Exchange 2007 – Outlook Web Access Publishing with ISA Server 2006

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how to publish Outlook Web Access in Exchange Server 2007 Beta 2 with the help of ISA Server 2006

Let's begin

Exchange Server 2007 is currently in Beta 2 status but the Outlook Web Access functionality is nearly feature complete I think. ISA Server 2006 is RTM since 31st July 2006 and has many new and improved features for Webserver- and Server Publishing rules. One of the enhancements is the Exchange Webclient Access Publishing rule. With ISA Server 2006 it is possible to publish version specific Exchange Servers (including Exchange Server 2007). There are several other enhancements like the option to change user passwords during Outlook Web Access logon. Administrators can now customize the HTML forms for the forms based authentication and ISA supports some new authentication types like RADIUS-OTP and LDAP. It is also possible to do some delegation of authorization.

On Exchange Server site

We must start our configuration on Exchange Server site. Start the Exchange Management Console (EMC) navigate to the Server configuration container, select the Client Access role and select the new OWA directory. The OWA directory is new in Exchange Server 2007 and will be used by OWA clients when they access Exchange Server 2007. You must enable Basic Authentication in the Authentication tab if it is not already configured.

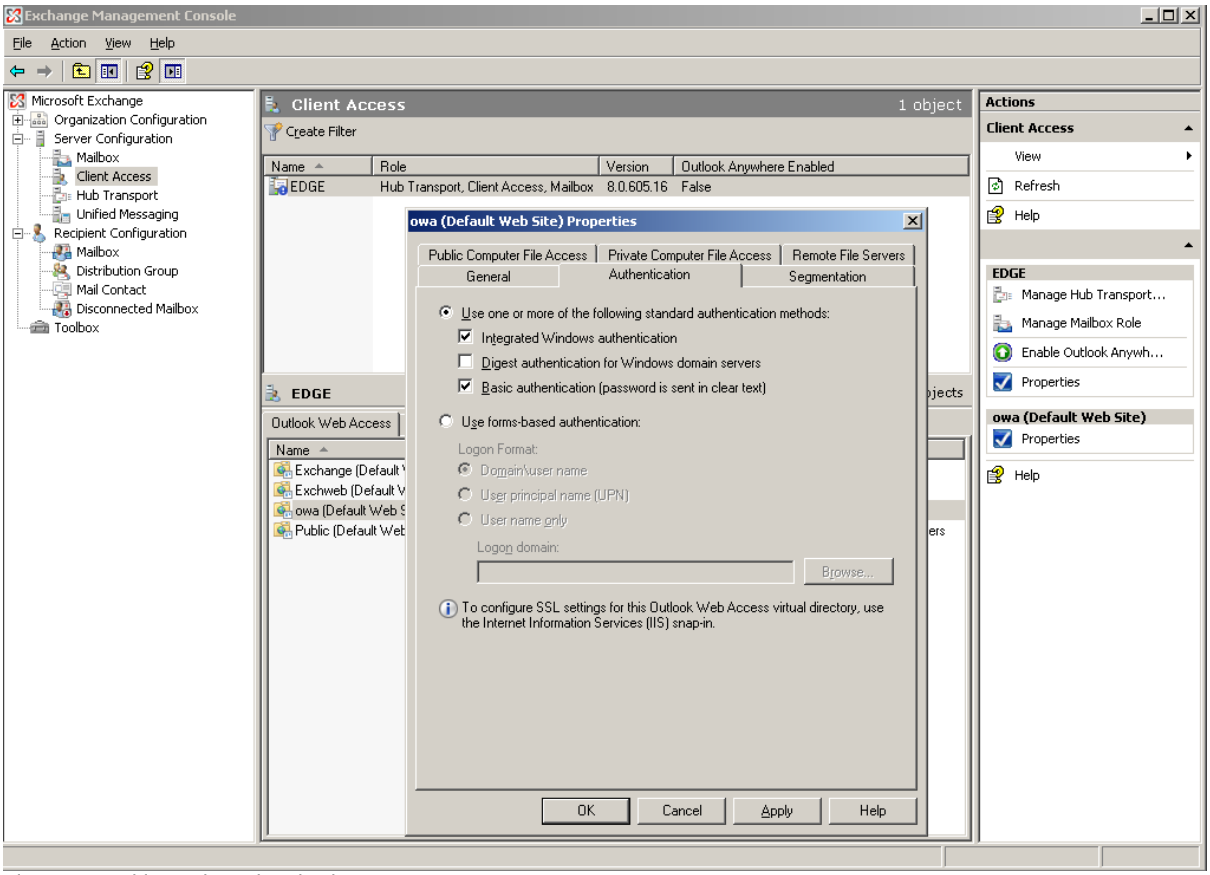

Figure 1: Enable Basic Authentication

On IIS site

Next we must issue a certificate from an internal CA or a commercial CA for the Default Web Site. After issuing the certificate, navigate to the OWA directory – go to the Directory Security tab and enable SSL and 128-bit encryption as you can see in the following figure.

