

Musterlösung für  
Schulen in  
Baden-Württemberg

# Windows 2003

## Tipps zum ISA 2006

Hintergrundinformationen und  
weitergehende Möglichkeiten

Stand: 20.10.10



## **Impressum**

### **Herausgeber**

Zentrale Planungsgruppe Netze (ZPN)  
am Kultusministerium Baden-Württemberg

### **Autoren**

Martin Resch  
Andreas Kröll

### **Endredaktion**

Martin Resch  
Andreas Mayer

### **Weitere Informationen**

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

Veröffentlicht: 2008

© Zentrale Planungsgruppe Netze (ZPN)

# Inhaltsverzeichnis

1. Den ISA 2006 konfigurieren.....	4
1.1. Sichern und Wiederherstellen.....	4
1.2. Firewallregeln.....	7
1.2.1. Eigenschaften einer Richtlinie.....	7
1.2.2. Beispiel 1: Herr Hahn will immer surfen können.....	10
1.2.3. Beispiel 2: Vom Lehrerrechner soll FTP möglich sein.....	11
1.2.4. Beispiel 3: Benutzer sollen private Mails abrufen können.....	13
1.2.5. Beispiel 4: Schüler sollen keine MP3 und Filme laden dürfen.....	13
1.2.6. Beispiel 5: Das Programm LernOfix benötigt den Port 47110.....	14
1.2.7. Beispiel 6: Private Notebooks der Lehrer sollen freien Zugang zum Internet erhalten.....	15
1.3. Überwachungsfunktion verwenden.....	18
1.3.1. Echtzeitprotokollierung.....	18
1.3.2. Internetprotokollierung.....	19
1.3.3. Auswertung der Logdateien per Tool.....	20
1.4. Den Cache konfigurieren.....	21
1.5. Zugriff von extern.....	24
1.6. Weitergehende Anleitungen.....	24

# 1. Den ISA 2006 konfigurieren

Der ISA-Server 2006 bietet nicht nur ein stabiles, moderneres System, sondern lässt durch recht einfache Konfigurationsänderungen Anpassungen an eine individuelle Schulkonfiguration zu.

Die grundlegende pädagogische Funktionalität wird jedoch immer über die Schulkonsole gewährleistet. An deren Regeln dürfen nur die beschriebenen Änderungen durchgeführt werden, damit die dynamischen Einstellungen weiterhin von der Schulkonsole erledigt werden können.

Prinzipiell ist weniger mehr. Versuchen Sie sich auf ein möglichst einfaches, in sich stimmiges Regelwerk zu beschränken. Je mehr Spezialregeln Sie anlegen, desto komplexer wird die Fehlersuche und desto mehr Performance kostet die Auswertung bei jedem Internetzugriff.

Diese Anleitung hat weder den Anspruch, eine vollständige Einführung in die Bedienung des ISA zu liefern noch auch nur annähernd die Möglichkeiten aufzuzeigen, die sich durch dieses Programm ergeben. Der geneigte Leser sei hierfür an die Onlinehilfe, die technische Referenz und die im letzten Abschnitt gelisteten weiterführenden Werke verwiesen. Zudem kann auf viele Möglichkeiten nur in Stichworten oder anhand von Beispielen eingegangen werden, die vorliegende Anleitungen ist also nicht unbedingt für Anfänger geeignet. Trotzdem erhalten Sie vielleicht einen kleinen Einblick in die Prinzipien und Hintergründe.

## 1.1. Sichern und Wiederherstellen

---

Im Gegensatz zum ISA 2000 können Sie die komplette Konfiguration des ISA 2006 jederzeit in eine externe Datei abspeichern und auch wieder einlesen. Die Daten werden in einer XML-Datei abgelegt. Es ist sogar möglich, diese zu Wartungszwecken an die Hotline zu senden, so dass dort Ihre Einstellungen überprüft werden könnten.

Bitte beachten Sie, dass der Support sich immer nur auf die verbindlichen Grundeinstellungen beziehen kann.

Unmittelbar nach der Installation des ISA-Servers befindet sich dieser in einem absolut sicheren Zustand - so sicher, dass viele wichtige Netzwerkfunktionalitäten im internen Netz nicht gegeben sind. Durch Einlesen der paedML-Grundkonfiguration werden geeignete Voreinstellungen gesetzt und die Basisregeln für die Schulkonsole angelegt.

Bitte beachten Sie: durch Zurücksetzen auf diesen Grundzustand gehen alle individuellen Änderungen verloren!

**Übung 1:** Grundzustand wiederherstellen

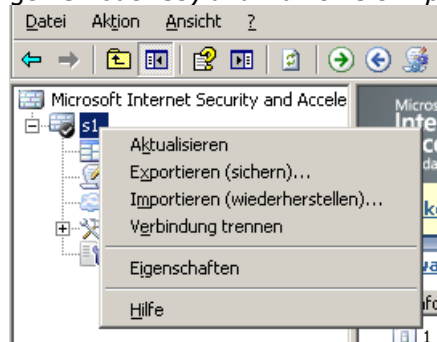
Der Grundzustand wird über ein Skript eingestellt, das die notwendige Konfigurationsdatei automatisch einliest.

Starten Sie die Datei `configISA2006.vbs` im Ordner  
`c:\setup2003\isa2006.`

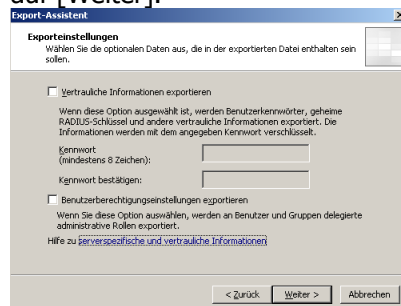
Bevor Sie größere Änderungen an Ihrem System vornehmen, sollten Sie die aktuelle Konfiguration abspeichern.

**Übung 2:** Abspeichern der Gesamtkonfiguration

1. Starten Sie auf Ihrem Server die ISA-Verwaltungskonsolle durch *Start | Programme | Microsoft ISA Server | ISA Server-Verwaltung*
2. Klicken Sie mit der rechten Maustaste auf `s1` (in Mehrserverumgebungen `S2` oder `S3`) und wählen Sie *Exportieren*.



3. Klicken Sie auf [Weiter].
4. Lassen Sie im nächsten Schritt beide Felder ohne Haken und klicken Sie auf [Weiter].



5. Geben Sie nun einen Dateinamen an, z.B. `c:\isakonfig.xml`. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.
6. Schließen Sie nach dem erfolgreichen Export die Aktion mit [OK] ab.

Sie könnten sich die Einstellungen in der soeben gespeicherten Datei ansehen. Diese ist jedoch ca. 500kB groß und nur sehr schlecht zu verstehen.

Praktisch genauso können Sie eine zuvor gespeicherte Konfiguration auch wieder einlesen. Bitte beachten Sie, dass sich, wenn diese Datei alt war, IP-Adressen der Arbeitsstationen mittlerweile geändert haben könnten. Deshalb sollten Sie wie unten beschrieben diese Einträge über die Schulkonsole auf den aktuellen Stand bringen.

