

paedML Die Musterlösung
Baden-Württemberg

Windows 2003 Server paedML[®] Windows 2.1 für schulische Netzwerke

WebSSL mit ISA 2006 / Installationsanleitung
Stand 17.12.2007



Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Projekt „Support-Netz“
Rosensteinstraße 24
70191 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Projekt „Support-Netz“, LMZ

Tamer, Berber
Carsten Brotz
Adrian Koch
Martin Resch
Jürgen Schnaiter

Endredaktion

Ulrike Boscher

Weitere Informationen

www.support-netz.de
www.lmz-bw.de
www.medienoffensive.schule-bw.de

Veröffentlicht: **2007**

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	Einführung	2
2.	Systemvoraussetzungen	2
3.	Vorbereitung	3
4.	Installation WebSSL	4
5.	Veröffentlichen des Exchange OWA	6
6.	Zugriff auf Tausch- und Homeverzeichnisse	16
6.1.	Einrichten von Webfreigaben	16
6.2.	Veröffentlichen der Webfreigaben	18
6.3.	Veröffentlichung der Schulkonsole	27
7.	Quellen und weiterführende Links	28

0. Einführung

In dieser Anleitung wird gezeigt, wie über das Protokoll 443 SSL (Secure Socket Layer) ein sicherer webbasierter Zugriff auf den Exchange Server (Outlook Web Access) erfolgt. Zusätzlich werden Tausch- und Homeverzeichnisse über Webfreigabe externen Benutzern zur Verfügung gestellt.

Die Verbindung erfolgt über SSL und ist somit für Dritte nur schwer bzw. nur mit immensem Zeitaufwand zu entschlüsseln.

Für die Verschlüsselung ist ein Zertifikat notwendig, welches Sie selbst erstellen oder käuflich von einer öffentlichen Zertifizierungsstelle, z.B. VeriSign, erwerben können. Da das Zertifikat relativ teuer ist, erstellen wir es automatisch selbst.

Dadurch ergibt sich eine Einschränkung: Ein solches Zertifikat kann nicht bis zur Zertifizierungsstelle überprüft werden, da keine Zertifizierungsstelle existiert.

Aufgrund dessen werden Sie beim externen Zugriff einen Sicherheitshinweis erhalten, dass das Zertifikat fehlerhaft ist. Die Verbindung erfolgt aber trotzdem verschlüsselt, so dass dieser Sicherheitshinweis ignoriert werden kann.

1. Systemvoraussetzungen

Die folgende Anleitung setzt folgendes Grundsystem voraus:

paedML Windows 2.0 für Windows 2003 Server

- Windows 2003 Server Standard Edition
- Exchange 2003 Server Standard Edition
- ISA 2006 Server Standard Edition
- Schulkonsole ab 2.1

Über den Stand der aktuellen Service Packs und Aktualisierungen können Sie sich unter <http://www.support-netz.de/nc/kundenportal/updates-und-patches/windows.html> informieren. Dort finden Sie immer die aktuellen Freigaben für die Musterlösung.

Hinweis: Musterlösungen mit Windows 2000 Server (WML 1.1) werden bei diesem Update nicht mehr unterstützt.

Es wird für die externe Anbindung des Servers (Routers) eine feste IP Adresse (empfohlen) oder ein DYN DNS Konto mit eingerichtetem IP-Update benötigt.

(siehe http://www.msisafaq.de/Anleitungen/2000/Internet/dsl_router.htm).

Bei Verwendung eines Routers (empfohlen!):

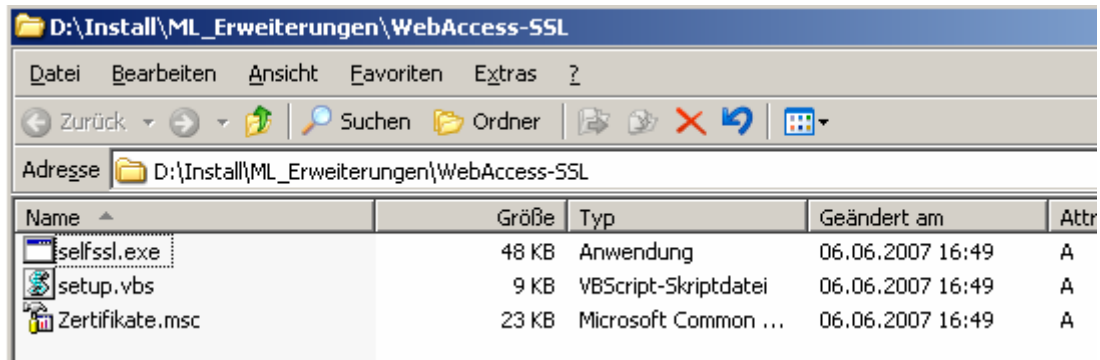
- Sie müssen eine feste IP an der externen Netzwerkkarte eintragen, da der ISA 2006 eine Zuweisung per DHCP von außen nicht gestattet.
- Sie müssen eine Weiterleitung des Ports TCP 443 an diese externe IP des Servers bzw. Eintrag des Servers als DMZ-Server im Router eintragen (eigener Router) bzw. bei Belwue einrichten lassen.

2. Vorbereitung

Die Installationsdateien erhalten Sie unter <http://www.support-netz.de/nc/kundenportal/updates-und-patches/windows/isa-2006-server-fuer-paedml-windows-2003-server.html>.

Laden Sie die Datei *SSL_ISA 2006.zip* herunter und führen die *SSL_ISA2006.exe* aus.

Die Dateien werden nach `D:\Install\ML_Erweiterungen\WebAccess-SSL` kopiert.



3. Installation WebSSL

Funktionen der Dateien:

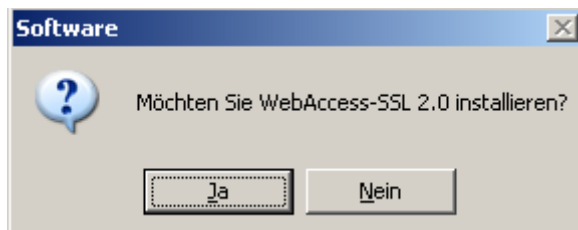
- *setup.vbs*: Skript zum Konfigurieren des Webabhörers und Erstellen des Zertifikats;
- *selfssl.exe*: Programm von Microsoft zur Zertifikaterzeugung;
- *Zertifikate.msc*: Tool zum Anzeigen und Verwalten von Zertifikaten.

Aufgaben des Scripts:

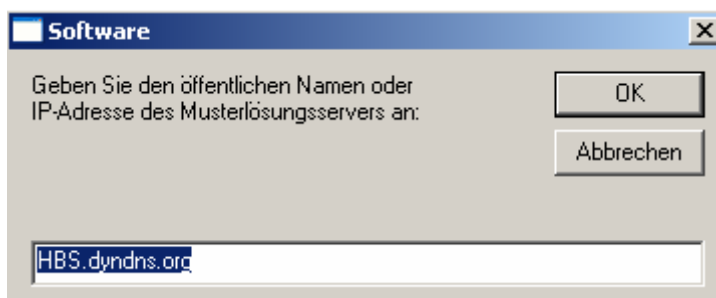
- Wenn auf dem ISA-Server gleichzeitig der IIS-Dienst läuft, wird zunächst das *Socket Pooling* des IIS deaktiviert. Der IIS hört danach nur noch das interne Interface am Port 80 (HTTP) und 443 (HTTPS) ab.
- Durch den Aufruf von *selfssl* wird ein Zertifikat auf die öffentliche IP bzw. URL der Schule angelegt. Dieses ist ca. 5 Jahre lang gültig.

Starten Sie die *Setup.vbs*, um die Installation zu starten.

Klicken Sie auf *Ja*.

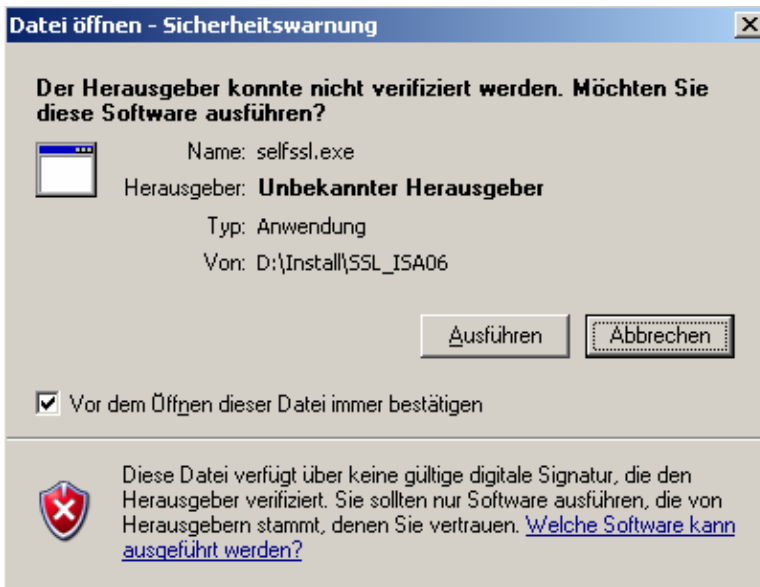


Geben Sie die IP-Adresse der externen Netzwerkkarte oder den dazugehörigen externen Namen an

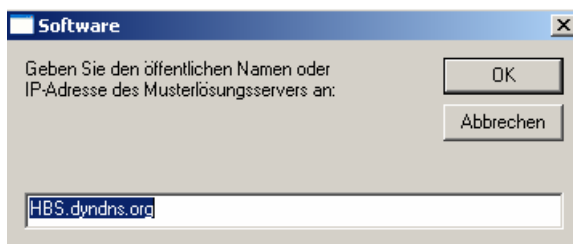


Hinweis: Es kann sein, dass an dieser Stelle eine Sicherheitswarnung des Betriebssystems erscheint (siehe Abbildung auf der nächsten Seite).

