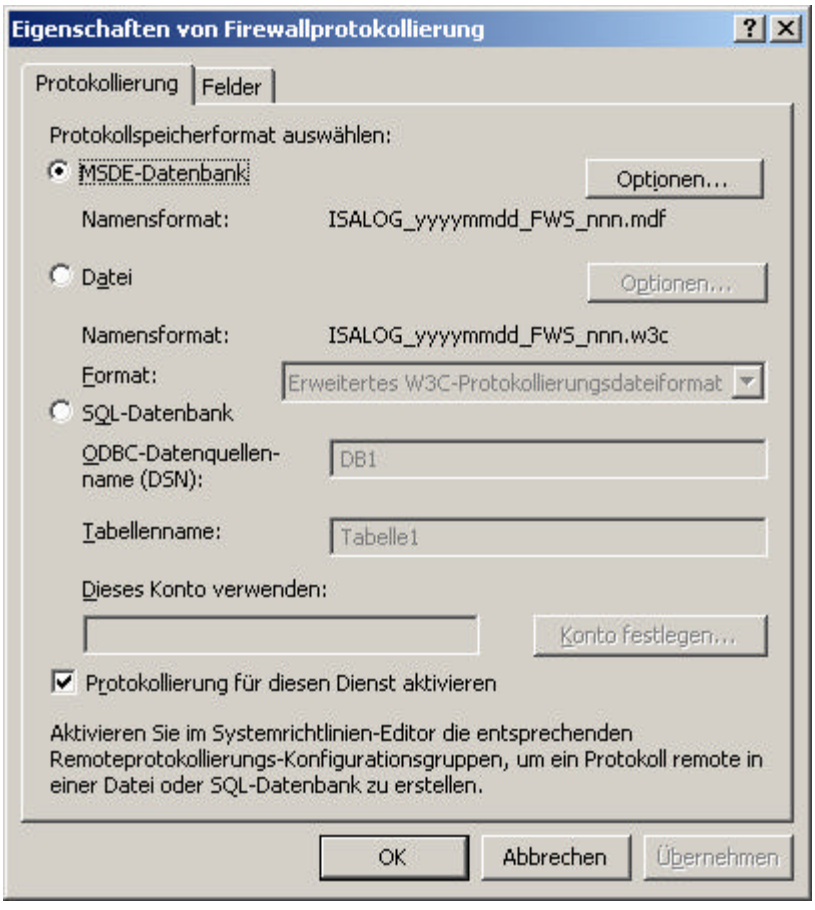
- MSDE-Datenbank
- Datei
  - W3C-Protokollierugsformat
  - ISA-Server Dateiformat
- SQL Datenbank über ODBC

Der Firewall- und Webproxydienst protokollieren die Daten per Default in eine MSDE Datenbank.
Bei der MSDE (Microsoft SQL Server Desktop Engine) handelt es sich um eine kostenlose, funktionsreduzierte Datenbank aus dem Hause Microsoft. Für mehr Informationen über die MSDE sei auf folgende Webseite verwiesen:
http://www.microsoft.com/sql/msde/

Bemerkung: Während der Installation des ISA Server 2004 wird eine MSDE Datenbank installiert.

Die SMTP Nachrichtenüberwachungsprotokollierung erfolgt per Default im erweiterten W3C Nachrichtenformat.

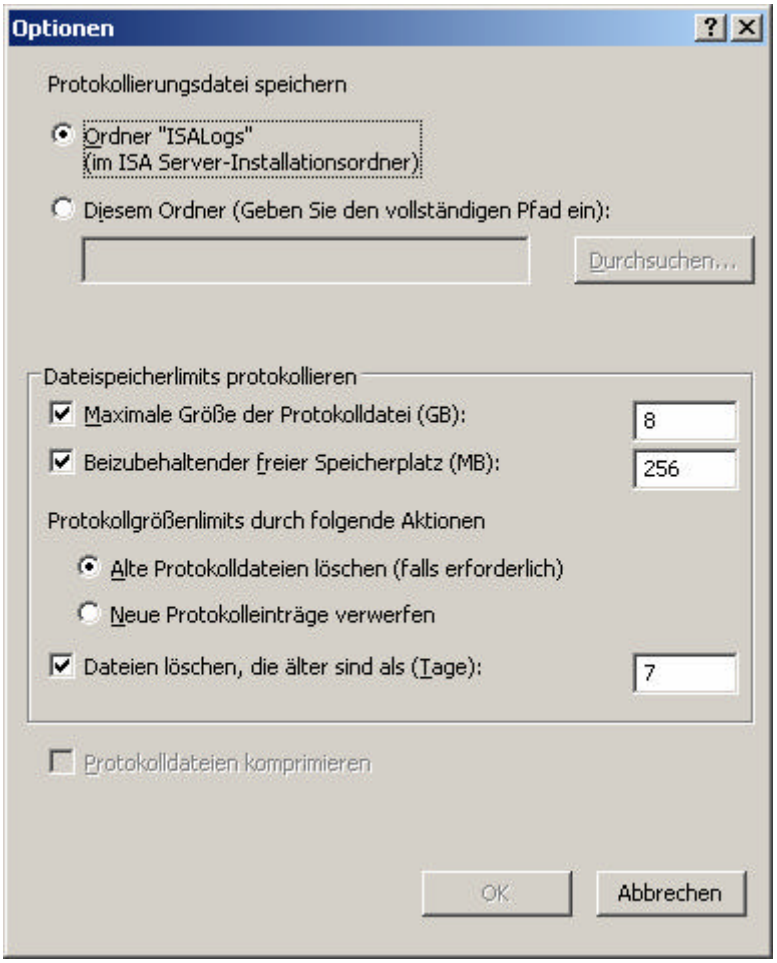
Im folgenden Bild sehen Sie die Möglichkeit das Protokollspeicherformat auszuwählen.



