Freigabe von Terminal Services Web Access für externe Benutzer

von Wolfgang Bauer
Publiziert auf faq-o-matic.net. Alle Rechte liegen beim Autor.

1. Ausgangssituation

Es wurde im Rahmen eines Serverumzuges der Terminal Services von dem Serverbetriebssystem Windows Server 2003 auf die nächste Generation, Windows Server 2008, gewechselt. Bei diesem Serverbetriebssystem wurden die Terminal Services grundlegend überarbeitet und bieten nun neue Möglichkeiten. Ein Teil davon ist die Möglichkeit, einzelne Applikationen Benutzern remote zur Verfügung zu stellen, ohne eine komplette normale Remotedesktopverbindung herstellen zu müssen. Außerdem lässt sich über den Terminaldienste-Gatewayserver (TS Gateway) eine Remotedesktopverbindung zu jedem internen Windowssystem herstellen, welches RDP-Verbindungen zulässt. Es lassen sich auf dem Terminalserver mittels des NPS (Network Policy Server), der auch Funktionen des ehemaligen IAS (Internet Authentication Service) übernimmt, dediziert Gruppen erstellen, die festlegen welche Rechte ein bestimmter Benutzer hat, also ob und welche RemoteApp-Dienste und/oder das TS-Gateway zu welchen Servern/Systemen genutzt werden darf. Dadurch fällt z.B. für Administratoren das oftmals aufwendige VPN weg, um einzelne Server kurzfristig zu warten oder zu kontrollieren.

2. Schwerpunkt

Dieser Artikel beschreibt eine konkrete Implementierung der Terminalsienste für den sicheren Zugriff durch Benutzer, die sich außerhalb des Unternehmensnetzwerks befinden.

3. Umsetzung

3.1 Grundsätzliche Überlegungen

Um den Server und das Netzwerk vor Angriffen und Bedrohungen zu schützen, muss der Server über eine Firewall und am besten zusätzlich über einem Proxy veröffentlicht werden. Der Terminalzugriff selbst und die Authentifizierung werden bereits über die Einstellungen auf dem Terminalserver sicher geregelt und müssen nicht extra konfiguriert werden.

Da die zukünftigen Benutzer über diese Freigabe ganz normal arbeiten sollen und somit auch geschäftskritische und schützenswerte Daten bearbeiten, muss die Verbindung vom User zum Proxy

geschützt erfolgen. Die Grundlage der Dienste ist eine Webseite, daher bietet sich eine verschlüsselte Verbindung (https) an.

3.2 Technische Mittel

Da bereits ein ISA-Server 2006 im Firmennetzwerk integriert ist, der in der Lage ist, als Firewall und Proxy zu gleich zu agieren, wird als Freigabemethode der ISA-Server gewählt. Desweiteren ist für die sichere HTTPS-Verbindung ein Zertifikat nötig, welches die Verbindung zumindest zum Client verschlüsselt. Dieses lässt sich kostenlos bei der bereits bestehenden Zertifizierungsstelle des Unternehmens ausstellen. Die Alternative wäre ein Zertifikat einer öffentlichen Zertifizierungsstelle.

Das Zertifikat der unternehmenseigenen Zertifizierungsstelle wird von allen internen (Domänen-) Computern als vertrauenswürdig angesehen, da die Zertifizierungsstelle im Active Directory integriert ist. Bei externen Anwendern, deren Computer nicht Teil der Domäne sind, wird eine Warnmeldung angezeigt, dass das Zertifikat nicht überprüft werden kann. Dies ist oft unerwünscht, weil es Benutzer daran gewöhnt, eine Zertifikatswarnung zu ignorieren. In der konkreten Situation wird dies in Kauf genommen, und die User werden darüber informiert. Zusätzlich ist es als Benutzer möglich, sich das öffentliche CA-Root-Zertifikat zusenden zu lassen, um es Kunden oder dem Homeoffice-PC zur Verfügung zu stellen.

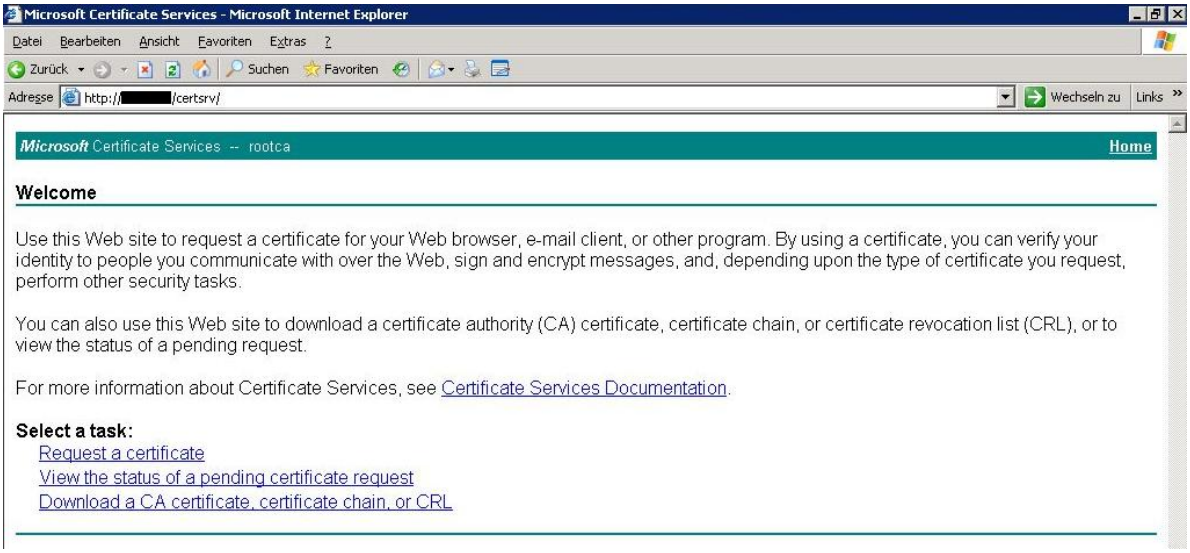
Voraussetzung für die Nutzung der Dienste ist Windows XP SP3, Vista SP1, Windows Server 2008.