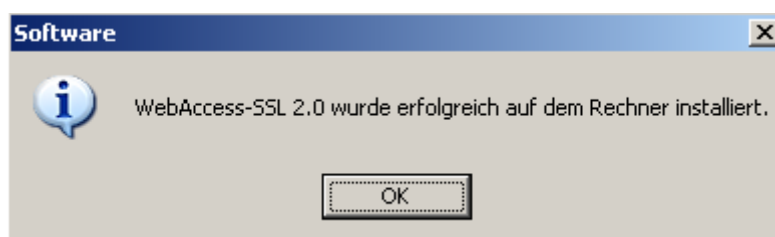
Klicken Sie auf *Ausführen*, um mit Hilfe des SSL Tools *selfssl.exe* das benötigte Zertifikat zu erstellen.



Im nächsten Schritt müssen Sie den Namen oder die feste IP-Adresse, unter der Ihr Netzwerk von außen erreichbar ist eingeben. Unter diesem Name wird das Zertifikat erstellt.



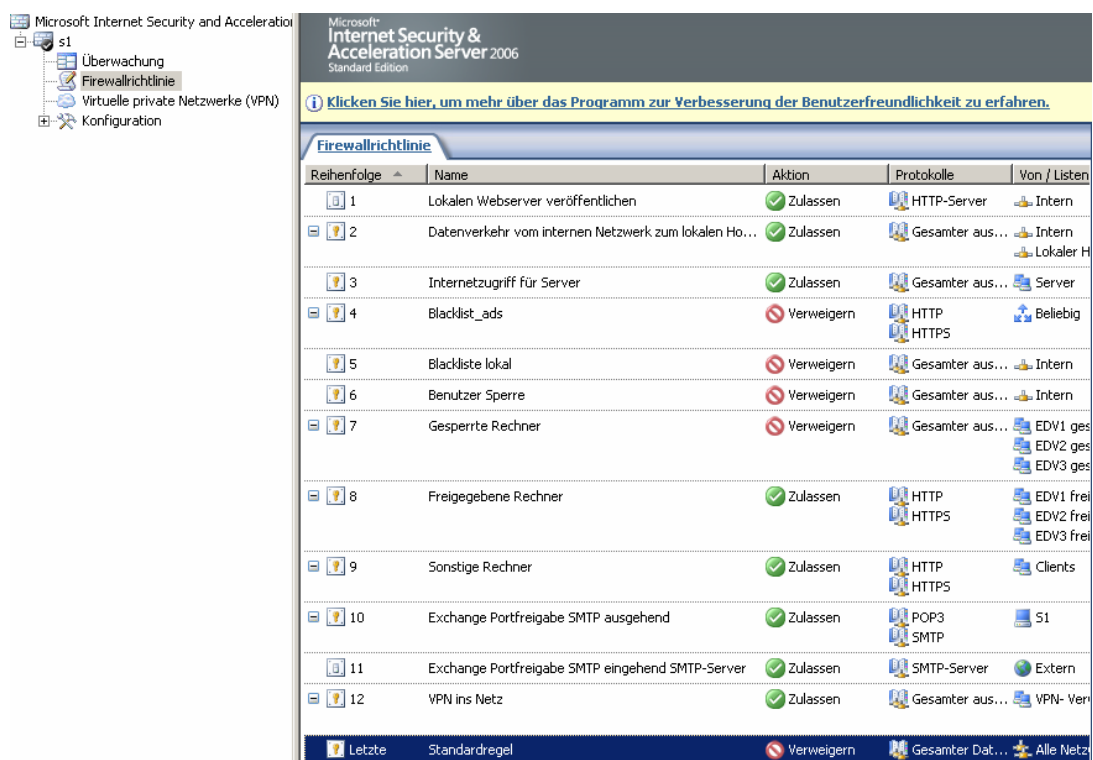
Schließen Sie das Setup mit **OK** ab.



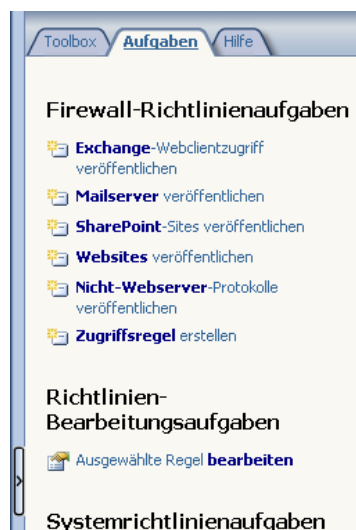
4. Veröffentlichen des Exchange OWA

In diesem Kapitel wird beschrieben, wie man den OWA (Outlook Web Access) extern verfügbar macht. Damit sind Sie in der Lage von Zuhause oder einem sonstigen externen Ort, mit Hilfe des Webbrowsers auf Ihr Postfach zuzugreifen.

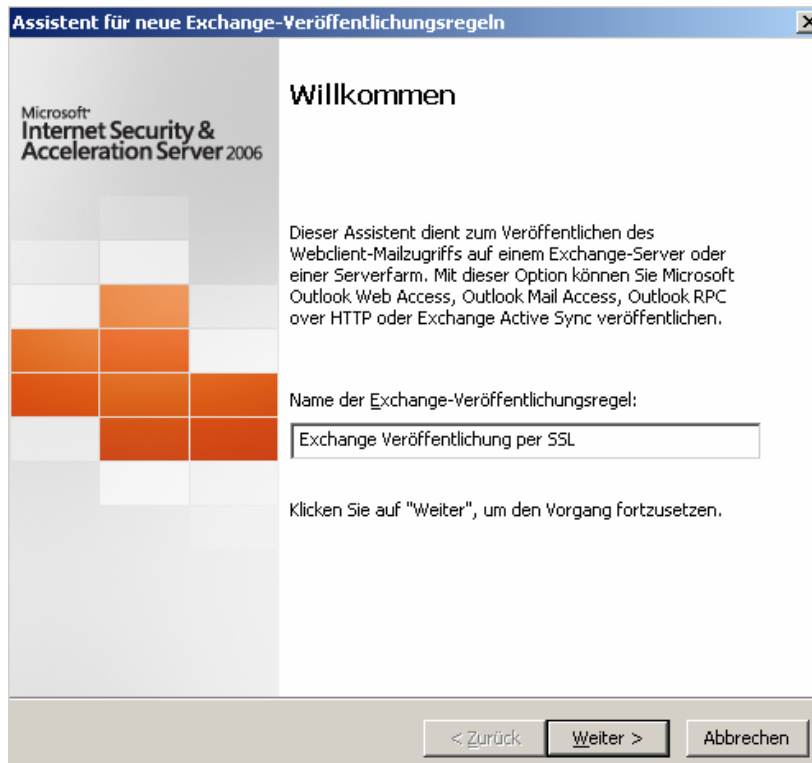
Starten Sie die ISA-Verwaltungstools über *Start| Programme| Microsoft ISA Server| ISA Server-Verwaltung*. Markieren Sie im rechten Fenster Firewallrichtlinien, danach muss im mittleren Fenster die Standardregel ausgewählt werden.



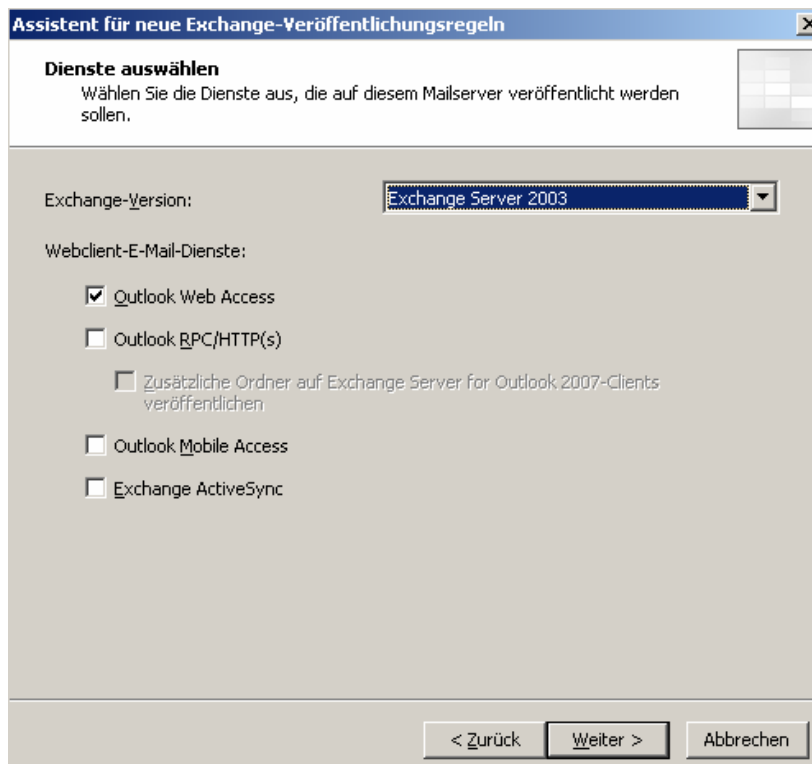
Wählen Sie im rechten Fensterbereich die Registerkarte *Aufgaben* aus und klicken auf *Exchange-Webclientzugriff* veröffentlichen. (Dieser Fensterbereich muss unter Umständen erst aufgeklappt werden).



Geben Sie als Namen Exchange Veröffentlichung per SSL an.
Setzen Sie den Assistenten mit *Weiter* fort.



Die Einstellungen bleiben unverändert. Klicken Sie auf *Weiter*.



Die Voreinstellung *Einzelne Website oder Lastenausgleich veröffentlichen* bleibt unverändert. Klicken Sie auf *Weiter*.

Assistent für neue Exchange-Veröffentlichungsregeln X

Veröffentlichungstyp
 Wählen Sie, ob diese Regel eine einzelne Website oder einen externen Lastenausgleich, eine Webserverfarm oder mehrere Websites veröffentlichen soll.

Einzelne Website oder Lastenausgleich veröffentlichen
 Mit dieser Option können Sie eine einzelne Website oder ein Lastenausgleichsverfahren veröffentlichen, das als Vorstufe für mehrere Server herangezogen wird.
 Hilfe zu [Veröffentlichen einer einzelnen Website oder eines Lastenausgleichsverfahrens](#)

Serverfarm mit Webserver-Lastenausgleich veröffentlichen
 Mit dieser Option ermöglichen Sie ISA Server-Lastenausgleichsanforderungen innerhalb einer Serverfarm (gespiegelte Server).
 Hilfe zu [Veröffentlichen von Serverfarmen](#)

Klicken Sie auf *Weiter*.

