

Musterlösung für
Schulen in
Baden-Württemberg

Windows 2003

Basiskurs Windows-Musterlösung Version 3

Stand: 15.01.07



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: 2006

© Zentrale Planungsgruppe Netze (ZPN)

Inhaltsverzeichnis

13. Internetsteuerung.....	1
13.1. Installation und Grundeinstellungen.....	1
13.1.1. Proxyserver auf den Clients konfigurieren.....	2
13.1.2. Konfiguration der Räume.....	3
13.1.3. Voreinstellungen festlegen.....	4
13.2. Die ISA-Konsolensteuerung.....	5
13.2.1. Protokollregeln und Clientadresssätze.....	6
13.2.2. Site- und Inhaltsregeln und Zielsätze.....	7
13.3. Internetsteuerung im Raum.....	8
13.4. Der Webfilter.....	10
13.4.1. Schuleigene Blacklist.....	10
13.4.2. Einträge als Lehrer hinzufügen.....	10
13.4.3. Freischalten von Seiten.....	11
13.4.4. Einträge als Administrator verwalten.....	12
13.4.5. Einlesen externer Blacklisten.....	13
13.4.6. Sperren von Werbeeinblendungen.....	14
13.4.7. Temporäres Abschalten des Webfilters.....	15
13.4.8. Blacklisten löschen.....	15
13.4.9. Die Internet-Statusanzeige für Schülerinnen und Schüler.....	16
13.5. Benutzerbasierte Zugangskontrolle.....	17
13.5.1. Internetsperre für Klassen.....	17
13.5.2. Internetsperre für einzelne Schüler.....	17
13.6. Whitelisten.....	18
13.7. Protokollierung.....	19
13.7.1. Konfiguration der Protokollierung.....	19
13.7.2. Logdateien auswerten.....	20
13.7.3. Datenschutz.....	20

13. Internetsteuerung

Eine wichtige Funktionalität der Musterlösung ist die dynamische Steuerung des Internetzugangs. Dabei lassen sich vom Administrator Standardeinstellungen festlegen, aber auch von Lehrern in der Unterrichtssituation individuelle Regeln auf Knopfdruck durchsetzen. Schüler haben über die Schulkonsole 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 für den jeweiligen Raum oder für einzelne Arbeitsstationen gesperrt oder freigegeben werden.
- Der Internetzugriff kann für einzelne Klassen blockiert werden, dies gilt dann jedoch für beliebige Rechner.
- Der Administrator kann auch für einzelne Schüler ein Verbot des Netzzugangs durchsetzen.
- Für Klassen/Projektgruppen kann eine so genannte Whitelist vorgegeben werden, das Surfen auf davon abweichenden Seiten ist dann verboten.
- Einzelne Seiten können in eine Sperrliste (Blacklist) eingetragen werden; auch das Einlesen einer großen Liste gesperrter Seiten ist möglich.
- 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.

13.1. Installation und Grundeinstellungen

Mit der Installation der Schulkonsole werden zunächst keine Regeln angelegt, da diese je nach Struktur der Schule unterschiedlich aussehen müssen.

Allerdings ist bereits nach der Installation folgende Struktur vorgegeben:

- Die Seiten- und Inhaltsregel „Zulassungsregel“ wird so umgestellt, dass nur Lehrer, Schüler und Administratoren Internetzugang haben. Dazu werden alle Benutzer gegenüber dem ISA authentifiziert¹. Das ist notwendig, damit Benutzergruppen gesperrt werden können. Zugleich werden ab sofort in den Log-Einträgen die Benutzer mit Namen erfasst. Bitte beachten Sie die Anmerkungen zum Datenschutz im Abschnitt 13.7.3.
- Falls einem Client der Zugriff zum Internet verboten ist, wird statt der Standardfehlermeldung auf eine Informationsseite der Schulkonsole umgeleitet:



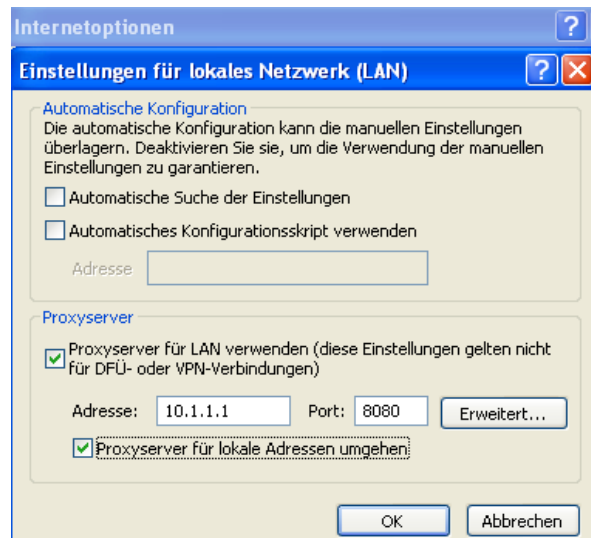
Die aktivierte Authentifizierung macht es notwendig, dass im Browser der ISA-Server als Proxy eingetragen ist. Dies lässt sich zentral über die Profile erledigen.

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*.

¹ Das bedeutet, dass beim Zugriff auf das Internet der Name des Benutzers bekannt sein muss. Wird mit dem Internetexplorer gesurft, so wird der Name des angemeldeten Benutzers automatisch weitergegeben, bei Verwendung eines anderen Browsers muss man sich ein zweites Mal anmelden.



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 *aproschueler* und kopieren Sie das Profil anschließend in jede Schulart.

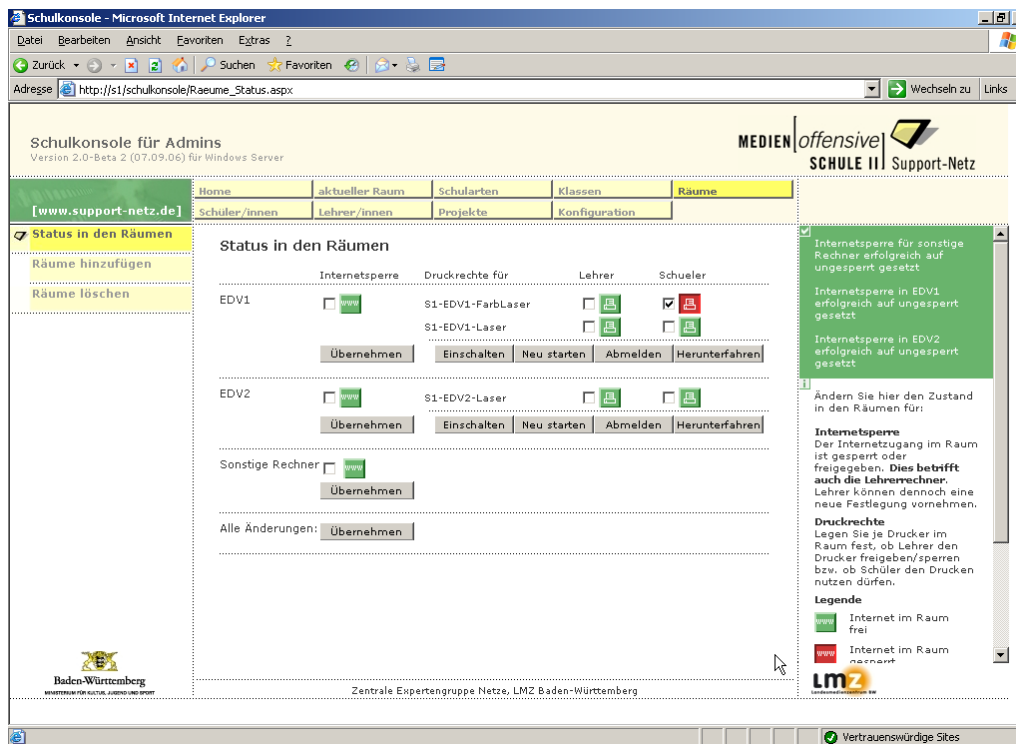
Dieses Verfahren wirken sich jedoch nicht auf den Administrator aus, da er auf jedem Client ein eigenes, lokales Profil besitzt.

Sie müssten daher den Proxyeintrag 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.

