

Musterlösung für
Schulen in
Baden-Württemberg

Windows 2003

Basiskurs Windows-Musterlösung Version 3

Stand: 26.07.10



Impressum

Herausgeber

Zentrale Planungsgruppe Netze (ZPN)
am Kultusministerium Baden-Württemberg

Autor:

Martin Resch

Endredaktion

Adrian Koch, Martin Resch

Weitere Informationen

<http://www.lehrerfortbildung-bw.de/netz/>

Veröffentlicht: 2010

© Zentrale Planungsgruppe Netze (ZPN)

Inhaltsverzeichnis

13. Internetsteuerung.....	1
13.1. Festlegen von Standardeinstellungen.....	2
13.1.1. Proxyserver auf den Clients konfigurieren.....	2
13.1.2. Konfiguration der Räume.....	3
13.1.3. Voreinstellungen festlegen.....	3
13.2. Die ISA-Konsolensteuerung.....	4
13.2.1. Der Grundzustand.....	5
13.2.2. Speichern und Wiederherstellen.....	6
13.2.3. Die Regeln.....	6
13.2.4. Lokaler Webserver veröffentlichen.....	6
13.2.5. Datenverkehr vom internen Netzwerk zum lokalen Host.....	6
13.2.6. Internetzugriff für Server.....	6
13.2.7. Blacklist_ads.....	7
13.2.8. Blackliste lokal.....	7
13.2.9. Benutzersperre.....	7
13.2.10. Gesperrte Rechner.....	7
13.2.11. Freigegebene Rechner.....	8
13.2.12. Sonstige Rechner.....	8
13.3. Internetsteuerung im Raum.....	9
13.4. Der Webfilter.....	11
13.4.1. Schuleigene Blacklist.....	11
13.4.2. Einträge als Lehrer hinzufügen.....	11
13.4.3. Freischalten von Seiten.....	12
13.4.4. Einträge als Administrator verwalten.....	13
13.4.5. Einlesen externer Blacklisten.....	14
13.4.6. Sperren von Werbeeinblendungen.....	15
13.4.7. Temporäres Abschalten des Webfilters.....	16
13.4.8. Blacklisten löschen.....	16
13.4.9. Die Internet-Statusanzeige für Schülerinnen und Schüler.....	17
13.5. Benutzerbasierte Zugangskontrolle.....	18
13.5.1. Internetsperre für Klassen.....	18
13.5.2. Internetsperre für einzelne Schüler.....	18
13.6. Whitelisten.....	19
13.7. Protokollierung.....	20
13.7.1. Konfiguration der Protokollierung.....	20
13.7.2. Logdateien auswerten.....	21
13.7.3. Datenschutz.....	21

13. Internetsteuerung

Eine wichtige Funktionalität der Musterlösung ist die dynamische Steuerung des Internetzugangs. Dabei lassen sich vom Administrator Standardeinstellungen festlegen, aber auch von Lehrerin oder Lehrer in der Unterrichtssituation individuelle Regeln auf Knopfdruck durchsetzen. Schülerinnen und Schüler haben die Möglichkeit, ihren Internetstatus abzufragen und somit gegebenenfalls zu erfahren, warum sie eine gewünschte Webseite nicht aufrufen dürfen.

Im einzelnen bestehen folgende Möglichkeiten, den Internetzugang zu kontrollieren:

- Der Internetzugang kann raumweise oder für einzelne Arbeitsstationen gesperrt oder freigegeben werden.
- Der Internetzugriff kann für einzelne Klassen blockiert werden; das gilt dann für beliebige Rechner.
- Der Administrator kann auch für einzelne Schülerinnen oder Schüler ein Verbot des Netzzugangs durchsetzen.
- Für Klassen/Projektgruppen kann eine Whitelist vorgegeben werden, das Surfen auf davon abweichenden Seiten ist dann verboten.
- Einzelne Seiten können in eine Sperrliste eingetragen werden; auch das Einlesen einer großen Liste gesperrter Seiten ist möglich.
- Lehrerinnen und Lehrer können in ihrem Raum die Blacklisten vorübergehend außer Kraft setzen oder einzelne Einträge wieder aus der Sperrliste entfernen.

Die Steuerung des Internetzugangs erfolgt intern über den ISA-Server (Internet Security & Acceleration Server). Der ISA ist ein Programm auf dem Server, das zum einen einen zentralen Internetzugang für alle Rechner im Netz zur Verfügung stellt, zum anderen die Möglichkeit bietet, Regeln zu definieren, die z. B. nach Benutzer, Rechner oder aufgerufener Seite den Zugriff sperren. Der Zugang aufs Internet erfolgt dann nicht mehr direkt, sondern über den ISA-Server. Dieser wird dann auch als Proxyserver der Arbeitsstationen bezeichnet.

Die Musterlösung gibt hierzu ein schulspezifisches Standardregelwerk vor, das über die Schulkonsole dynamisch verwaltet wird. Die Schnittstelle ist die Schulkonsole, Sie müssen also den ISA-Server nicht direkt konfigurieren. Die Schulkonsole kann die beiden Versionen des ISA-Server 2000 oder 2006 steuern, an der Oberfläche ist hierbei kein Unterschied wahrnehmbar.

Die abgebildeten Beispiele beziehen sich auf die aktuelle Version ISAServer 2006.

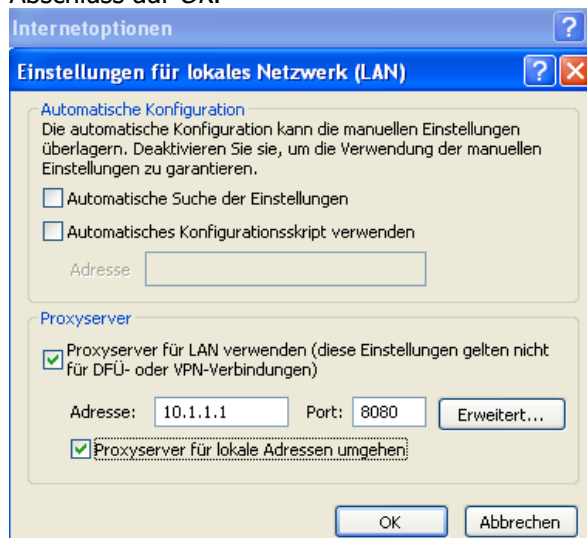
13.1. Festlegen von Standardeinstellungen

Unmittelbar nach der Installation der Schulkonsole ist zwar das Standardregelwerk eingerichtet, die spezifischen Einstellungen der Schule (z.B. Aufteilung der Rechner nach Räumen) fehlen jedoch noch. In einem ersten Schritt muss der Administrator daher eine Konfiguration vornehmen.

