Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

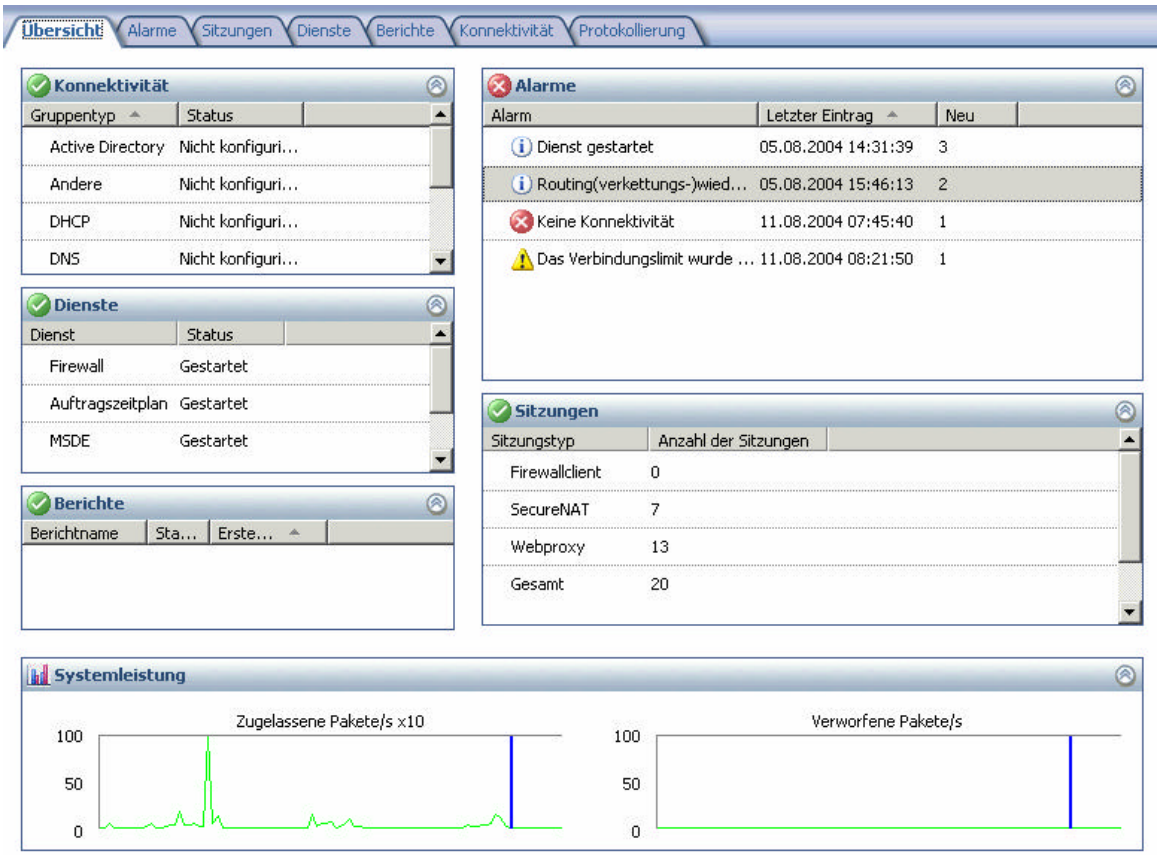
Einleitung

Der Microsoft ISA Server 2004 bietet sehr umfangreiche Monitoring Möglichkeiten um den Status der Firewall und des Proxy-Servers zu überwachen.
Im Vergleich zum ISA Server 2000 stehen jetzt leistungsfähige Analysetools zur Verfügung. Eines der Highlights ist die Möglichkeit, die ISA Protokolldaten in Echtzeit zu analysieren und mit Filtern nach den gewünschten Daten zu filtern.

Dashboard

Zentrale Anlaufstelle ist das so genannte „Dashboard“ In der Übersichtsansicht der ISA Server-Verwaltung wird in Echtzeit eine Momentaufnahme der zusammengefassten ISA Server-Aktivität angezeigt. Mit den übersichtlich auf einer Seite angeordneten wichtigen Informationen können Probleme schnell erkannt und behoben werden.