4. Durchführung

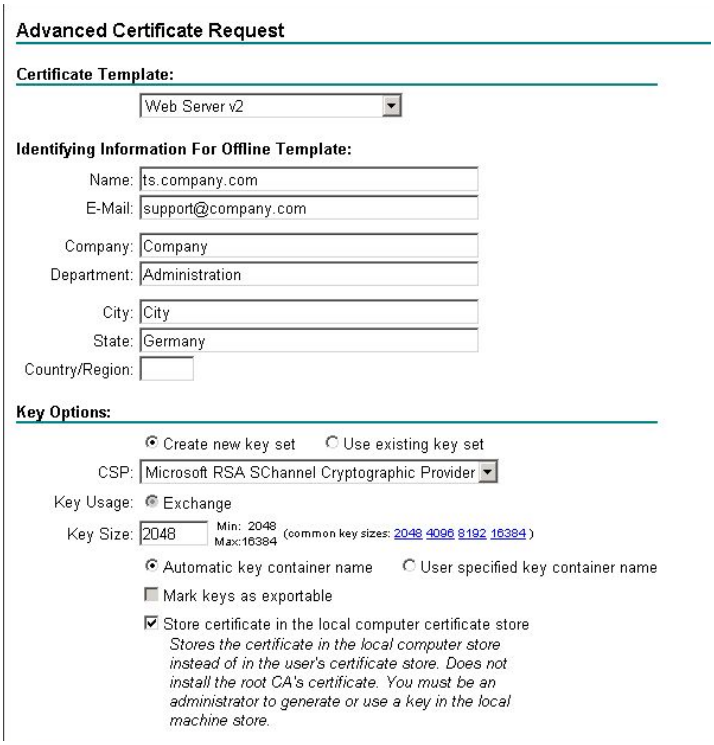
Folgend werden die Schritte der Realisierung als „Howto“ dargestellt.

4.1 Anfordern des Zertifikats

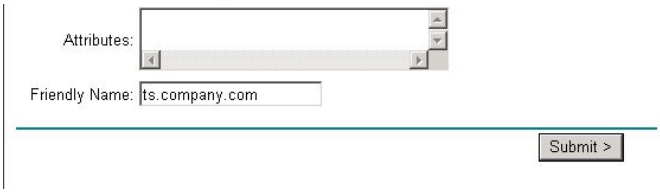
Als erstes benötigen wir ein Zertifikat für die HTTPS-Verbindung vom Client zum ISA-Server. Dazu gehen wir vom ISA Server aus auf die Seite http://enterprise-ca-server/certsrv:



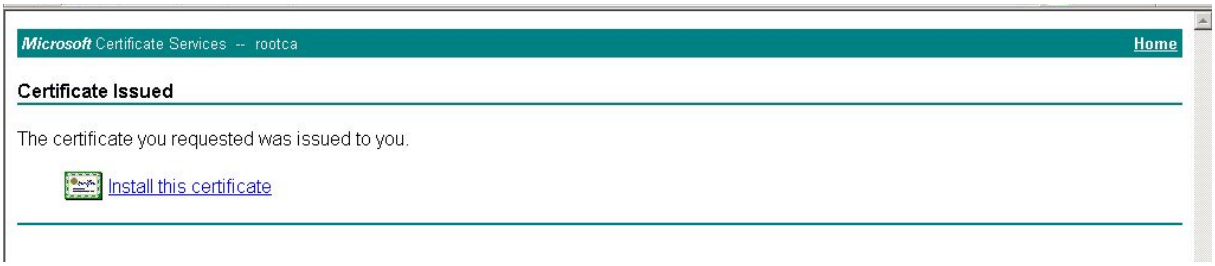
Dort beantragen wir ein Webserverzertifikat das in dem Zertifikatsstore des lokalen Computers abgelegt werden soll, da es ja für einen Server und nicht für einen Benutzer gedacht ist.



Der Friendly Name muss dem Namen der späteren Webadresse des TS-Webservers entsprechen, damit der Browser später das Zertifikat akzeptiert.



Abschließend muss das Zertifikat nur noch mit dem Klick auf den Link installiert werden:

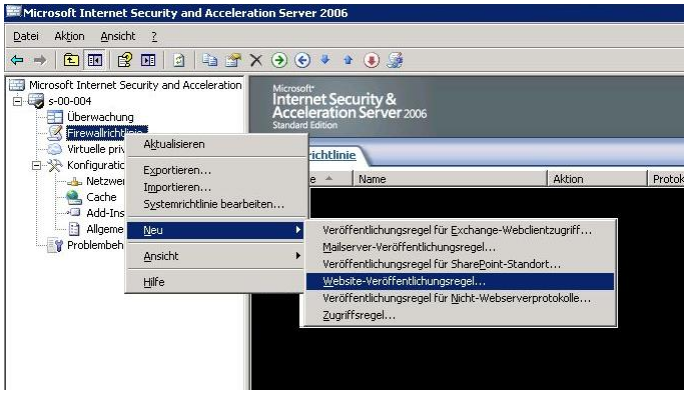


Um zu kontrollieren, ob alles geklappt hat, können wir mit *Start/Ausführen: mmc* in einer neuen MMC-Konsole das Zertifikats-Snap-In einbinden und dort den Zertifikatsspeicher des lokalen Computers auswählen. Dort sollte unter *Eigene Zertifikate/Zertifikate* das angeforderte Zertifikat auftauchen.