**Übung 3:** Wiederherstellen einer gespeicherten Konfiguration

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]), z.B. `c:\isakonfig.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].
8. Starten Sie nun die Schulkonsole und wählen Sie den Menüpunkt *Räume*. Nehmen Sie, falls gewünscht, Veränderungen an den Einstellungen vor und klicken Sie abschließend auf *Alle Änderungen übernehmen*.

## 1.2. Firewallregeln

Die meisten Einstellungen am ISA-Server werden die Firewallrichtlinien betreffen. Hier wird schließlich eingestellt, wer von welchem Rechner aus auf welche Ressourcen Zugriff hat.<sup>1</sup>

### 1.2.1. Eigenschaften einer Richtlinie

Klickt man mit der rechten Maustaste auf eine der Richtlinien und wählt Eigenschaften, so erscheint eine Art Karteikasten mit einer ganzen Reihe von Reitern.

**Eigenschaften von Freigegebene Rechner**

Auswahl der Unterpunkte

Name der Regel

Beschreibungs-text

Zugriffsregeln gehen von innen nach außen, Webveröffentlichungen geben interne Server frei.

Hier kann die Regel abgeschaltet werden, ohne sie zu löschen

**Eigenschaften von Benutzer Sperre**

Entscheidet, ob die Regel den Zugriff erlaubt oder verbietet

Optional kann man beim Verbot eine Umleitung definieren

Die Anfrage wird ins Protokoll geschrieben. Das ist nicht immer sinnvoll

1 Eine Übersicht zu den von der paedML vorgegebenen Standardregeln finden Sie im Basiskurs.

The screenshot shows the 'Eigenschaften von Freigegebene Rechner' dialog box with the 'Protokolle' tab selected. The 'Regel wird angewendet für:' section has a dropdown menu set to 'Ausgewählte Protokolle'. Below this, a list of protocols includes FTP, HTTP, and HTTPS, with the first three checked. To the right of the list are buttons for 'Hinzufügen...', 'Bearbeiten...', and 'Entfernen'. At the bottom right, there are buttons for 'Ports...' and 'Filterung...'. Three blue callout boxes provide instructions: one points to the dropdown menu, another to the 'Hinzufügen...' button, and a third to the 'Filterung...' button.

Sie legen fest, ob die Regel für alle oder nur die unten definierten Protokolle gilt

Sie können weitere Protokolle hinzufügen oder bestehende anklicken und dann bearbeiten/entfernen

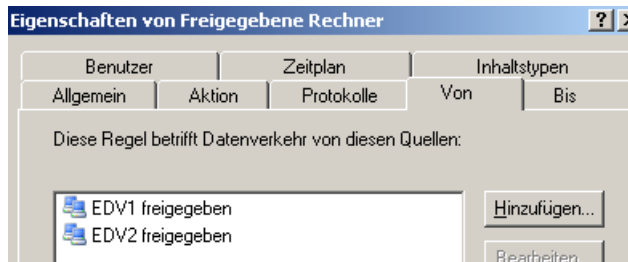
Diese Protokolle wurden ausgewählt

Hier können ganz spezielle Zusatzeinstellungen gemacht werden

Informationen zur HTTP-Filterung finden Sie z.B. unter

<http://www.msisafaq.de/Anleitungen/2006/Firewallrichtlinien/HTTPFilter.htm>

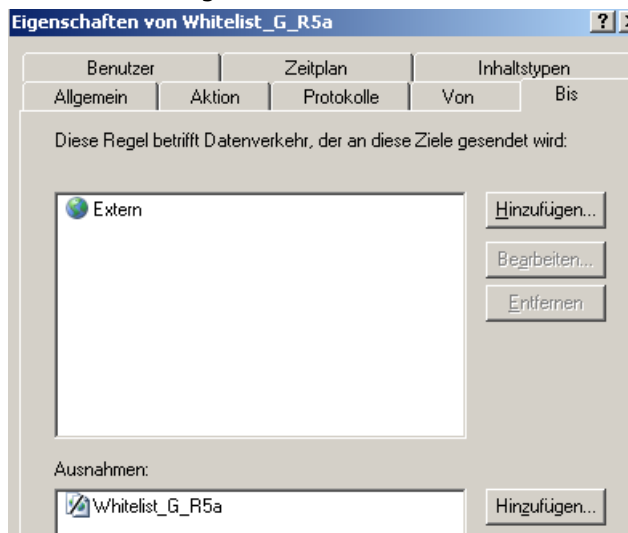
<http://www.isaserver.org/tutorials/Configuring-ISA-Server-2006-HTTP-Filter.html>

Reiter *VON* und *BIS* : Quelle und Ziel

Die Regel wird immer auf den Datenverkehr zwischen den zwei Stationen angewendet, die als *Von* bzw. *Bis* definiert sind. Bei beiden können verschiedene Arten von Adressen eingetragen sein, vom einzelnen Computer bzw. einer URL über Computer- oder Netzwerksätzen bis hin zum gesamten internen Netz bzw. Internet.

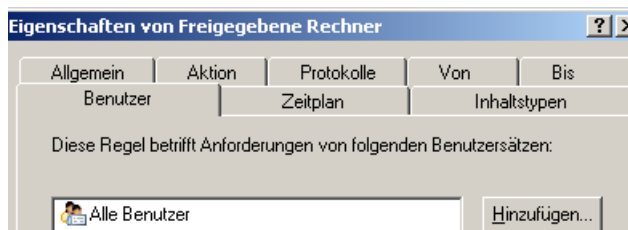
Einzelne Computer müssen im ISA zunächst eingetragen werden; sie sind letztendlich ausschließlich durch ihre IP-Adresse gekennzeichnet. Die hier abgebildeten Computersätze wurden für die Schulkonsole eingerichtet und werden bei jeder Aktion "im Raum" aktualisiert.

Bei den Adressen könnten im unteren Fensterbereich Ausnahmen getroffen werden. Davon wird z.B. bei Regeln für Whitelisten Gebrauch gemacht: hier wird einer Gruppe der Zugang ins komplette WWW außer den im URL-Satz der Whiteliste aufgeführten Adressen verweigert.



Das Anlegen der entsprechenden Objekte geht über die Toolbox (aufklappbarer Fensterbereich ganz rechts). Sie können sich dabei an den bereits vorhandenen Objekten orientieren, auch die Onlinehilfe beantwortet manche Fragen.

Sollten Sie einzelne Computer verwenden, ist es sehr hilfreich, diesen über DHCP-Reservierungen eine feste IP-Adresse zuzuordnen. Eine Anleitung dazu finden Sie z.B. unter <http://www.wintotal.de/Artikel/w2003server5/w2003server5.php>.



