

Ergänzungen zur Handreichung Windows 2000 – Netzwerkverwaltung in der Schule

Eine Handreichung ist nie ganz fertig. Kaum gedruckt, kommen neue Aspekte hinzu, werden Fehler entdeckt und manche Dinge unter anderen Gesichtspunkten betrachtet.

Insbesondere ist seit dem Erscheinen der Handreichung „Windows 2000 – Netzwerkverwaltung in der Schule“ die sogenannte „Musterlösung Windows 2000“ fertiggestellt worden. Sie soll das Leben der Netzwerkverwalterinnen und –verwalter leichter machen und eine einheitliche Supportstruktur ermöglichen..

Andererseits erscheint die Trennung von Domain-Controller und Kommunikationsserver unter Sicherheitsaspekten als empfehlenswert. Dies sieht die Musterlösung aber momentan nicht vor.

Beides unter einen Hut zu bringen, und die erforderlichen Modifikationen zu beschreiben, das ist der Sinn dieser Ergänzungsblätter.

Außerdem beinhalten diese Ergänzungsblätter noch nützliche Graphiken und eine Lösung für das Problem des Abgleichs der Zeit im Netzwerk mit der „gesetzlichen“ Zeit.

Viel Erfolg bei der Arbeit mit diesen Blättern!

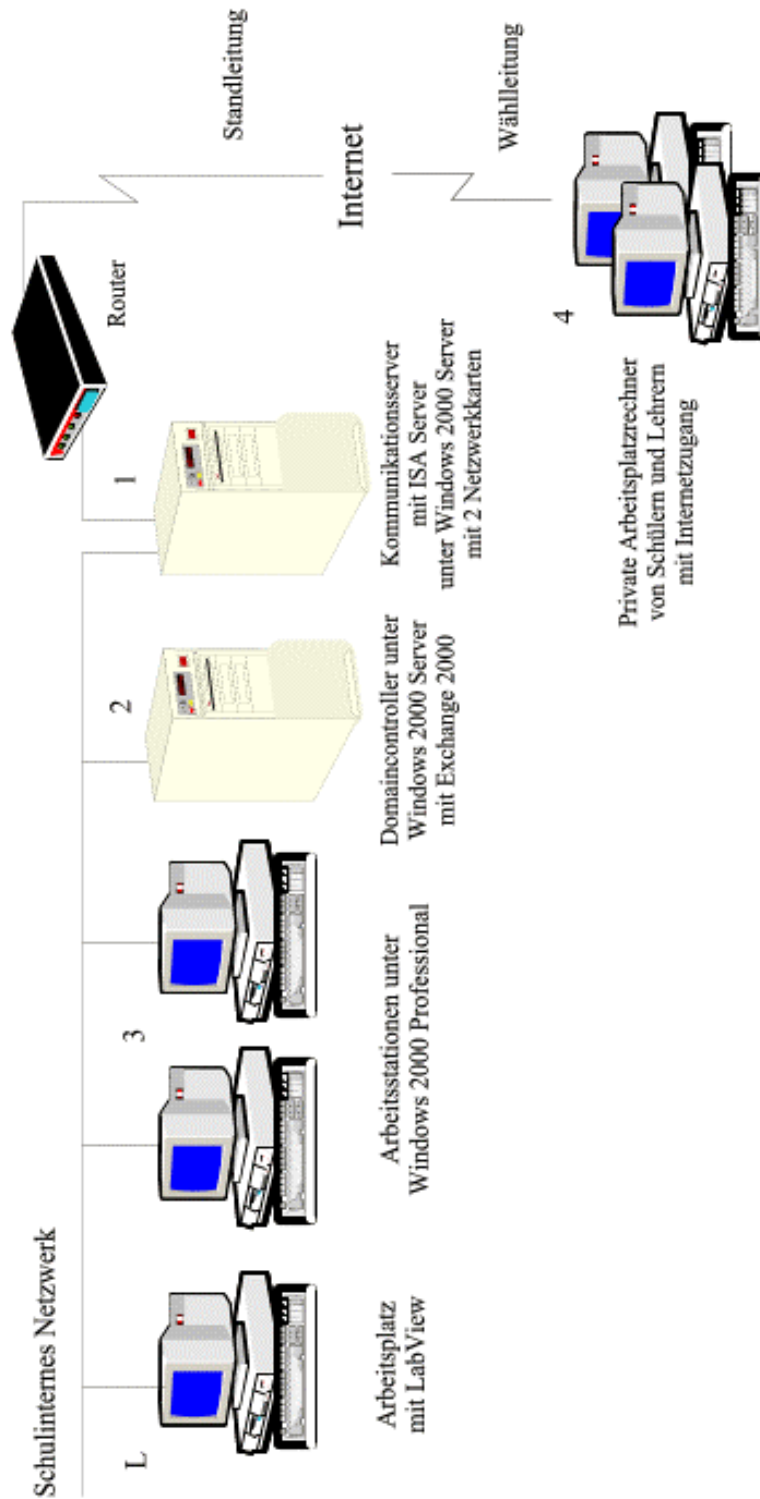
Rudolf Arnold

11. November 2002

Übersicht:

	Inhalt	Seite
E.1	Struktur der Internetanbindung des Schulnetzes	E - 2
E.2	Modifikation der Musterlösung für die Trennung zwischen Domain-Controller und Kommunikationsserver	E - 3
E.3	Der Weg einer E-Mail	E - 6
E.4	Struktur des ISA Server 2000	E - 7
E.5	Veröffentlichen des Exchange 2000 Servers bei der Zwei-Server-Lösung	E - 8
E.6	Synchronisation mit externen Zeitservern	E - 16

E.1 Struktur der Internetanbindung des Schulnetzes



E.2 Modifikation der Musterlösung für die Trennung zwischen Domain-Controller und Kommunikationsserver

Die Musterlösung für Windows 2000 sieht in der Originalfassung vor, dass sich neben Windows 2000 Server und Exchange 2000 Server auch der ISA Server 2000 auf dem selben Rechner befindet.

Möchte man den ISA Server 2000, so wie es auch von Microsoft und der Online-Arbeitsgruppe empfohlen wird, auf einer separaten Maschine betreiben, so sind einige Modifikationen an den Installationsdisketten der Musterlösung vorzunehmen.

E.2.1 Erstellung der Installationsdisketten

Erstellen Sie die Installationsdisketten wie in der Anleitung zur Musterlösung beschrieben. An dieser Stelle sind also noch keine Modifikationen nötig.

E.2.2 Modifikationen an den Installationskripten für den Server

Die Installationskripte für den Server befinden sich auf **Diskette 1** im Unterverzeichnis **\SInst**. Bei fortgeschrittener Installation wird der Server automatisch wiederholt neu gestartet. Bei jedem Neustart werden Skripte automatisch über Autostart aufgerufen. Vor einem neuen Start wird das alte Skript automatisch gelöscht und das nächste Skript wird von der Diskette in den Autostart-Ordner kopiert.