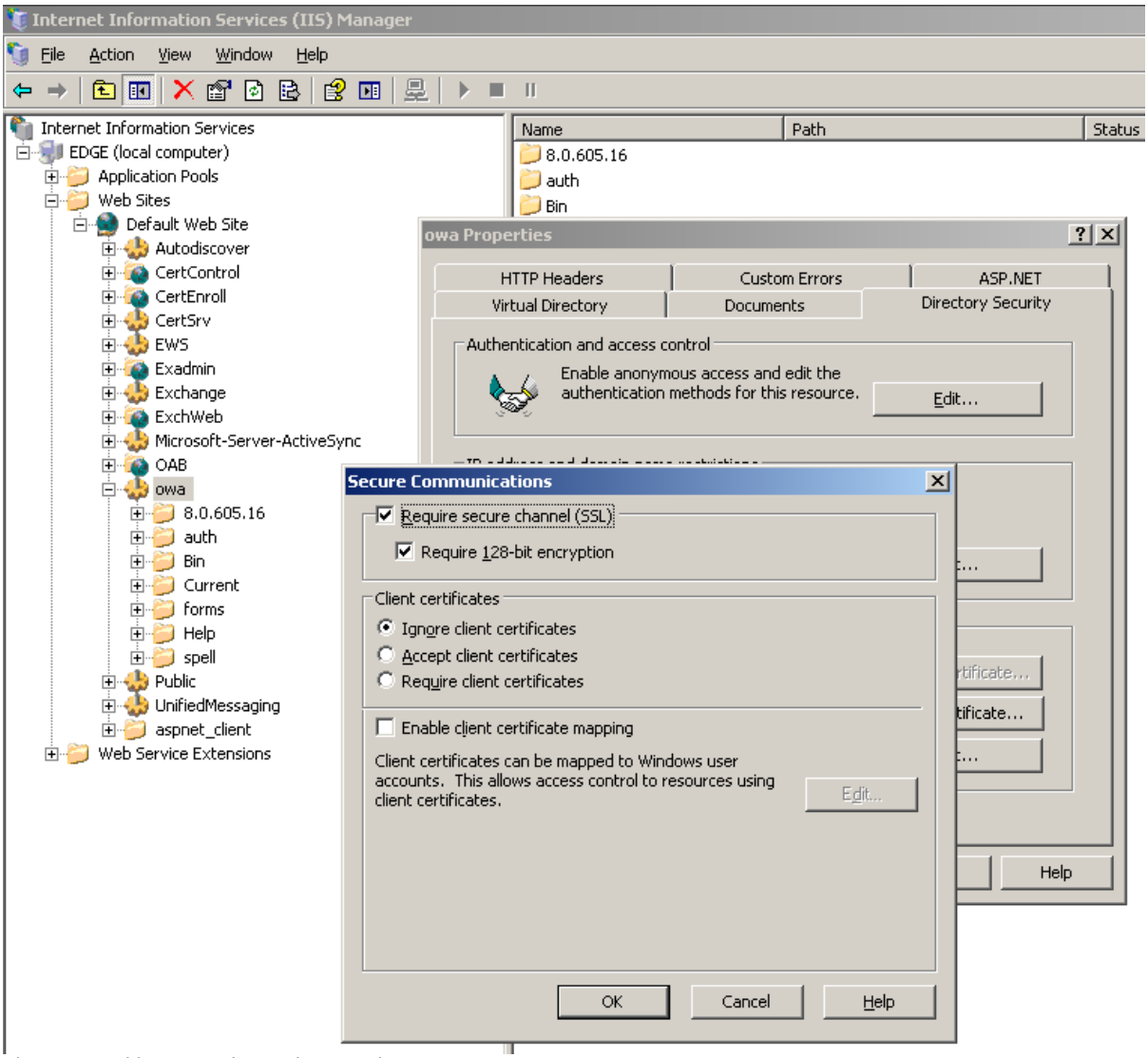

Figure 2: Enable SSL and 128-Bit encryption

On ISA site

Before we start the Exchange Webclient Access Publishing rule wizard we must request a certificate for the ISA Server Weblistener because we are using HTTPS-Bridging, ISA Server terminates the SSL connection from the OWA client, inspects the traffic and encrypts the connection to the Exchange Server again. The common name (CN) of the requested certificate must match the Name of the Server that OWA clients specify in their browsers. In this example the Public FQDN is OWA.IT-TRAINING-GROTE.DE so the CN of the certificate must be OWA.IT-TRAINING-GROTE.DE. You can request certificates via the CA servers webconsole (http://caservername/certsrv). You must request a Webserver certificate as shown in the following figure.