13.1.1. Proxyserver auf den Clients konfigurieren

Übung 1:

1. Melden Sie sich an einem Client als *aproflehrer* mit dem Kennwort *muster* an.
2. Starten Sie den Internetexplorer.
3. Klicken Sie auf *Extras / Internetoptionen* und wählen Sie den Reiter *Verbindungen*.
4. Klicken Sie im unteren Bereich, LAN-Einstellungen, auf *Einstellungen...* Füllen Sie das Formular genau wie abgebildet aus und klicken Sie zum Abschluss auf *OK*.



In einer Mehrserverumgebung muss hier die IP-Adresse des ISA-Servers eingetragen werden. Das ist die 10.1.1.2 bei der Zwei- und 10.1.1.3 bei der Dreiserverlösung.

5. Melden Sie sich an dem Computer ab.
6. Kopieren Sie als Administrator mit der Schulkonsole das Lehrerprofil.
7. Wiederholen Sie die Schritte 1-6 als *aprofschueler* und kopieren Sie das Profil anschließend in jede Schulart.

Dieses Verfahren wirken sich jedoch nicht auf den Administrator aus, da er auf jedem Client ein eigenes, lokales Profil besitzt.

Sie müssten daher den Proxeintrag für den Administrator auf jedem Client, auf dem Sie sich anmelden, neu vornehmen, um auf das Internet zugreifen zu können. Allerdings sollten Sie aus Sicherheitsgründen eine Anmeldung als Administrator auf den Clients und erst recht den Internetzugriff ohnedies vermeiden.

Auch auf dem Server müssen Sie diese Einstellung einmalig vornehmen.

13.1.2. Konfiguration der Räume

Um die Rechner der einzelnen Räume dem ISA bekannt zu machen, rufen Sie als Administrator in der Schulkonsole den Menüpunkt *Räume / Status in den Räumen* auf.

Sie können hier für jeden einzelnen Raum festlegen, ob die Internetsperre aktiviert sein soll oder nicht. Durch *Übernehmen* können Sie die Veränderung durchführen, entweder für einen einzelnen Raum oder unten für das gesamte Netzwerk.

Sonstige Rechner betrifft dabei alle Clients, die eine IP-Adresse aus dem DHCP-Bereich des Servers erhalten haben, aber keinem Raum zugeordnet sind (insbesondere z.B. private Notebooks).

Beim ersten Aufruf dieser Seite werden die den Räumen zugeordneten Regeln im ISA-Server eingerichtet. Später können Sie hier als Administrator den Internetzugang der einzelnen Räume komplett (ent)sperren. Das Sperren gilt auch für den Lehrer-PC und wird sofort umgesetzt.

13.1.3. Voreinstellungen festlegen

Unter *Konfiguration / Raumkonfiguration* können Sie anschließend noch einen Defaultwert für alle Räume festlegen. Auf Wunsch (Radiobutton unten) wird dann der gewünschte Zustand für Internet- und Druckersperre beim Abmelden eines Lehrers für dessen Raum wiederhergestellt. Der Webfilter wird beim Abmelden auf jeden Fall wieder aktiviert.

Übung 2:

1. Stellen Sie als Defaultwert für den Raum EDV1 die *Internetsperre* auf *aktiviert*. Setzen Sie *Defaultzustand wiederherstellen* auf *Ja* und übernehmen Sie die Konfiguration mit *Speichern*.
2. Melden Sie sich an einem Client als Lehrer, am anderen als Schüler an. Schalten Sie im *aktuellen Raum* die Internetsperre an und aus und beobachten Sie die Auswirkung auf den Schüler.
3. Sperren Sie alle Rechner außer Ihrem eigenen.
4. Schalten Sie die Internetsperre für alle Rechner ab und melden Sie sich ab. Auf dem Schülerrechner sollte jetzt der Internetzugang gesperrt sein.

Bitte beachten Sie:

Nehmen Sie hier Veränderungen an den Internetzeinstellungen vor, so werden diese *nicht* im Regelwerk des ISA-Servers umgesetzt – Sie modifizieren hier nur die Voreinstellungen für das Abmelden der Lehrer. Soll der Defaultzustand beim Abmelden nicht wiederhergestellt werden, so haben die Einstellungen keine Auswirkung.

13.2. Die ISA-Konsolensteuerung

Schnittstelle zum ISA-Server ist in der Regel im täglichen Betrieb ausschließlich die Schulkonsole, die die meisten Einträge verwaltet. Zur Kontrolle, Fehlersuche im Supportfall oder für spezielle zusätzliche Konfigurationen können Sie die ISA-Konsole verwenden.

Sie starten diese über *Start | Programme | Microsoft ISA Server | ISA Verwaltung*.

Im folgenden wird kurz auf grundlegende Funktionen und die einzelnen von der Schulkonsole verwendeten Regeln im ISA2006 eingegangen.

Da beim bisherigen Arbeiten mit der Schulkonsole bereits automatische Einstellungen vorgenommen wurden, stellen wir in der folgenden Übung zunächst den ISA-Grundzustand wieder her. Dadurch werden alle Änderungen seit der Installation der Schulkonsole verworfen.

13.2.1. Der Grundzustand

Übung 3: Zurücksetzen der ISA-Einstellungen

1. Starten Sie die ISA-Verwaltungskonsolle durch *Start / Programme / Microsoft ISA Server / ISA Server-Verwaltung*
2. Klicken Sie mit der rechten Maustaste auf *S1* und wählen Sie *Importieren...* Klicken Sie auf *Weiter*.
3. Wählen Sie jetzt die Datei (*Durchsuchen*)
d:\install\ML_Erweiterungen\isa2006\Dateien\isa2006.xml. *Weiter*.
4. Sie möchten die alten Einstellungen verwerfen. Wählen Sie daher die untere Option *Überschreiben*. *Weiter*.
5. *Serverspezifische Einstellungen* werden nicht verwendet. Klicken Sie auf *Weiter*.
6. Klicken Sie auf *Fertigstellen* und bestätigen Sie die Warnmeldung mit *OK*.
7. Zum Abschluss bestätigen Sie noch einmal mit *OK* und anschließend oben in der Mitte *Übernehmen*.