Die Anweisungen für die Installation des ISA Server 2000 befinden sich im Skript **inst5.cmd**. Es genügt, die entsprechenden Zeilen mit dem Hochkommazeichen (‘) zu versehen, um sie als Kommentar zu kennzeichnen und damit unwirksam zu machen:

```
start /b /wait netsh dhcp server initiate auth
    copy c:\Temp\Sinst\msisaund.ini c:\
    ' ISA Server installieren oder nicht
    ' start /wait c:\temp\Sinst\isa2k.vbs
del c:\msisaund.ini
start /b /wait netsh dhcp server initiate auth
start /wait c:\Temp\Sinst\iadstools.vbs
start /wait c:\Temp\Sinst\ris.vbs
copy c:\Temp\SInst\gpo.vbs "c:\dokumente und
Einstellungen\Administrator\Startmenü\programme\autostart"
    ' ISA Server Service Pack installieren oder nicht
    ' start /wait c:\temp\Sinst\isaspl.vbs
    ' Das ISA Servicepack macht automatisch einen Neustart
    start /wait c:\temp\Sinst\neustart.vbs
```

Am Ende muss allerdings die normalerweise deaktivierte letzte Zeile durch Entfernen des Hochkommazeichens aktiviert werden, da ja kein Servicepack für den ISA Server installiert wurde, also auch kein automatischer Neustart erfolgt.

Die Fehlermeldungen, die bei der späteren automatischen Überprüfung der Serverinstallation erscheinen und sich auf den ISA Server beziehen, können ignoriert werden.

E.2.3 Modifikation des Benutzeranmeldeskripts

Alle Benutzer, die mit den Tools der Musterlösung angelegt werden, arbeiten bei der Anmeldung ein einheitliches Benutzeranmeldeskript ab. Dieses befindet sich zunächst auf der **Diskette 1** im Verzeichnis **\SInst** und heißt **Benutzer.vbs**.

Achtung:

Hier sind nur Modifikationen nötig, wenn mehr als ein Domain-Controller benutzt wird, also nur bei größeren Strukturen. Die beschriebene Modifikation hat nichts mit der Abtrennung des ISA Servers zu tun!

Beschreibung:

Im Benutzeranmeldeskript wird die Variable **NTInfo.pdc** benutzt, um den Namen des Servers zu ermitteln, an dem sich der Benutzer angemeldet hat. Dies kann bei mehreren Domain-Controllern jedes mal ein anderer Server sein. Deshalb kommt es z.B. bei der Verbindung von Netzwerk-Laufwerken häufig zu Fehlern. Man muss das Skript also durch Einfügen von Kommentarzeichen und einer neuen Zeile so abändern, dass bei der Verbindung der Netzwerk-Laufwerke der Server angesprochen wird, auf dem die entsprechenden Freigaben liegen. Das ist im vorliegenden Beispiel **\\VDC1**.

Da das Skript sehr lang ist, wird hier nur der entsprechende Ausschnitt wiedergegeben:

```
'-----
'Bereitstellen der Netzlaufwerke
'-----

'logonserver = "\\\" & NTInfo.pdc <<<Voreinstellung laut
Musterloesung <<< deaktiviert von Rudolf Arnold 08.08.2002
' <<< Neue Zeile eingefuegt von Rudolf Arnold 08.08.2002
logonserver = "\\vdc1"

WshNet.MapNetworkDrive "h:", logonserver & "\" & username & "$"
WshNet.MapNetworkDrive "p:", logonserver & "\PGM$"

'--->>>fie<<< macht nur für Lehrer Sinn, siehe unten
'WshNet.MapNetworkDrive "t:", logonserver & "\T_Alle$"
```

Wie gesagt, sind diese Änderungen nur nötig, wenn mehrere Domain-Controller benutzt werden.

E.2.4 Modifikation der Clientinstallationsskripte

Bei der automatischen Installation und Konfiguration der Workstations über RIS wird auch der Firewall-Client installiert. Dazu wird eine Freigabe benutzt, die der ISA Server bei seiner Installation erstellt. In der vorliegenden Variante befindet sich der ISA Server aber nicht auf dem Domain-Controller, sondern auf einem separaten Server, hier **\\via5**.

Diese Tatsache muss im Clientinstallationskript berücksichtigt werden. Das Skript befindet sich auf **Diskette 1** im Verzeichnis **\Clnst** und heißt **InstCl.vbs**.

Da das Skript relativ lang ist, hier nur die relevanten Ausschnitte:

```
rem Lesen des Servernamens

const serverkey = "HKEY_LOCAL_MACHINE\Software\microsoft\Windows
NT\Currentversion\SourcePath"

rem servername=wshshell.regread(serverkey)

rem servername=left(servername, instr(3,servername,"\")-1)

servername="\\via5"
```

Die Anweisungen zur Bildung des Servernamens wurden hier durch Voranstellung von **rem** (remark) deaktiviert. Dann wurde der Name des ISA Servers (hier \\via5) über **servername =“via5“** direkt zugewiesen.

Da die Variable **servername** weiter unten nochmals benutzt wird, wurde die obige Änderung rückgängig gemacht, in dem der Name des Domain-Controllers (hier \\vdc1) zugewiesen wurde.

```
if not fso.folderexists("C:\Programme") then
    fso.createfolder("C:\Programme")
end if

servername="\\vdc1"

'if not fso.folderexists("C:\Programme\Internet") then
'    fso.createfolder("C:\Programme\Internet")
' end if

' pfad = servername &
"remInst\setup\german\images\win2000.pro\i386\Internet.exe"
' fso.copyfile pfad, "C:\Programme\Internet\"
' regpfad= "c:\Dokumente und Einstellungen\All Users\Desktop"
```

E.2.5 Weiteres Vorgehen

Nach der Modifikation der **Diskette 1** lässt man die Installation des Domain-Controllers wie in der Anleitung zur Musterlösung ablaufen. Eventuelle Fehlermeldungen in Bezug auf fehlende Dienste des ISA Servers können ignoriert werden.

Danach wird auf dem **Kommunikationsserver** Windows 2000 Server als „**Einzelner Server**“, also nicht als Domain-Controller installiert. Der Server wird wie eine Workstation in die Domäne eingebunden (er erscheint im AD des Domain-Controllers in der OU Computers). Dann werden nacheinander Windows 2000 Servicepack, ISA Server 2000 und ISA Server Servicepack installiert. Anschließend kann der ISA Server wie in der Handreichung bzw. in der Anleitung zur Musterlösung beschrieben, konfiguriert werden.