Please note:

Depending on your ISA Server Firewall rules you must create a Firewall rule that allows HTTP or HTPS access from your ISA Server to the CA Server.

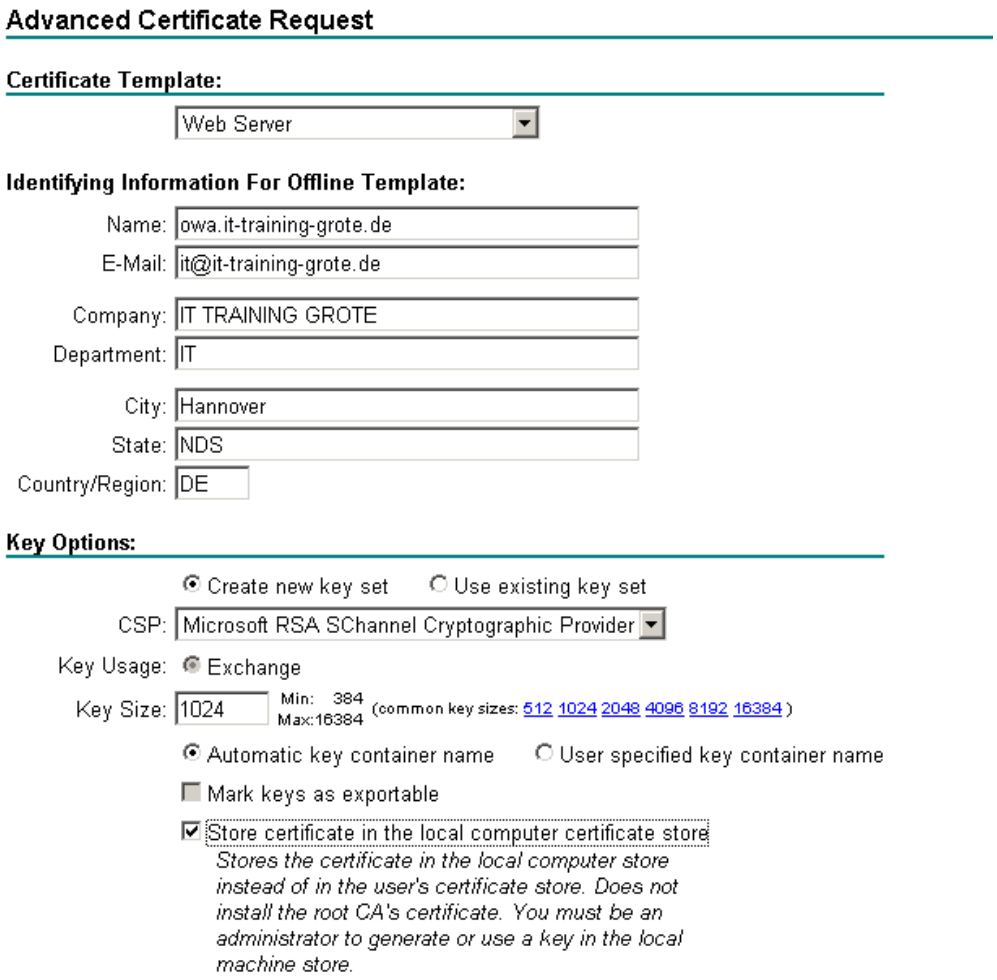

Figure 3: Advanced certificate request

Split DNS or HOSTS file?

The Public Name OWA.IT-TRAININGR-GROTE.DE in the OWA Weblistener must be resolvable to the internal Exchange Server IP adderss, so you have two options:

- Split-DNS or
- HOSTS file

If you are using Split DNS you must create a new Forward Lookup zone in DNS named *IT-TRAINING-GROTE.DE*. Second you must create a new A-record named *OWA* in the new Forward Lookup zone with the IP Address of the internal Exchange Server.