Assistent für neue Exchange-Veröffentlichungsregeln X

Sicherheit der Serververbindung
 Wählen Sie den Typ der Verbindungen aus, die ISA Server mit dem veröffentlichten Webserver oder der Serverfarm aufbauen soll.

SSL verwenden, um eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm herzustellen
 ISA Server stellt über HTTPS eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm her (empfohlen). 

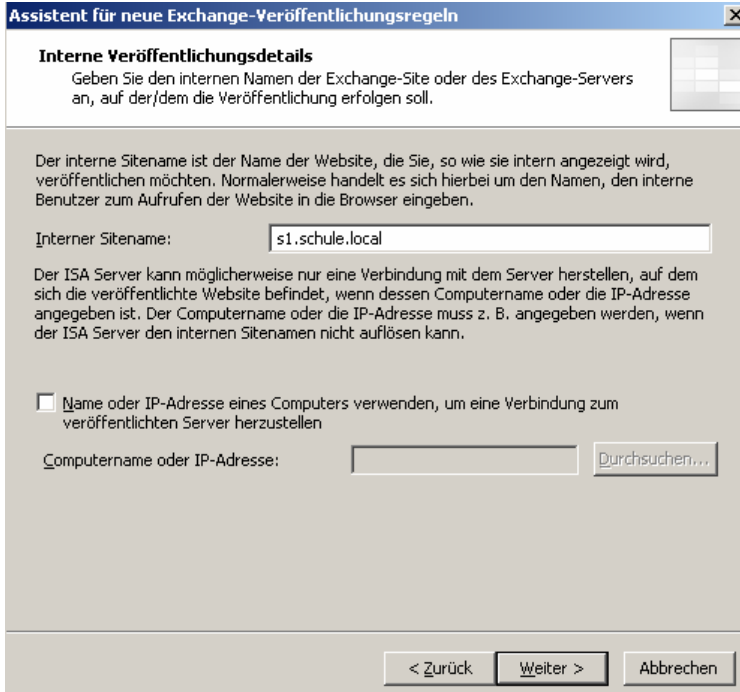
Nicht sichere Verbindungen verwenden, um eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm herzustellen
 ISA Server stellt über HTTP eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm her. 

 Wenn die Clientauthentifizierung erforderlich ist, werden die Benutzeranmeldeinformationen ggf. in Klartext über das Netzwerk gesendet, abhängig von der ausgewählten Clientauthentifizierungsmethode. Durch die Authentifizierung mit SSL werden die Clientanmeldeinformationen geschützt.

Hilfe über [Sicherheit von Serververbindungen](#)

Geben Sie unter *Interner Sitename* `s1.schule.local` ein.

Mehrserverbetrieb: Bei Zwei- und Dreiserverlösungen muss `s2.schule.local` eingegeben werden, da sich dann der Exchange Server auf dem Server S2 befindet.



Assistent für neue Exchange-Veröffentlichungsregeln

Interne Veröffentlichungsdetails
Geben Sie den internen Namen der Exchange-Site oder des Exchange-Servers an, auf der/dem die Veröffentlichung erfolgen soll.

Der interne Sitename ist der Name der Website, die Sie, so wie sie intern angezeigt wird, veröffentlichen möchten. Normalerweise handelt es sich hierbei um den Namen, den interne Benutzer zum Aufrufen der Website in die Browser eingeben.

Interner Sitename:

Der ISA Server kann möglicherweise nur eine Verbindung mit dem Server herstellen, auf dem sich die veröffentlichte Website befindet, wenn dessen Computername oder die IP-Adresse angegeben ist. Der Computername oder die IP-Adresse muss z. B. angegeben werden, wenn der ISA Server den internen Sitenamen nicht auflösen kann.

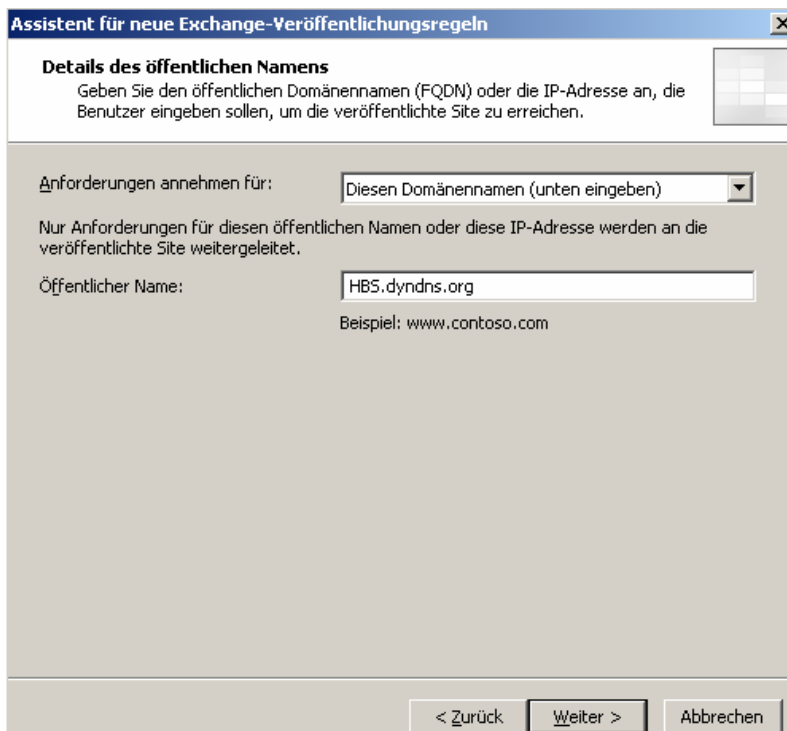
Name oder IP-Adresse eines Computers verwenden, um eine Verbindung zum veröffentlichten Server herzustellen

Computername oder IP-Adresse:

< Zurück Weiter > Abbrechen

Klicken Sie auf *Weiter*.

Geben Sie die externe IP-Adresse oder den dazugehörigen Domännennamen (übereinstimmend mit Ihrer Eingabe bei der Zertifikaterstellung!) ein. Klicken Sie auf *Weiter*.



Assistent für neue Exchange-Veröffentlichungsregeln

Details des öffentlichen Namens
Geben Sie den öffentlichen Domännennamen (FQDN) oder die IP-Adresse an, die Benutzer eingeben sollen, um die veröffentlichte Site zu erreichen.

Anforderungen annehmen für:

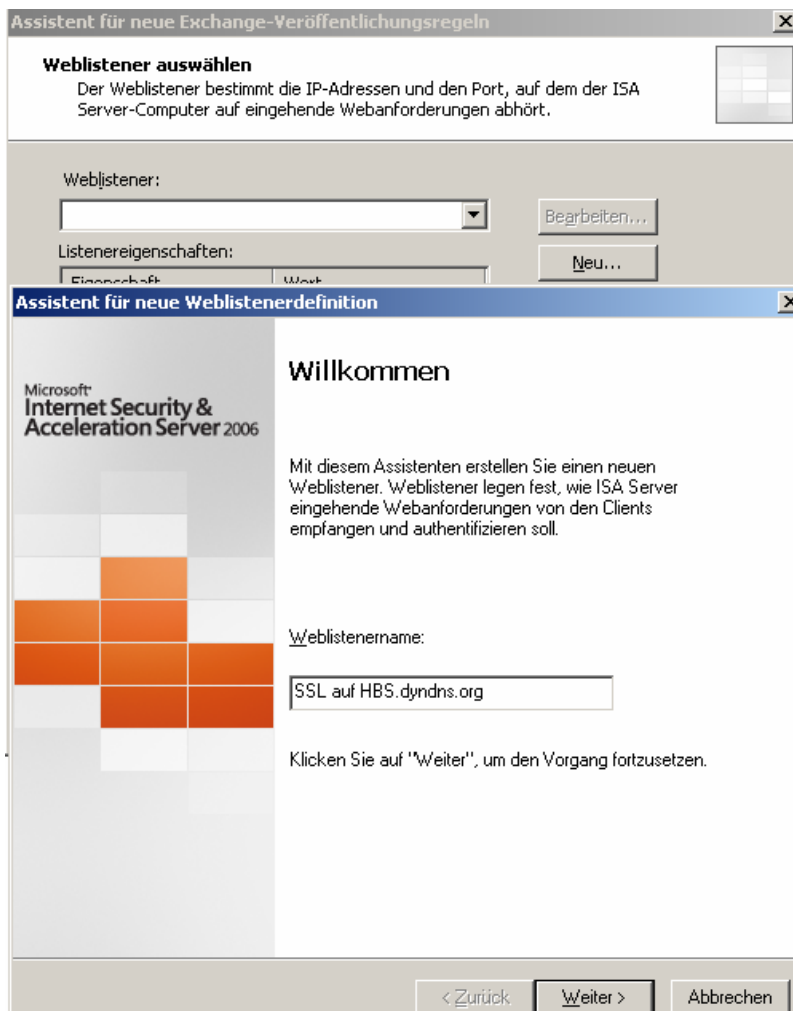
Nur Anforderungen für diesen öffentlichen Namen oder diese IP-Adresse werden an die veröffentlichte Site weitergeleitet.

Öffentlicher Name:
Beispiel: `www.contoso.com`

< Zurück Weiter > Abbrechen

Im nächsten Schritt wird mit dem Weblistener die Schnittstelle nach außen abgefragt. Da noch keine definiert ist, müssen Sie das jetzt tun. Bitte beachten Sie, dass wieder pro IP-Adresse und Port nur ein solcher Listener möglich ist.