Damit haben Sie jetzt den Ausgangszustand der Schulkonsol-Regeln wiederhergestellt. Nach einem Klick links auf *Firewallrichtlinie* können Sie sie ansehen:

Reihenfolge	Name	Aktion	Protokolle	Von / Listener	Bis	Bedingung	Beschreibung
1	Lokalen Webserv...	Zulassen	HTTP-Server	Intern	10.1.1.1		Erlaubt den Z
2	Datenverkehr vo...	Zulassen	Gesamter aus...	Intern Lokaler Host	Intern Lokaler Host	Alle Benutzer	Lässt den vol
3	Internetzugriff fü...	Zulassen	Gesamter aus...	Server	Beliebig	Alle Benutzer	Schulkonsolel
4	Blacklist_ads	Verweigern	HTTP HTTPS	Beliebig		Alle Benutzer	Schulkonsolel
5	Blackliste lokal	Verweigern	Gesamter aus...	Intern		Alle Benutzer	Schulkonsolel
6	Benutzer Sperre	Verweigern	Gesamter aus...	Intern	Extern		Schulkonsolel
7	Gesperrte Rechner	Verweigern	Gesamter aus...		Extern	Alle Benutzer	Schulkonsolel
8	Freigegebene Re...	Zulassen	HTTP HTTPS		Extern	Alle Benutzer	Schulkonsolel
9	Sonstige Rechner	Zulassen	HTTP HTTPS	Clients	Extern	Alle authenti...	Schulkonsolel
Letzte	Standardregel	Verweigern	Gesamter Dat...	Alle Netzwerk...	Alle Netzwerk...	Alle Benutzer	Vordefinierte

Jede Regel besteht dabei aus Name, Aktionsart, Protokollen, anfragende Computer, Zieladresse der Anfrage und betroffener Benutzergruppe.

Die Regeln werden von oben nach unten abgearbeitet. Die Erste, die in allen Punkten zutrifft, wird dann angewendet, was spätestens bei der ganz unten stehenden Standardregel der Fall ist.

Fehlen Teile in einer Regel, so wird sie ignoriert. Wie man an der Abbildung oben sieht, ist das bei den Regeln Nr. 4-8 zunächst der Fall, hier müssen noch schulspezifische Daten ergänzt werden.

13.2.2. Speichern und Wiederherstellen

Dieselbe Funktionalität kann dazu verwendet werden, eine komplette Konfiguration des ISA-Servers zu speichern und bei Bedarf wiederherzustellen.

Eine Anleitung dazu finden Sie z.B. unter

<http://www.microsoft.com/germany/technet/datenbank/articles/600496.msp>.

13.2.3. Die Regeln

Erweitern Sie die Ansicht zunächst wie in der Abbildung. Sie finden jetzt Ihren Server (S1) und die eingerichteten Zugriffsregeln, nämlich Site- und Inhaltsregeln für Benutzer- und URL-bezogene Regeln und Protokollregeln für die Rechnerbezogene Freigabe oder Sperrung.

Wesentliche Grundlage der ISA-Steuerung sind die abgebildeten neun Regeln der Schulkonsole. Sie werden anschließend detailliert beschrieben und mögliche Anpassungen beschrieben¹. Darüber hinausgehende Änderungen an diesen Regeln werden nicht supportet!

13.2.4. Lokaler Webserver veröffentlichen

Diese zunächst etwas eigenartig anmutende Regel (im Intranet ist der Webserver sowieso zugänglich) wird für die Schulkonsole benötigt. Durch sie kann der Aufruf einem bestimmten Client zugeordnet werden und scheint nicht vom Server selbst zu kommen. Sie darf nicht verändert werden, da sonst die Zuordnung eines Computers zu einem Raum nicht mehr möglich ist.

13.2.5. Datenverkehr vom internen Netzwerk zum lokalen Host

Diese Regel erlaubt den kompletten Datenverkehr zum und vom Rechner, auf dem der ISA-Server 2006 läuft. Sie ist notwendig, sobald der ISA-Server zugleich Domänencontroller ist, der Standard in der Musterlösung. Ohne diese Regel scheitern praktisch alle Zugriffe auf den Server.

Für diese Regel ist die Protokollierung per Default deaktiviert. Sie könnte zur Kontrolle/Fehlersuche eingeschaltet werden, erzeugt aber ein sehr hohes Datenvolumen. An dieser Regel werden durch die Schulkonsole keine Veränderungen durchgeführt.

13.2.6. Internetzugriff für Server

Unabhängig vom sonstigen Netzwerk ist es durch diese Regel vorgesehen, den Servern (zunächst definiert als 10.1.1.1 bis 10.1.1.3) einen Zugang zum Internet zu ermöglichen (notwendig für WSUS, Virenupdates...).

Zugleich erlaubt sie den Servern auch einen unbeschränkten Zugang auch im Intranet. Die Regel ist völlig statisch. Sie könnte nach Protokollen und/oder Zielen eingengt werden, wenn die Schule eine entsprechende Sicherheitspolicy fahren möchte. Die Protokollierung ist voreingestellt eingeschaltet, kann jedoch auch deaktiviert werden. Es ist sinnvoll, keine Authentifizierung zu verlangen, so dass Virenscanner und andere Dienste keinen eingetragenen Proxybenutzer benötigen.

¹ Diese Änderungen sind nicht Bestandteil des Basiskurses. Sie werden z.B. in regionalen Arbeitskreissitzungen besprochen.

13.2.7. Blacklist_ads

Diese Filterregel ist für Werbeadressen vorgesehen. Alle enthaltenen Ziele werden auf die leere Seite null.html umgeleitet. Dadurch ist es z.B. möglich, Werbebanner zu unterdrücken. Solange keine Einträge eingelesen wurden, ist diese Regel außer Kraft. Sie gilt sinnvollerweise für alle Benutzer; ihre Anwendung wird protokolliert. Die Benutzung der Regel ist optional.

13.2.8. Blackliste lokal

Hier werden die gesperrten Internetadressen verarbeitet. Vorgegeben sind zunächst zwei Ziele, einer für URLs und einer für Domänen. Beide kann der Administrator oder jeder Lehrer über die Schulkonsole pflegen, das System entscheidet automatisch, ob es ein URL oder ein Domäneneintrag ist.

Da beim ISA2006 mehrere Zielangaben parallel möglich sind, könnten hier auch eingelesene Adresssätze angefügt werden.

Beim temporären Abschalten des Webfilters in einem Raum werden dessen Clients als Ausnahme in die Regel eingetragen und beim Einschalten wieder entfernt. Außerdem finden Änderungen an den Zielsätzen statt.

Die Regel gilt für alle Rechner und alle Benutzer (außer auf den Servern). Denkbar wäre es, die Anwendung auf Schüler zu beschränken. Die Anwendung dieser Regel wird protokolliert, allerdings standardmäßig anonym. Um eine namentliche Erfassung zu ermöglichen, muss die Benutzerzuordnung auf Authentifizierte Benutzer oder eine selbstdefinierte Gruppe geändert werden.

13.2.9. Benutzersperre

Diese Regel sperrt der Benutzergruppe `g_kein_Internet` den Zugang. Änderungen werden durch die Schulkonsole an den Mitgliedern dieser Gruppe (ADS) vorgenommen, sie sind deshalb in der ISA-Konsole nicht sichtbar.

Die Anwendung wird namentlich protokolliert, allerdings treten hier eine ganze Reihe von anonymous-Einträgen auf. Diese entstehen dadurch, dass dies die erste Regel ist, für die eine Benutzeridentifikation erforderlich ist. Die Anfrage geht daher an dieser Stelle erst einmal zurück an den Client mit der Bitte um Benutzerauthentifizierung. Um das Protokolldatenvolumen zu verringern, kann die Protokollierung dieser Regel abgeschaltet werden.