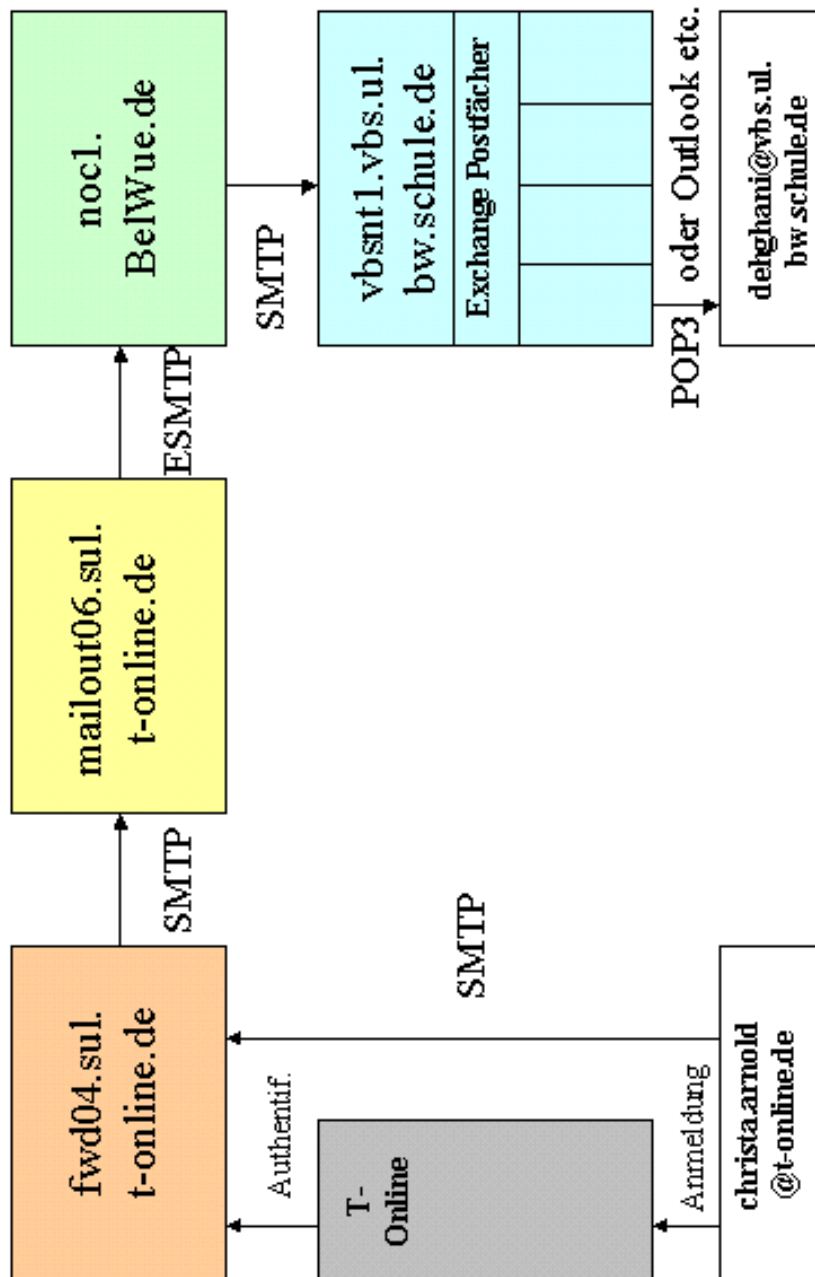
Erst dann kann mit der Installation der Workstations begonnen werden!

E.2.6 Modifikation von bsa.cmd in der Freigabe NETLOGON

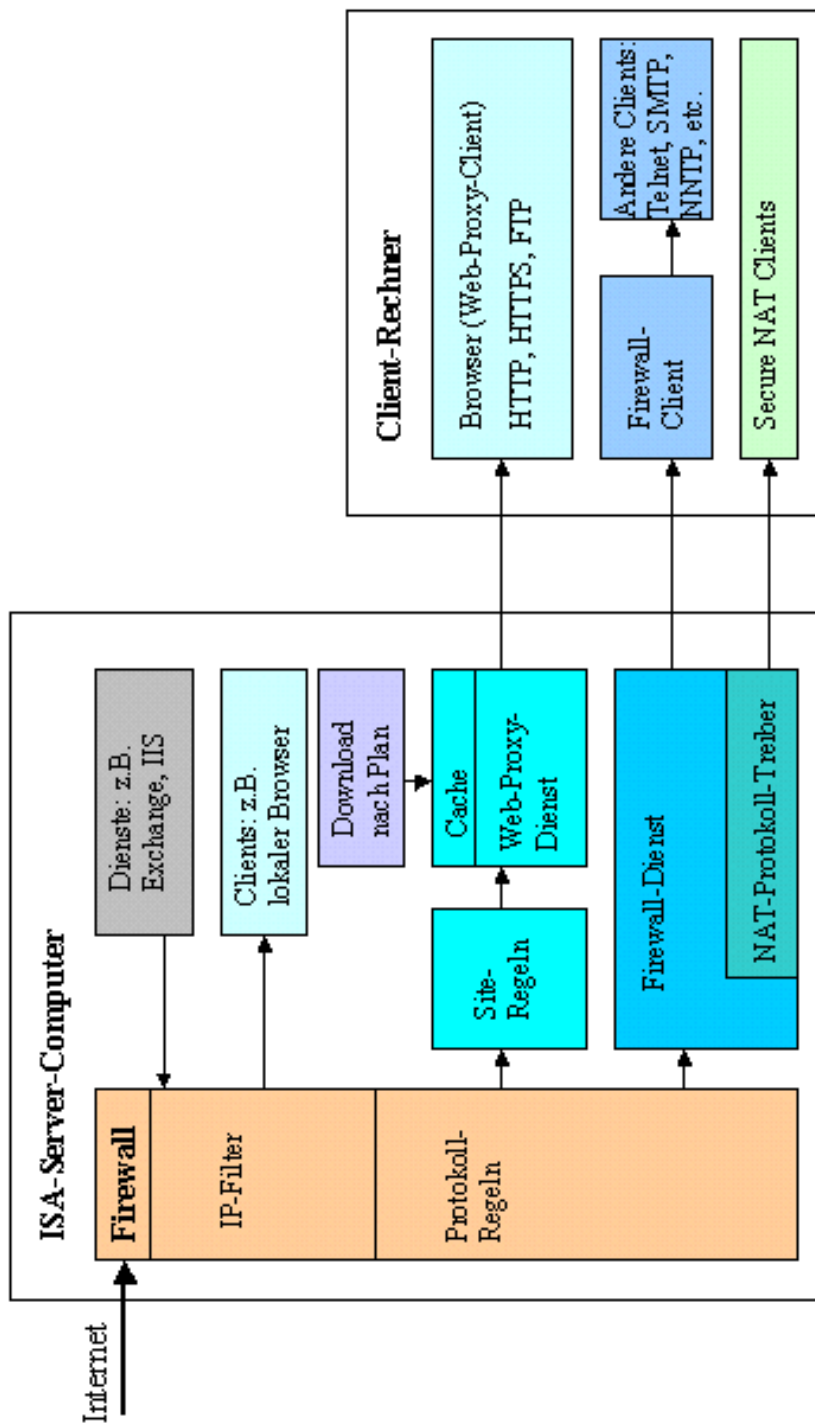
Bei mehreren Domain-Controllern muss in NETLOGON das Skript bsa.cmd nach folgendem Muster abgeändert werden:

```
\\vdc1\bsac$\bsac.exe `BSA-Module liegen auf vdc1
```