Beim Reiter *Benutzer* wird festgelegt, ob die Regel (wie abgebildet) für alle, oder nur für bestimmte Benutzer gelten soll. Per Grundeinstellung sind nur die Einträge "Alle Benutzer" und "Authentifizierte Benutzer" vorhanden. Der Unterschied ist klein, aber wesentlich:

- bei "Alle Benutzern" sind die Log-Einträge anonym
- bei "Authentifizierte Benutzer" müssen sich Benutzer, die den Firefox benutzen oder die nicht mit einem Domänenaccount angemeldet sind, nochmals anmelden.

Auch hier sind wieder Ausnahmefälle eintragbar. Ein Beispiel zu den Benutzern folgt weiter unten.

Der Reiter *Zeitplan* ist selbsterklärend. Er wird nur in wenigen Fällen in der Schule seine Anwendung finden.

Die *Inhaltstypen* können verwendet werden, um nur bestimmte Dateitypen in einer Regel zu erlauben oder um diese zu verbieten. Auch hierzu wird ein Beispiel gegeben.

### 1.2.2. Beispiel 1: Herr Hahn will immer surfen können

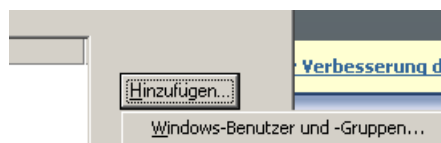
**Situation:** Hans Hahn ist Rektor einer Grundschule. Dort ist für die meisten Computer per Defaulteinstellung der Internetzugang gesperrt. Herr Hahn will aber trotzdem, ohne den Rechner erst freischalten zu müssen, Internetzugang haben.

Des weiteren möchte er nicht, dass seine Internetaufrufe protokolliert werden.

**Analyse:** Auf einem Client kommt man nur ins Internet, wenn er freigeschaltet ist. Es nützt auch nicht, bei der Regel "gesperrte Rechner" Herrn Hahn als Ausnahme einzutragen, da der Rechner explizit in einer Zulassungsregel vorkommen müsste. Wir richten daher eine zusätzliche Regel für ihn ein. Diese muss auf jeden Fall oberhalb der Sperrregel eingetragen sein, da die Regeln von oben nach unten abgearbeitet werden und der erste Treffer das Verhalten bestimmt.

#### Übung 4: Neue Firewallregel mit neuem Benutzer

1. Starten Sie am Server die ISA-Verwaltungskonsolle und navigieren Sie zu den Firewallrichtlinien. Klappen Sie, falls erforderlich, den rechten Bereich aus und wählen Sie die *Toolbox*.
2. Wählen Sie den Bereich *Benutzer* und klicken Sie dort auf *Neu*. Es öffnet sich der Assistent zum Anlegen von Benutzern.
3. Geben Sie als Namen *Rektor* ein. *Weiter*.
4. Im nächsten Feld klicken Sie auf *Hinzufügen... | Windows-Benutzer und -Gruppen*



5. Geben Sie nun den Namen des Benutzers oder der Gruppe ein, hier ist das *Hahn.Hans*, und klicken Sie auf OK. Wenn der Name nicht eindeutig ist (wie z.B. bei *g\_lehrer*), bekommen Sie eine Liste angezeigt, aus der Sie das gewünschte Objekt auswählen können.

- Sie können diesen Schritt wiederholen, um mehrere Benutzer oder Gruppen zu einer ISA-Gruppe zusammenzufassen.
6. Mit *Weiter* und *Fertigstellen* schließen Sie diese Aktion ab.
  7. Wählen Sie nun im mittleren Fenster die Regel "*Gesperrte Rechner*" durch einen Klick aus. Vor dieser Regel soll jetzt eine neue eingefügt werden.
  8. Wechseln Sie rechts von *Toolbox* auf *Aufgaben* und klicken Sie mit der linken Maustaste *Zugriffsregel erstellen* aus. Wieder startet ein Assistent.
  9. Geben Sie der Regel einen aussagekräftigen Namen, z.B. *Internetzugang Hahn. Weiter*.
  10. Als Aktion wählen Sie *Zulassen*. [Weiter].
  11. Im nächsten Schritt stellen Sie um auf *Gesamten ausgehenden Datenverkehr*. *Weiter*.
  12. Bei den Zugriffsquellen wählen Sie [Hinzufügen], dann bei den *Computersätzen Clients*. [Schließen], [Weiter].
  13. Analog wählen Sie bei den Zielen *Netzwerke / Extern*.
  14. Bei den Benutzern klicken Sie zunächst *Alle Benutzer an*, [Entfernen] diese und fügen dann den Rektor hinzu.
  15. Stellen Sie die Regel fertig. Jetzt fehlt nur noch, das Logging zu verhindern. Dazu klicken Sie die neue Regel mit der rechten Maustaste an, wählen Sie *Eigenschaften* und entfernen Sie bei *Aktion* unten den Haken bei *Anwendungen protokollieren...* [OK].
  16. Ganz zum Abschluss müssen Sie nun noch oben auf [Übernehmen] klicken. Jetzt können Sie das Ergebnis auf einem Client testen.

### 1.2.3. Beispiel 2: Vom Lehrerrechner soll FTP möglich sein

**Situation:** Eine AG hilft bei der Pflege der schuleigenen Homepage. Der betreuende Lehrer möchte gerne per FTP auf Daten dieser externen Seite zugreifen können.

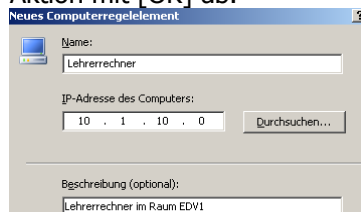
**Analyse:** Im Prinzip könnte man die benötigten Protokolle einfach in der Regel "Freigegeben Rechner" ergänzen. Aus Sicherheitsgründen soll das jedoch nur für den Lehrerrechner gelten. Auf diesem ist der Firewallclient installiert, er hat per DHCP-Reservierung die IP 10.1.10.0.

#### Übung 5: FTP am Lehrerrechner

1. Reservieren Sie für den Rechner PC1 die IP-Adresse 10.1.10.0 im DHCP.
2. Starten Sie am Server die ISA-Verwaltungskonsole. Gehen Sie links auf Firewallrichtlinie und im kleinen Fenster rechts (evtl. ausklappen!) die *Toolbox*. In dieser suchen Sie den Bereich *Netzwerkobjekte* (ganz unten).



3. Klicken Sie mit der rechten Maustaste auf *Computer* und wählen Sie *Neuer Computer...*
4. Geben Sie die Daten wie unten abgebildet ein und schließen Sie die Aktion mit [OK] ab.



5. Erstellen Sie nun wie in der letzten Übung eine neue Zugriffsregel oberhalb von "Gesperrte Rechner". Verwenden Sie folgende Einstellungen:  
**Name:** *FTP Lehrerrechner*  
**Regelaktion:** *Zulassen*  
**Protokolle:** *Ausgewählte Protokolle*; Fügen Sie das Protokoll *Web / FTP* hinzu.  
**Quellen:** Fügen Sie Ihren *Lehrerrechner* hinzu.  
**Ziele:** *Extern*.  
**Benutzer:** *Alle authentifizierte Benutzer<sup>2</sup>* (Sie könnten auch eine neue Gruppe anlegen und hier eintragen).
6. [Fertigstellen]. Klicken Sie jetzt mit der rechten Maustaste auf die neue Regel. Wählen Sie den untersten Punkt *FTP konfigurieren* und entfernen Sie den Haken bei *Nur lesen*. Sonst könnten Sie keine Daten uploaden.
7. Sie können zumindest den Download auf diesem Client testen. Benutzen Sie dazu den IE und z.B. <ftp://ftp.heise.de>.  
 Generell ist aber die Verwendung des Browsers als FTP-Client nicht zu empfehlen!