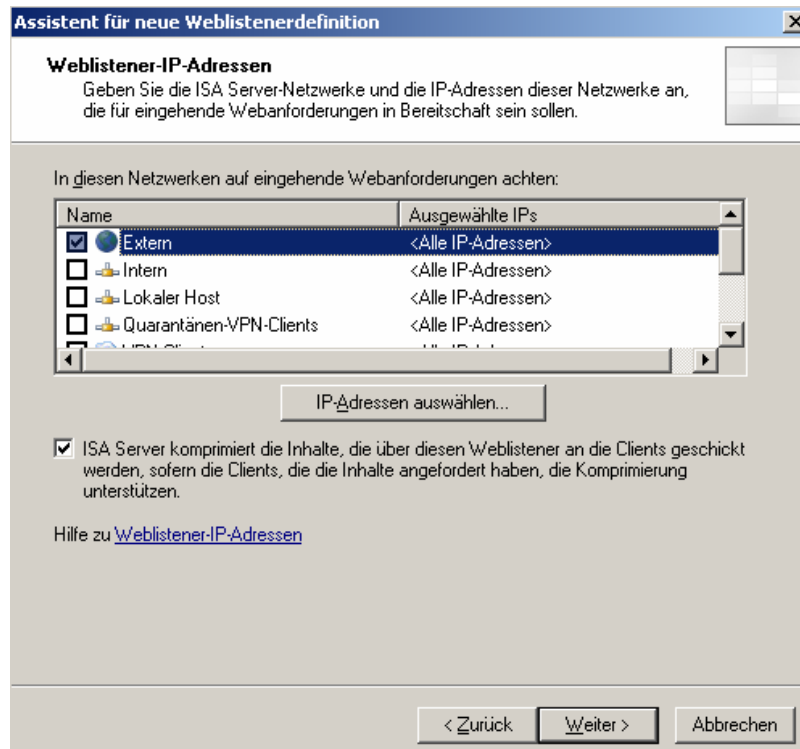
Klicken Sie auf *Neu* und geben als Namen `SSL auf externe IP an`.



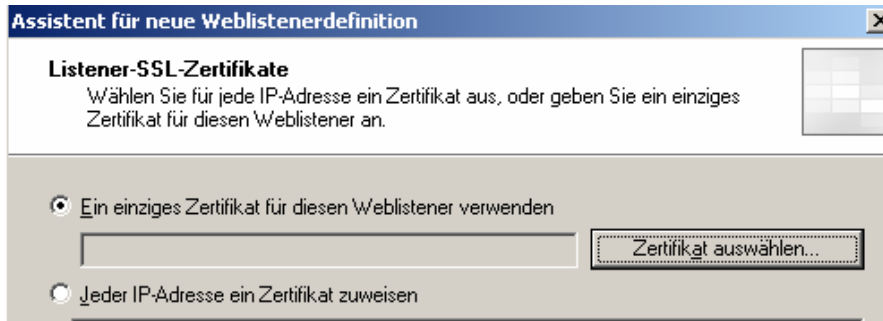
Es geht dieses mal um die Verbindung nach außen, daher wird die Auswahl „*Sichere SSL-Verbindungen mit Clients erforderlich*“ beibehalten. Assistent mit *Weiter* fortsetzen.



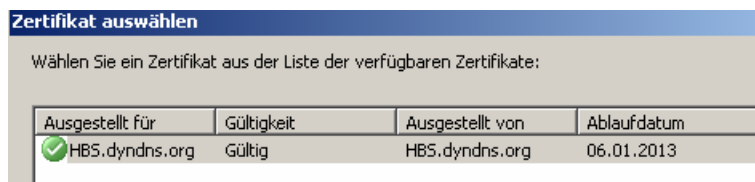
Wählen Sie *Extern* aus und bestätigen mit *Weiter*.



Wählen Sie *Ein einziges Zertifikat für den Weblistener verwenden* aus und klicken auf *Zertifikat auswählen...*

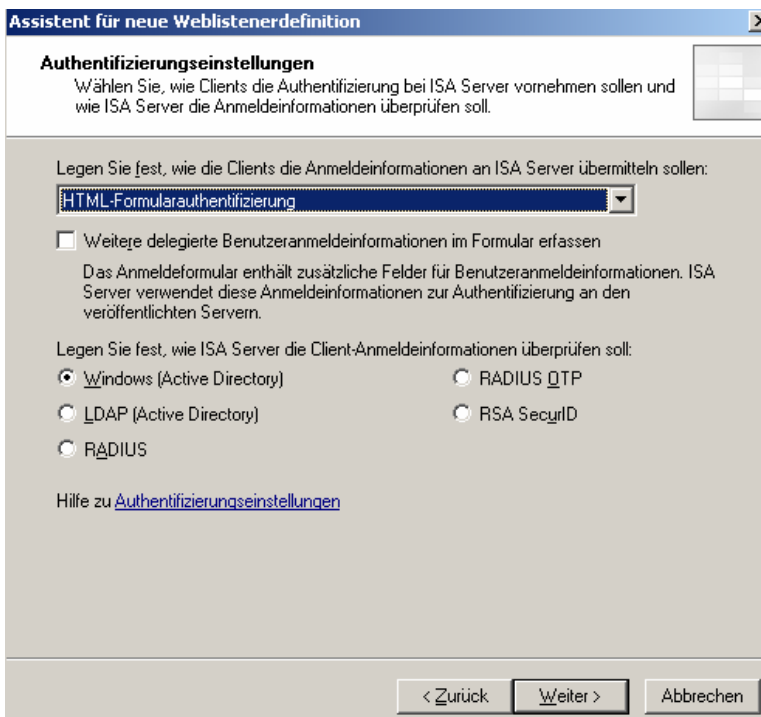


Markieren Sie das Zertifikat und übernehmen dieses mit *Auswahl*.

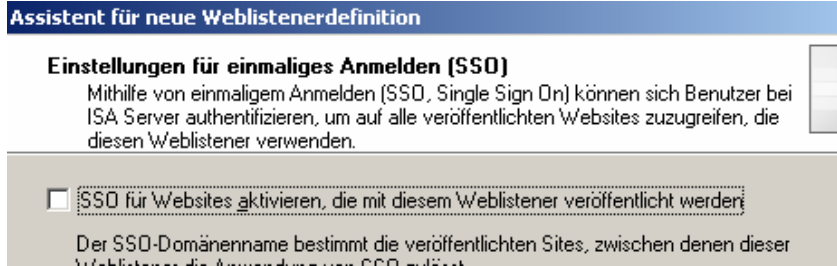


Setzen Sie den Assistenten im Fenster *Listener-SSL-Zertifikate* mit *Weiter fort*.

HTML-Formularauthentifizierung bedeutet, dass der Benutzer beim Anmelden ein Formular für Name und Passwort zu sehen bekommt; wir belassen diese. Klicken Sie ohne Änderungen auf *Weiter*.



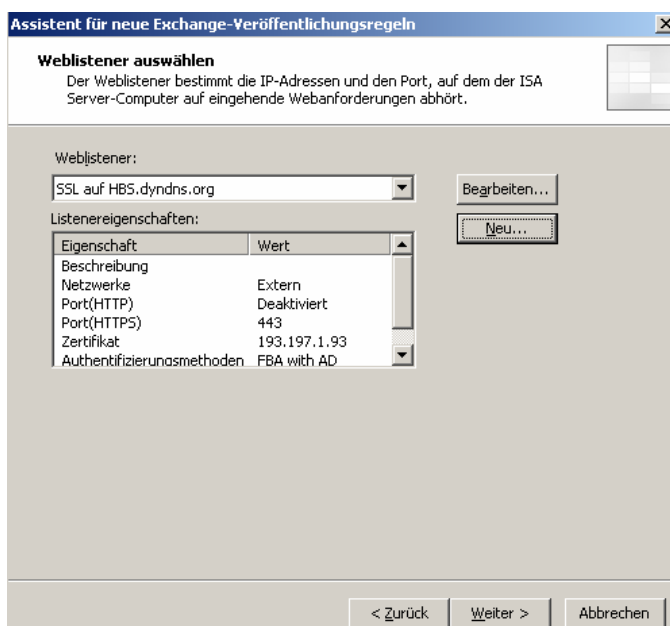
Deaktivieren Sie die Option *SSO für Websites aktivieren, die mit diesem Weblistener veröffentlicht werden*. Bestätigen Sie die Auswahl mit *Weiter*.



Beenden Sie den Assistenten mit *Fertig stellen*.




Wieder zurück bei der Veröffentlichungsregel klicken Sie auf *Weiter*.



Die Authentifizierungsmethode stellen Sie auf *Aushandeln (Kerberos/NTLM)*.

Im unteren Feld geben Sie `http/s1.schule.local` ein

Mehrserverbetrieb: Geben Sie bei Zwei- und Dreiserverlösungen `http/s2.schule.local` ein.



Assistent für neue Exchange-Veröffentlichungsregeln

Authentifizierungsdelegierung
Authentifizierungsdelegierung ist die Methode, mit der ISA Server die Sitzung authentifiziert, die mit der veröffentlichten Site geöffnet wird.

Legen Sie die Methode fest, mit der ISA Server sich beim veröffentlichten Webserver authentifizieren soll:

Aushandeln (Kerberos/NTLM)

Beschreibung
ISA Server verwendet die Verhandlungsauthentifizierung (SPNEGO), um Clients beim Webserver zu authentifizieren. ISA Server versucht als Erstes, die Authentifizierung über Kerberos vorzunehmen. Falls es nicht möglich ist, ein Kerberos-Ticket für den Webserver abzurufen, wird die NTLM-Authentifizierung verwendet. Der Webserver muss die Verhandlungsauthentifizierung akzeptieren. Liegt ein IIS-Webserver vor, muss dieser die integrierte Authentifizierung akzeptieren.

Geben Sie den Dienstprinzipalnamen (SPN) ein, der von ISA Server für die Kerberos-Authentifizierung verwendet wird:

`http/s1.schule.local`

Diese SPN muss ggf. in Active Directory eingefügt werden.
Hilfe zu [Authentifizierungsdelegierung](#)

< Zurück Weiter > Abbrechen

Die Regel wird mit *Übernehmen* aktiviert.



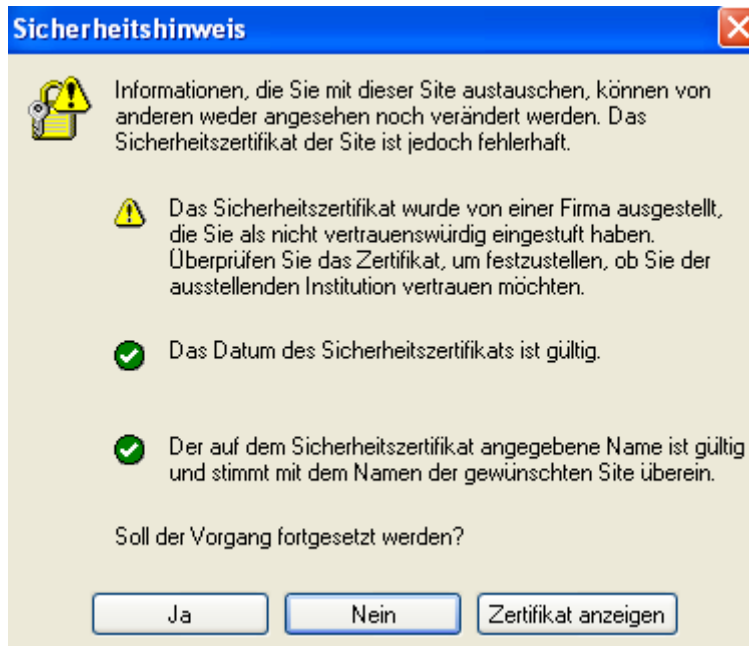
Ab jetzt sollte die Verbindung zum OWA über einen externen Client möglich sein.