E.3 Der Weg einer E-Mail



E.4 Struktur des ISA Server 2000



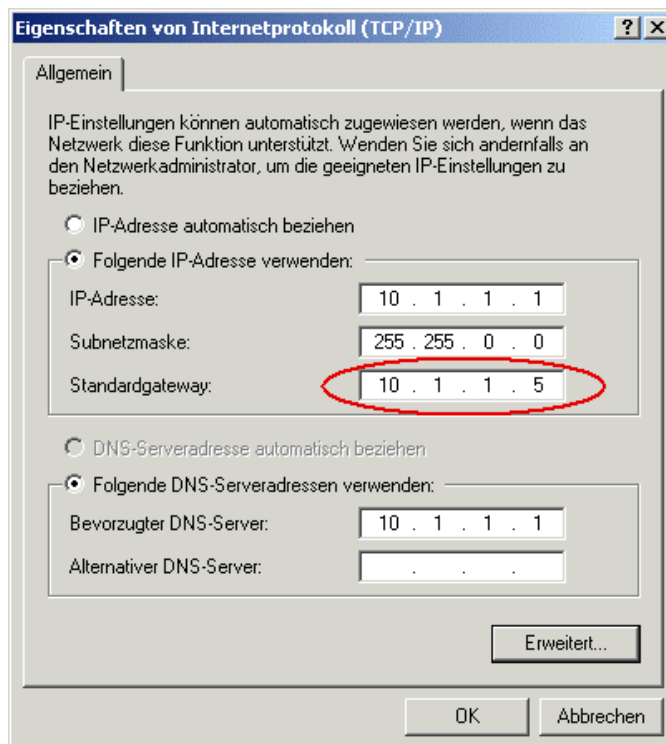
E.5 Veröffentlichen des Exchange 2000 Servers bei der Zwei-Server-Lösung

E.5.1 Konfiguration der Netzwerkkarte auf dem Exchange 2000 Server

Soll ein Dienst, der sich auf einem internen Server befindet, über ISA Server im Internet veröffentlicht werden, so muss dieser Server als so genannter „NAT-Client“ (Network Address Translation) gegenüber dem ISA-Server fungieren.

Auf dem **internen Server** muss dazu die Netzwerkkarte, die Verbindung zur internen Netzwerkkarte des ISA Server hat, nachkonfiguriert werden:

- Kontextmenü der Netzwerkumgebung - *Eigenschaften*
- Kontextmenü der Netzwerkkarte – *Eigenschaften*
- Im Fenster Eigenschaften den Punkt *Internetprotokoll (TCP/IP)* markieren und auf die Schaltfläche *Eigenschaften* klicken. Das Fenster Eigenschaften on Internetprotokoll (TCP/IP) öffnet sich:



- Unter *Standardgateway* die **IP-Adresse des ISA Servers** eintragen. (Dieses Feld ist normalerweise leer!)
- Mit OK bestätigen
- Alle Fenster wieder schließen

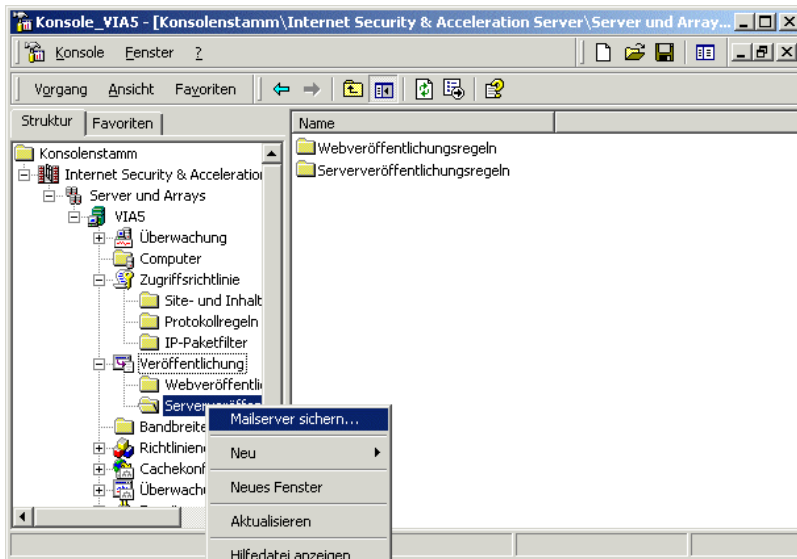
Achtung:

Auf einem Server, der als NAT-Client fungiert darf **kein Firewall-Client** installiert sein. Man sollte auf einem Server generell keinen Firewall-Client installieren!

E.5.2 Veröffentlichen des internen Mailservers auf dem ISA Server

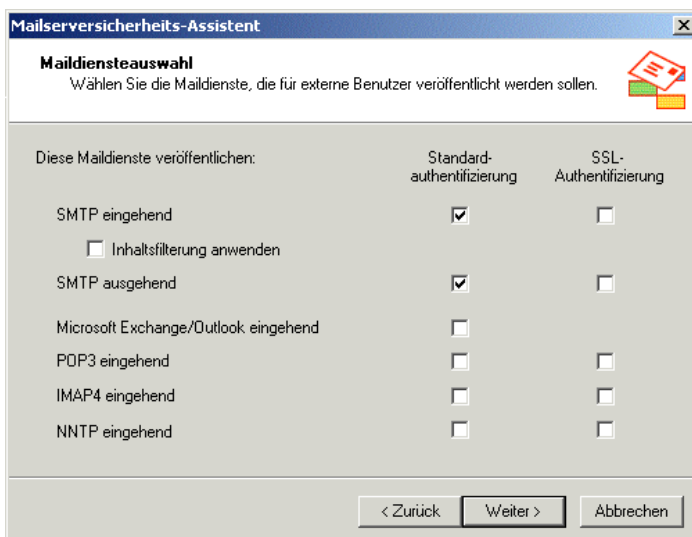
Da das Veröffentlichen eines Mailservers über normalerweise ein komplexe Angelegenheit ist, bietet ISA Server 2000 dafür einen speziellen Assistenten an.

Öffnen Sie dazu in der MMC des ISA-Servers das Kontextmenü von *Internet Security & Acceleration Server – Server und Arrays – Servername* (hier VIA5 ... an der Akademie K1...K7) – *Veröffentlichung – Serververöffentlichungsregeln* und wählen Sie den Punkt *Mailserver sichern...*

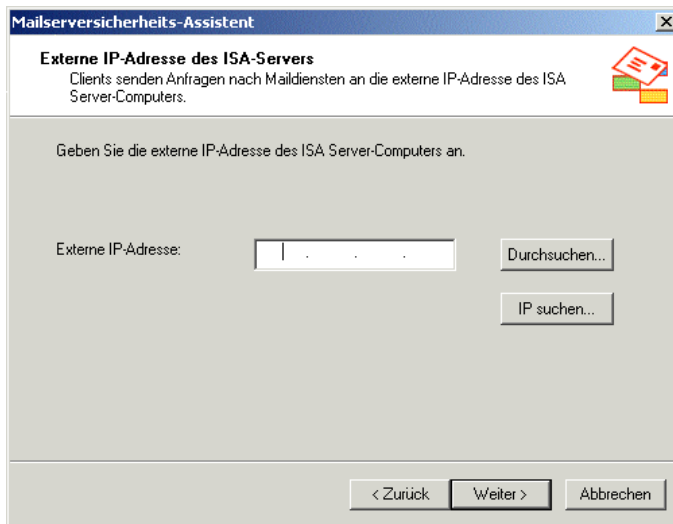


Der Mailserverversicherungs-Assistent startet und Sie klicken auf *Weiter*.