Hinweise:

- Aus Sicherheitsgründen könnten Sie auch den Zielbereich einschränken. Sie müssten hierzu einen Domännennamensatz mit den freigegebenen Domänen anlegen.
- Wenn Sie FTP an allen Rechnern nutzen wollen, können Sie das Protokoll einfach bei der Regel "Freigegebene Rechner" ergänzen.

<sup>2</sup> Eine Authentifizierung ist nur möglich, wenn der Firewallclient installiert ist. Andernfalls müssen hier "Alle Benutzer" stehen bleiben.

### 1.2.4. Beispiel 3: Benutzer sollen private Mails abrufen können

**Situation:** Einige Kolleginnen und Kollegen wollen z.B. mit der portablen Version von Thunderbird gerne per POP3 oder IMAP auf ihren privaten E-Mail-Account zugreifen können. Das soll nur von Rechnern im Lehrerzimmer möglich sein.

**Analyse:** Lehrerinnen und Lehrern soll im Raum (OU) "Lehrerzimmer" diese Protokolle freigeschaltet werden. Dazu wird eine neue Firewallrichtlinie erstellt.

#### Übung 6: Portable Thunderbird freischalten

1. Erstellen Sie wie in der letzten Übung eine neue Zugriffsregel.  
Protokolle: Mail -> *IMAP4, IMAP4S, POP3, POP3S, SMTP, SMTPS*.  
Von: *EDV1 freigegeben*  
Bis: *Extern*  
*Alle Benutzer*.
2. (Optional, wenn Sie die Daten für einen Mail-Account parat haben)  
Melden Sie sich als Huber.Hanne an einem Client an und kopieren Sie den portable Thunderbird<sup>3</sup> in Ihr Homeverzeichnis. Testen Sie die Verbindung. Deaktivieren Sie die Mailregel und testen Sie erneut.

### 1.2.5. Beispiel 4: Schüler sollen keine MP3 und Filme laden dürfen

**Situation:** Schülerinnen und Schüler versuchen bei jeder Gelegenheit Filme oder MP3-Dateien herunterzuladen, weil der Internetzugang in der Schule so schön schnell ist. Auch ist das Ansehen dubioser "Spaßfilmchen" bei youtube & Co. im Unterricht zum Volkssport geworden. Andererseits nutzen Kolleginnen und Kollegen mitunter youtube, um den Fremdsprachenunterricht zu bereichern.

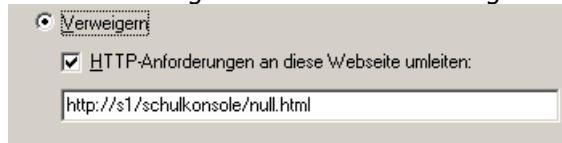
**Analyse:** Das Ziel ist nicht leicht zu erreichen. Aufgrund der vielen möglichen Quellen ist eine Regelung über Blacklisten nicht möglich. Es bleibt eine Sperrung nach Inhaltstypen — über eine Zugriffsregel oder über HTTP-Filterung.

#### Übung 7: Anlegen einer Filmsperrregel

1. Legen Sie wie in den vorherigen Übungen eine neue Zugriffsregel an. Nennen Sie die Regel "*Blackliste Videoverbot*". *Verweigern*. Alle Protokolle. Von *Clients* bis *Extern*. Benutzer Schueler (neuen Benutzer mit *g\_schueler* erstellen).
2. Jetzt kommt das Feintuning: Klicken Sie die neue Regel mit der rechten Maustaste an und wählen Sie *Eigenschaften*.

<sup>3</sup> Im Moment downloadbar unter <http://portable-thunderbird.softonic.de/>.

3. Unter Aktion ergänzen Sie eine Umleitung<sup>4</sup> wie abgebildet:



4. Bei den *Inhaltstypen* setzen Sie einen Haken bei *Audio* und *Video*. Übernehmen Sie die Änderungen.
5. Testen Sie Youtube als Lehrer und Schüler.
6. Deaktivieren Sie auf dem einen Client in EDV1 den Webfilter und testen Sie jetzt nochmals den Zugriff als Schüler vom anderen Client.<sup>5</sup> Beobachten Sie in der ISA-Konsole, was genau beim Deaktivieren des Webfilters passiert (mit **F5** aktualisieren!)

Hinweise:

1. Analog können Sie auch andere Dateitypen sperren. Sie können auch einen eigenen "Dateitypkorb" zusammenstellen.
2. Leider funktioniert die Sperrung nicht zu 100% zuverlässig. Eine genauere Trefferzahl erreicht man über die sogenannte HTTP-Filterung. Das Thema sprengt jedoch den Rahmen und eine einfache Abschaltbarkeit ist hier nicht gegeben.

### 1.2.6. Beispiel 5: Das Programm LernOfix benötigt den Port 47110

**Situation:** Das Programm LernOfix zur Leseförderung arbeitet mit tagesaktuellen Artikeln. Dieses lädt es sich verschlüsselt beim Programmstart von einem zugriffsgeschützten Server herunter und benötigt dafür zwingend den Port 47110 aus- und eingehend. Am Router wurde dieser Port schon von BelWue freigeschalten, jetzt muss nur noch der ISA konfiguriert werden.

**Analyse:** Am einfachsten ist es hier, ein neues Protokoll<sup>6</sup> für den notwendigen Port zu definieren. Selbst wenn man den gesamten ausgehenden Datenverkehr freigibt, werden nämlich nur diejenigen Protokolle durchgelassen, die im ISA-Server definiert sind.

Auf die zusätzliche Sicherheit, über eine neue Zulassungsregel diesen Datenverkehr auf eine bestimmte Ziel-Domäne zu beschränken, kann vermutlich verzichtet werden.

#### Übung 8: Erstellung eines neuen Protokolls

1. Starten Sie die ISA-Konsole und wechseln Sie in die Firewallrichtlinien-*Toolbox*. Wählen Sie den obersten Bereich, *Protokolle*.
2. Legen Sie ein neues Protokoll mit dem Namen LernOfix an. [Weiter].
3. Fügen Sie über *Neu* ein neues Protokoll hinzu (Hierzu würden Sie die technische Dokumentation des Programms benötigen).
4. Stellen Sie das Protokoll fertig und fügen Sie es zu "Freigegebene Rechner" hinzu.

---

4 Wenn Sie das nicht tun, kommt jedes Mal ein Authentifizierungsfenster, wenn eine Datei gesperrt ist.

5 Der Trick an der Sache ist der Name der Zugriffsregel. Alle, die mit *Blackliste* beginnen, unterliegen der Steuerung durch den Webfilter.