Das Dashboard und alle folgenden Monitoring Möglichkeiten findet Ihr im Container „Überwachung“ des ISA Verwaltungstool unterhalb des ISA Server Computerobjektes.



Ich beschreibe jetzt die Funktion der einzelnen Fenster des ISA Dashboards:

Konnektivität:

ISA 2004 bietet die Möglichkeit zur Überprüfung der Konnektivität von wichtigen Systemen innerhalb der Organisation wie DHCP Server, DNS Server und Active Directory, sowie z. B. der Prüfung der Verfügbarkeit einer Website durch das Ausführen eines HTTP GET Befehls. Mit diesem Feature kann ein Administrator schnell reagieren, wenn unternehmenskritische Komponenten nicht erreichbar sind, von denen der ISA Server zum Beispiel abhängig sein könnte.

Dienste:

Listet den Status der installierten ISA 2004 Dienste auf.

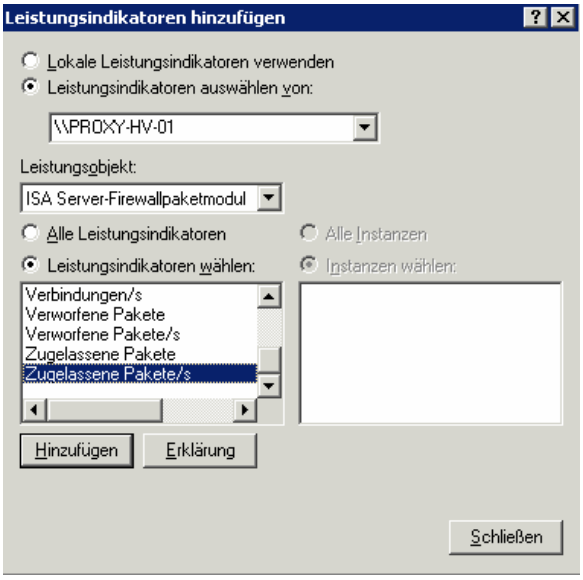
Berichte:

ISA 2004 bietet die Möglichkeit der Definition so genannter Berichtsaufträge mit welchen man sich zum Beispiel die protokollierte Internetaktivität in grafisch aufbereiteter Form anzeigen lassen kann. Dieses Feature ist sehr hilfreich zur Präsentation von Daten für Führungsstellen oder einfach nur zur Übersicht für den Firewall-Administrator. Das Dashboard zeigt den Status der konfigurierten Berichtsaufträge an.

Systemleistung:

Die Systemleistung zeigt zwei Zähler des Systemmonitors an.

- Zugelassene Pakete pro Sekunde x10 zeigt die Datenmengen an, welche der ISA pro Sekunde durch die Firewallengine führt.
- Verworfene Pakete pro Sekunde zeigen die Datenmengen an, welche der ISA pro Sekunde an der Firewall verweigert (verwirft).



Bemerkung:

Eine hohe Anzahl verworfener Pakete ist häufig ein Anzeichen für Denial of Service (DoS) Angriffe auf den ISA Server.

Alarme:

Hier werden ISA Server Systemmeldungen angezeigt, welche für den einwandfreien ISA Betrieb sehr wichtig sind. Wie man der Grafik entnehmen kann, werden hier z. B. gestartete ISA Dienste angezeigt oder Informationen über Webverkettungsprobleme uvm.

Sitzungen:

Hier wird die Anzahl der Verbindungen (Sitzungen) der drei ISA 2004 Clientarten . . .

- SecureNAT Client
- Firewall Client
- Webproxy Client

angezeigt.

Die Anzahl spiegelt nicht unbedingt die tatsächliche Anzahl der Client Computer wieder, weil ein Client mehrere Clientarten gleichzeitig verwenden kann.