If you are using the HOSTS file you only need to extend the file with an entry like that:

IP address of the Exchange Server OWA.IT-TRAINING-GROTE.DE

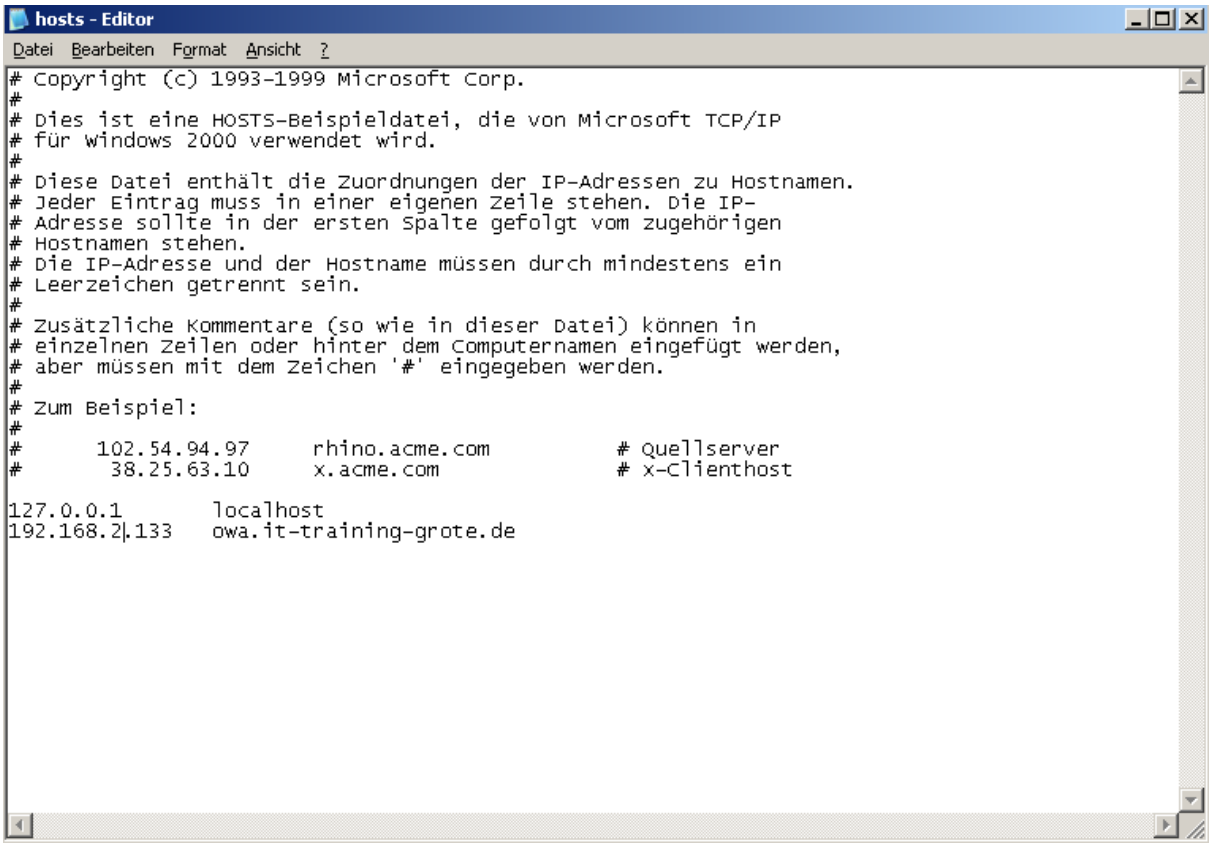

Figure 4: HOSTS file

Now it is time to create the Exchange Webclient Access Publishing rule.

Start the ISA MMC click - *New - Exchange Webclient Access Publishing Rule*. Name the rule and select the Exchange Version and that you want to publish Outlook Web Acess.