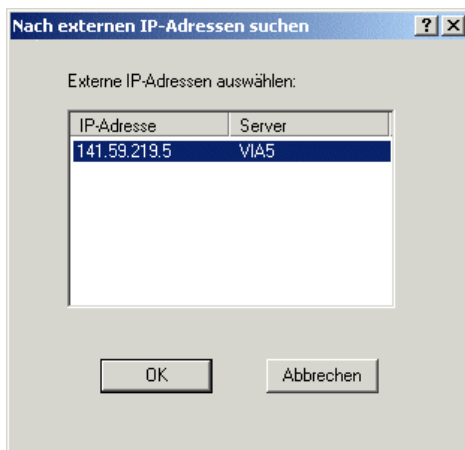
Unter *Maildienstauswahl* aktivieren Sie in der Spalte *Standardauthentifizierung* die Maildienste *SMTP eingehend* und *SMTP ausgehend*. Klicken Sie dann auf *Weiter*.



Jetzt werden Sie aufgefordert, die externe IP-Adresse des ISA Server-Computers anzugeben.

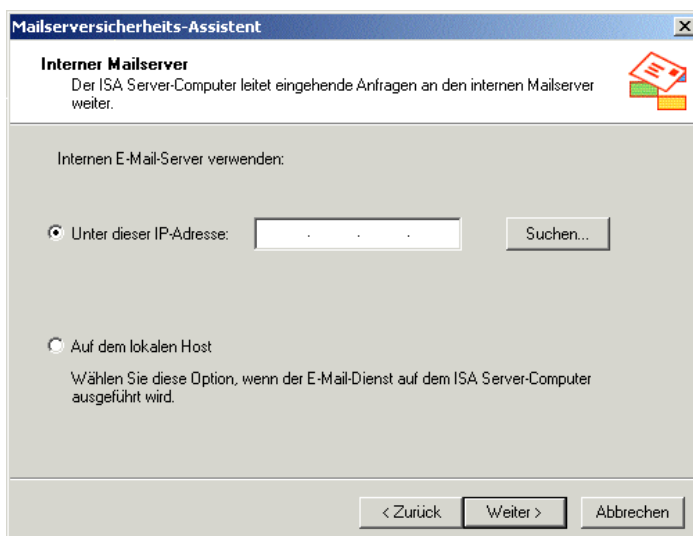


Klicken Sie auf *Durchsuchen* und wählen Sie im folgenden Fenster die externe IP-Adresse aus und klicken Sie auf *OK*.

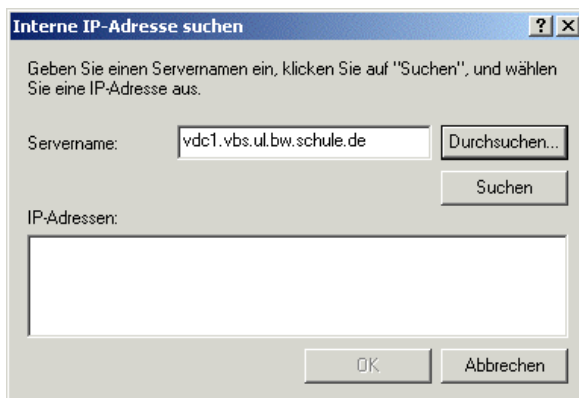


Dadurch wurde die externe IP-Adresse übernommen und Sie gelangen über *Weiter* zum Fenster, in dem Sie Informationen zum internen Mailserver angeben müssen.

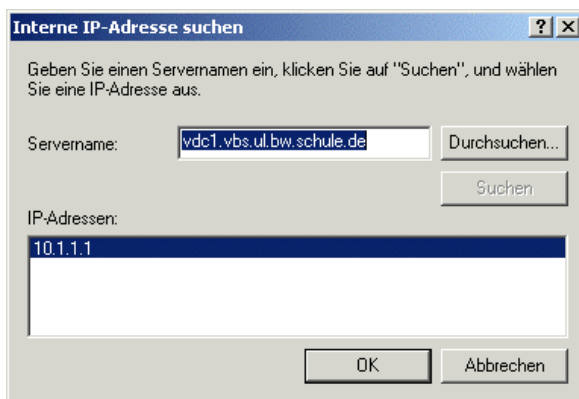
Beachten Sie, dass in dieser Variante (im Gegensatz zur Dokumentation in der Handreichung) der Mailserver nicht auf dem gleichen Computer wie der ISA-Server liegt. Man muss also den Punkt *Unter dieser IP-Adresse* aktivieren und auf *Suchen...* klicken



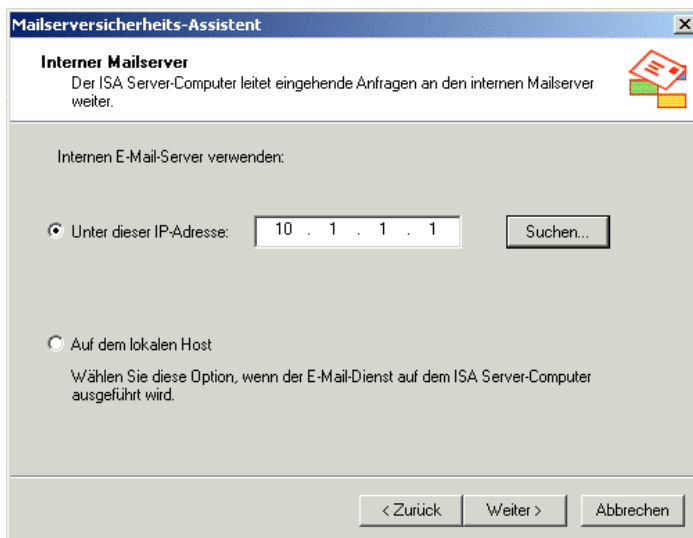
Dann unter *Servername*: den vollständigen Servernamen des internen Servers angeben, also z.B. `s1.dom1.es.bw.schule.de` und auf *Suchen* klicken.



Dann eine der angezeigten *IP-Adressen* (in der Regel ist es nur eine) *auswählen* und das Fenster mit *OK* verlassen



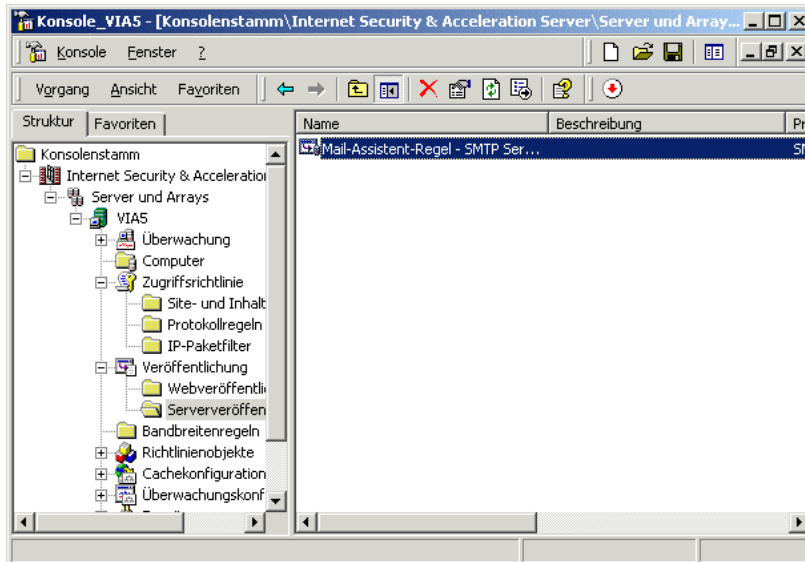
Die IP-Adresse des internen Servers wird dadurch im Fenster *Interner Mailserver* übernommen.