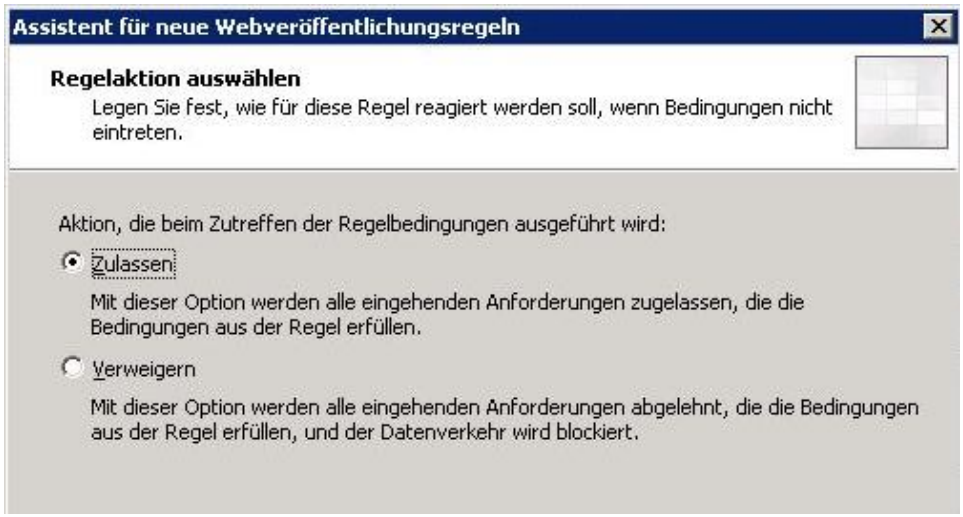
Damit sind die Vorbereitungen für die Veröffentlichung erledigt.

4.2 Veröffentlichungen

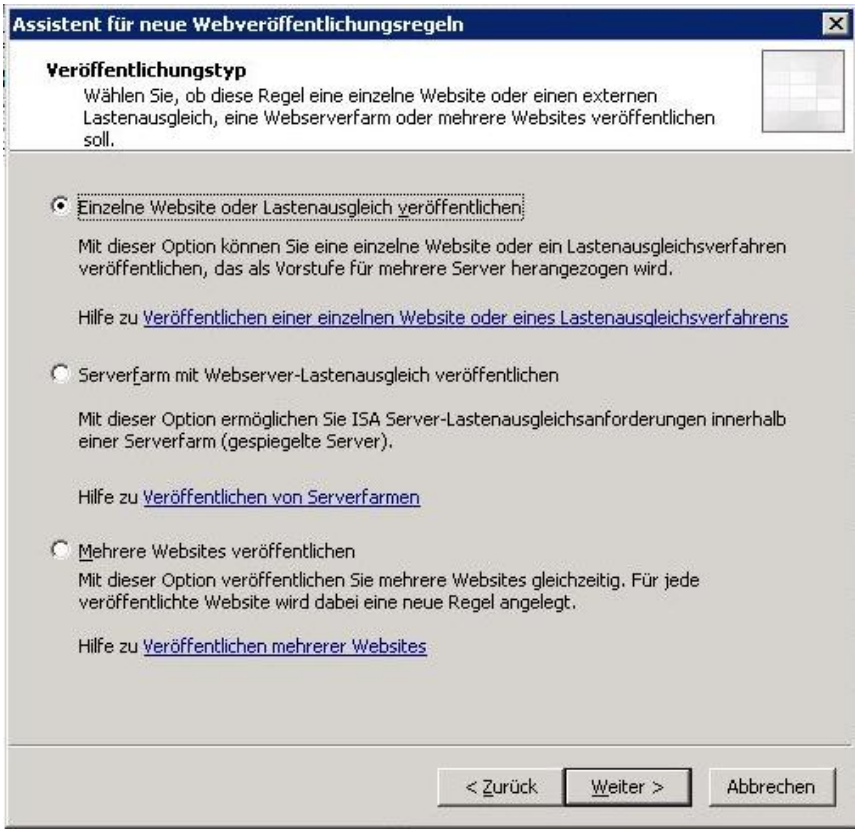
Nun erstellen wir eine neue Website-Veröffentlichungsregel. Dazu öffnen wir die ISA-Server Konsole und klicken rechts auf Firewallrichtlinien und wählen Neu/Website-Veröffentlichungsregel:



Es ist sinnvoll, die Namen so zu wählen, dass man später auf einen Blick weiß, was die Regel macht:

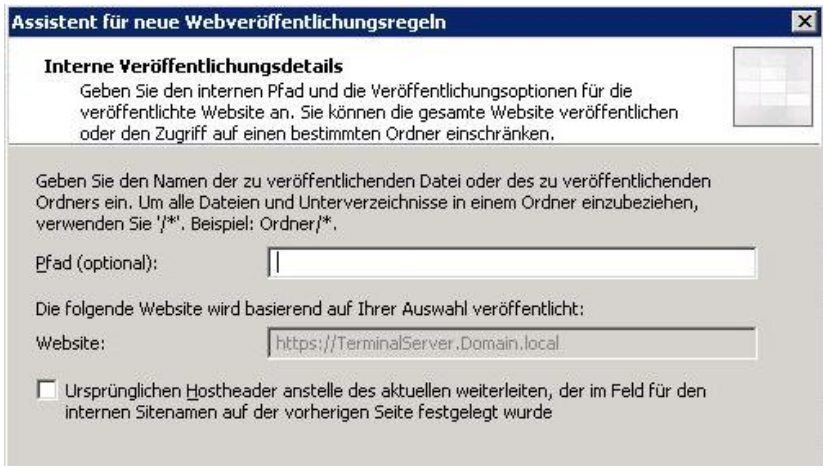


Das TS Web Access läuft nur auf einem Server und ist auch nur eine Website, also wählen wir die erste Auswahlmöglichkeit:

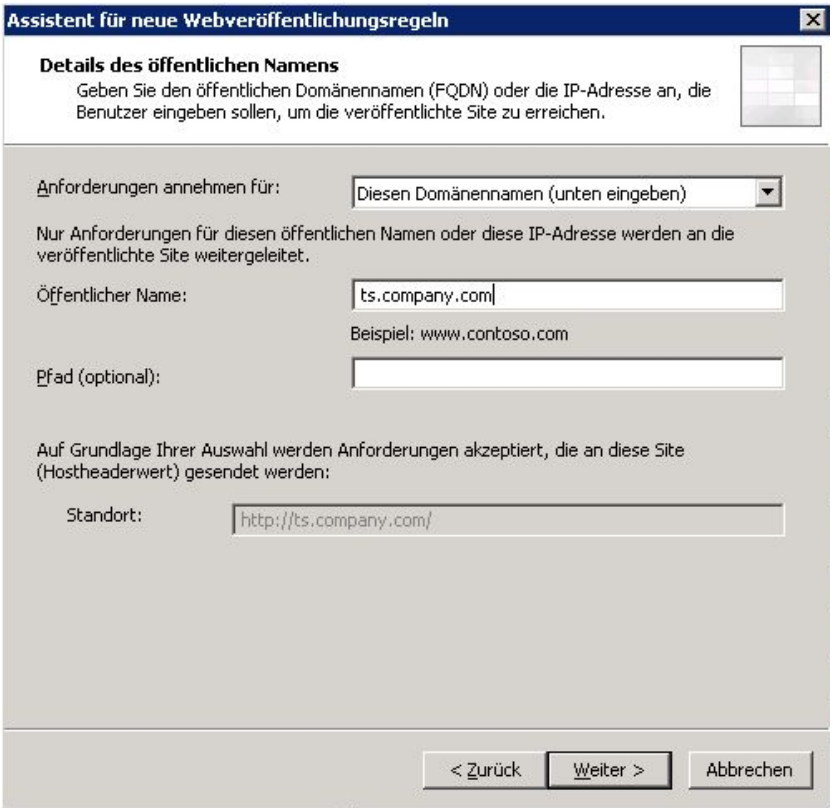


Der interne Sitename ist der Name des Terminal Servers. Damit der Service noch funktioniert, wenn der DNS-Server aus irgendeinem Grund nicht erreichbar ist, geben wir die IP-Adresse mit an:

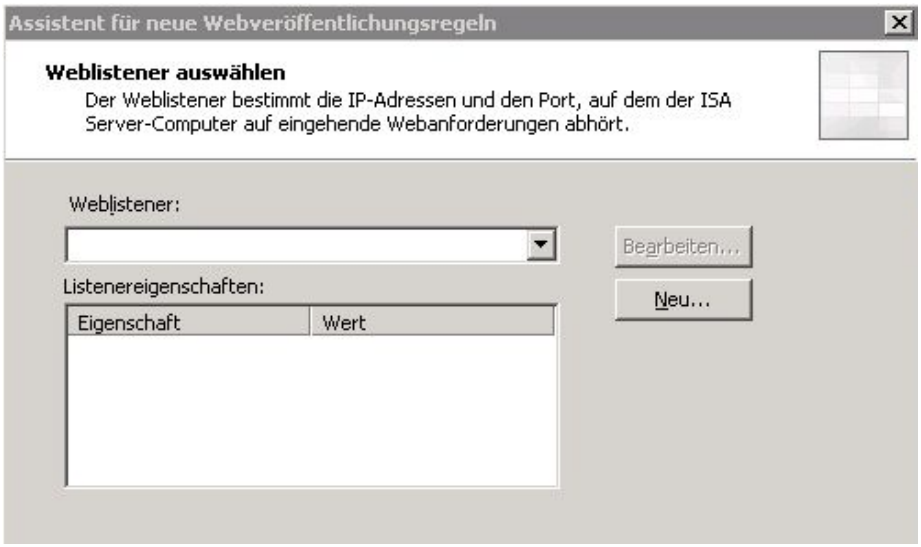
Der Pfad zur Webseite (http://terminalserver.domain.local/ts) kann nicht direkt angegeben werden, da wir auf zwei verschiede Unterpfade zugreifen müssen. Also wählen wir die 1:1-Übersetzung, indem wir nichts eintragen:



Als öffentlicher Name wird die geplante URL der Veröffentlichung eingetragen welcher, wie eingangs erwähnt, der gleiche ist muss wie der Friendly Name des Zertifikats.

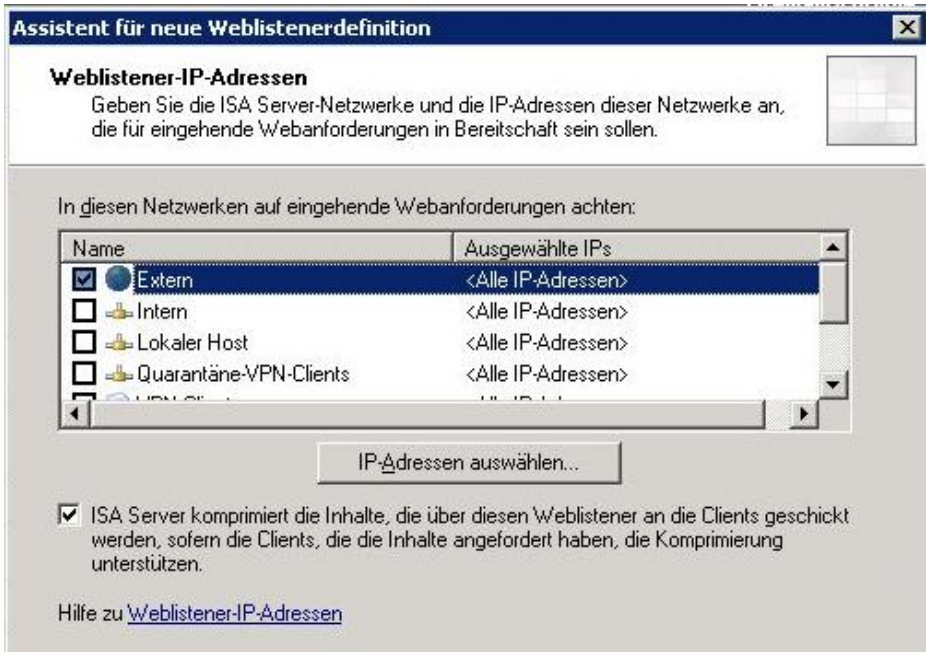


Als nächstes wird mit einem Klick auf *Neu* der Weblistener erstellt:

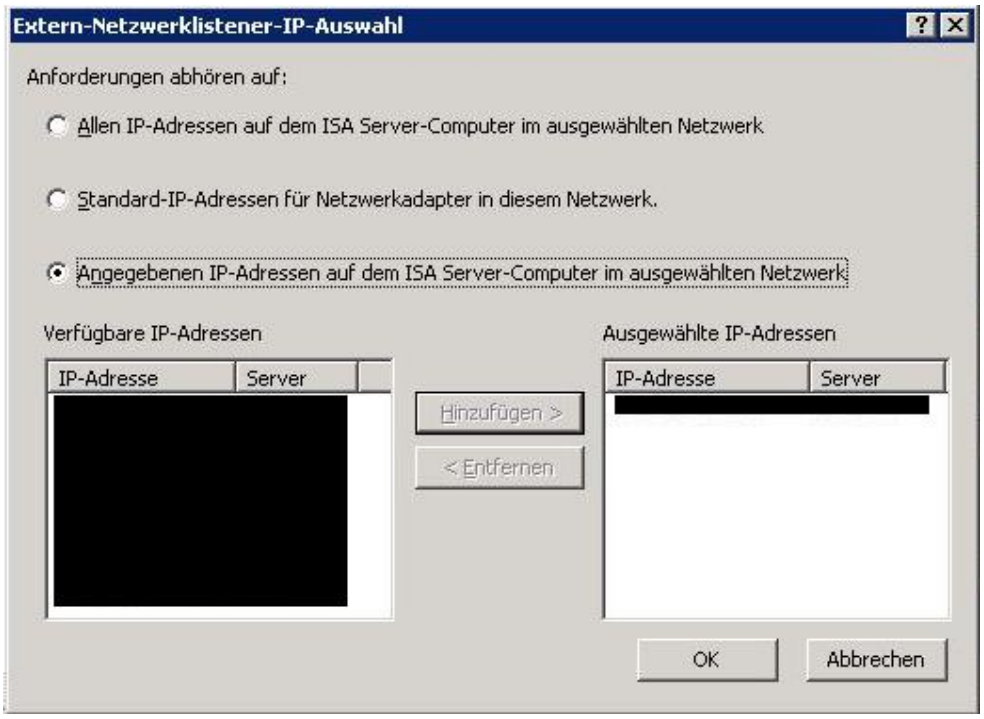


Die Clients sollen nur über eine sichere HTTPS-Vebindung mit dem ISA-Server kommunizieren:

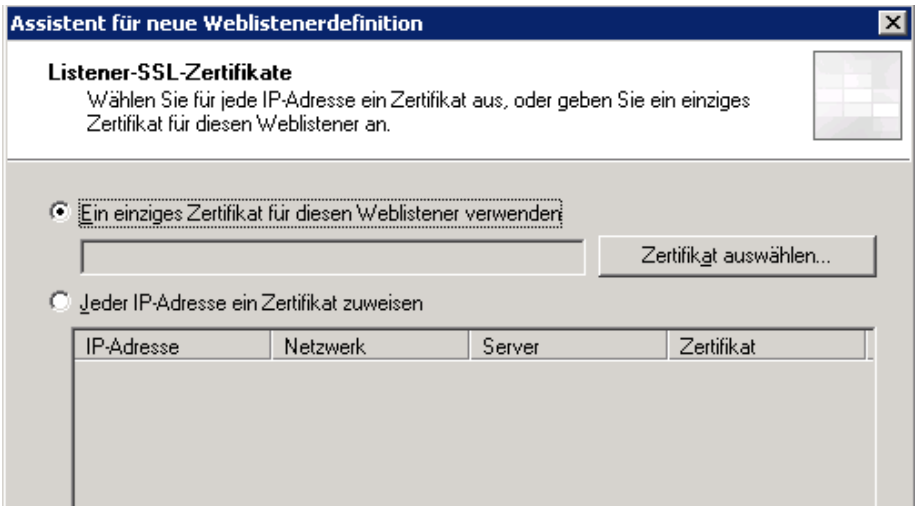
Als nächstes wählen wir das Netzwerk, auf auf dem der Listener horchen soll:



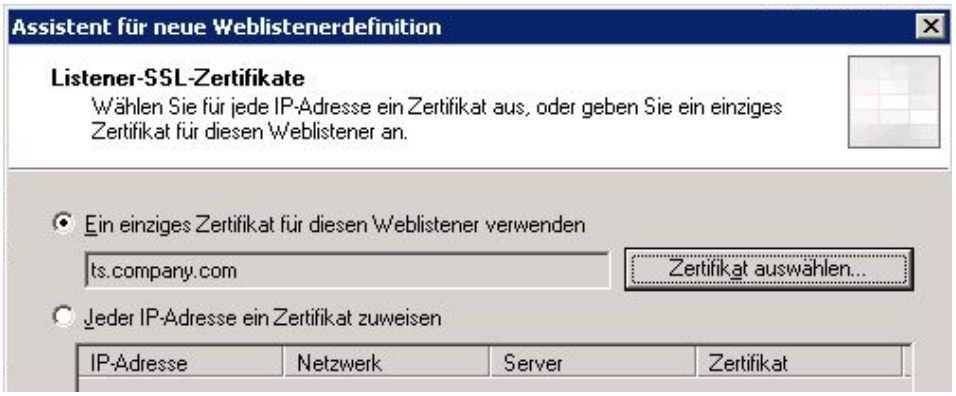
Mit einem Klick auf *IP-Adressen auswählen* legen wir die IP fest, indem wir die gewünschte, nach anwählen der letzten Option, mit einem Klick auf *Hinzufügen* einstellen. Denn der Port 443 (der Standard HTTPS-Port) soll ja nicht auf allen IP-Adressen des Netzwerks in Benutzung sein, denn sonst könnte man keine andere HTTPS-Verbindung mehr auf dem Netzwerk veröffentlichen:



Nach dem Klick auf *OK* und *Weiter* erscheint die Auswahl des Zertifikats. Da wir nur auf einer IP veröffentlichen, lassen wir die Auswahl so und klicken auf Zertifikat auswählen:



Hier muss das beantragte Zertifikat durch anklicken eingebunden werden. Am grünen Haken lässt sich erkennen, dass mit dem Zertifikat alles in Ordnung ist:

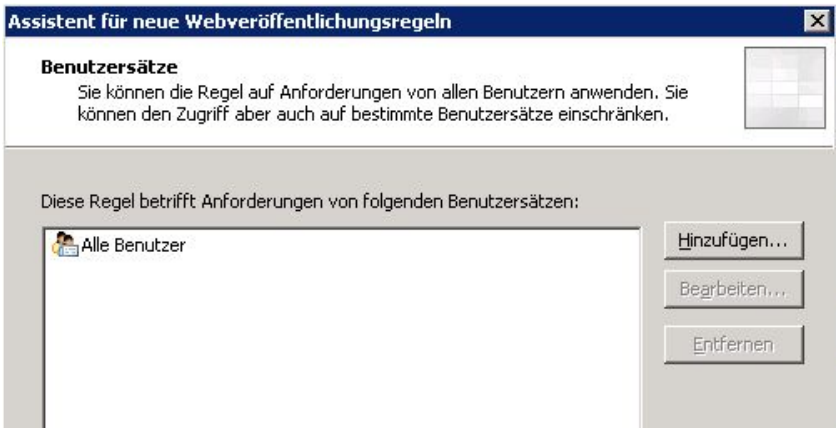


Im nächsten Fenster wählen wir „Keine Authentifizierung“, da das TS Web über eine eigene verfügt:

Nun ist der Weblistener fertig gestellt.

Damit die Authentifizierung von Terminal Server zum User durchgereicht wird, wählen wir nun „Keine Delegierung, aber direkte Authentifizierung des Clients“:

Da die Authentifizierung durch den Terminal Server vorgenommen wird, lassen wir Alle Benutzer stehen:

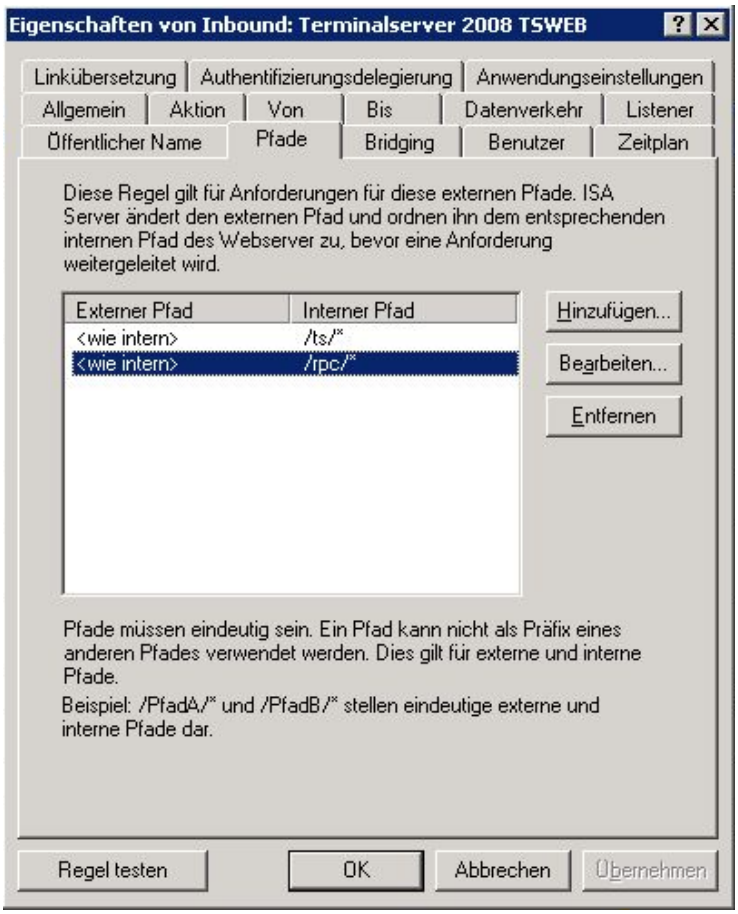


Damit ist die Regel fertig gestellt. Abschließend muss die Regel noch wie folgt bearbeitet werden, da der Wizard nicht alle Einstellmöglichkeiten bietet.

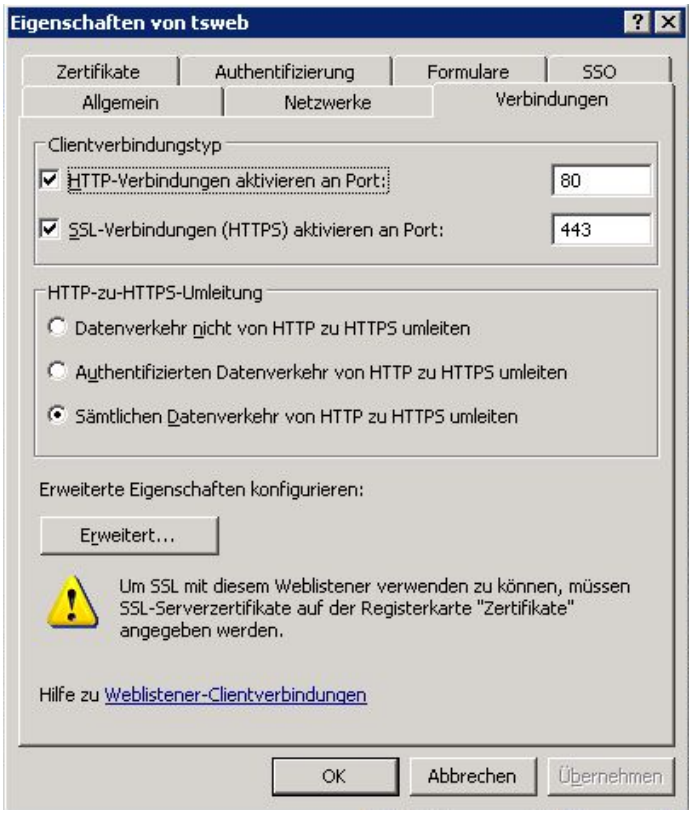
Nach einem Doppenklick auf die Regel finden wir unter *Pfade* die veröffentlichten Pfade, diese müssen geändert werden. Wir löschen den vorhandenen und erstellen zwei neue mit Hinzufügen. Dabei wählen wir immer „wie veröffentlichter Ordner“ und tragen folgendes ein:

- */ts/** für die Webseite an sich und
- */rpc/** für die Funktionen das Terminal Server Gateways.