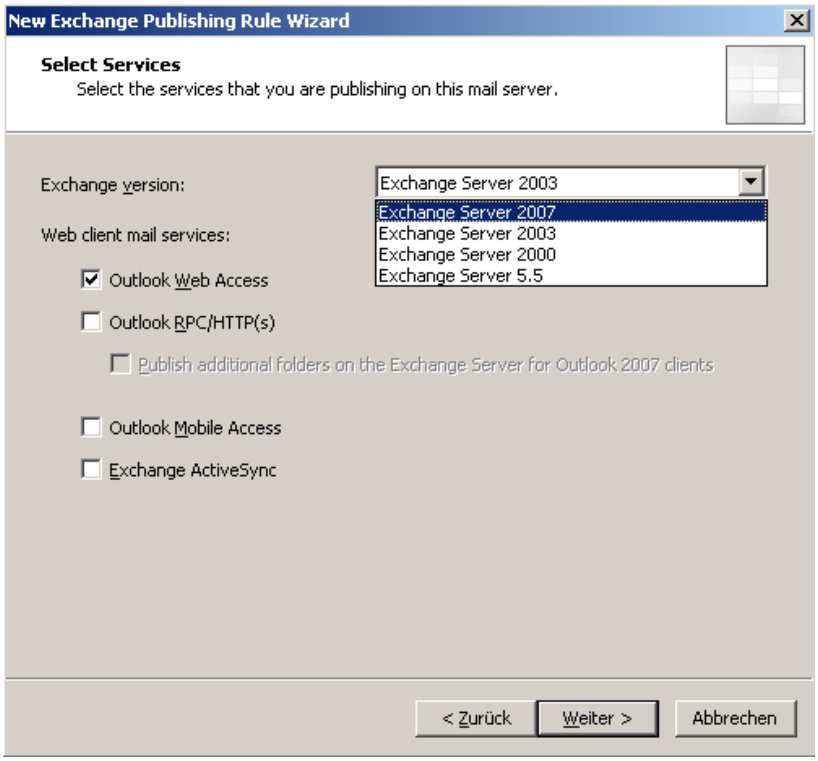

Figure 5: New OWA Publishing rule

Select *Publish a Single Website or load balancer*

In the next window of the Wizard select the option *Use SSL to connect to the published Web server or server farm.*

Enter the Name of the Internal Site Name. You can specify a NetBIOS servername or DNS FQDN.

Next you must enter the Public Name that Outlook Web Access users must use when they want to access the Outlook Web Access Server from the Internet. You can see the configuration in the next figure.