13.2.10. Gesperrte Rechner

Über diese Regel und die folgende wird die Internetsperre von Rechnern und Räumen realisiert. Je Raum existieren zwei Clientsätze, die Rechnernamen und IP der gesperrten bzw. zugelassenen Rechner enthalten.

Die Clientsätze werden beim Erstellen oder Löschen von Räumen nach der nächsten Steuerungsaktivität des Internets aktualisiert. Der Inhalt des betroffenen Clientsatzes auch.

Eine Protokollierung erscheint nicht sinnvoll und ist deshalb als Standard abgeschaltet. Wird eine Sperrung für Lehrer nicht gewünscht, kann die Anwendung auf die Gruppen `g_schueler` und `g_ka` eingeschränkt werden (diese Gruppen müssen zuvor im ISA angelegt werden).

13.2.11. Freigegebene Rechner

Über diese Regel findet der Internetzugriff aller Clients in Räumen der Schule statt. Wie bei den gesperrten Rechnern erfolgt der Eintrag dynamisch über die Schulkonsole. Die Regel gilt zunächst für alle Benutzer, dadurch erfolgt die Protokollierung anonym. Wenn eine namentliche Erfassung gewünscht wird, muss der Eintrag hier auf Authentifizierte Benutzer geändert werden.

Weiterhin erlaubt die Regel nur http(s). Sie können weitere Protokolle freischalten oder den gesamten Datenverkehr erlauben, wenn Sie es wünschen. Bitte beachten: FTP-Upload muss gesondert freigeschalten werden (rechte Maustaste auf die Regel).

13.2.12. Sonstige Rechner

Mitunter mag es erwünscht sein, einen Defaultzustand für alle Rechner festzulegen, die nicht in einem der Raumclientsätze erfasst sind. Diese Regel bestimmt das Verhalten sonstiger Rechner. Sie kann über die Schulkonsole (de)aktiviert werden. Standardmäßig erfasst sie nur die IP-Adressen 10.1.10.0 - 10.1.20.255, die an Clients über DHCP zugewiesen werden. Der Zugriff wird namentlich protokolliert, um einen Missbrauch einzuschränken sind per Vorgabe nur Authentifizierte Benutzer freigeschaltet.

13.3. Internetsteuerung im Raum

Ab sofort wird die Internetsteuerung über die Schulkonsole beschrieben. Sie könne die dadurch vorgenommenen Veränderungen in der ISA-Konsole nachverfolgen.

An einem Client angemeldet kann jeder Lehrer für alle Rechner im selben Raum das Internet freischalten oder sperren. Dazu gibt es einen Button auf der Statusseite und einen Menüpunkt für die differenzierte Steuerung.


Im abgebildeten Beispiel ist das Internet bei allen Rechnern freigeschaltet, erkennbar am grünen Symbol oben bei Internetsperre wie auch unten bei jedem einzelnen Rechner (zur Deutlichkeit wurden hier alle vier Rechner in den Raum EDV1 verschoben).


Aktueller Status im Raum EDV1


Angemeldeter Benutzer: **Hahn.Hans**


dieser Rechner: **pc1**
IP: 10.1.10.0








Druckerstatus:













BSA:  inaktiv (BenutzerSelbstAnmeldung)

Webfilter:  aktiv

Internetsperre:  nicht gesperrt

KA:  inaktiv (Klassenarbeitsmodus)

Aktion auf andere Rechner:       

	Gestartet	Benutzer	Internetsperre	Rechnersperre
PC1		Hahn.Hans		
PC2		Annika.Brav		
PC3		Helge.Schludrig		
PC4				

Klickt nun Hans Hahn, der angemeldete Lehrer an PC1, auf das rote **www**-Symbol in der Zeile *Aktion auf andere Rechner*, so werden alle Rechner außer seinem eigenen gesperrt.

Webfilter:		aktiv		
Internetsperre:		teilweise gesperrt		
KA:		inaktiv (Klassenarbeitsmodus)		
Aktion auf andere Rechner				
	Gestartet	Benutzer	Internetsperre	Rechnersperre
PC1		Hahn.Hans		
PC2		Annika.Brav		
PC3		Helge.Schludrig		
PC4				

Die Symbole ändern entsprechend ihre Farbe und der neue Status wird angezeigt. Bis die Internetsperre durchgesetzt wird, kann es etwa 30 Sekunden dauern. Auch werden bereit geöffnete Browserfenster erst dann gesperrt, wenn der Benutzer auf eine neue Seite wechseln will.

Eine differenziertere Sperrung ist über den Menüpunkt *Internet steuern* auf der linken Menüleiste möglich:

Internetsperre im Raum EDV1

Dieser Platz: pc1

Rechner im Raum:

PC2 PC3

PC4

Setzen Sie den Haken bei den zu sperrenden PCs und klicken Sie auf *Übernehmen*. Alle aus/abwählen setzt nur die Haken, führt aber noch keine Aktion durch. Die angezeigten Symbole geben mit ihren Farben den aktuellen Status wieder.

Bitte beachten Sie: nach dem Abmelden des Lehrers wird gegebenenfalls der Internetzustand auf den gewählten Defaultwert zurückgesetzt. Deshalb ist oft ein (Ent)sperren des eigenen Rechners und anschließendes Anmelden eines Schülers nicht sinnvoll.

In der ISA-Konsole können Sie bei diesen Aktionen Veränderungen in den Clientsätzen wahrnehmen. Wenn Sie auf *EDV1_gesperrt* oder *EDV1_freigegeben* doppelklicken, können Sie erkennen, dass die jeweiligen IP-Adressen der betroffenen Rechnern ein- bzw. ausgetragen werden.

13.4. Der Webfilter

Die Schulkonsole ermöglicht es Ihnen, bestimmte Internetadressen zu sperren, also sogenannte Blacklisten anzulegen. Dabei werden drei Kategorien unterschieden:

- In einer (üblicherweise kleinen) schulinternen Liste können alle Lehrer Einträge machen.
- Über eine besondere Schnittstelle können nach Kategorien sortierte, frei verfügbare Filterlisten mit bis zu mehreren zehntausend Einträgen eingelesen werden.
- Adressen, die ausschließlich Werbebanner und andere sogenannte Ads zur Verfügung stellen, können über eine eigene Regel blockiert werden. In diesem Fall wird keine Umleitung auf eine Benutzerinformation vorgenommen, sondern das Element kommentarlos verworfen.

Generell lassen sich zwar unerwünschte Inhalte auf diese Weise filtern, aufgrund der Vielzahl von sich ständig ändernden Adressen ist es aber allein mit den Funktionalitäten der Schulkonsole nicht möglich, Jugendschutz beim Internetzugang auch nur annähernd zu gewährleisten. Ferner leidet mit einer Vielzahl von Blacklisteinträgen auch die Performance des Servers.