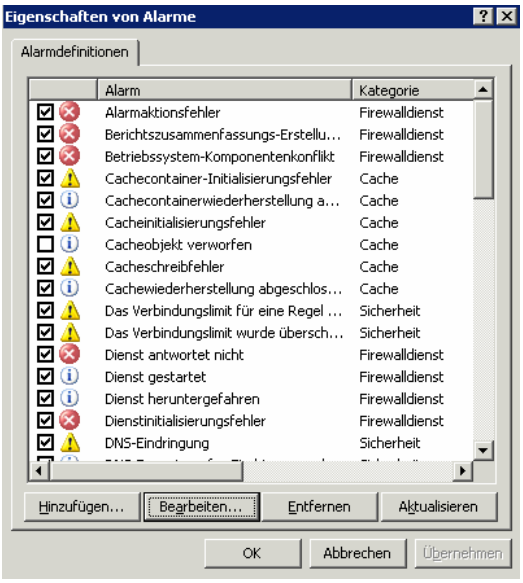
Alarme

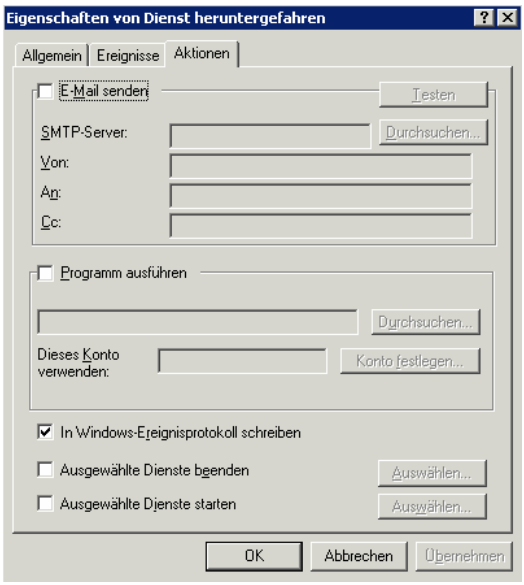
In der Registerkarte „Alarme“ protokolliert der ISA Server wichtige Systemereignisse wie das Starten und Beenden von ISA 2004 Diensten und zum Beispiel fehlende Konnectivity-Verbindungen. In der Spalte „Kategorie“ wird die beteiligte ISA 2004 Komponente angezeigt.

Alarm	Letzter Eintrag	Status	Kategorie
Dienst gestartet	05.08.2004 14:31:39	Neu	Firewalldienst
Dienst gestartet	05.08.2004 14:31:04	Neu	Firewalldienst
Dienst gestartet	05.08.2004 14:31:38	Neu	Firewalldienst
Dienst gestartet	05.08.2004 14:31:39	Neu	Firewalldienst
Routing(verkettungs-)wiederherstellung	05.08.2004 15:46:13	Neu	Routing
Routing(verkettungs-)wiederherstellung	05.08.2004 15:41:03	Neu	Routing
Routing(verkettungs-)wiederherstellung	05.08.2004 15:46:13	Neu	Routing
Keine Konnektivität	11.08.2004 07:45:40	Neu	Firewalldienst
Keine Konnektivität	11.08.2004 07:45:40	Neu	Firewalldienst
Das Verbindungslimit wurde überschritten	11.08.2004 08:21:50	Neu	Sicherheit
Das Verbindungslimit wurde überschritten	11.08.2004 08:21:50	Neu	Sicherheit

Der ISA 2004 bietet auch ausgefeilte Benachrichtigungsoptionen, welche bei Erreichen eines bestimmten Systemzustandes aktiv werden.

Etwas versteckt findet Ihr in der Aufgaben Taskbar die Möglichkeit Alarmdefinitionen zu konfigurieren. Mit Hilfe dieser Konfiguration kann sich der ISA Administrator bei dem Eintreten bestimmter Ereignisse z. B. per E-Mail informieren zu lassen.