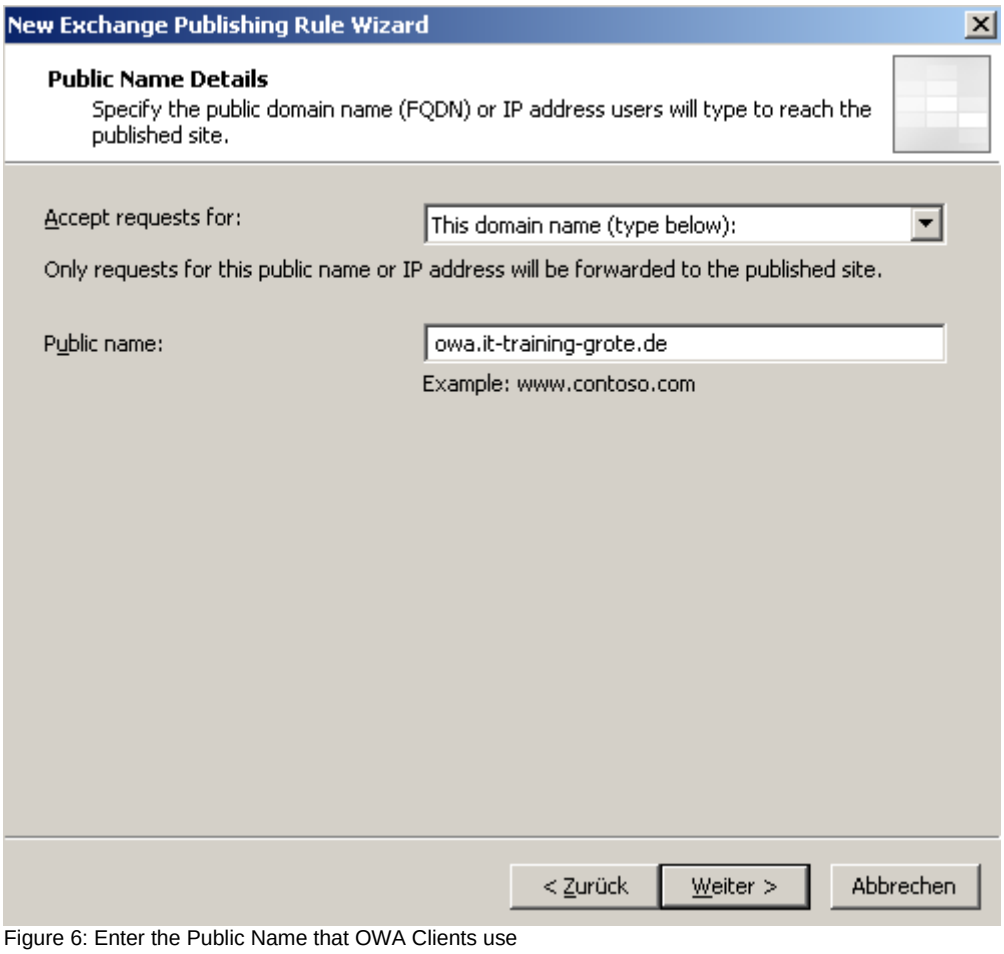

Figure 6: Enter the Public Name that OWA Clients use

New Weblistener

The next step in the wizard is to create a Weblistener. ISA Server uses Weblisteners to listen for incoming requests that matches the Listener settings. A Weblistener is the combination of an IP address, a Port and when you use SSL a certificate. You must give the Weblistener a unique name.

In the next window of the Wizard select *Require SSL secured connections with clients*.

You must specify the Web Listener IP Address. If the request comes from the Internet you must select the Network External. If your ISA Server has more than one IP Address bound to the External Network Interface you can select the IP Address used for Outlook Web Access.

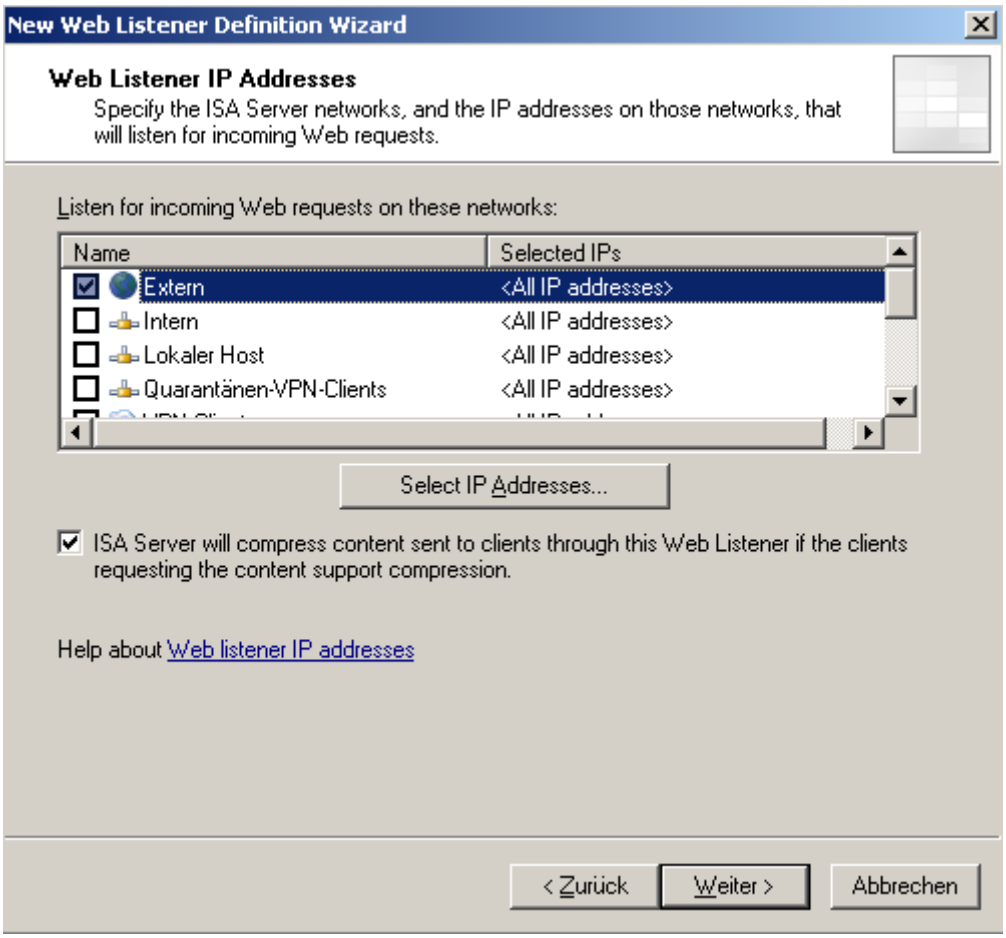

Figure 7: Specify the Weblistener network

Select the Certificate that you had requested from the internal CA server and click *Next*.