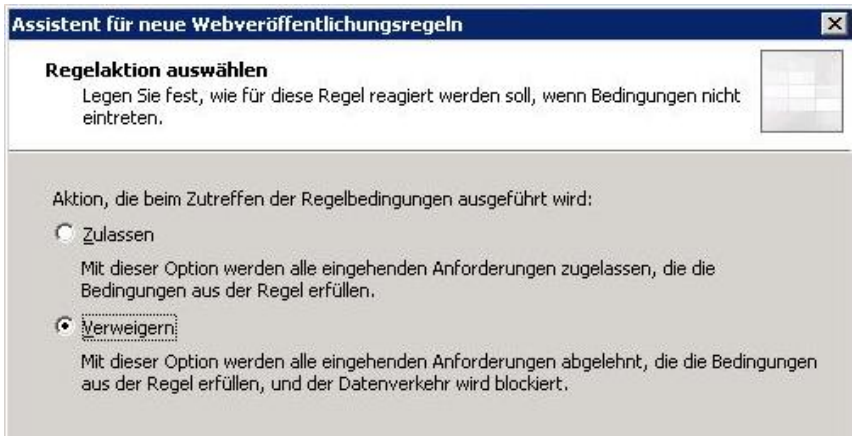
Mit dem *Regel-testen*-Knopf lässt sich die Regel schon testen. Die Warnung bei */rpc/** kann Ignoriert werden, da wir keine Exchange Inhalte freigeben:



Nun noch im Listener (Reiter *Listener* und auf *Berarbeiten* klicken) die Verbindungen editieren, damit automatisch eine HTTPS-Verbindung aufgebaut wird, ohne dass der User im Browser „https“ vor die URL schreiben muss:

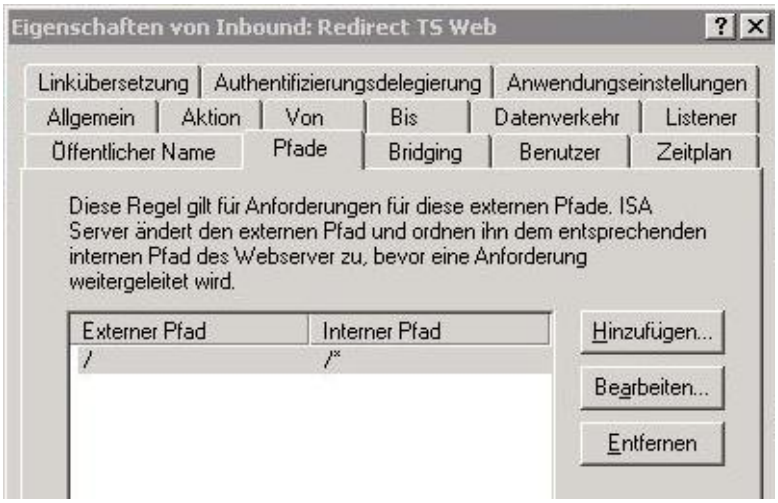


Als nächstes erstellen wir eine Regel, die *ts.company.com*-Aufrufe automatisch zu *ts.company.com/ts* umleitet, um die Userfreundlichkeit weiter zu erhöhen, da man ohne Regel sonst immer *ts.company.con/ts* in den Browser eintippen müsste, um auf die TS-Web-Webseite zu kommen. Hier wird *Verweigern* gewählt, da sonst die Redirect-Option nicht auswählbar ist:

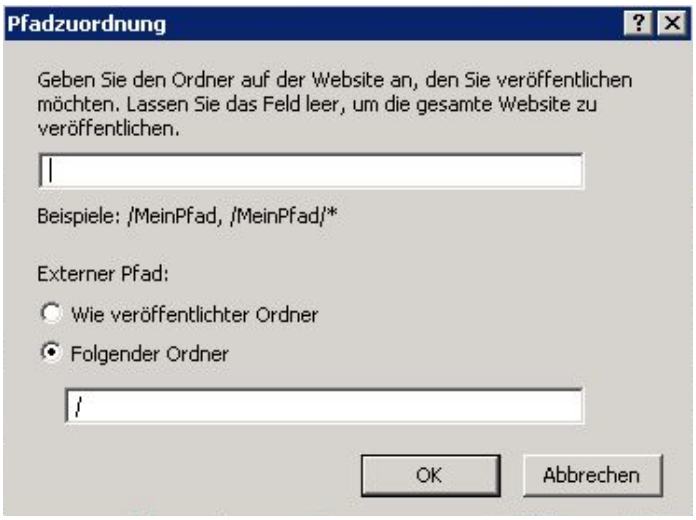


Der restliche Klickweg ist genau gleich, bis auf die Tatsache, dass der für die erste Regel erstellte Listener wieder ausgewählt wird. Danach müssen ein paar andere Modifikationen an der Regel vorgenommen werden.