Auf *Weiter* klicken und schon ist man im Schlussfenster. Hier auf *Fertig stellen* klicken und man ist tatsächlich fertig!

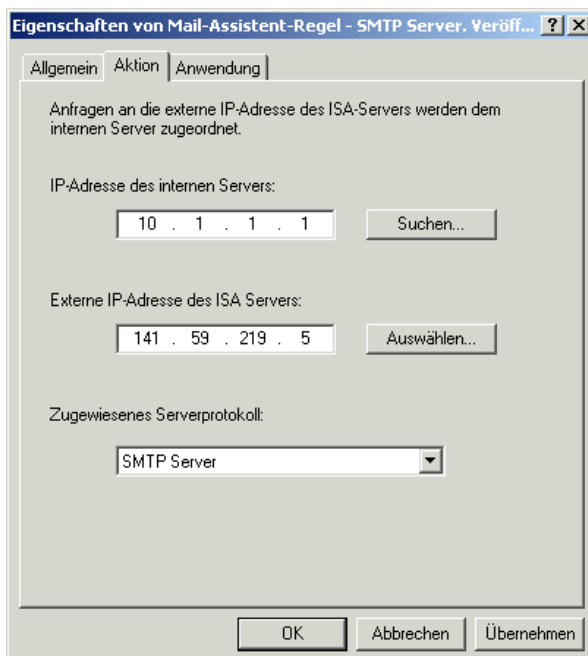
E.5.3 Regeln die bei der Mailserver-Veröffentlichung erstellt wurden

Wir wollen uns noch kurz ansehen, welche Regeln bei der Mailserver-Veröffentlichung erstellt wurden. Zuerst ist da *die Mail-Assistent-Regel für SMTP-Server*. Sie ist in der MMC unter *Security & Acceleration Server – Server und Arrays – Servername- Veröffentlichung – Serververöffentlichungsregeln* zu finden:

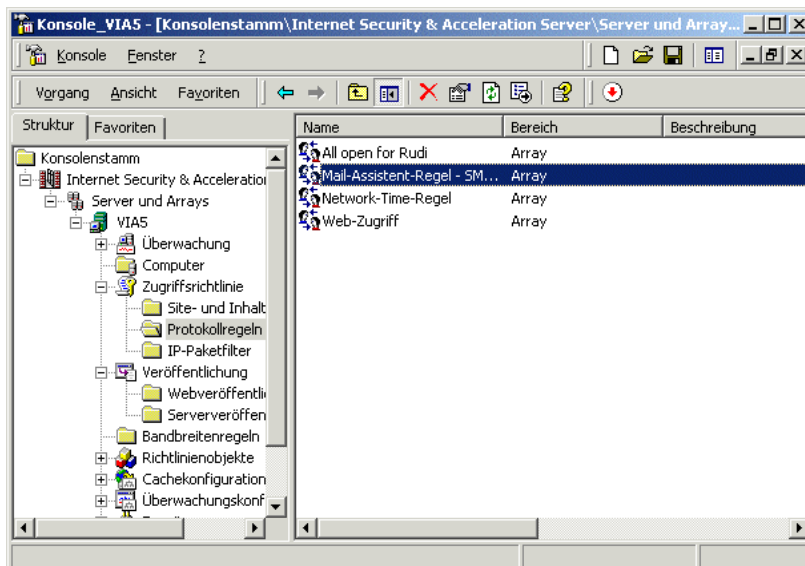


Serververöffentlichung bedeutet in diesem Zusammenhang, dass der interne SMTP-Server von Außen auf Port 25 sichtbar ist.

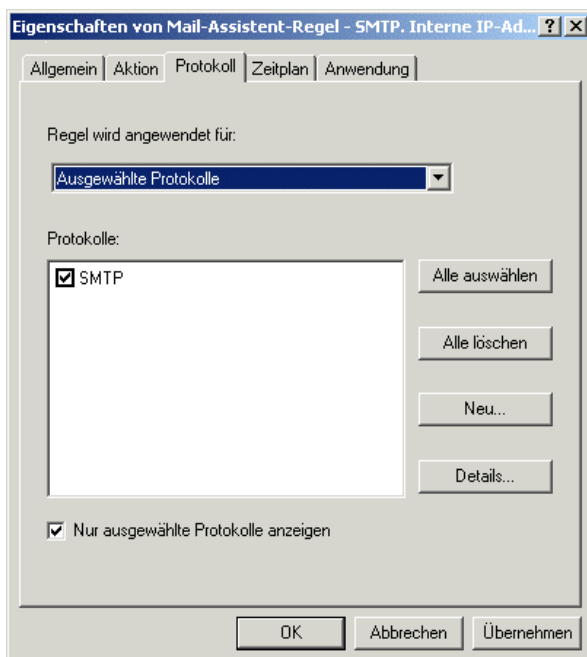
Ein Doppelklick auf die Regel öffnet das Eigenschaftfenster. Die wichtigen Einstellungen befinden sich im Register *Aktion*:



Natürlich muss auch eine Verbindung von Innen nach Außen existieren. Dies wird wie schon an anderer Stelle gezeigt, durch Protokollregeln festgelegt. Ein kleiner Blick auf *Security & Acceleration Server – Server und Arrays – Zugriffsrichtlinie – Protokollregeln* zeigt, dass dort eine neue Regel existiert, nämlich *Regel Mail-Assistent-Regel – SMTP interne IP...*



Interessant ist das Register Protokoll: Hier wird angezeigt, dass sich die Regel, des Protokolls SMTP bedient.



Ein Klick auf *Details* verrät der Fachfrau und dem Fachmann, dass *SMTP* auf *Port 25* unter *TCP* verwendet wird und dass die Richtung *Ausgehend* ist.

Protokolldefinitionsdetails

Name: SMTP

Beschreibung: Simple Mail Transfer-Protokoll (SMTP)

Portnummer: 25

Protokolltyp: TCP

Richtung: Ausgehend

Sekundäre Verbindungen:

Portbereich	Protokolltyp	Richtung
-------------	--------------	----------

OK

Das Register *Anwendung* zeigt eine weitere Besonderheit: Die obige Regel wird nämlich nicht für alle Anfragen verwendet, sondern nur für bestimmte Clients. Diese kann man in sogenannten **Clientadresssätzen** zusammenfassen.

Eigenschaften von Mail-Assistent-Regel - SMTP. Interne IP-Ad...