Klare Empfehlung ist daher die Benutzung eines Internetzugangs über BelWü. Der dann (auch mit der Musterlösung) nutzbare Jugendschutzfilter wird ständig aktualisiert und genügt auch professionellen Ansprüchen.

13.4.1. Schuleigene Blacklist

Die schuleigene Blacklist ist auf jeden Fall vorhanden und kann sinnvoll eingesetzt werden, um spezifisch störende Seiten zu sperren. Je nachdem können das Chat-Seiten, Seiten mit Party-Fotos oder Spielen oder z.B. Seiten wie `ebay.de` sein. Also Seiten, die zwar nicht dem Jugendschutz unterliegen (und deshalb auch nicht von BelWü gesperrt werden), aber in Ihrer Schule als nicht sinnvoll eingeordnet werden.

Die Liste gilt immer schulweit, von daher sind pädagogische Absprachen sinnvoll.

13.4.2. Einträge als Lehrer hinzufügen

Das Interface zur Bedienung des Webfilters wird durch den Lehrer in der Schulkonsole über *Aktueller Raum | Webfilter steuern* aufgerufen.

Sie können hier Einträge hinzufügen oder entfernen, die schuleigene Blacklist anzeigen oder den Webfilter für den aktuellen Raum aus- oder einschalten.

Wenn Sie auf *Einträge hinzufügen* klicken, öffnet sich ein Eingabefeld:

Blacklisteneintrag hinzufügen

Adresse/IP:

Sie können jetzt hier einen kompletten URL eingeben, um eine einzige Seite oder ein einzelnes Bild zu sperren (wie abgebildet), einen Teil einer Adresse wie z.B. `ml-tipps.de/cms` um einen ganzen Bereich zu blocken oder auch nur den Domännennamen (`ml-tipps.de`), um auf keine Seite der Domäne Zugriff zu gestatten.

13.4.3. Freischalten von Seiten

Lehrer und Administratoren können gesperrte Seiten freischalten. Die Funktion ist unter *Aktueller Raum | Webfilter steuern | Einträge entfernen* zu finden. Auch hier kann wieder ein kompletter URL oder ein Teil davon eingegeben werden.

Das Verfahren des Entsperrens versucht sicherzustellen, dass die Webseite danach tatsächlich erreichbar ist. Haben Sie z.B. `ml-tipps.de/cms/home` als Adresse eingegeben, so werden zusätzlich `ml-tipps.de/cms` und `ml-tipps.de` aus den Blacklisten gelöscht, denn auch diese Einträge würden den Aufruf der Seite ja verhindern.

Das Löschen erfolgt aus allen Blacklisten und gilt schulweit. Die zugehörigen IP-Adressen werden in der Regel automatisch mit gelöscht.²

Durch das insgesamt komplexe Verfahren kann das Entsperrern einer Seite einige Zeit dauern.

Übung 4:

1. Melden Sie sich als Lehrer an einem Client an.
2. Sperren Sie einige Internetadressen.
3. Lassen Sie sich eine Liste der gesperrten Adressen anzeigen.
4. Probieren Sie die Adressen aus.
5. Löschen Sie als Lehrer oder Administrator einen Filtereintrag und kontrollieren Sie das Ergebnis in der ISA-Konsole.

² Dazu werden per DNS-Abfrage die IP-Adressen ermittelt. Bei manchen sehr stark frequentierten Websites wie z.B. `google.de` ändern sich diese von Zeit zu Zeit. Dadurch kann es vorkommen, dass die Seite erneut entsperrt werden muss.

13.4.4. Einträge als Administrator verwalten

Als Administrator haben Sie die gleichen Verwaltungsmöglichkeiten der lokalen Blackliste wie ein Lehrer. Zusätzlich finden Sie unter *Konfiguration / Webfilter im Netz* diese Funktionen samt weiterer, die den Webfilter betreffen, zusammengefasst.

Schulkonsole für Admins Version 2.5 Patch 1 (17.09.2009) für Windows Server		MEDIEEN offensive SCHULE III Support-Netz			
[www.support-netz.de]	Home	aktueller Raum	Schularten	Klassen	Räume
	Schüler/innen	Lehrer/innen	Projekte	Konfiguration	
Raumkonfiguration	Webfilter				<p>Hier haben Sie die Möglichkeit, bereits bestehende Webfilterlisten einzulesen oder die Einträge auch wieder komplett zu löschen.</p> <p>Zu diesen Listen können weitere Domänen einzeln hinzugefügt bzw. wieder entfernt werden.</p> <p>(Domänen-)Einträge in diesen Listen sorgen dafür, dass diese Webseiten von Schülern beim Surfen nicht mehr erreichbar sind.</p> <p>Die Einträge gelten zunächst in allen Räumen, können aber durch den Lehrer im aktuellen Raum deaktiviert werden.</p>
Profilverwalter	lokale Blackliste anzeigen:	Sollte die Blackliste sehr viele Einträge enthalten, kann das Auslesen sehr lange dauern.	Anzeigen		
Webfilter im Netz	Blacklisten einlesen:	Über diese Funktion können Sie Blacklisten einlesen. Bitte beachten Sie: das Einlesen benötigt relativ viel Zeit.	Listen einlesen		
Basiseinstellungen	lokale Blackliste bearbeiten:	Einträge hinzufügen	Einträge entfernen		
Menüeinstellungen	Webfiltereinträge löschen:	Hier können Sie ganze Listen unwiderruflich löschen.	Löschen		
Schülerbildschirme					

Übung 5: Sperren über eine IP-Adresse

Auch Sperrungen über IP-Adressen sind möglich. So kann man eine Seite, die über verschiedene Namen aufrufbar ist, bequem über einen Eintrag sperren.

1. Melden Sie sich als Administrator an einem Client an.
2. Ermitteln Sie die IP-Adresse von der oft unerwünschten Chat-Seite <http://www.kwick.de/> :
Öffnen Sie hierzu über *Start / Ausführen / cmd* eine Kommandozeile und geben Sie dort `nslookup kwick.de` ein:

```
C:\Dokumente und Einstellungen\Administrator>nslookup kwick.de
Server: localhost
Address: 127.0.0.1

Nicht-autorisierende Antwort:
Name: kwick.de
Address: 85.236.198.250
```

3. Sperren Sie jetzt über die Schulkonsole *Konfiguration / Webfilter im Netz / Eintrag* hinzufügen die IP 85.236.198.250.
4. Melden Sie sich an einem Client als Schüler an und testen Sie den Zugriff auf www.kwick.de, www.kwick.at und www.offlineversand.de.
Diese Seiten wurden jetzt alle gesperrt.