Raumkonfiguration

	Internetsperre	Druckrechte für	Lehrer	Schueler
EDV1	<input type="checkbox"/>	S1-EDV1-FarbLaser S1-EDV1-Laser	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
EDV2	<input checked="" type="checkbox"/>	S1-EDV2-Laser	<input type="checkbox"/>	<input type="checkbox"/>
Defaultzustand wiederherstellen?	Soll der oben eingestellte Zustand nach jedem Abmelden eines Lehrers im Raum wiederhergestellt werden?		<input checked="" type="radio"/> Ja	<input type="radio"/> Nein
Speichern	<input type="button" value="Letzte Einstellung laden"/>		<input type="button" value="Speichern"/>	

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:

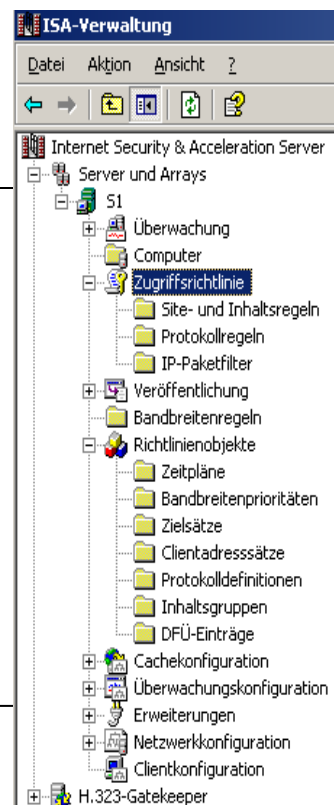
Nehmen Sie hier Veränderungen an den Interneteinstellungen vor, so werden diese *nicht* im Regelwerk des ISA-Servers umgesetzt – Sie modifizieren hier nur die Voreinstellungen für das Abmelden der Lehrer. Soll der Defaultzustand beim Abmelden nicht wiederhergestellt werden, so haben die Einstellungen 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 die einzelnen von der Schulkonsole verwendeten Bereiche im ISA2000 eingegangen.



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.

Weiter unten, unter Richtlinienobjekte, sind unter Zielsätze die Listen mit URLs für den Webfilter und unter Clientadresssätze die IP-Adressen der einzelnen Arbeitsstationen abgelegt.

Alle Objekte, die von der Schulkonsole verwaltet werden, erhalten in der Spalte *Beschreibung* den Kommentar *Schulkonsole*. Sie sollten nicht von Hand manipuliert werden.

13.2.1. Protokollregeln und Clientadresssätze

Zu jedem Raum gehören zwei Clientadresssätze, die jeweils die IP-Adressen der freigegebenen bzw. gesperrten Rechner enthalten.

Clientadresssätze konfigurieren

für S1

Clientsätze bestehen aus mindestens einem Computer.

Für Zugriffsrichtlinienregeln enthalten Clientsätze Computer, die Teil des internen Netzwerks sind.

Für Webveröffentlichungsregeln enthalten Clientsätze Computer des externen Netzwerks.



Name	Beschreibung	Clients
Dummy CS	Schulkonsole	
EDV1 freigegeben	Schulkonsole	
EDV1 gesperrt	Schulkonsole	10.1.10.0;10.1.10.1
EDV2 freigegeben	Schulkonsole	10.1.10.2;10.1.10.3
EDV2 gesperrt	Schulkonsole	
Schulnetz	Schulkonsole	10.1.10.0 - 10.1.20.255
Server	Schulkonsole	10.1.1.1 - 10.1.1.3

Der leere *Dummy CS* ist bei den Protokollregeln notwendig, da leere Protokollregeln schwerwiegende Fehler verursachen können.

In der Abbildung sind alle Rechner im Raum *EDV 1* gesperrt, die in *EDV 2* freigegeben. Die Namen der Rechner sind den Clientsätzen nicht zu entnehmen, Sie müssten sie anhand der IP im DNS-Server nachschlagen.

In zwei Protokollregeln werden diese Rechnersätze dann gesperrt oder erhalten Zugang zum Internet.

Die dritte Protokollregel der Schulkonsole regelt den Zugriff für sonstige Arbeitsstationen. Sie wird je nach Einstellung aktiviert oder deaktiviert.

Protokollregeln konfigurieren

für S1

Protokollregeln legen fest, welche Protokolle für die Kommunikation mit dem Internet verwendet werden können.