Sie können jetzt über einen externen Client den OWA Zugriff testen.

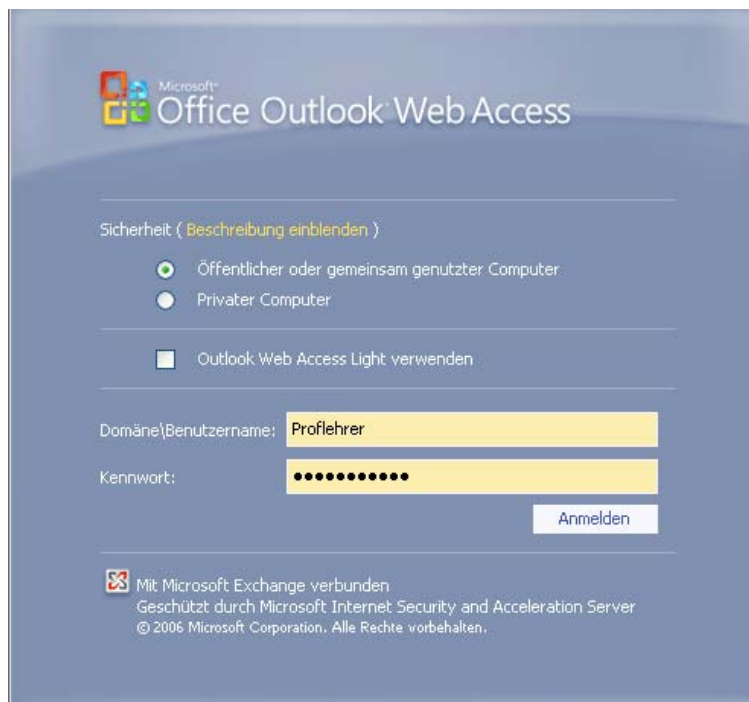
Öffnen Sie den Internet Explorer und geben als URL die externe IP-Adresse oder den DYNDNS-Namen an. In diesem Beispiel wird ein DYNDNS-Name verwendet. Bei der Anbindung über BelWue steht dort aber die statische IP-Adresse.



Bestätigen Sie den Sicherheitshinweis mit *Ja*.



Sie bekommen ein Anmeldefenster, in dem Sie Ihre Benutzerdaten eingeben.



Danach sollten Sie die gleiche OWA Ansicht erhalten wie im lokalen Netzwerk.

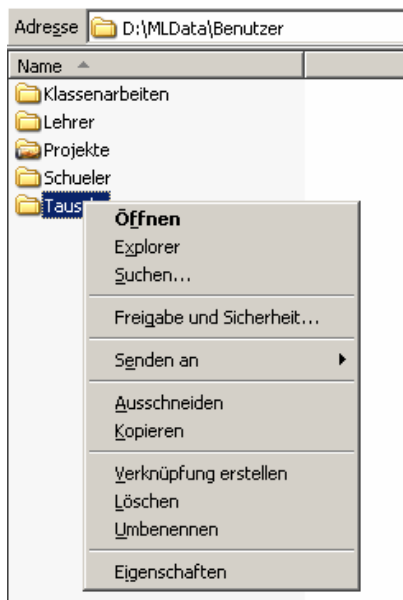
5. Zugriff auf Tausch- und Homeverzeichnisse

Auch von extern haben Sie die Möglichkeit über SSL eine sichere Verbindung zu Ihren Tausch- und Homeverzeichnissen herzustellen. Dazu sind zunächst Webfreigaben zu erstellen. In diesem Kapitel wird an einem Beispiel gezeigt, wie man für Lehrer den externen Zugriff auf folgende Verzeichnisse ermöglicht.

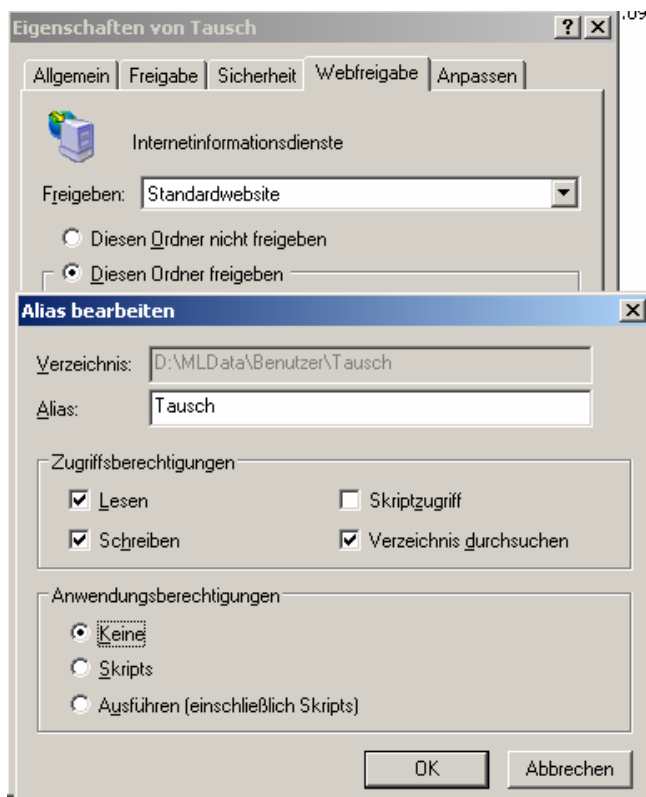
Verzeichnis	Webfreigabe
D:\MLData\Benutzer\Tausch	Tausch
D:\MLData\Benutzer\Lehrer	Lehrer
D:\MLData\Benutzer\Projekte	Projekte

5.1. Einrichten von Webfreigaben

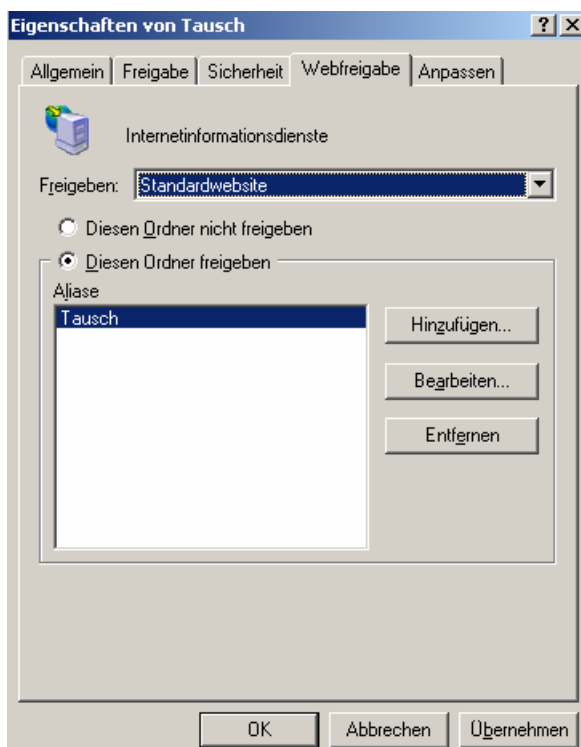
Gehen Sie nach D:\MLData\Benutzer und klicken mit der rechten Maustaste auf den Ordner *Tausch*. Wählen Sie *Eigenschaften* aus.



Rufen Sie die Registerkarte *Webfreigabe* auf und aktivieren *Diesen Ordner freigeben*. Konfigurieren Sie das Fenster *Alias bearbeiten* wie abgebildet und bestätigen mit *OK*.



Schließen Sie den Vorgang mit *OK* ab.



Wiederholen Sie analog zum Ordner *Tausch* die Webfreigabe der Verzeichnisse *Lehrer* und *Projekte*.

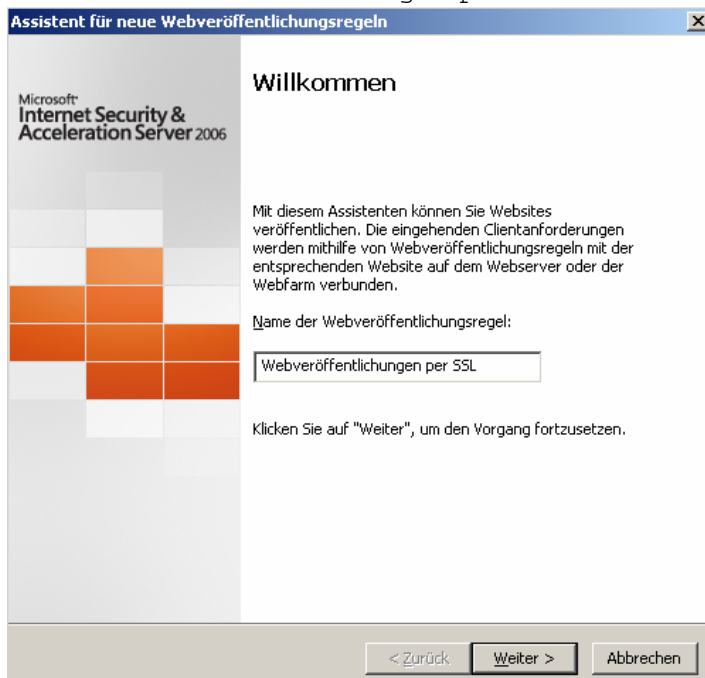
5.2. Veröffentlichen der Webfreigaben

Jetzt sind die Webfreigaben für den externen Zugriff im ISA Server freizugeben.