Bitte beachten Sie, dass besonders im nicht-professionellen Bereich sich mehrere Domänen oft eine IP-Adresse teilen. Sie sollten also von dieser Möglichkeit nur in Ausnahmefällen Gebrauch machen, um Fehlspernungen zu meiden.

Hinweis: In der ISA-Konsole wird jeder gesperrte Eintrag doppelt aufgeführt. Das ist wichtig, da sich viele Internetseiten mit oder ohne das Präfix `www.` aufrufen lassen.

Sperrt man nur z.B. `sex.de`, so ist `www.sex.de` weiterhin aufrufbar; diese Adresse wird daher durch den zusätzlichen Eintrag `*.sex.de` verboten.

Als Administrator haben Sie zusätzlich die Möglichkeit, eine Textdatei mit einer Reihe von zu sperrenden Webseiten einzulesen. Sie erreichen diese Funktion über *Konfiguration | Webfilter im Netz | Listen einlesen*. Suchen Sie dann mit *Durchsuchen...* nach Ihrer Textdatei und starten Sie das Einlesen mit *Einzelne Datei importieren*. Sie können diese Funktion auf dem Server oder auf einem Client durchführen.

Ebenso können Sie die schuleigene Blacklist komplett leeren. Wählen Sie hierzu *Konfiguration | Webfilter im Netz | Löschen*, setzen Sie den Haken bei *lokale Blacklist* und klicken Sie dann auf *Ja, Listen löschen*.

13.4.5. Einlesen externer Blacklisten

Dieser Abschnitt ist optional und nur für Fortgeschrittene gedacht.

Wie oben bereits erwähnt – Sperrlisten können nur ein Notbehelf sein. Trotzdem ist die Schulkonsole in der Lage, nach Kategorien sortierte Filterlisten, wie sie im Internet für den Squid-Filter angeboten werden, zu importieren.

Um die Performance des ISA-Servers nicht zu sehr zu belasten, sollten diese Listen aber nicht zu groß werden. In der Praxis haben sich Listen mit bis zu etwa zwanzigtausend Einträgen als brauchbar erwiesen, abhängig allerdings von der Hardware und Speicherausstattung des Servers.

Importiert werden Dateien mit dem Namen `domains`, `urls` oder `blacklist.txt`. Jede Zeile entspricht einem Sperreintrag, die Zuordnung zu Domännennamen und URL erfolgt automatisch.

Dagegen werden alle Einträge aus Dateien mit der Endung `.exclude` aus sämtlichen Filterlisten ausgetragen – nach den Regeln vom Abschnitt 13.4.3.

Wenn Sie also sicher sein wollen, dass gewisse Seiten wie z.B. *google.de* in keiner Blackliste enthalten sind, so fügen Sie im (alphabetisch) letzten Ordner eine Textdatei *Ausnahmen.exclude* mit diesen Adressen hinzu. Diese Ausnahmelisten werden z.B. bei der u.a. deutschen Blackliste verwendet. Sie sollten allerdings zuvor einen Blick auf die Einträgen werfen, nicht immer sind alle sinnvoll.

Internationale Blackliste:

<http://www.squidguard.org/blacklist/>

Deutsche Blackliste:

<http://gone.bn-paf.de/filter/de-blacklists.tar.gz>

Leider sind beide zwar für den Einsatz geeignet, aber nicht sehr aktuell.

Die beiden deutlich größeren Listen unter

ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

und

<http://squidguard.mesd.k12.or.us/blacklists.tgz>

enthalten im Bereich *adult* mehrere hunderttausend Einträge. Das Einlesen dauert daher viele Stunden bis Tage, eine Verwendung dieser Liste wird nicht empfohlen.

Übung 6:

1. Laden Sie das Archiv <http://gone.bn-paf.de/filter/de-blacklists.tar.gz> herunter und entpacken Sie es auf dem Server nach `D:\ISAlisten`. Dort entsteht dann eine Ordnerstruktur mit verschiedenen Kategorien.
2. Löschen Sie den Ordner `D:\ISAlisten\de-blacklists\mail` um Webmail-Anbieter nicht zu sperren.
3. Starten Sie als Administrator die Schulkonsole und wählen Sie *Konfiguration | Webfilter im Netz | Listen einlesen*.
4. Geben Sie bei Serverpfad eingeben `D:\ISAlisten\de-blacklists` ein und klicken Sie auf *Listensatz importieren*.
5. Nach einigen Minuten ist die Aktion abgeschlossen. Sehen Sie sich das Ergebnis in der ISA-Konsole an. Sie finden neue Einträge unter *Zielsätzen* und *Site- und Inhaltsregeln*, jeweils mit dem Namen der Kategorie.

13.4.6. Sperren von Werbeeinblendungen

Dieser Abschnitt ist optional und nur für Fortgeschrittene gedacht.

Viele Anbieter kostenlos nutzbarer Internetseiten finanzieren sich durch Werbung. Da eine Häufung von Werbebildern und -bannern mitunter dazu führt, dass man den eigentlichen Inhalt der Seite nur noch schwer lesen kann, gibt es mittlerweile einige Programme oder Browser-Plugins, die den unerwünschten Inhalt abzublocken versuchen.

Auch der ISA-Server kann diese sogenannten *Ads* sperren, allerdings nur insoweit, wie die Adresse der Anbieter bekannt ist. Über die dafür vorgesehene Regel erfolgt eine Umleitung auf die absolut leere Seite `null.html`, so dass die Banner etc. einfach nicht angezeigt werden.

In der Schulkonsole gibt es auch die Möglichkeit, sogenannte *hosts*-Dateien in die Blacklist einzulesen (vgl. <http://de.wikipedia.org/wiki/Hosts>)

Übung 7:

1. Erstellen Sie, falls nicht bereits geschehen, auf dem Server im Stammverzeichnis von Laufwerk `D` den Ordner `D:\ISAlisten`. Anderenfalls löschen Sie bitte die Unterordner.
2. Erstellen Sie in diesem den Unterordner `D:\ISAlisten\ads`.
3. Laden Sie aus dem Internet unter der Adresse <http://pgl.yoyo.org/adserver/serverlist.php?showintro=0;hostformat=hosts> eine Textdatei mit zu sperrenden Adressen und speichern Sie diese als `D:\ISAlisten\ads\blacklist.txt` ab.
4. Öffnen Sie die Schulkonsole, rufen Sie *Konfiguration | Webfilter im Netz | Listen einlesen* auf.

5. Geben Sie bei *Serverpfad eingeben* `D:\ISAlisten` ein und klicken Sie auf `Listensatz importieren`.
Nach kurzer Zeit ist die Aktion abgeschlossen und Sie haben eine große Zahl von Werbeseiten ausgeblendet.

Als Administrator können Sie auch einzelne Werbeseiten ergänzen, indem Sie die der Übung genannte Datei `blacklist.txt` editieren oder selbst anlegen.

Ergänzen Sie einfach eine neue Zeile mit z.B.