Neben der Möglichkeit eine E-Mail Benachrichtigung könnt Ihr bei Erreichen des konfigurierten Alarms auch ein Programm ausführen lassen, Informationen in das Windows Ereignisprotokoll schreiben lassen und z. B. bestimmte Dienste zu beenden. Aus Sicherheitsgründen kann es empfehlenswert sein, bei einem Angriff auf den ISA Server welche die Funktionalität des Systems kompromittiert, die ISA Firewalldienste zu Beenden. Dann ist zwar keine Internetkonnektivität mehr möglich, der ISA und das dahinterliegende LAN vor Angriffen geschützt. Das Beenden der Firewalldienste sollte auf alle Fälle in der Security Policy der EDV Abteilung vermerkt werden und von der Geschäftsführung abgesegnet sein.

Der ISA Server 2004 macht von dem Beenden des Firewallengine Dienstes Gebrauch, wenn z. B. das Firewall Logging nicht mehr gewährleistet ist

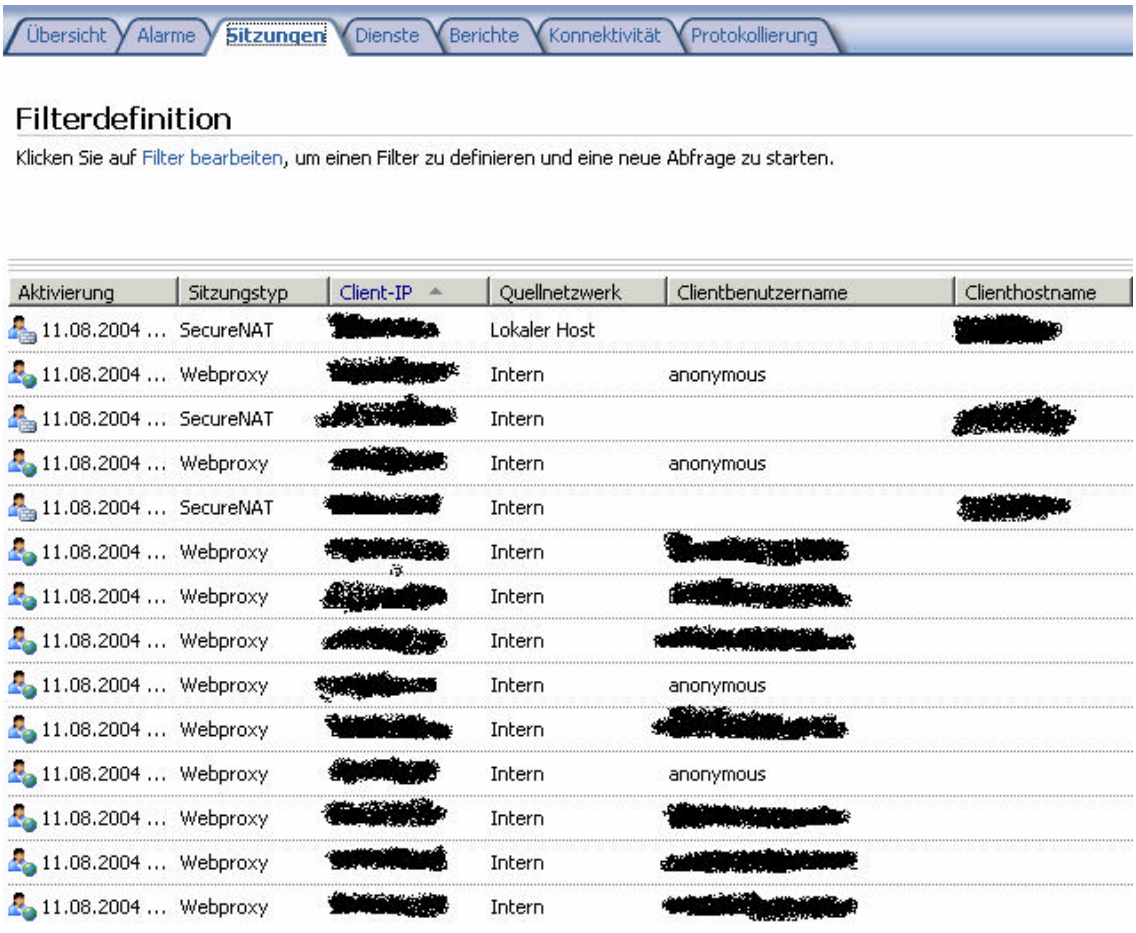
Sitzungen

Im Reiter „Sitzungen“ werden alle Verbindungen zum ISA Server 2004 angezeigt.