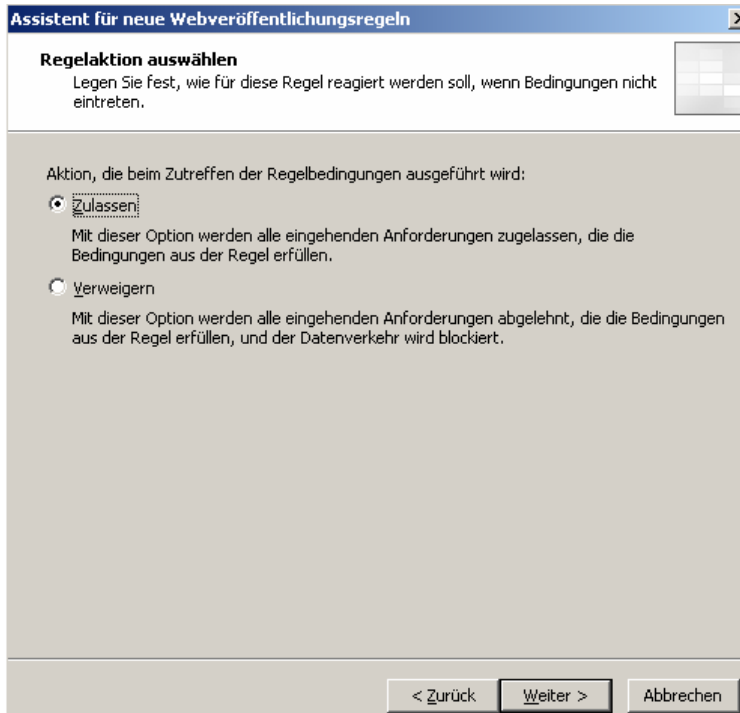
Starten Sie die ISA-Verwaltungstools und markieren Sie die *Standardregel* im mittleren Fenster. Klicken Sie im rechten Fenster in der Registerkarte *Aufgaben* auf *Websites veröffentlichen*.



Geben Sie Webveröffentlichungen per SSL ein, und klicken auf *Weiter*.



Wählen Sie *Zulassen* aus.



Assistent für neue Webveröffentlichungsregeln [X]

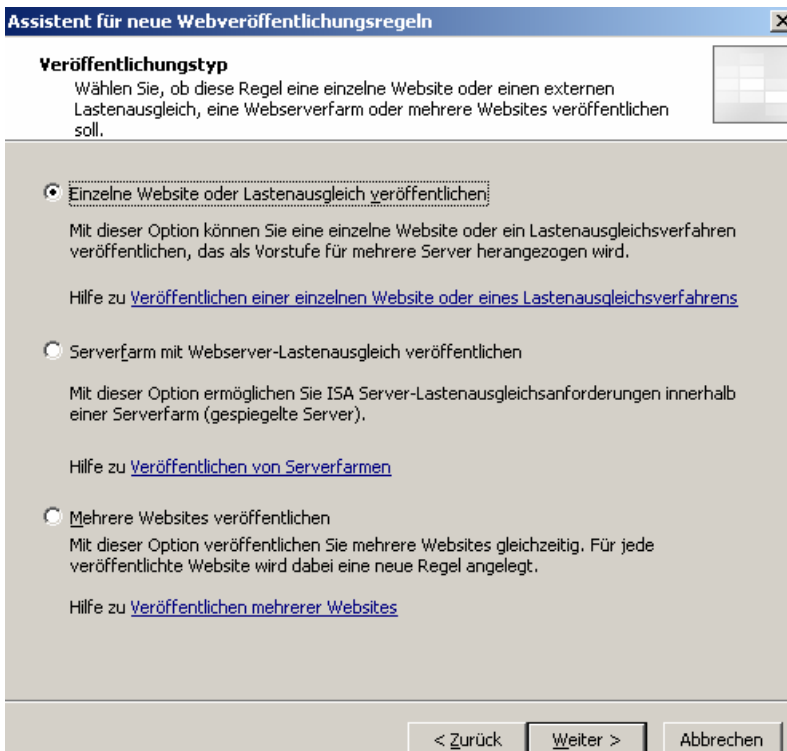
Regelaktion auswählen
Legen Sie fest, wie für diese Regel reagiert werden soll, wenn Bedingungen nicht eintreten.

Aktion, die beim Zutreffen der Regelbedingungen ausgeführt wird:

- Zulassen**
Mit dieser Option werden alle eingehenden Anforderungen zugelassen, die die Bedingungen aus der Regel erfüllen.
- Verweigern**
Mit dieser Option werden alle eingehenden Anforderungen abgelehnt, die die Bedingungen aus der Regel erfüllen, und der Datenverkehr wird blockiert.

< Zurück Weiter > Abbrechen

Einstellungen unverändert lassen und mit *Weiter* bestätigen.



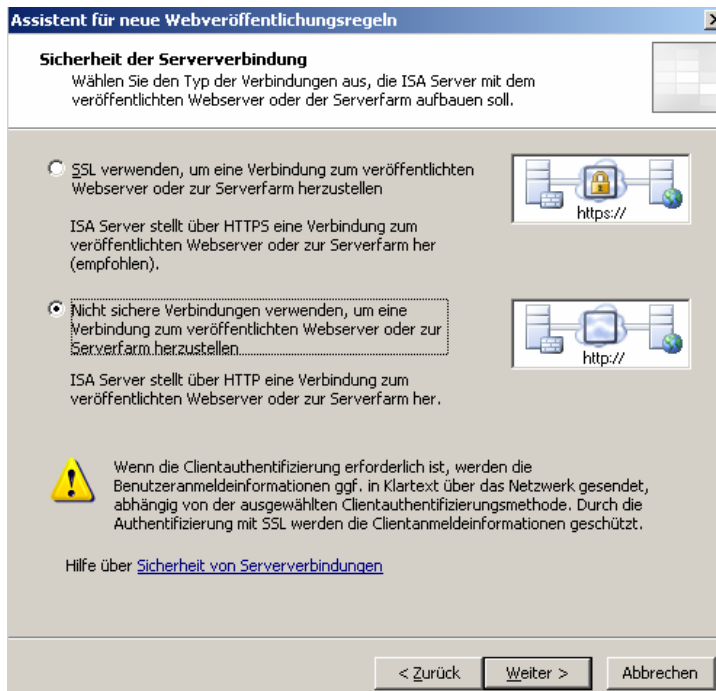
Assistent für neue Webveröffentlichungsregeln [X]

Veröffentlichungstyp
Wählen Sie, ob diese Regel eine einzelne Website oder einen externen Lastenausgleich, eine Webserverfarm oder mehrere Websites veröffentlichen soll.

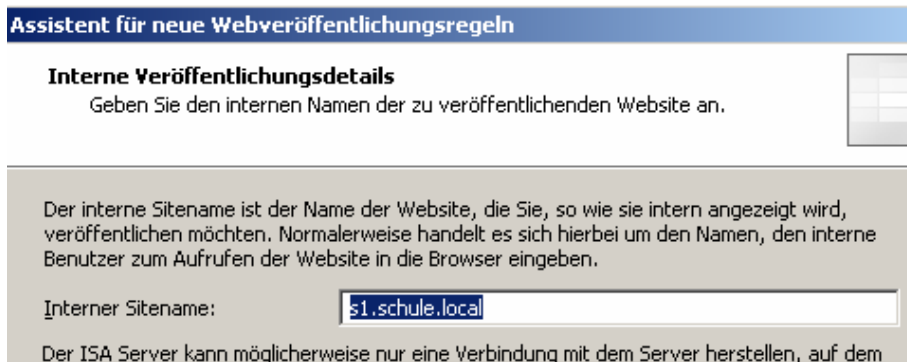
- Einzelne Website oder Lastenausgleich veröffentlichen**
Mit dieser Option können Sie eine einzelne Website oder ein Lastenausgleichsverfahren veröffentlichen, das als Vorstufe für mehrere Server herangezogen wird.
Hilfe zu [Veröffentlichen einer einzelnen Website oder eines Lastenausgleichsverfahrens](#)
- Serverfarm mit Webserver-Lastenausgleich veröffentlichen**
Mit dieser Option ermöglichen Sie ISA Server-Lastenausgleichsanforderungen innerhalb einer Serverfarm (gespiegelte Server).
Hilfe zu [Veröffentlichen von Serverfarmen](#)
- Mehrere Websites veröffentlichen**
Mit dieser Option veröffentlichen Sie mehrere Websites gleichzeitig. Für jede veröffentlichte Website wird dabei eine neue Regel angelegt.
Hilfe zu [Veröffentlichen mehrerer Websites](#)

< Zurück Weiter > Abbrechen

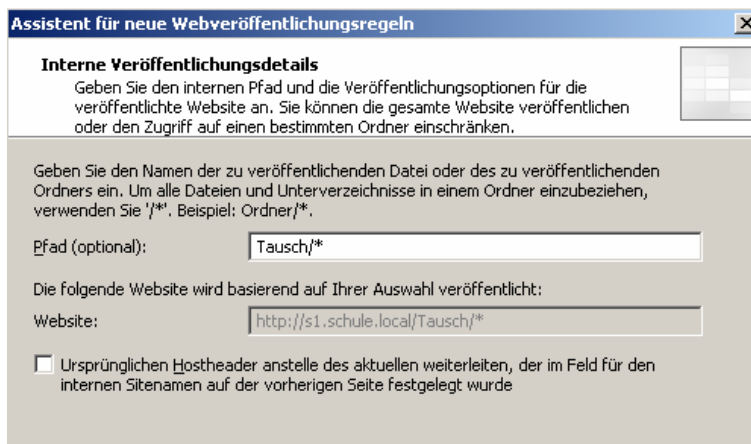
Aktivieren Sie die Optionen wie abgebildet und bestätigen mit *Weiter*.



Geben Sie `s1.schule.local` ein und klicken auf *Weiter*.



Geben Sie `Tausch/*` ein und klicken *Weiter*.



Geben Sie die externe IP-Adresse oder den DYNDNS-Namen ein. Mit *Weiter* bestätigen.

Assistent für neue Webveröffentlichungsregeln

Details des öffentlichen Namens
Geben Sie den öffentlichen Domännennamen (FQDN) oder die IP-Adresse an, die Benutzer eingeben sollen, um die veröffentlichte Site zu erreichen.