Allgemein | Aktion | Protokoll | Zeitplan | Anwendung

Regel wird angewendet für:

Alle Anfragen

Unten angegebene Clientadresssätze

Unten angegebene Benutzer und Gruppen

Gilt für Anfragen von:

Clientsätze

Mail-Assistent-Satz: 10.1.1.1

Hinzufügen...
Entfernen
Details...

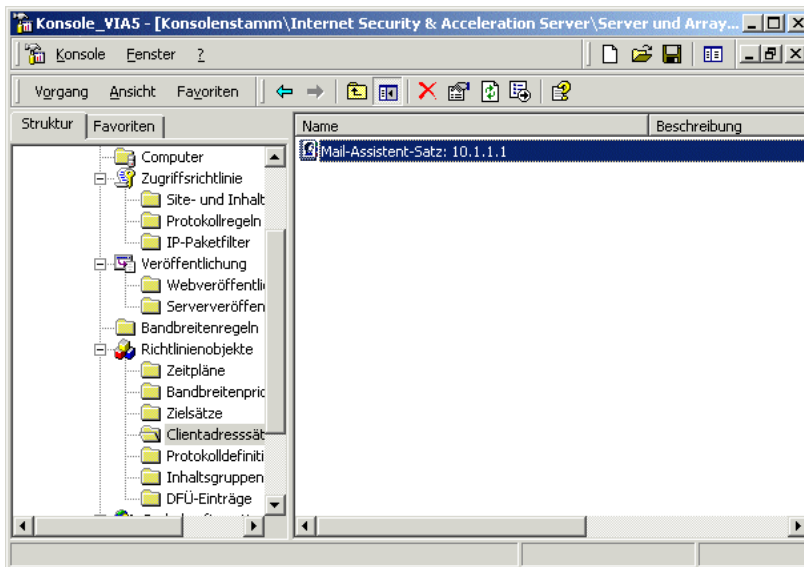
Ausnahmen:

Clientsätze

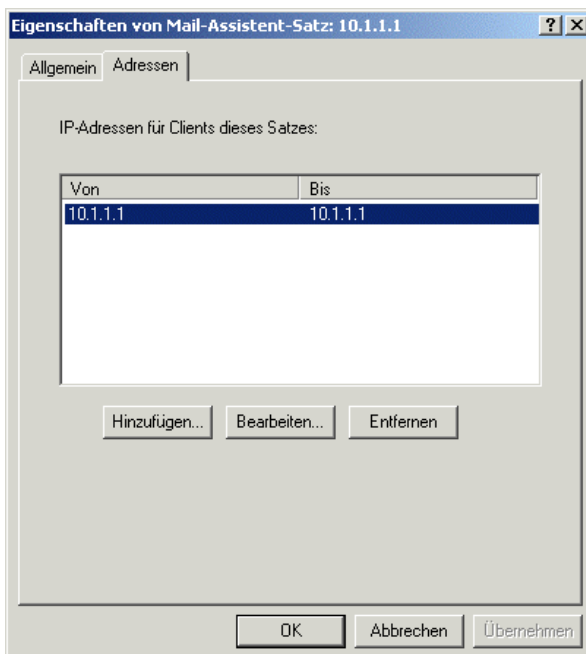
Hinzufügen...
Entfernen
Details...

OK Abbrechen Übernehmen

Clientadresssätze findet man in der MMC unter auf *Security & Acceleration Server – Server und Arrays – Servername – Richtlinienobjekte – Clientadresssätze*:



Ein Doppelklick öffnet das entsprechende Fenster und zeigt die IP-Adressen der Clients des betreffenden Satzes an. Hier sind Start- und Endadresse gleich, d.h. die obige Regel wird nur für einen Client angewandt. Und das ist, ganz klar, der interne Mailserver.

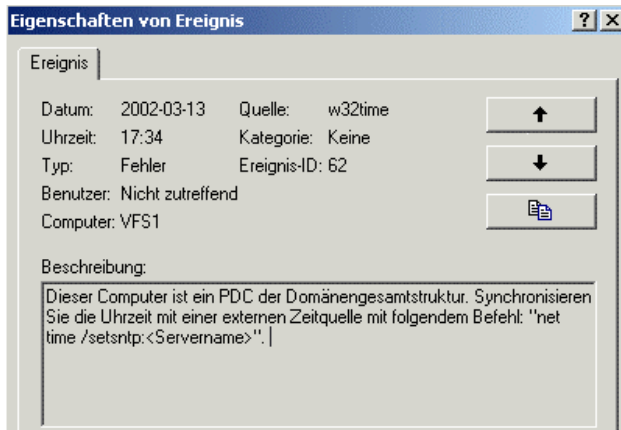


Die Erkenntnisse, die diese kurze Analyse der Mailserver-Veröffentlichungs-Regeln zu Tage gefördert hat, ist auch ganz nützlich wenn es darum geht auch andere Dienste zu veröffentlichen bzw. anzusprechen.

E.6 Synchronisation mit externen Zeitservern

Vielleicht haben Sie als aufmerksame/-r Administrator/-in schon einmal einen Blick in die Ereignisanzeige ihres Domaincontrollers geworfen. Dann ist Ihnen wahrscheinlich im Systemprotokoll aufgefallen, dass der Dienst W32Time regelmäßig Fehler verursacht. Auf alleinstehenden Servern wie dem ISA-Server oder auf den Workstations erscheint diese Meldung nicht, obwohl auch dort der Dienst W32Time läuft.

Ein genauer Blick auf das Ereignis gibt Aufschluss über die Ursache und deutet auch Lösungen für das Problem an.

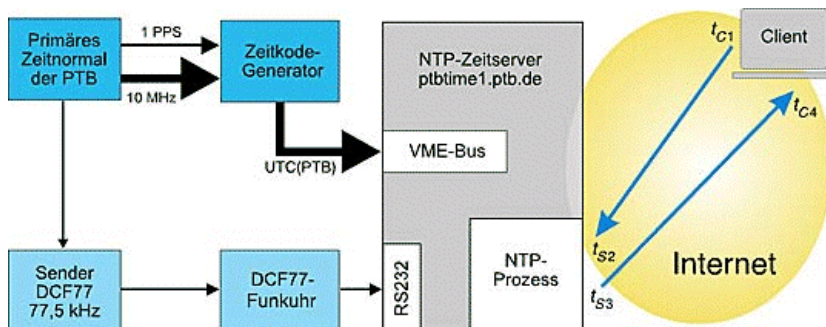


Verkürzt gesagt geht es darum, dass unter Windows 2000 alle Computer der Domain ihre Uhren mit der Uhr des Domaincontrollers synchronisieren. Das geschieht beim Hochfahren und dann in der Regel alle 8 Stunden, was für praktisch alle Belange eine ausreichende Übereinstimmung gewährleistet.

Aber der Domaincontroller muss ja auch irgendwoher wissen, dass seine Uhr richtig geht.

Zu diesem Zweck gibt es im Internet verschiedene Protokolle wie **daytime** (Port 13), **time** (Port 37) und **ntp** bzw. **sntp** = simple network time protocol (Port 123). Und genau auf letzteres hat die obige Ereignisanzeige (wenn auch etwas versteckt) verwiesen.