ISA 2004 zeigt hier den Verbindungszeitpunkt, den Sitzungstyp, die Client IP Adresse und viele weitere Informationen an.

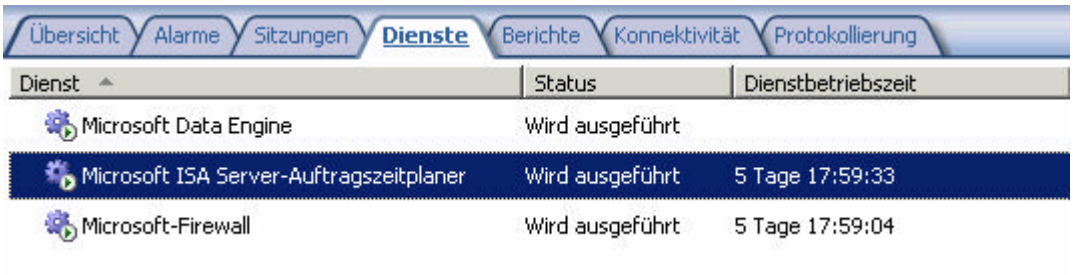
Mit einem Rechtsklick auf eine der Spaltenüberschriften besteht die Möglichkeit, selbst Spalten hinzuzufügen bzw. zu entfernen. Es ist ebenfalls möglich die Spalten individuell zu verschieben.

Über den Punkt „Filter bearbeiten“ kann man eigene Abfragen definieren um das Suchergebnis zum Beispiel einzuschränken.



Dienste

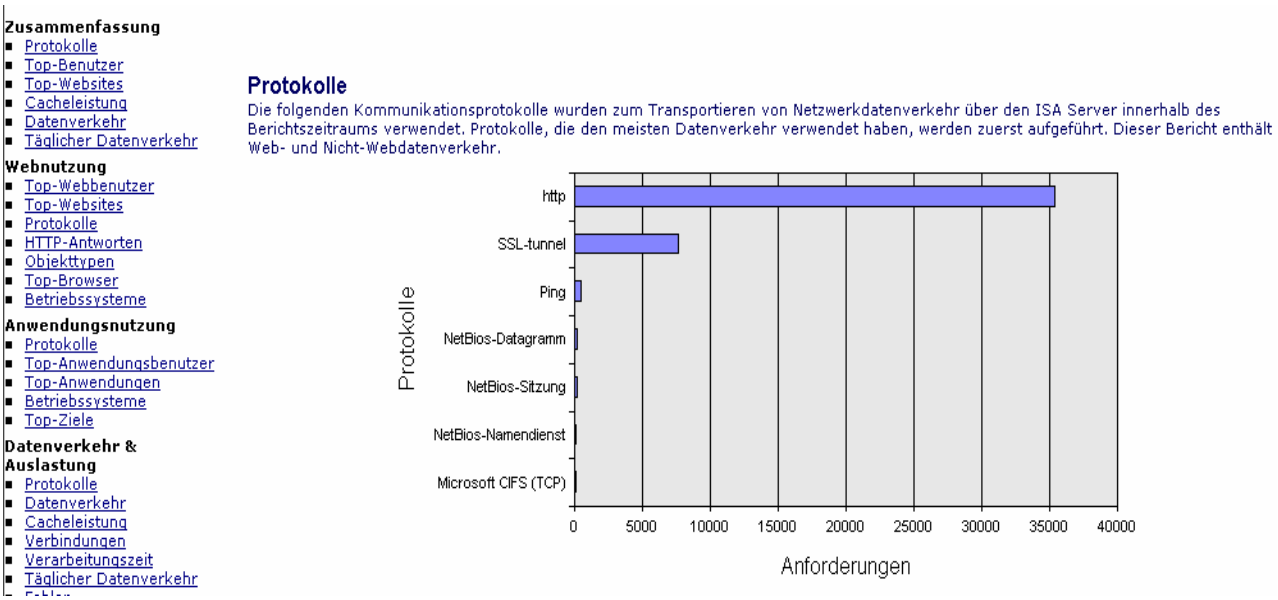
In dem Reiter „Dienste“ kann man sich den Status der einzelnen ISA 2004 Dienste anzeigen lassen und jeden der Dienste Starten und Beenden.