Anforderungen annehmen für:

Nur Anforderungen für diesen öffentlichen Namen oder diese IP-Adresse werden an die veröffentlichte Site weitergeleitet.

Öffentlicher Name:
Beispiel: www.contoso.com

Pfad (optional):

Auf Grundlage Ihrer Auswahl werden Anforderungen akzeptiert, die an diese Site (Hostheaderwert) gesendet werden:

Standort:

Wählen Sie den bereits vorhandenen Weblistener *SSL auf HBS.dyndns.org* aus und klicken auf *Weiter*.

Assistent für neue Webveröffentlichungsregeln

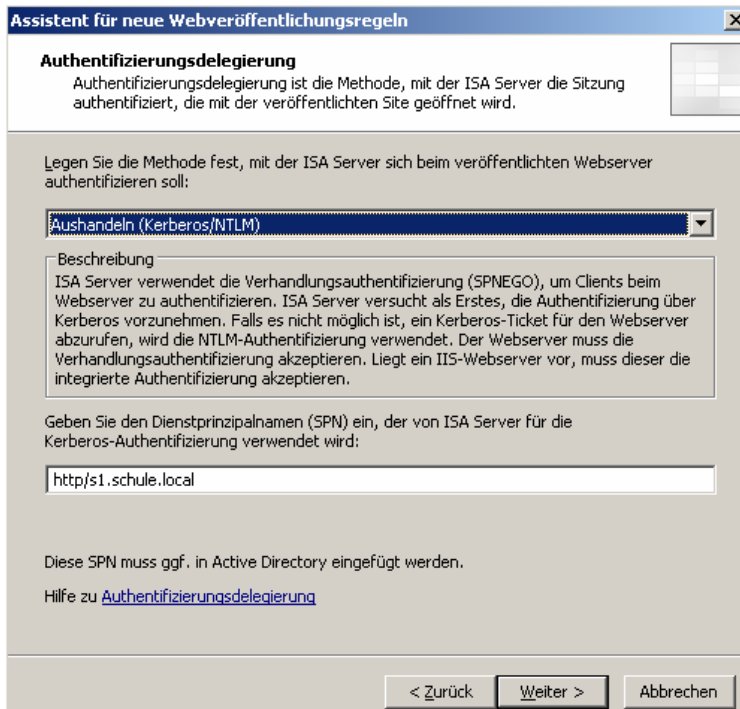
Weblistener auswählen
Der Weblistener bestimmt die IP-Adressen und den Port, auf dem der ISA Server-Computer auf eingehende Webanforderungen abhört.

Weblistener:

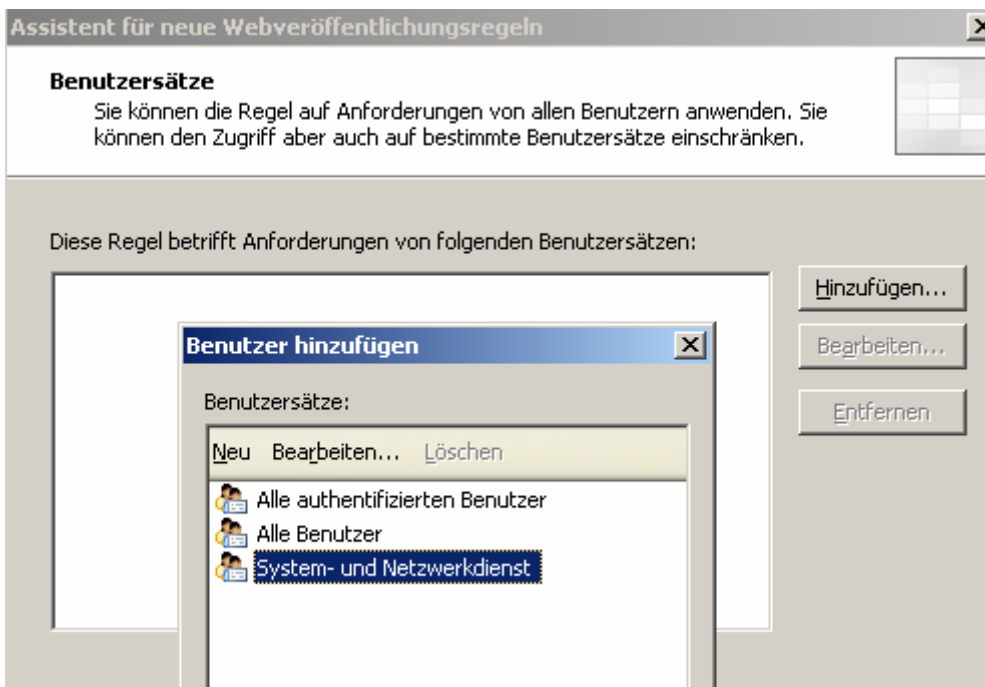
Listeneigenschaften:

Eigenschaft	Wert
Beschreibung	
Netzwerke	Extern
Port(HTTP)	Deaktiviert
Port(HTTPS)	443

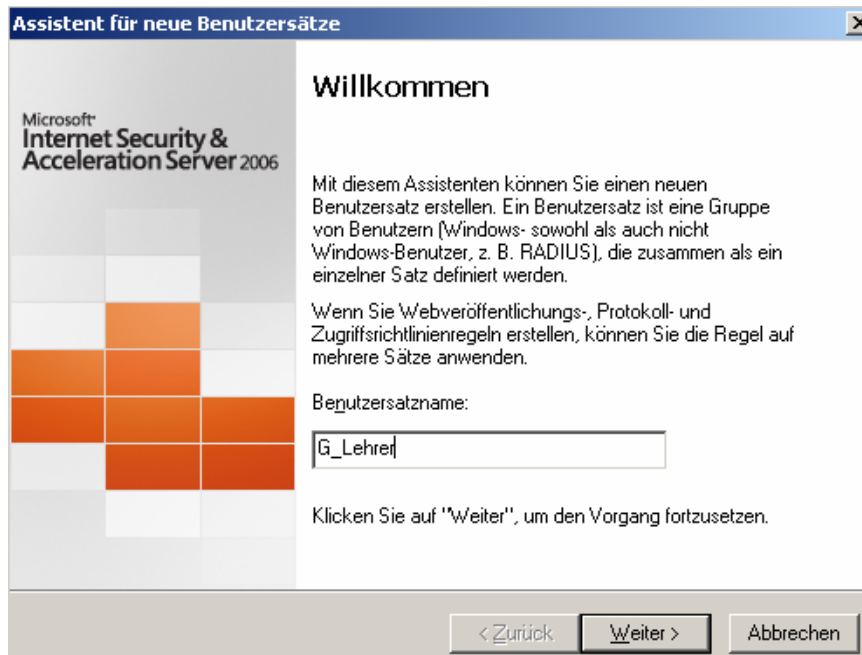
Wählen Sie *Aushandeln(Kerberos/NTLM)* aus und klicken auf *Weiter*.



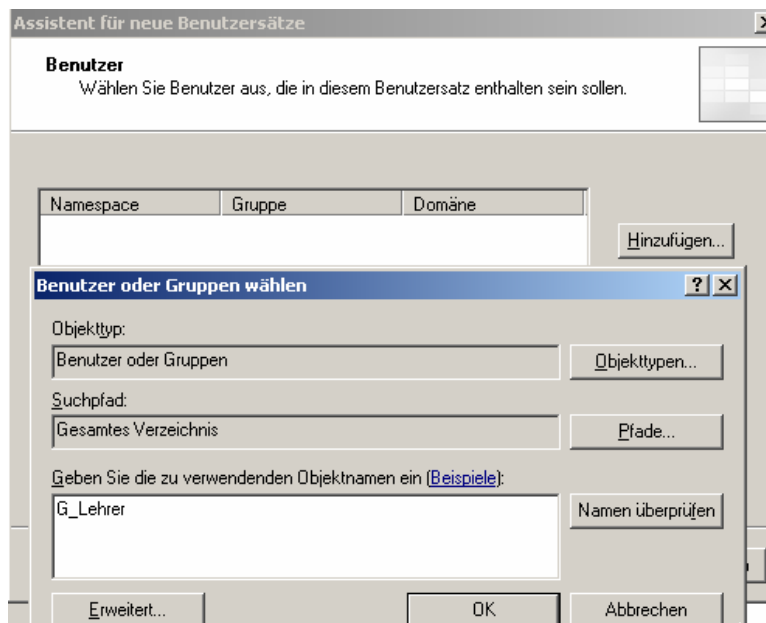
Entfernen Sie *Alle authentifizierten Benutzer* und klicken auf *Hinzufügen*. Im Fenster *Benutzer hinzufügen* klicken Sie auf *Neu*.



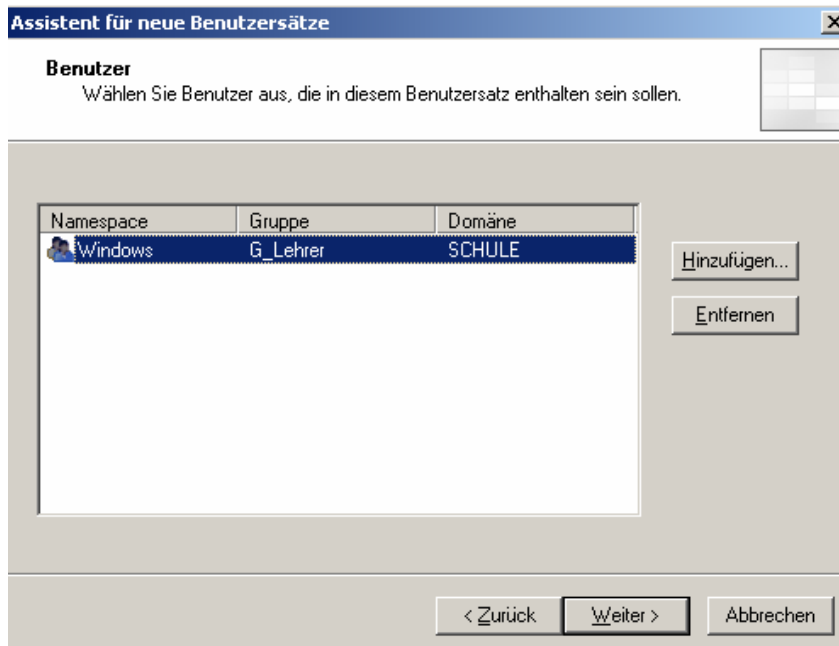
Geben Sie `G_Lehrer` ein und klicken auf *Weiter*.