`http://adserv.quality-channel.de`

und wiederholen Sie die Schritte 4 und 5 der Übung.

Falsche Einträge können Sie wie im Abschnitt 13.4.3 erläutert entfernen.

Hinweis: Ausgeblendete Werbeelemente können den Aufbau einer Webseite verändern, so dass es im Extremfall dazu kommen kann, dass Teile nicht mehr lesbar sind, weil Inhaltsabschnitte jetzt übereinander liegen. Auch können links unten im Browser Seitenfehler angezeigt werden, da in der Seite eingebundene Skripte auf nicht mehr vorhandene Objekte zuzugreifen versuchen.

13.4.7. Temporäres Abschalten des Webfilters

Hat die Schule sich für eingeleseene große Listen entschieden, so kann es in gewissen Unterrichtssituationen wünschenswert sein, diese außer Kraft zu setzen. Zum einen sind in den Listen aus dem Internet eine ganze Reihe Seiten irrtümlich gesperrt, wodurch man mit dem Entsperren gar nicht hinterher kommt, zum anderen wäre es denkbar, dass man mit Schülern gerade das thematisieren möchte, auf das kein Zugriff möglich ist.

Vielleicht sind auch für Schüler Onlineshops und Auktionsmärkte gesperrt, während Kolleginnen und Kollegen diese in ihrer Freistunde im Lehrerzimmer nutzen wollen.

Zu diesem Zweck lässt sich der Webfilter in einem Raum zeitweilig (bis zur Abmeldung eines Lehrers) abschalten. Das gilt dann immer für alle Rechner des Raums sowie alle gesperrte Adressen und wird auf Seite mit dem Raumstatus angezeigt.

Aufrufen können Sie diese Funktion über *aktueller Raum / Webfilter steuern / Webfilter aus/an*.

13.4.8. Blacklisten löschen

Unter dem Menüpunkt *Konfiguration / Webfilter im Netz / Löschen* können Sie Filterlisten löschen. Sie können einen oder mehrere der folgenden Optionen auswählen:

- lokale Blackliste – alle Einträge aus der schuleigenen Filterliste werden entfernt.
- sonstige Blacklisten – alle eingeleseenen Blacklisten werden entfernt.
- alle Whitelisten – alle Whitelisteneinträge für Klassen und Projekte werden samt der zugehörigen Regeln gelöscht.

Das Löschen von Blacklisten kann eine gewisse Zeit dauern.

13.4.9. Die Internet-Statusanzeige für Schülerinnen und Schüler

Ist der Zugriff auf eine Webseite gesperrt, so erfolgt zunächst eine Umleitung auf eine Informationsseite, die einen Grund für den verweigerten Zugriff angibt:



Durch Anklicken des Links (oder allgemein einen Aufruf der Schulkonsole als Schüler) wird eine Zusammenfassung aller relevanter Internetrechte angezeigt.

Lehrerinnen und Lehrer haben damit die Möglichkeit, sich die konkreten Gründe für eine Sperrung nennen zu lassen und falls gewünscht aufzuheben.

Ein Schüler kann genau dann auf das Internet zugreifen, wenn alle Symbole grün sind (oder er sich auf die erlaubten Seiten der Whitelist beschränkt).

Meine aktuellen Internetrechte

Internet Sperre	für diesen Platz:	www	aktiv
	für meine Klasse:	www	inaktiv
	für mich:	www	inaktiv
	über Whitelist:	www	inaktiv
<input type="button" value="Aktualisieren"/>			

Im abgebildeten Fall wäre also der Zugang für den Rechner des Schülers gesperrt und ließe sich durch einen Lehrer in diesem Raum über die Internetsteuerung im Raum freischalten.

Die Sperrung des Zugangs für eine einzelne Person kann als disziplinarische Maßnahme nur durch einen Administrator erfolgen oder aufgehoben werden.

13.5. Benutzerbasierte Zugangskontrolle

Die Steuerung des Internetzugangs wird in der Regel durch Lehrerinnen und Lehrer rechnerbasiert erfolgen, wenn Unterricht in einem Computerraum stattfindet. Da differenziert jeder Rechner steuerbar ist, sind die meisten Anforderungen an eine Zugangskontrolle hierdurch bereits abgedeckt.

In machen Situationen, z.B. wenn Klassen unbeaufsichtigt am Rechner arbeiten, kann es wünschenswert sein, einer Klasse den Internetzugang zu verwehren; aus disziplinarischen Gründen ist nach Regelverstößen auch die Sperrung für einzelne Personen durch den Administrator denkbar.

13.5.1. Internetsperre für Klassen

Jedem Lehrer ist es möglich, Schüler einer gesamten Klasse vom Internet auszuschließen oder diese Sperre wieder aufzuheben.

Sie finden diese Funktion unter *Klassen / Internet steuern*. Nach Auswahl der gewünschten Schulart werden alle Klassen aufgelistet. Die mit einem Häkchen versehenen Klassen werden beim Klicken auf den Button *Übernehmen* gesperrt, die anderen freigeschalten.

Intern werden die Gruppen der gesperrten Klassen in die Gruppe *g_kein_Internet* aufgenommen, für die der Webzugang generell gesperrt ist.

13.5.2. Internetsperre für einzelne Schüler

Auf die gleiche Weise kann vom Administrator ein einzelner Schüler gesperrt werden. Da es sich hierbei in der Regel um eine disziplinarische Maßnahme handelt, kann die Sperre auch wiederum nur vom Administrator aufgehoben werden.

Lehrer können einzelnen Schülern das Internet in ihrem Unterricht sperren, indem sie über die Internetsteuerung im Raum den von ihnen verwendeten Rechner sperren. Eine generelle Sperrung ist hingegen nicht möglich.

Die Funktion ist in der Schulkonsole unter *Schüler/innen / Internet steuern* verfügbar. Nach Auswahl von Schulart und Klasse können die zu sperrenden Schüler ausgewählt werden und die Aktion wird mit *Übernehmen* durchgeführt.

Da diese Maßnahme beim PC-gestützten Arbeiten im Unterricht zu Einschränkungen führt, sollten die Kolleginnen und Kollegen darüber informiert werden.

13.6. Whitelisten

In vielen unterrichtlichen Situationen sollen Schüler mit dem Computer im Internet arbeiten. Manchmal ist es dabei wünschenswert, den Zugriff auf eine oder wenige Seiten zu beschränken.

Möglich ist dies über Whitelisten, die jeder Lehrer für Klassen seiner Schulart oder für Projektgruppen eintragen kann. Damit wird dann der Zugriff auf alle anderen Seiten verboten.

Wichtig: Links, die auf eine andere Seite verweisen, sind dann nicht mehr ausführbar oder müssen zusätzlich angegeben werden. Auch eingebundene Objekte (z.B. Werbeanzeigen oder Bilder anderer Seiten) sind dann gesperrt; dies kann das Aussehen der Seite verändern.