6 Siehe auch <http://www.msisafaq.de/Anleitungen/2006/Grundlagen/Protokoll.htm>

### 1.2.7. Beispiel 6: Private Notebooks der Lehrer sollen freien Zugang zum Internet erhalten

**Situation:** Eine Reihe von Kollegen nutzt private Notebooks auch in der Schule. Diese Geräte sollen grundsätzlich für den Internetzugang freigeschaltet werden.

**Analyse:** Da die betreffenden Rechner nicht Teil der Domäne sind, lässt sich der Zugang am besten über einen neuen *Computersatz* und eine entsprechende Freigabe-richtlinie erreichen. Dazu müssen die Lehrernotebooks aber im Netz jedesmal dieselbe IP-Adresse erhalten, so dass sie von der neu anzulegenden Zulassungsregel auch erkannt werden können. Der Weg dorthin besteht aus *mehreren* Schritten:

Zuerst muss ein *Adressbereich* für die Notebooks festgelegt und im ISA ein entsprechendes *Netzwerkobjekt* angelegt werden.

Anschließend kann dieser Adressbereich für den Internetzugriff freigegeben werden. Zudem erhält jedes freizugebende Notebook über den DHCP-Server eine feste IP-Adresse zugeteilt, so dass die Netzwerkeinstellungen auf den Geräten nicht jedesmal manuell festgelegt werden müssen (die Netzwerkeinstellungen müssen dazu auf „automatisch“ stehen. Dies ist der Normalfall).

Wichtig: Der freizugebende IP-Bereich sollte unbedingt außerhalb des normalerweise vom DHCP-Server verwendeten Bereiches für die Workstations des Schulnetzes liegen, ansonsten könnten einzelne Rechner im Netz ungewollt eine grundsätzlich freigegebene IP erhalten! Hierzu stehen die Bereiche 10.1.21.xxx bis 10.1.255.xxx zur Verfügung. Wählen Sie zur Sicherheit in Ihrem System einen anderen Bereich als in dieser Anleitung verwendet. Der Adressbereich sollte aus Sicherheitsgründen auch nicht größer sein als unbedingt nötig!

#### Übung 9: Neuer Adressbereich und DHCP-Reservierungen

1. Starten Sie die ISA-Konsole und wechseln Sie in der Firewallrichtlinien-*Toolbox* auf Netzwerkobjekte.
2. Klicken Sie im Menübereich auf *Neu* und anschließend auf *Adressbereich*.
3. Geben Sie dem neuen *Adressbereich* einen sprechenden Namen wie „Lehrernotebooks“ und geben Sie die erste und letzte IP-Adresse des gewünschten Bereiches an (hier 10.1.255.1-10.1.255.20 für maximal 20 Notebooks). Ein erklärender Eintrag im Feld *Beschreibung* dient dem Verständnis auch für spätere bzw. externe Betreuer. Mit [OK] schließen Sie diesen Schritt ab.
4. Wählen Sie nun im mittleren Fenster die oberste Regel durch einen Klick aus. Vor dieser Regel soll jetzt eine neue eingefügt werden.
5. Legen Sie eine neue Zugriffsrichtlinie mit dem Namen „Internet für Lehrernotebooks“ an (alternativ könnte z.B. die Zulassungsregel *Internetzugang Hahn* aus Übung 4 erweitert und entsprechend umbenannt werden). [Weiter]
6. Als Regelaktion wählen Sie „Zulassen“. [Weiter].
7. Die Regel soll für den gesamten ausgehenden Datenverkehr angewandt werden. [Weiter].
8. Fügen Sie bei den *Zugriffsregelquellen* mit Klick auf *Hinzufügen* den neu angelegten *Adressbereich* hinzu.

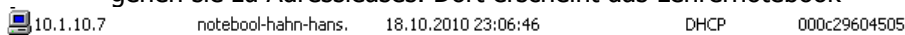
9. Stellen Sie die Zulassungsregel für alle externen Ziele und alle Benutzer fertig.
10. Die neue Regel muss unbedingt vor der ersten Regel mit einer Verweigerung stehen<sup>7</sup>. Verschieben Sie sie daher ggf. an die oberste Stelle. Damit ist der zweite Schritt abgeschlossen.

Nun muss dem privaten Notebook noch eine feste IP zugewiesen werden. Die IP muss im Bereich des eben erstellten Adressbereichs für Lehrernotebooks liegen (also in unserem Fall zwischen 10.1.255.1 und 10.1.255.20).

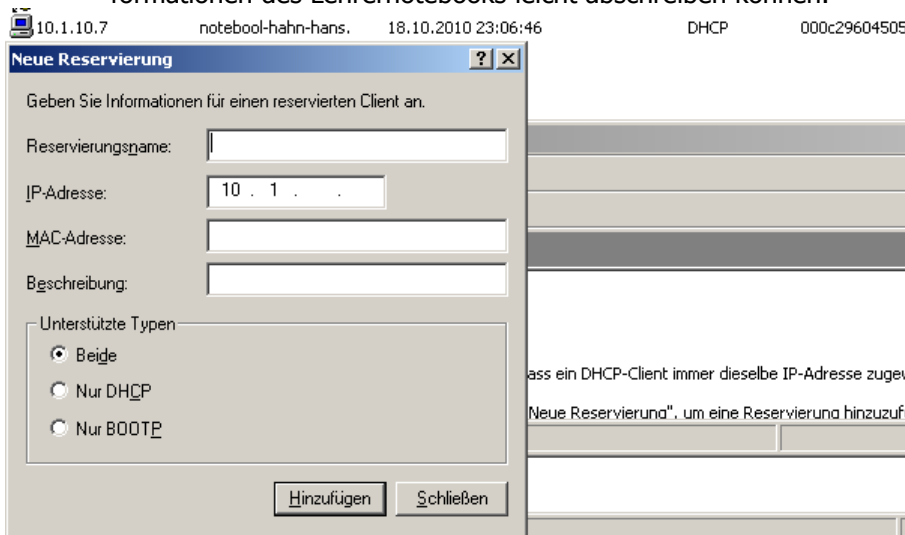
Zur Reservierung benötigen Sie den *Namen* des Lehrernotebooks und dessen *MAC-Adresse*. Diese Informationen erhalten Sie z.B. über die Eigenschaften des Computers. Einfacher geht es, wenn Sie das Notebook einmal mit dem Schulnetz verbinden. Es erhält dann per DHCP eine IP Adresse. Alle zur Reservierung benötigten Informationen finden Sie dann in der DHCP Verwaltung.

### Übung 10: Feste IP für Lehrernotebooks mit SKAddons reservieren

1. Verbinden Sie das Lehrernotebook mit dem Schulnetz und starten Sie es.
2. Öffnen Sie die DHCP Verwaltung (*Start | Programme | Verwaltung*) und gehen sie zu Adressleases. Dort erscheint das Lehrernotebook



3. Öffnen Sie nochmals die DHCP Verwaltung, dieses mal gehen Sie zu Reservierungen. Klicken Sie rechts auf *Reservierungen* und wählen Sie *Neue Reservierung*. Ordnen Sie das neue Fenster so an, dass Sie die Informationen des Lehrernotebooks leicht abschreiben können.