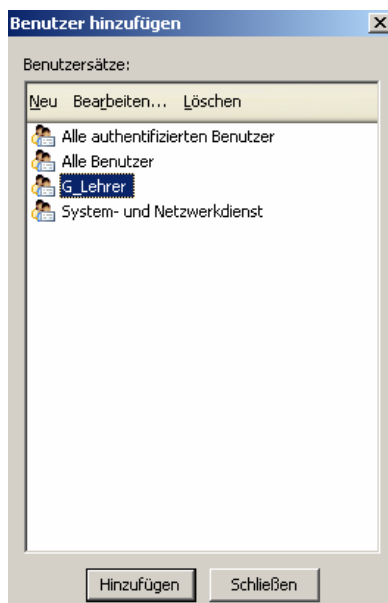
Klicken Sie auf *Hinzufügen...* und geben im Fenster *Benutzer oder Gruppen wählen* `G_Lehrer` ein. Bestätigen Sie mit *OK*.



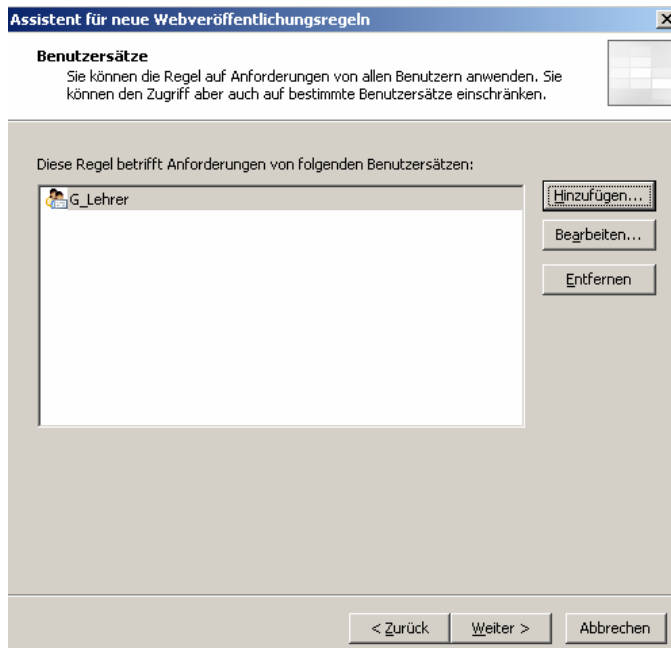
Klicken Sie auf *Weiter* und schließen den Assistenten mit *Fertig stellen* ab.



Markieren Sie *G_Lehrer* und bestätigen mit *Hinzufügen*. *Schließen* Sie das Fenster.



Klicken Sie auf *Weiter*.

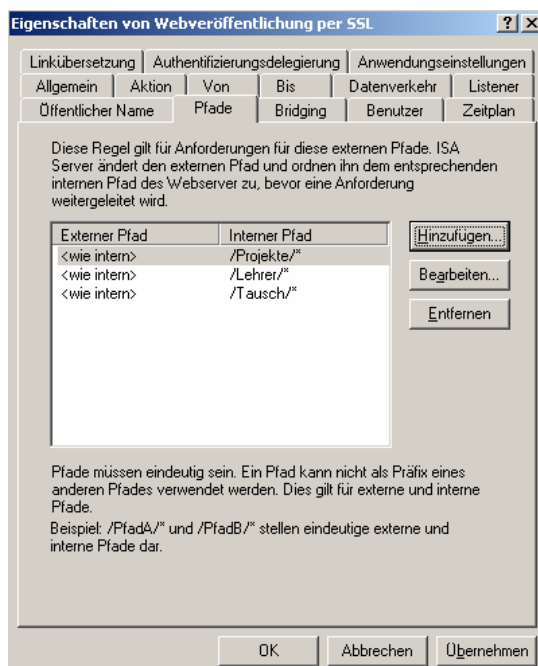


Schließen Sie den Regel Assistenten mit *Fertig stellen* ab.

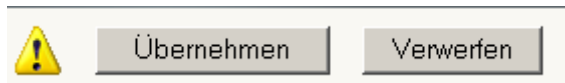
Öffnen Sie die neu erstellte Regel mit einem Doppelklick.



Wählen Sie die Registerkarte *Pfade* aus und tragen über *Hinzufügen...* die Webfreigaben */Lehrer/** und */Projekte/** ein. Klicken Sie auf *OK*.

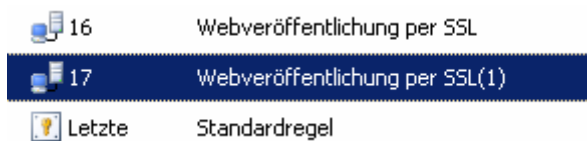


Jetzt muss nur noch die Regel mit *Übernehmen* aktiviert werden.

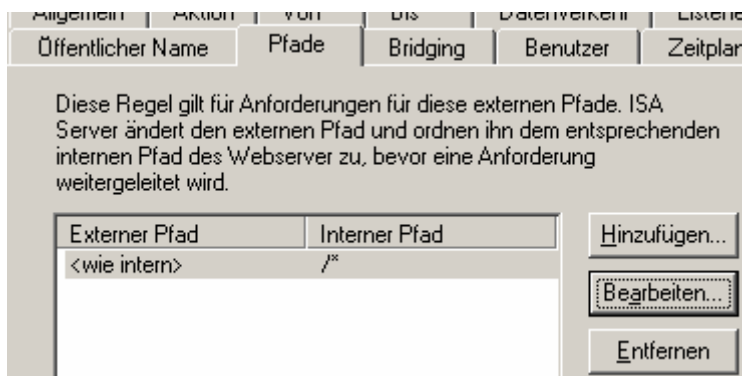


Durch einen Fehler im WebDav-Client von Windows XP muss man sich später bei der Verwendung der Freigabe häufiger authentifizieren als notwendig. Durch einen Trick kann man dieses Problem umgehen.

Kopieren Sie die neue Regel *Webveröffentlichung per SSL* und fügen diese als letzte Regel vor der *Standardregel* wieder ein.



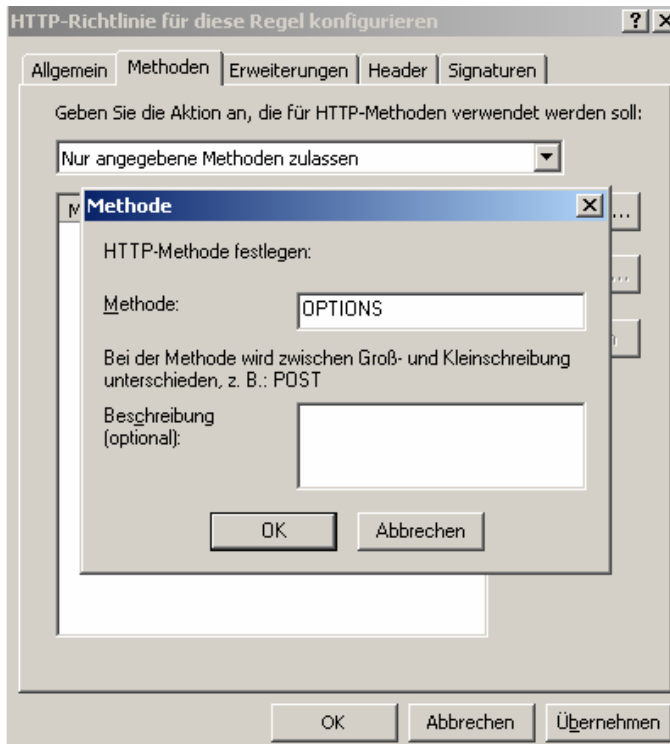
Mit einem Doppelklick auf die kopierte Regel werden die *Eigenschaften* angezeigt. Wechseln Sie in die Registerkarte *Allgemein* und geben als Regelnamen *WebDav Fehlerbehebung* ein. Unter *Pfade* werden alle Einträge gelöscht und nur */** hinzugefügt. Klicken Sie auf *OK*, so dass die Eigenschaften geschlossen werden.



Klicken Sie mit der rechten Maustaste auf die Regel *WebDav Fehlerbehebung* und wählen *HTTP konfigurieren* aus.



Wechseln Sie auf die Registerkarte Methoden, und stellen Sie auf *Nur angegebene Methoden zulassen* um. Klicken Sie auf *Hinzufügen* und tragen Sie die Methode *OPTIONS* (Großschreibung wichtig!) ein.



Klicken Sie zweimal auf *OK*, um die Fenster zu schließen.

Klicken im ISA Server auf *Übernehmen*.

5.3. Veröffentlichung der Schulkonsole

Auch die Schulkonsole kann für den externen Zugriff konfiguriert werden. Dazu kopieren Sie erneut die Regel *Webveröffentlichung per SSL* und fügen diese wieder vor der Regel *WebDav Fehlerbehebung* ein.

Ändern Sie den Namen in *Webveröffentlichung Schulkonsole* und geben unter *Pfade* *Schulkonsole/** ein.

Vergessen Sie nicht, die Regel mit *Übernehmen* zu aktivieren.

Hinweis: Mit dieser Regel können jetzt nur *G_Lehrer* auf die Schulkonsole zugreifen. Sie können natürlich noch eine Gruppe für Administratoren anlegen und diese hinzufügen.

6. Quellen und weiterführende Links

Dieses Dokument beruht auf den Fortbildungsunterlagen zum Fernzugriff auf das Musterlösungsnetzwerk, <http://lehrerfortbildung-bw.de/netz/muster/win2000/material/remote/remote06.pdf>.

Darin enthalten sind weitere Hinweise, z.B. Konfiguration der Clients.

Unter <http://www.microsoft.com/technet/downloads/isa/2006/trials/default.mspx> kann man eine Evaluationsversion (gültig für 180 Tage) des ISA 2006 herunterladen.

Das Buch **Microsoft ISA Server 2006 - Das Handbuch.** von [Marc Grote](#), [Christian Gröbner](#) und [Dieter Rauscher](#) enthält sehr viel Wissenswertes zum ISA 2006 Server.