Beispiel: In einer Physikstunde soll die Seite „Leifiphysik“ der Universität München genutzt werden. Für die Schülerinnen und Schüler soll zusätzlich ein externes Applet nutzbar sein.

Die Konfiguration erfolgt in der Schulkonsole über *Klassen / Whitelist*. Dort wird die entsprechende Klasse ausgewählt und die beiden Adressen in das Eingabefeld eingetragen. (Hat man mehrere Adressen, so lassen sich diese auch mittels *kopieren / einfügen* aus einer vorbereiteten Textdatei übernehmen.)

Whitelist für Klassen

Schulart	test
Klasse	11A
Whitelist:	inaktiv
	leifi.physik.uni-muenchen.de/ www.walter-fendt.de
	<input type="button" value="aktivieren"/> <input type="button" value="deaktivieren"/>

Nach Abschließen der Aktion durch *aktivieren* ist die Whitelist wirksam.

Sie kann jederzeit auf den selben Weg wieder deaktiviert oder durch neue Einträge überschrieben werden; auch kann man auf diese Weise feststellen, ob eine Whitelist für eine bestimmte Klasse aktiv ist.

Schüler bekommen eine aktive Whitelist über ihren Internetstatus angezeigt.

Als Administrator kann man, z.B. am Schuljahresende, auch alle noch aktiven Whitelisten löschen. Das geht in der Schulkonsole über *Konfiguration / Webfilter im Netz / Lö-*

sch. Wählt man hier *alle Whitelisten* und klickt dann auf *Ja, Listen löschen*, so werden alle Regeln und zugehörigen URL-Listen gelöscht.

Übung 8: Whitelisten

1. Legen Sie als Lehrer auf dem Client eine Whitelist für eine Klasse an.
2. Betrachten Sie die Veränderungen in der ISA-Konsole auf dem Server: Vor den Blacklisten wird eine neue Regel ergänzt.
3. Melden Sie sich auf einem Client als ein Schüler dieser Klasse an und kontrollieren Sie die Funktionsweise der Whitelist.
4. Löschen Sie als Administrator alle vorhandenen Whitelisten und überprüfen Sie das Ergebnis in der ISA-Konsole.

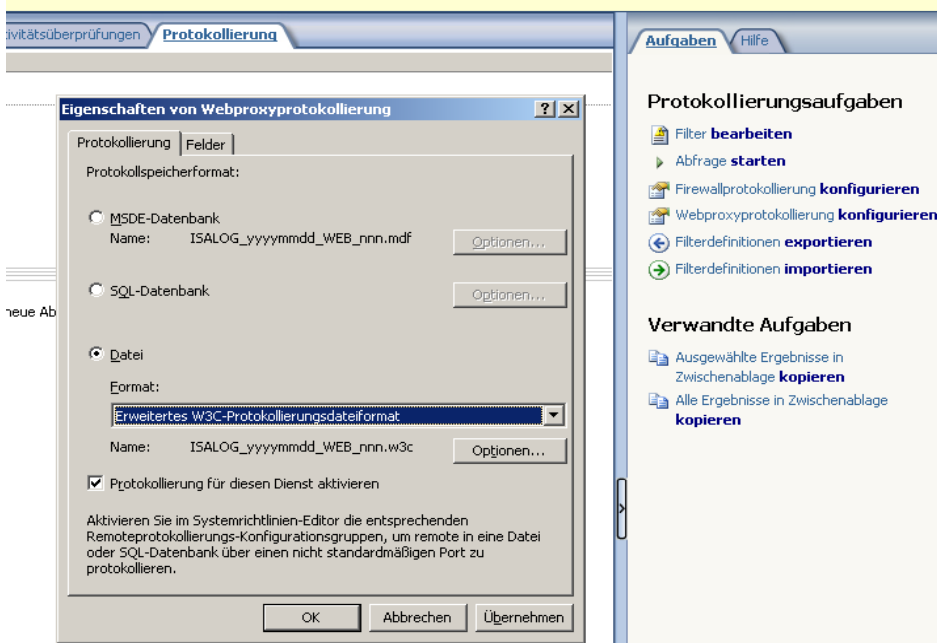
13.7. Protokollierung

Alle Internetzugriffe werden standardmäßig vom ISA-Server in Protokolldateien festgehalten. Die Einträge umfassen neben dem Benutzernamen im Wesentlichen auch aufrufenden Rechner, Datum und Uhrzeit sowie natürlich URL der abgefragten Seite.

13.7.1. Konfiguration der Protokollierung

Die Konfiguration finden Sie in der ISA-Verwaltung auf dem Server unter *Überwachung | Protokollierung | Protokollierungsaufgaben*. Webseitenaufrufe, also Zugriffe über das http(s)-Protokoll laufen über den Webproxydienst. Sie können Einstellungen über den Menüpunkt *Webproxieprotokollierung konfigurieren* vornehmen.

[Anleitung zur Benutzerfreundlichkeit zu erfahren.](#)



Die Protokollierung erfolgt bei der Musterlösung immer in Dateien; die MSDE-Datenbank wird bei der Installation nicht mitinstalliert³.

Über *Optionen* können Sie u.a. festlegen, wie lange die Protokolldateien aufbewahrt werden.

Es ist möglich, das Dateiformat auf *ISA-Server-Dateiformat* umzustellen, da in diesem Fall die korrekte Uhrzeit im Protokoll eingetragen wird⁴.

Über der Reiter *Felder* können Sie schließlich noch dezidiert festlegen, welche Eigenschaften im Protokoll enthalten sind.

13.7.2. Logdateien auswerten

Leider gibt es von Haus aus keine Möglichkeit, die Protokolldateien sinnvoll auszuwerten. Sie finden diese als reine Textdateien im Ordner `C:\Programme\Microsoft ISA Server\ISALogs`. Da der Zugriff auf jedes einzelne Webelement, z.B. jede Grafik, einzeln protokolliert wird, sind die Dateien sehr unhandlich und unübersichtlich. Trotzdem weisen sie im Einzelfall zweifelsfrei nach, wer welche Webseite besucht hat.

13.7.3. Datenschutz

Es ist zwar durchaus zulässig, den Internetverkehr zu protokollieren und gehört in fast allen größeren Firmen zu den Standardvereinbarungen. Trotzdem müssen Sie Ihre Benutzer – Schüler wie Kollegen – darüber aufklären, gegebenenfalls sogar auf Elternabenden darauf hinweisen. Ein Hinweis auf die Protokollierung in der Benutzerordnung ist sinnvoll.

3 Insbesondere aus Performancegründen: die Datenbank erstellt gigantische Protokolldateien.

4 Allerdings gib es Auswertungstools wie den kostenlosen LogParser (<http://www.microsoft.com/germany/technet/datenbank/articles/600371.mspx>), die nur mit der w3c-Struktur zurecht kommen.