4. Geben Sie unter Reservierungsname den Namen des Notebooks ein. Als IP wählen Sie eine aus dem Adressbereich für die Lehrernotebook, z.B. 10.1.255.1. Die MAC Adresse steht in der letzten Spalte. Das Eintragen einer Beschreibung ist optional.

<sup>7</sup> Nach dem Firewallrichtlinien-Update ISA 2006 ist dies die Regel BSA\_Internetsperre.

Neue Reservierung

Geben Sie Informationen für einen reservierten Client an.

Reservierungsname: notebook-hahn-hans.

IP-Adresse: 10 . 1 . 255 . 1

MAC-Adresse: 000c29604505

Beschreibung: Notebook des Kollegen Han

Unterstützte Typen

Beide

Nur DHCP

Nur BOOTP

Hinzufügen Schließen

5. Wählen Sie Hinzufügen und Schließen. Damit ist die Reservierung der IP Adresse abgeschlossen.
6. Die DHCP-Reservierung muss für jedes gewünschte Notebook einzeln jeweils mit einer noch freien IP-Adresse aus dem oben angelegten Adressbereich durchgeführt werden. Sollte dieser Adressbereich sich im Laufe der Zeit als zu klein erweisen, lässt er sich im ISA jederzeit unter Netzwerkobjekte erweitern, indem die Endadresse des Bereiches entsprechend geändert wird.

## 1.3. Überwachungsfunktion verwenden

Der ISA 2006 ist mit vielen Funktionen ausgestattet, die eine Überwachung gestatten. Dabei geht es zum einen um das Aufspüren möglicher Fehler oder Fehlkonfigurationen, zum anderen um die Auswertung aufgerufener Webseiten.

Per Grundeinstellung sind alle Protokollierungen anonym. Das muss schon aus Datenschutzgründen so voreingestellt sein. Wenn Sie personenbezogene Daten erheben und speichern möchten, müssen Sie in Ihrer Schule ein Konzept dazu erarbeiten. Hierbei ist z.B. Schulleitung und Personalrat einzubeziehen, wenn auch Lehrerdaten erfasst werden. Im Fall von Schülerinnen und Schülern sind diese und ihre Erziehungsberechtigten über dieses Vorgehen zu informieren. Am einfachsten kann das über eine Benutzerordnung geschehen, die einmalig oder jährlich zu unterzeichnen ist.

### 1.3.1. Echtzeitprotokollierung

Im Bereich *Überwachung* | *Protokollierung* der ISA-Konsole können Sie in Echtzeit beobachten, welcher Datenverkehr durch den ISA läuft. Das ist besonders zur Fehlersuche recht praktisch, z.B. auch um bei der Verwendung von Blacklisten festzustellen, warum der Zugriff auf eine Seite scheitert.

Die Überwachung wird noch übersichtlicher, wenn Sie zuvor das ISA-Featurepack installieren<sup>8</sup>.

Protokollierung...	Ziel-IP	Zielport	Protokoll	Aktion	Regel	Client-IP	Clientbenutzern...	Quelle
12.12.2007 07:45:27	80.67.17.116	80	HTTP	Initiiert...		192.168.3.3		Lokaler
12.12.2007 07:45:27	10.1.1.1	80	http	Zugela...	Internetzugriff fü...	10.1.1.1	anonymous	Lokaler
12.12.2007 07:45:27	80.67.17.116	80	HTTP	Initiiert...		192.168.3.3		Lokaler
12.12.2007 07:45:27	80.67.17.116	80	http	Zugela...	Internetzugriff fü...	10.1.1.1	anonymous	Lokaler
12.12.2007 07:45:27	80.67.17.116	80	HTTP	Getren...		192.168.3.3		Lokaler
12.12.2007 07:45:27	10.1.1.1	80	http	Zugela...	Internetzugriff fü...	10.1.1.1	anonymous	Lokaler
12.12.2007 07:45:27	195.189.236.30	80	HTTP	Initiiert...		192.168.3.3		Lokaler
12.12.2007 07:45:28	195.189.236.30	80	http	Zugela...	Internetzugriff fü...	10.1.1.1	anonymous	Lokaler
12.12.2007 07:45:28	195.189.236.30	80	HTTP	Getren...		192.168.3.3		Lokaler

**Zugelassene Verbindung** 51 12.12.2007 07:45:27  
**Protokollierungstyp:** Webproxy (Forward)  
**Status:** 0 Der Vorgang wurde erfolgreich beendet.  
**Regel:** Internetzugriff für Server  
**Quelle:** Lokaler Host (10.1.1.1)  
**Ziel:** Extern (10.1.1.1:80)  
**Anforderung:** GET http://ml-tips.de/cms/home/logo.gif  
**Filterinformationen:**  
**Protokoll:** http  
**Benutzer:** anonymous  
 ⓘ Zusätzliche Informationen

Auf die vielfältigen Möglichkeiten der Überwachungsfunktion insgesamt kann hier nicht weiter eingegangen werden. Vieles erschließt sich aber intuitiv oder wird ausführlich in der Onlinehilfe (rechts oben, Reiter "Hilfe") erklärt.

<sup>8</sup> Einfach heruntergeladen und doppelklicken. Download unter <http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=6f629eac-d8c6-4437-9d20-b47b02db413a>

### 1.3.2. Internetprotokollierung

Der ISA wird so konfiguriert, dass alle Internetzugriffe in einer Textdatei protokolliert werden. Die Alternative (Daten MSDE) wäre schwieriger zu handhaben und kostet deutlich mehr an Speicherplatz und Performance.

Für den Alltag an der Schule sollten Sie die Protokollierungseinstellungen anpassen. Dazu müssen Sie vorher planen,

- ob überhaupt und wenn ja welche Regeln protokolliert werden sollen,
- wie lange die Daten vorrätig gehalten werden sollen,
- welche Felder zu protokollieren sind,
- ob anonym oder mit Namen protokolliert wird.

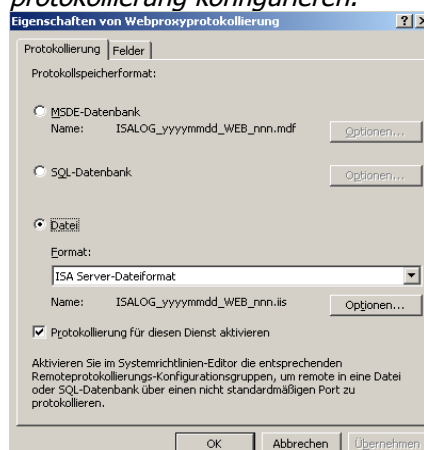
Bitte beachten Sie bei diesen Überlegungen unbedingt den Datenschutz!