Name	Ber...	Besch...	Protokoll	Aktion	Anwendung
Freigegebene Rechner	Array	Schulkonsole	Gesamter IP-...	Zulassen	Clientsätze: Dumm
Gesperrte Rechner	Array	Schulkonsole	Gesamter IP-...	Verwe...	Clientsätze: Dumm
Sonstige Rechner	Array	Schulkonsole	Gesamter IP-...	Zulassen	Jede Anfrage
Internetzugriff für Server	Array		Gesamter IP-...	Zulassen	Clientsätze: Server

13.2.2. Site- und Inhaltsregeln und Zielsätze

In der Grundeinstellung gibt es zwei Inhaltsregeln der Schulkonsole und einen Zielsatz. Die Regel *Blackliste lokal* ist zusammen mit dem gleichnamigen Zielsatz für die schulinterne Webfilterliste zuständig. In den Zielsatz können Lehrer per Schulkonsole Einträge hinzufügen oder daraus austragen.

Die Regel *Benutzer Sperre* sperrt die AD-Gruppe *g_kein_Internet*. Die Schulkonsole trägt Klassen oder Benutzer in diese Gruppe ein.

Liest man Webfilterlisten ein, so wird je Kategorie ein Zielsatz und eine korrespondierende Regel erstellt. Auch bei Whitelisten für Klassen und Projekte wird temporär ein Zielsatz samt Regel angelegt.





13.3. Internetsteuerung im Raum









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: pc 1

Rechner im Raum:

PC2 PC3

PC4

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. Dadurch ist oft ein (Ent)sperren des eigenen Rechners und anschließendes Anmelden eines Schülers nicht sinnvoll.

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 eingelezen 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 Domänennamen (`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 3:

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.

Übung 4: 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-autorisierte 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 *Konfigu-*

ration | *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 Einträge werfen, nicht immer sind alle sinnvoll.

Internationale Blackliste:

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

Deutsche Blackliste:

<http://www.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 bis zu mehreren Stunden, eine Verwendung dieser Liste wird nicht empfohlen.

Übung 5:

1. Laden Sie das Archiv <http://www.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 6:

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://ppl.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

Internetsperre	für diesen Platz:		aktiv
	für meine Klasse:		inaktiv
	für mich:		inaktiv
	über Whitelist:		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. Werbefbanner 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	<input type="text" value="test"/>
Klasse	<input type="text" value="11A"/>
Whitelist:	inaktiv <input type="text" value="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-*

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

Übung 7: 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. (Zielsätze und Site- und Inhaltsregeln).
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 *Überwachungskonfiguration | Protokollierungen*. Webseitenaufrufe, also Zugriffe über das http(s)-Protokoll laufen über den Webproxydienst. Klicken Sie auf *ISA Server-Webproxiedienst* mit der rechten Maustaste und dann auf *Eigenschaften*; jetzt können Sie die Protokollierung (de)aktivieren. Unter Optionen finden Sie in diesem Formular die Möglichkeit die Anzahl der Tage festzulegen, die die Protokolldaten aufbewahrt werden.

Komponente	Felder	Typ	Pfad	Unterverzeichnis
<input checked="" type="checkbox"/> Paketfilter	Standard	Text	ISA Server-Installations...	ISALogs
<input checked="" type="checkbox"/> ISA Server-Firewalldienst	Standard	Text	ISA Server-Installations...	ISALogs
<input checked="" type="checkbox"/> ISA Server-Webproxiedienst	Benutzerde...	Text	ISA Server-Installations...	ISALogs

Eigenschaften von ISA Server-Webproxiedienst

Protokollierung | Felder

Protokollierungsspeicherformat:

Datei

Format:

Neue Datei erstellen:

Name:

Datenbank

ODBC-Datenquelle (DSN):

Tabellenname:

Konto verwenden:

Protokollierung für diesen Dienst aktivieren

Es empfiehlt sich, das Dateiformat auf *ISA-Server-Dateiformat* umzustellen, da in diesem Fall die korrekte Uhrzeit im Protokoll eingetragen wird³.

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 Elternabend darauf hinweisen. Ein Hinweis auf die Protokollierung in der Benutzerordnung ist sinnvoll.

³ Weitere Einstellungsmöglichkeiten können Sie der Onlinehilfe entnehmen, die mit [F1] aufgerufen wird.