Achten Sie darauf, dass der Haken bei *Protokollierung für diesen Dienst aktivieren* aktiv ist. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden keine Ereignisse protokolliert.

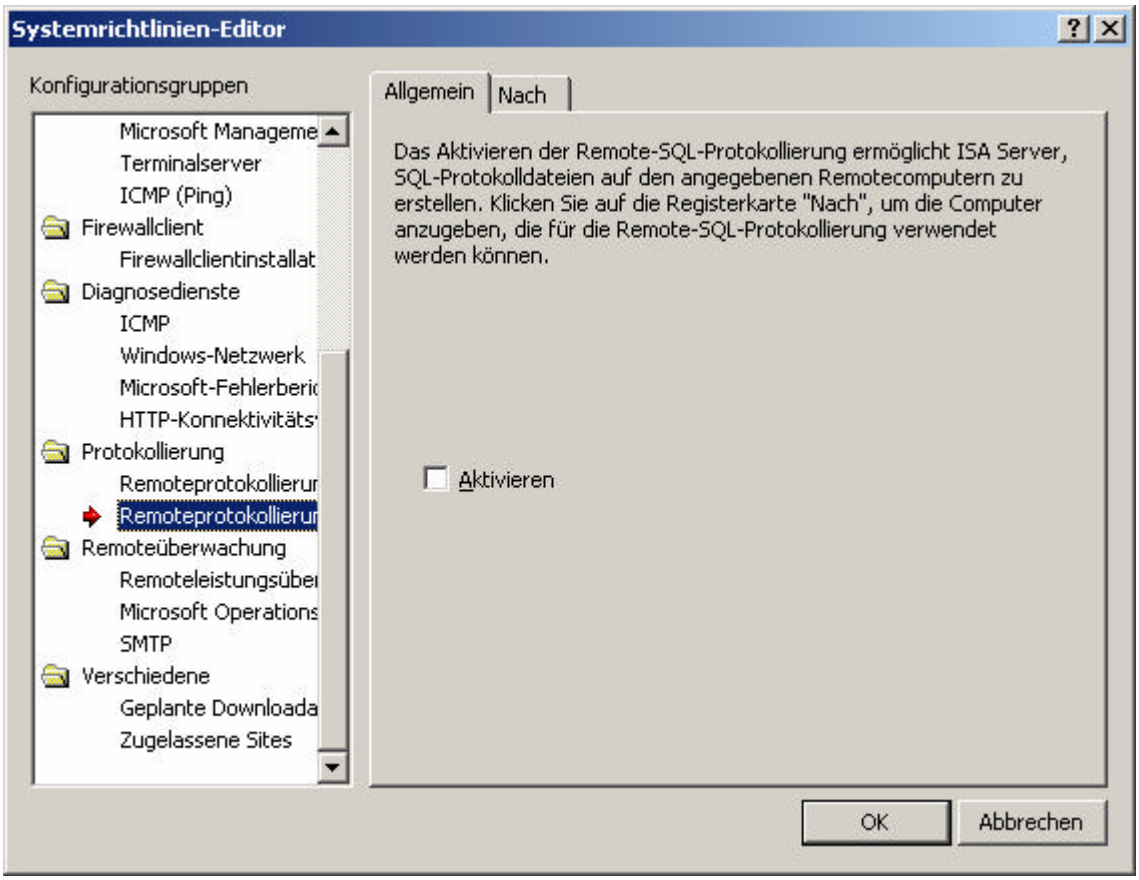
Sie können für die MSDE-Datenbank diverse Optionen konfigurieren.
Es besteht die Möglichkeit, den Ort der Protokolldatei anzugeben, Dateispeicherlimits festzulegen und eine Aktion zu definieren, welche Aktion beim Erreichen des Protokollgrößenlimits durchgeführt werden soll.

Die maximale Protokolldateigröße bei der Verwendung der MSDE beträgt 8 GB. Insider sehen hier schon, dass es sich nicht um die Standard MSDE handelt, deren Größe auf maximal 2 GB limitiert ist, sondern um die erweiterte MSDE.



Die Protokolldateien können zur Reduzierung des Platzbedarfs komprimiert werden. Dieses Feature steht jedoch nur auf Partitionen mit dem NTFS Dateisystem zur Verfügung.

Wenn Sie eine Protokollierung in eine SQL Datenbank AUSSERHALB des ISA Server 2004 planen, müssen Sie mit Hilfe des Systemrichtlinien-Editor die *Remoteprotokollierung für SQL* Aktivieren und im Reiter *Nach* das Netzwerk angeben, welches den Remote SQL Server beinhaltet.



Stand: 21.08.2004/MG. http://www.it-training-grote.de