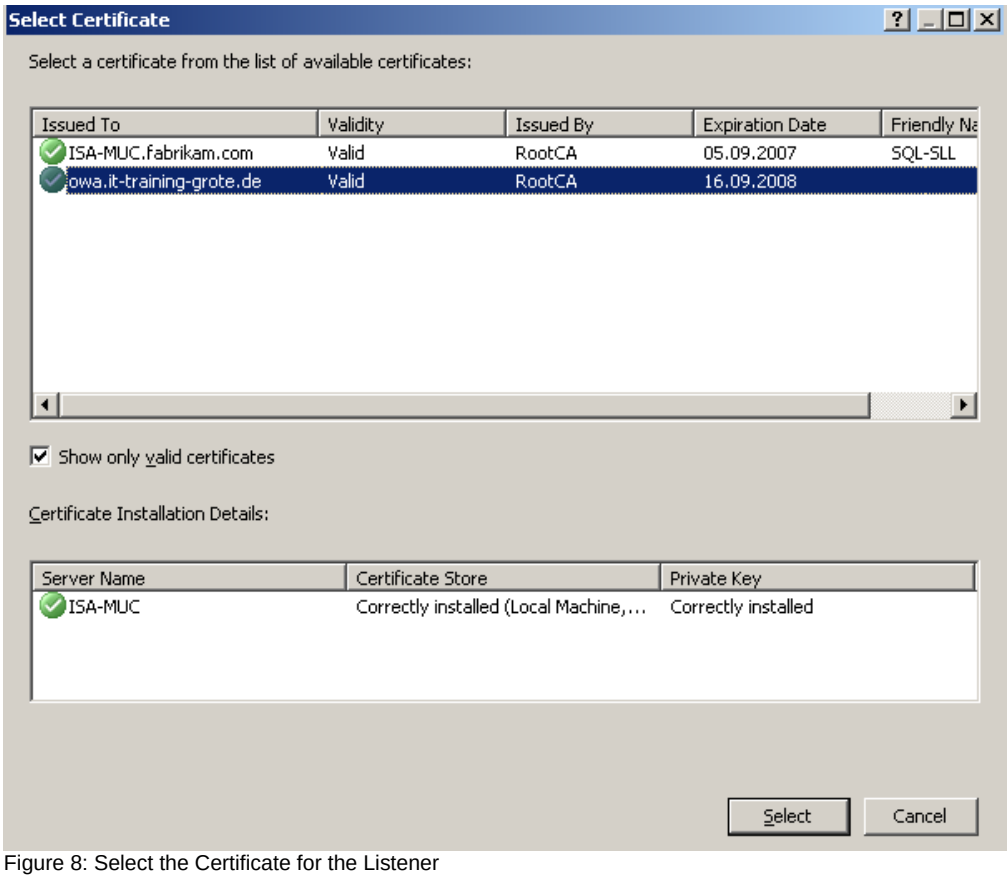

Figure 8: Select the Certificate for the Listener

Because we are using forms based Authentication with Outlook Web Access you must select *HTML Form Authentication* and Windows (Active Directory) for Authentication validation.