Berichte

ISA 2004 bietet die Möglichkeit der Definition von so genannten Berichtsaufträgen mit dessen Hilfe man sehr einfach grafische HTML Reports generieren kann. Berichtsaufträge sind ein sehr nützliches Werkzeug um sich zum Beispiel die Top 10 der am meisten aufgesuchten Webseiten anzuzeigen oder den Prozentsatz der eingesetzten Webbrowser.

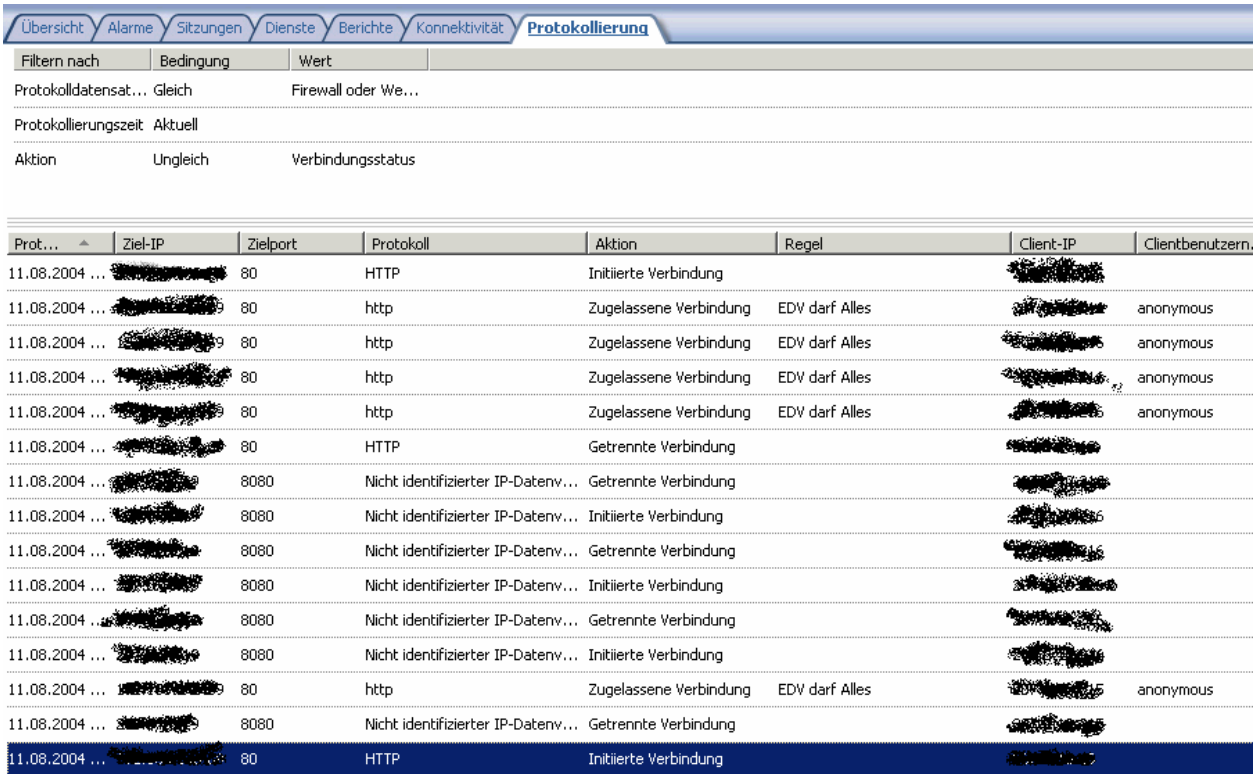
Durch einen Doppelkick auf den Berichtsnamen „Gesamtstatus“ öffnet sich nach kurzer Zeit der Webbrowser mit einem detailliertem HTML Report.