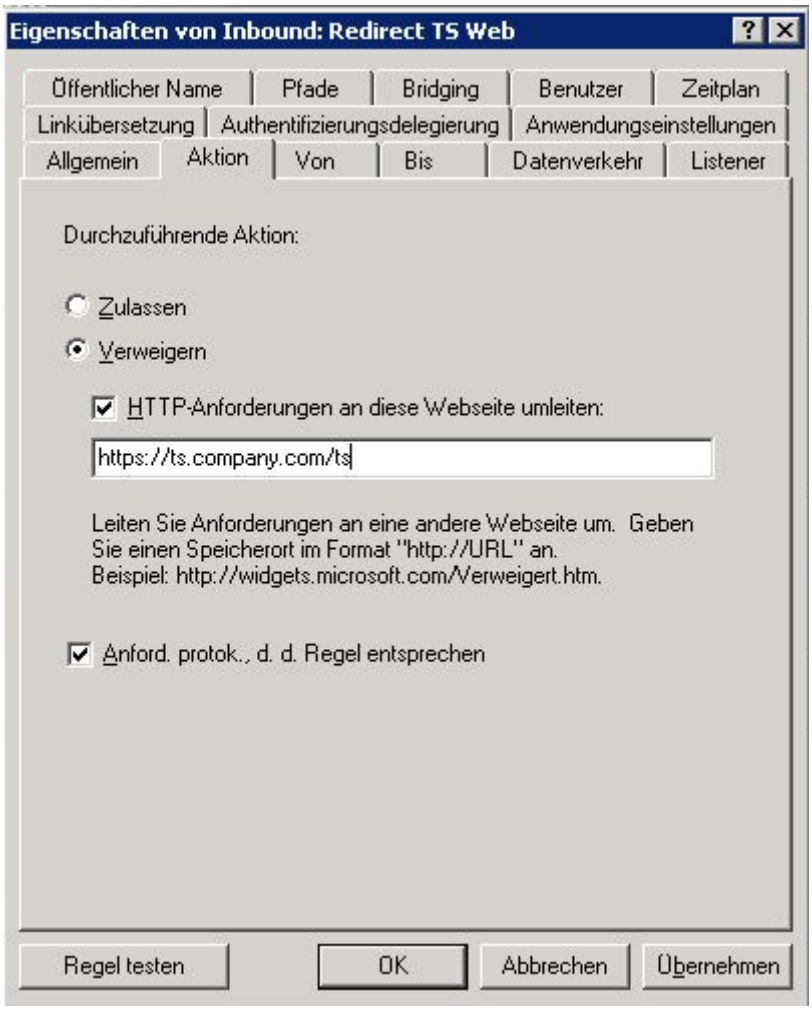
Mit Doppelklick auf die Regel unter *Pfade* den veröffentlichten Pfad editieren, indem wir auf *Bearbeiten* klicken.



Damit nur der Aufruf von *ts.company.com* umgeleitet wird, aber nicht die Aufrufe der Unterwebsites, muss der externe Pfad „/“ lauten:



Als nächstes aktivieren wir die Umleitung unter *Aktion* und geben als Pfad den Link zur TS-Web-Webseite (https://ts.company.com/ts) an:

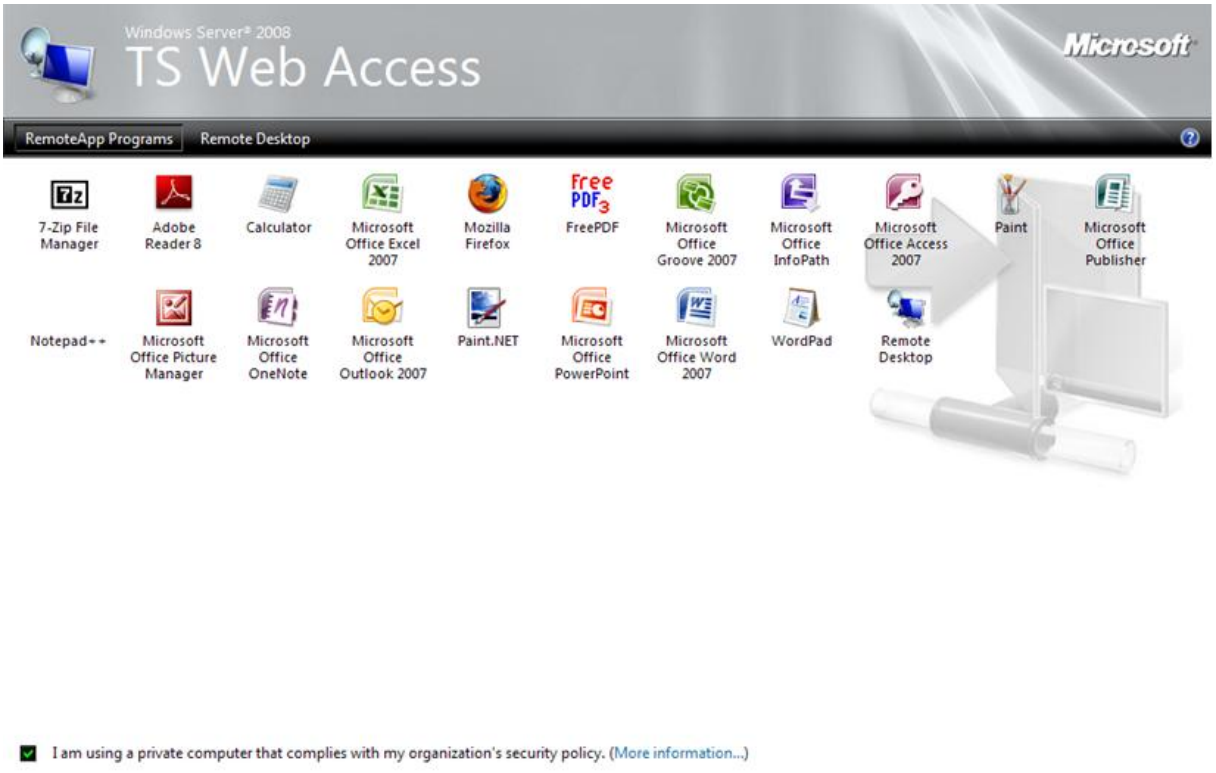


Die Redirect-Regel muss in der Liste über der normalen TS-Web-Regel stehen, damit diese den Aufruf von *ts.company.com* abfangen kann und nicht die Veröffentlichungsregel zuerst greift und der Redirect nie stattfindet, da die Firewallregeln von oben nach untern abgearbeitet werden.

Abschließend in der Console *Übernehmen* klicken. Dann muss auf dem DNS-Server nur noch ein DNS-Host-Eintrag erstellt werden der *ts.company.com*-Aufrufe auf die IP des Listeners lenkt.

5. Test

Beim Aufruf von ts.company.com erscheint nun eine Anmeldemaske. Nach erfolgreicher Anmeldung bekommen wir die TS-Web-Webseite präsentiert:



Auch die Webapplikationen und das Remotedesktop Gateway funktionieren.

6. Fazit

Die Freigabe ließ sich ohne größere Schwierigkeiten realisieren. Wichtig ist, dass (im Moment) der ISA2006 keine vorgeschaltete Authentifizierung, ähnlich zum Outlook Web Access bieten kann.

Nach ersten Tests zeigt sich das TS Web eine sehr gute Alternative zur normalen Terminalserververbindung ist. Das Gateway ermöglicht nun dediziert Administratoren und Entwicklern einfachen Zugriff von außen auf interne Server.