Die Protokolldateien werden standardmäßig im Ordner `C:\Programme\Microsoft ISA Server\ISALogs` abgelegt. Falls auf dem Systemlaufwerk der Speicherplatz knapp werden sollte, können Sie den Speicherort auf ein anderes Laufwerk verlegen.

Im folgenden Beispiel sollen die Daten mindestens vier Wochen aufbewahrt werden. Aus Platzgründen werden sie im zuvor neu angelegten Ordner `d:\MSISALOGS` abgelegt.

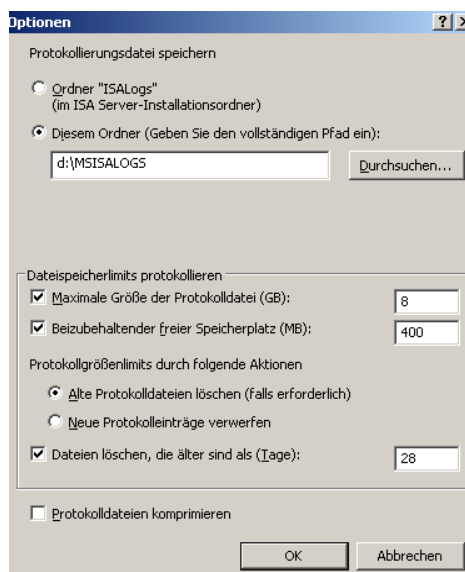
#### Übung 11: Protokolleinstellungen einrichten

1. Legen Sie vorbereitend den Ordner `d:\MSISALOGS` neu an.
2. Starten Sie die ISA-Verwaltungskonsole und wählen Sie links den Knoten *Überwachung*, in der Mitte den Reiter *Protokollierung*. Klappen Sie gegebenenfalls den rechten Fensterbereich aus und wählen Sie dort *Aufgaben*.
3. Im mittleren Bereich des Aufgabenfensters finden Sie die Möglichkeit, die Firewall- und Webproxyprotokollierung zu konfigurieren. HTTP(S) wird im Webproxy erfasst. Klicken Sie deshalb auf *Webproxyprotokollierung konfigurieren*.



Bei diesem Fenster sollten Sie alle Einstellungen belassen. Wenn Sie keine Protokollierung wünschen, können Sie diese hier abschalten, indem Sie den Haken bei *Protokollierung..aktivieren* entfernen. Klicken Sie aber jetzt auf *[Optionen...]*

4. Im sich jetzt öffnenden Formular können Sie die gewünschten Einstellungen vornehmen. Wenn Sie auf [F1], die Hilfetaste, drücken, bekommen Sie zu den einzelnen Punkten eine genauere Erklärung. Stellen Sie die Optionen wie im nächsten Screenshot abgebildet ein:



5. Schließen Sie die Aktion durch [OK] [OK] [Übernehmen] ab.
6. Rufen Sie einige externe Seiten im IE auf und kontrollieren Sie, ob die Protokolldatei am neuen Ort angelegt wird.

**Hinweise:**

1. Beachten Sie, dass die Logdateien pro Tag schnell 100MB und mehr umfassen können. Daher muss auf der Partition genügend Speicher vorhanden sein, damit die eingestellte Anzahl der Tage erreicht werden kann.
2. Sie könnten gegebenenfalls (Datenschutz beachten!) ältere Protokolldateien per geplantem Task an einen anderen Ort sichern.
3. Das Dateiformat w3c enthält nur die gewählten Felder, die durch ein Tabulatorzeichen getrennt sind. Die Zeit ist UTC, also gegenüber der "echten" Zeit ein bis zwei Stunden früher. Im ISA-Server Dateiformat werden immer alle Felder durch Kommata getrennt, nicht ausgewählte Felder werden durch einen "-" angegeben. Die Zeit ist die reale Zeit.
4. Die zu speichernden Felder können Sie im Reiter *Felder* auswählen. Im Allgemeinen enthalten nur wenige Felder nützliche Informationen. Hier lässt sich Speicherplatz einsparen - außerhalb der Fehlersuche notwendig sind eigentlich nur *Client-IP* und *-benutzername*, *Protokollierungsdatum* und *-zeit* und natürlich *URL*.

### 1.3.3. Auswertung der Logdateien per Tool

Logdateien bestehen aus Tausenden von Einträgen. Es ist unmöglich, diese alle in Augenschein zu nehmen.

Sie können dafür bei <http://support-netz.de> ein Excel-Tool herunterladen, dass Sie ein wenig beim Durchsuchen unterstützt<sup>9</sup>.

Features:

- Gesamte Logdateien können nach Stichworten durchsucht werden,
- Reine Textsuche, daher nach Benutzername, URL, Regel...
- Übersichtliche Ausgabe, nach Benutzername und Zeit sortiert
- Als zusätzliche Information Klasse und PC-Name

---

<sup>9</sup> Vermutlich ab März 2008 verfügbar.

- Lehrer werden für gewöhnlich nicht ausgewertet.
- Das Tool ist in gewissem Rahmen konfigurierbar bezüglich
- maximaler Trefferzahl
  - UND oder ODER-Suche bei maximal zwei Suchbegriffen
  - auszuschließende Begriffe
  - im Protokoll verwendete Felder und deren Position.

Natürlich kann keine Suche nach dem *Inhalt* aufgerufener Seiten stattfinden, es wird nur das gefunden, was in der Protokolldatei steht.

## 1.4. Den Cache konfigurieren

---

Ein Cache ist ein Zwischenspeicher für Dateien aus dem Internet, so dass diese schneller bereitstehen, wenn das selbe Objekt ein weiteres Mal aufgerufen wird. Jeder Browser verfügt heute über diese Funktionalität. Trotzdem kann es sinnvoll sein, auch auf dem Proxyserver, den der ISA ja darstellt einen Cache einzurichten. Dieser wird umso effizienter arbeiten, je mehr die Benutzer im Netzwerk dieselben Seiten aufrufen. Insbesondere kleine, statische Grafikdateien sind über den Cache sehr viel schneller aufzurufen. Damit wird die Netzlast über den Flaschenhals Internetanbindung reduziert und der Aufruf von Internetseiten für alle beschleunigt. Wichtig ist, dass die Kopien im Cache auf ihre Aktualität untersucht werden. Das alles kostet Rechenzeit, Hauptspeicher und Festplattenperformance.

Bei der Installation des ISA 2006 wird zunächst kein Cache eingerichtet. Sie können das jedoch jederzeit nachholen. Notwendig ist der Cache nicht, ob er objektiv einen Geschwindigkeitszuwachs bringt, müssen Sie selbst entscheiden.