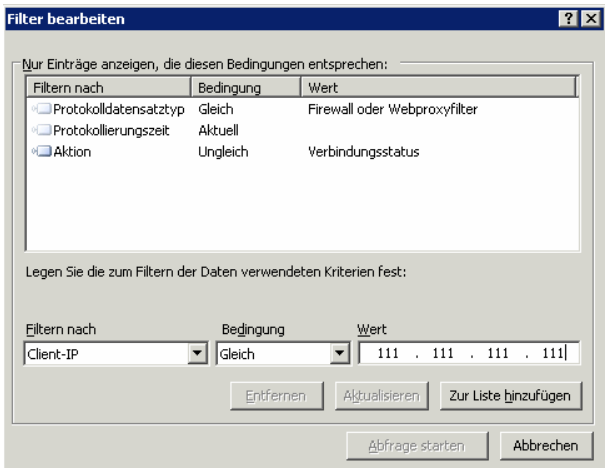
Protokollierung

Der Reiter „Protokollierung“ zeigt den Datenverkehr von und zum ISA 2004 endlich in „Echtzeit“ an. Über sehr umfangreiche Filter besteht die Möglichkeit, die angezeigten Protokolldaten zu modifizieren.

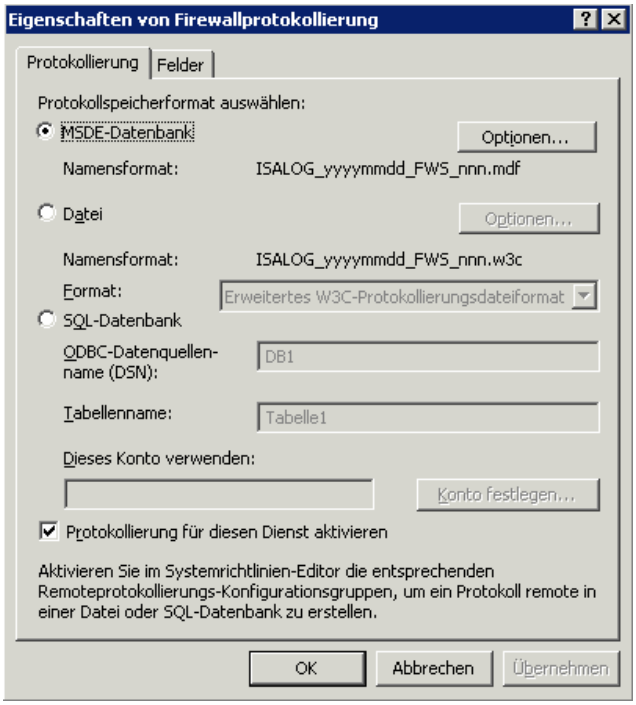
Auch hier besteht wieder die Möglichkeit durch einen Rechtsklick auf eine Spaltenüberschrift, Spalten hinzuzufügen und zu entfernen.



Über die sehr umfangreichen Filtermöglichkeiten kann man die Anzeige der geloggten Daten modifizieren um eine effektivere Suche zu ermöglichen.