Viele Stellen (wie z.B. BelWue) bieten sogenannte **Zeitserver** im Internet an, um den Clients zu sagen, „was die Uhr geschlagen hat“. Und in der Bundesrepublik Deutschland ist die **Physikalisch Technische Bundesanstalt (PTB)** in Braunschweig die oberste Instanz, wenn es um die Zeit geht.

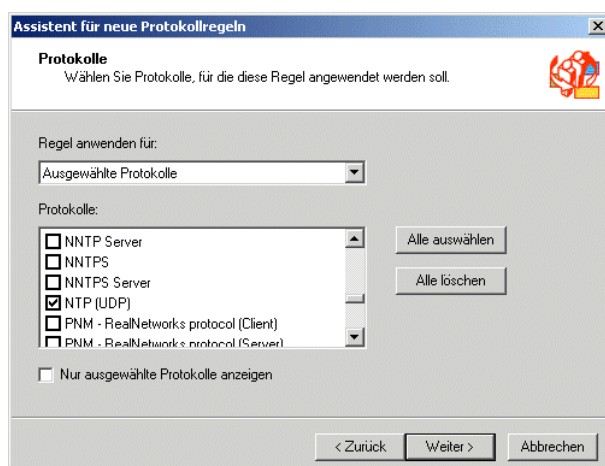


E.6.1 Erstellen einer Protokollregel für NTP auf dem ISA-Server

Zunächst einmal muss auf dem ISA-Server eine Protokollregel erstellt werden, die es dem Domaincontroller erlaubt, über das Protokoll NTP (Port 123) mit einem Zeitserver im Internet zu kommunizieren. Der Domaincontroller muss dabei als sogenannter „Secure NAT Client“ konfiguriert sein, was dadurch geschieht, dass dem Domaincontroller als Gateway die interne IP-Adresse des ISA-Servers eingetragen wird.

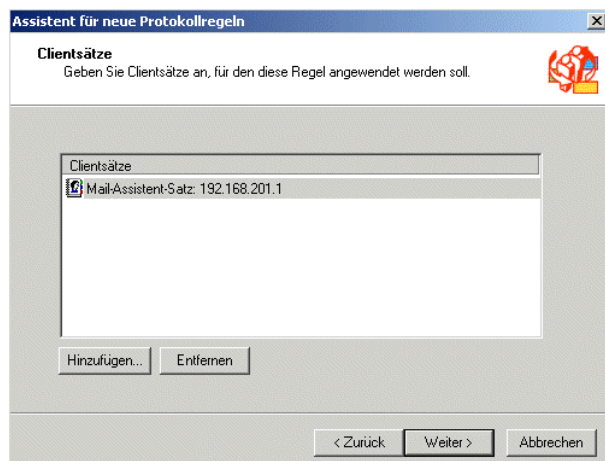
In der MMC über *Internet Security & Acceleration Server / Server und Arrays / <Servername> / Zugriffsrichtlinie / Protokollregel / Neu / Regel* auswählen. Im Assistent für Protokollregeln den Namen eingeben, z.B. Network-Time-Regel. Als *Regelaktion* Zulassen wählen.

Unter *Protokolle* die Option *Ausgewählte Protokolle* und dort NTP (UDP) wählen:



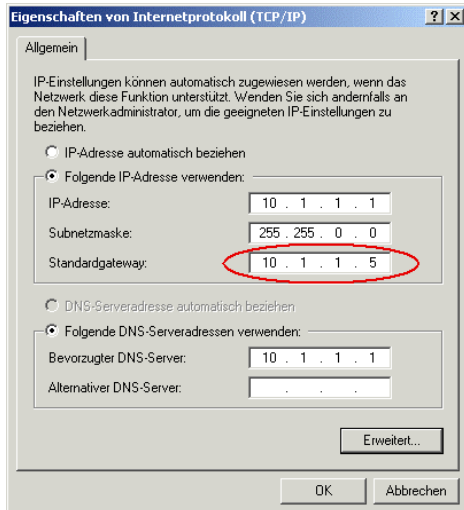
Unter *Zeitplan* Immer wählen und als *Clienttyp* Spezielle Computer (Clientdatensätze) angeben.

Im Fenster *Clientsätze* einen Clientsatz *hinzufügen*, der die IP-Adresse des Domaincontrollers enthält. Falls noch kein Satz existiert, muss man dessen Erstellung nachholen. Und am Schluss auf *Fertigstellen* klicken.



E.6.2 Konfiguration von W32Time auf dem Domaincontroller

Sie haben es hoffentlich nicht vergessen: Richtig! Der Domaincontroller muss noch als sogenannter „Secure NAT Client“ konfiguriert werden. Einfach unter *Eigenschaften von Internetprotokoll (TCP/IP)* als *Gateway*, die interne IP-Adresse des ISA-Servers eintragen.



Die eigentliche Konfiguration läuft dann so ab:

- Auf die Kommandozeilebene wechseln
- `net start w32time` eingeben (nur zur Sicherheit)
- `net time /setsntp:"192.53.103.103 192.53.103.104"` eingeben. Dadurch werden als SNTP-Server die Server mit den angegebenen IP-Adressen verwendet. Lässt der ISA-Server auch DNS-Anfragen durch, so kann stattdessen auch `net time /setsntp:"ptbtime1.ptb.de ptbtime2.ptb.de"` eingeben werden. (Die Anführungszeichen und das Leerzeichen zwischen den Adressen sind nötig, wenn mehr als eine Adresse angegeben wird).
- `net time /querysntp` zur Kontrolle eingeben.
- Die Uhrzeit verstellen.
- `net stop w32time` eingeben um den Zeitdienst anzuhalten. Dies ist nötig, um den folgenden Befehl ausführen zu können:
- `w32tm -once` eingeben. Dadurch wird eine einmalige Anfrage des Dienstes W32Time bei den angegebenen SNTP-Servern ausgelöst:

```

C:\WINNT\System32\cmd.exe
G:\>net stop w32time
Windows-Zeitgeber wird beendet.
Windows-Zeitgeber wurde erfolgreich beendet.

C:\>w32tm -once
W32Time: BEGIN:InitAdjIncr
W32Time:   Adj 100144 , Incr 100144 fAdjst 0
W32Time: END:Line 2476
W32Time: BEGIN:IsUpTheThread
W32Time: END Line 1385
W32Time: TimeWInit()
W32Time: Kernel timer : using default maximum resolution
W32Time:               MaximumTime = 100144
W32Time:               CurrentTime = 100144
W32Time: Timer calibrated, looped 1 times
W32Time: BEGIN:InitTmCfg
W32Time: END:Line 752
W32Time: BEGIN:InitTmCli
W32Time: END:Line 2569
W32Time: BEGIN:InitTmData
W32Time: END:Line 2591
W32Time: AvoidTimeSyncOnWan 0
W32Time: ntpserver = 192.53.103.103 192.53.103.104
W32Time: BEGIN:CMOSynchSet

```

- Die Uhrzeit überprüfen
- `net start w32time` eingeben: Der Zeitdienst startet wieder.