Leider gibt es keine allgemein gültigen Richtlinien, wieviel an Speicherplatz Sie reservieren sollen. Das hängt u.a. ab von

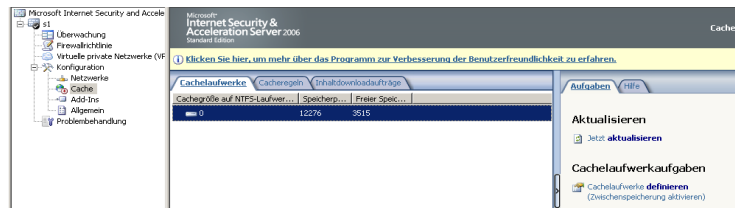
- Leistungsfähigkeit, Hauptspeicher und Festplattenkapazität
- Anbindungsgeschwindigkeit an das Internet
- Anzahl der gleichzeitigen User, die surfen
- Sonstige Dienste, die auf dem Server laufen (z.B. Virens Scanner)

Die für den professionellen Bereich ausgelegte Regel, für den Cache eine eigene Festplatte, wenn nicht gar einen RAID-Verbund einzuplanen, ist im Schulbereich sicher nicht notwendig.

Eine Cachegröße von 1000MB sollte mehr als ausreichend sein, u.U. liefert auch ein kleinerer Cache bessere Ergebnis. Eine untere sinnvolle Grenze sollte bei ca. 100MB liegen.

### Übung 12: Cache einrichten

1. Starten Sie die ISA-Verwaltungskonsole. Wechseln Sie im Bereich Konfiguration auf den Knoten Cache.



2. Klicken Sie rechts auf *Cacheaufwerke definieren*. Wählen Sie das Laufwerk `D` aus und geben Sie den Wert `150` (MB) ein. Klicken Sie auf [Festlegen], [OK] und dann oben auf [Übernehmen].
3. Wählen Sie *Änderung speichern und Dienste neu starten* (untere Option).

Der ISA wird jetzt oder spätestens beim nächsten Neustart eine Fehlermeldung generieren. Im *Alarme*-Bereich der *Überwachung* kann man sich den Grund dafür anzeigen lassen:

*Beschreibung: ISA Server konnte den Cache nicht initialisieren, weil das Netzwerkdienstkonto nicht über ausreichende Berechtigungen für den Stammordner und den Ordner "Urlcache" auf mindestens einem Cachelaufwerk verfügt. Das Netzwerkdienstkonto muss die Berechtigung "Ordner auflisten" und die Leseberechtigung für den Stammordner sowie die Leseberechtigung für den Ordner "Urlcache" besitzen, damit der Ordner "Urlcache" auf jedem Cachelaufwerk geöffnet werden kann. Stellen Sie sicher, dass das Netzwerkdienstkonto mindestens die Ordnerlisten- und die Leseberechtigung für den Stammordner sowie die Leseberechtigung für den Ordner "Urlcache" auf allen Cachelaufwerken besitzt.*

Leider ist die Fehlermeldung so nicht ganz korrekt. Im Ordner `URLCACHE` muss das Netzwerkdienstkonto Schreibrechte haben. Das hängt vermutlich damit zusammen, dass die Berechtigungen auf `D:` in der `paedML` sehr restriktiv gesetzt wurden.

Eine bebilderte Anleitung mit weiteren Hinweisen finden Sie unter <http://www.msisafaq.de/anleitungen/2004/Konfiguration/Cache.htm>  
ISA 2004 und 2006 unterscheiden sich in diesem Punkt kaum.

**Übung 13:** Berechtigungen für das Caching setzen

1. Starten Sie auf dem Server den Arbeitsplatz. Klicken Sie mit der rechten Maustaste auf das Laufwerk D, wählen Sie *Eigenschaften* und dort den Reiter *Sicherheit*. Sollte der Netzwerkdienst dort nicht aufgeführt sein<sup>10</sup>, so müssen Sie ihn über *Hinzufügen* ergänzen.



2. Legen Sie auf D: jetzt den Ordner URLCACHE an. Geben Sie unter *Eigenschaften* / *Sicherheit* dem Netzwerkdienst *Ändern*-Berechtigungen.
3. Beenden Sie in der ISA-Konsole unter *Überwachung* | *Dienste* den Firewalldienst (anklicken, rechts: Dienst beenden) und starten Sie ihn dann wieder.
4. Kontrollieren Sie, ob jetzt im Ordner URLCACHE die Datei `Dir1.cdat` angelegt wurde.
5. Sie müssen jetzt den Firewalldienst noch einmal neu starten, dann funktioniert der Cache.

Leider kann man in der ISA-Konsole nicht erkennen, was genau im Cache passiert. Microsoft bietet aber dafür ein kostenloses Tool zum Download an.

**Übung 14:** Das Cache Directory Tool installieren

1. Laden Sie auf dem Server das Tool unter <http://www.microsoft.com/downloads/details.aspx?familyid=b9ecf-cd3-c13f-4447-83ed-add9a8ea45db&displaylang=en> herunter.
2. Entpacken Sie die Dateien durch einen Doppelklick. Als Zielverzeichnis müssen Sie unbedingt `C:\Programme\Microsoft ISA Server` wählen, da sonst eine notwendige DLL nicht gefunden wird.
3. Starten Sie das Programm `Cachedir.exe` im o.a. Verzeichnis und testen Sie seine Funktionalität.

<sup>10</sup> Haben Sie z.B. den WSUS auf Ihrem System installiert, so ist dieser schon vorhanden.

## 1.5. Zugriff von extern

---

Mit dem ISA 2006 lässt sich ein Zugriff über das Internet professionell und sicher konfigurieren. Damit wird eine Fernwartung ebenso möglich wie ein Zugriff von Lehrerinnen und Lehrern auf ihr Homeverzeichnis oder Tauschlaufwerke.

Das Vorgehen hierzu sprengt den Rahmen dieser Kurzanleitung bei weitem. Sie finden deshalb eine ausführliche Anleitung nebst Übungen auf dem Landesbildungsserver.

## 1.6. Weitergehende Anleitungen

---

Kein Schnäppchen, aber sehr empfehlenswert für diejenigen, die viel mit dem ISA vorhaben:

Grothe, Gröber, Rauscher: ISA 2006, Das Handbuch. Microsoft Press 2007 (59€).

Dieselben Autoren haben auch einige Anleitungen im Internet veröffentlicht:

<http://www.msisafaq.de/Anleitungen/2006/index.htm>

Anleitungen von Martin Resch auf dem Lehrerfortbildungsserver:

Basiskurs, Internetsteuerung mit dem ISA 2006

[http://lehrerfortbildung-bw.de/netz/muster/win2000/material/basis30/pdf/kap\\_13\\_Internetsteuerung2006.pdf](http://lehrerfortbildung-bw.de/netz/muster/win2000/material/basis30/pdf/kap_13_Internetsteuerung2006.pdf)

Remotezugriff, Einrichtung von VPN und WebSSL mit dem ISA 2006,

<http://lehrerfortbildung-bw.de/netz/muster/win2000/material/remote/remote06.pdf>

Bei Microsoft, für Leute, die es ganz genau wissen wollen:

ISA 2006 SDK (Referenz, englisch)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=16682c4f-7645-4279-97e4-9a0c73c5162e&DisplayLang=en>

Evaluation Guide

<http://www.microsoft.com/isaserver/prodinfo/guide.msp>

180 Tage Testversion

<http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=84504-cad-893b-4212-9ab2-999ad1d8fe68>