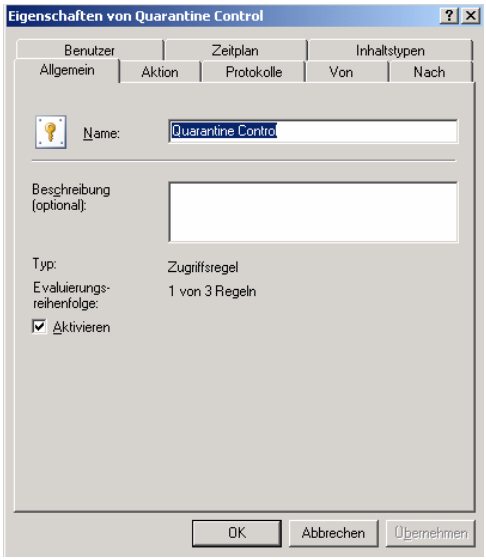
Es besteht die Möglichkeit, die Art des Loggings am ISA Server 2004 zu modifizieren. Per Default protokolliert der ISA 2004 die Protokolldaten in eine per Default installierte MSDE Version.



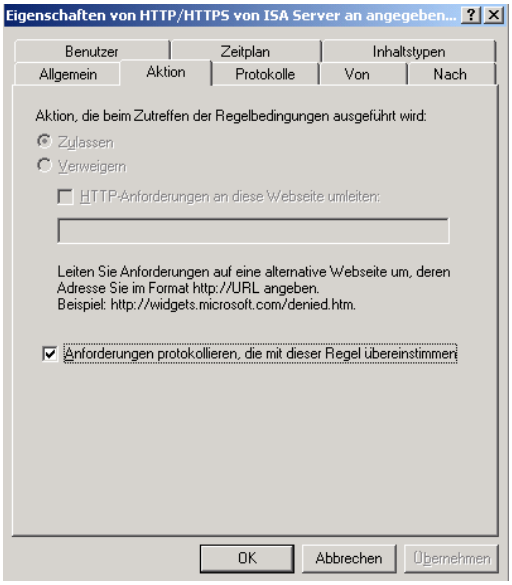
Was wird protokolliert

Der Administrator kann an verschiedenen Stellen des Systems festlegen, welche Informationen protokolliert werden soll.

Generell besteht für jede Firewall Regel die Möglichkeit, auf dieser Regel basierenden Datenverkehr zu protokollieren. Per Default ist auch jede Regel „Protokoll aktiviert“.



Per Default werden auch die ISA 2004 eigenen Systemrichtlinienregeln protokolliert. Um die Systemrichtlinienregeln anzeigen zu lassen müsst Ihr im ISA Verwaltungstool unterhalb des ISA Computerobjektes mit der rechten Maustaste auf „Firewallregel“ klicken und im Kontextmenü – Ansicht – Systemrichtlinien Regeln anzeigen – aktivieren. Danach könnt Ihr für die gewünschten Regeln im Reiter „Aktion“ die Protokollierung deaktivieren.



Zu guter Letzt ist es auch noch möglich, verworfene Pakete zu protokollieren. ISA 2004 protokolliert per Default jedes verworfene Paket.
Die Einstellung, ob verworfene Pakete protokolliert werden sollen, wird ebenfalls im ISA Verwaltungstool eingestellt. Der Weg zur Konfiguration lautet:
ISA Computer Objekt – Konfiguration – Allgemein – „Erkennung von Eindringversuchen und DNS Angriffen aktivieren“. Dort kann man im Reiter „Allgemeine Angriffe“ „Verworfene Pakete protokollieren“.

Bemerkung:

Es ist immer wichtig, das „gesunde Maß“ an dem Verhältnis zwischen protokollierten Daten und dem Verzicht auf Protokollierung zu finden. Zuviel Protokollierung führt zu unübersichtlichen Logdateien, verlangsamt das System und führt schnell zu überschriebenen Logdateien wenn das GrößenLimit der Protokolldatei erreicht ist.

Die Default Logdateigröße für das Firewall- und Webproxy Log beträgt 8 GB. Beide Logs werden in einer MSDE protokolliert. Nur die Logdatei für die SMTP Nachrichtenüberwachung wird im erweiterten W3C Format geschrieben.