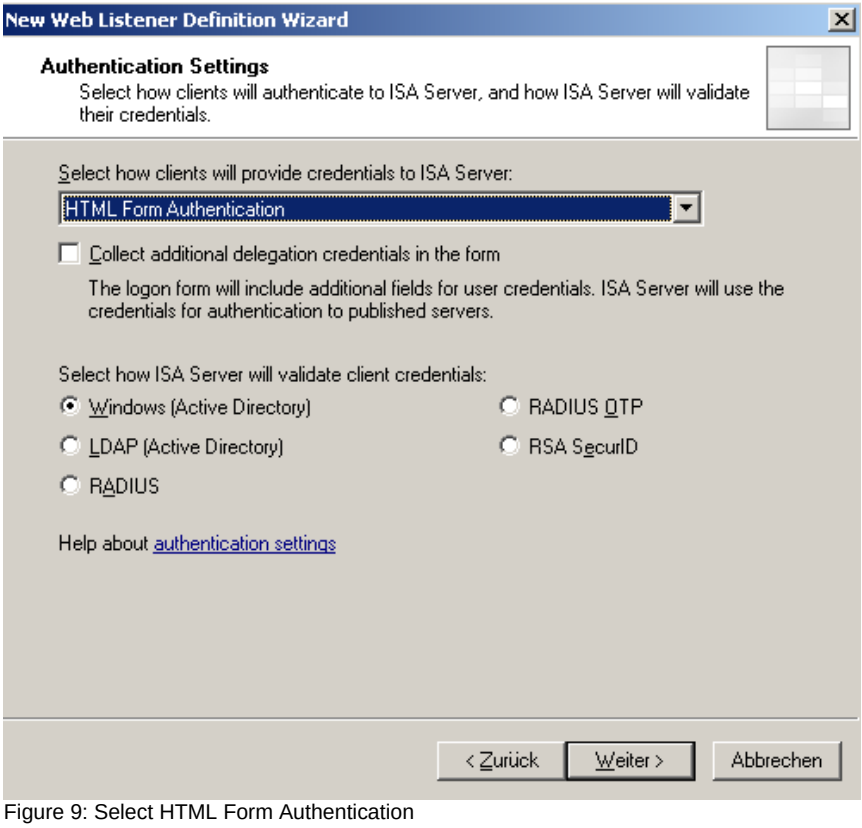

Figure 9: Select HTML Form Authentication

Single Sign ON (SSO) is one of the new features in ISA Server 2006 that allows clients to access different Published sites without the requirement of reauthentication. We don't need SSO in this example so you can disable it.
Select *Basic Authentication* because ISA Server will use this Authentication type to authenticate the Outlook Web Access clients to the published Exchange Server.

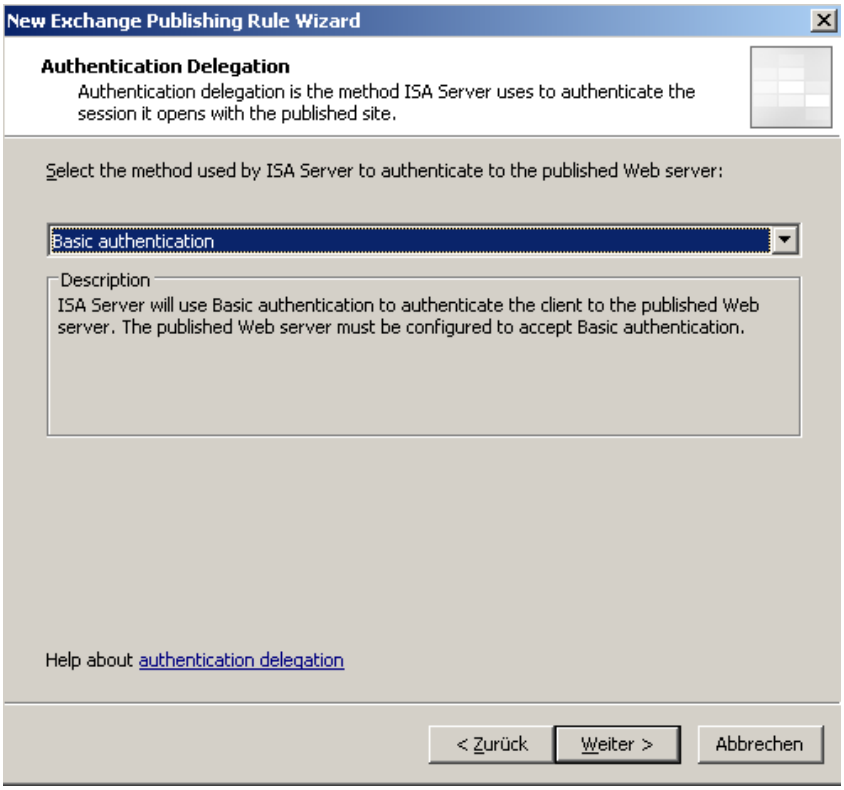

Figure 10: Authentication Delegation

The last step in the Wizard is to specify the user group for which the Firewall rule applies to. The default setting is "All Authenticated Users".

Finish the Wizard and Click *Apply* to save the settings.

After creating the OWA rule you should change some settings:

- Change "Requests appears to come from the original Client" in the "To" Tab
- Enable "Require 128 Bit encryption for HTTPS Traffic" in the "Traffic" Tab

Navigate to the Listener Properties and select the *Forms* tab. Under Password Management enable *Allow users to change their Passwords*.

Test the Client Connection

After successfully configuring Exchange Server 2007 and the Exchange-Webclient Publishing rule you can test the connection from one of your clients. For this article the client is a Windows XP Service Pack 2 machine.

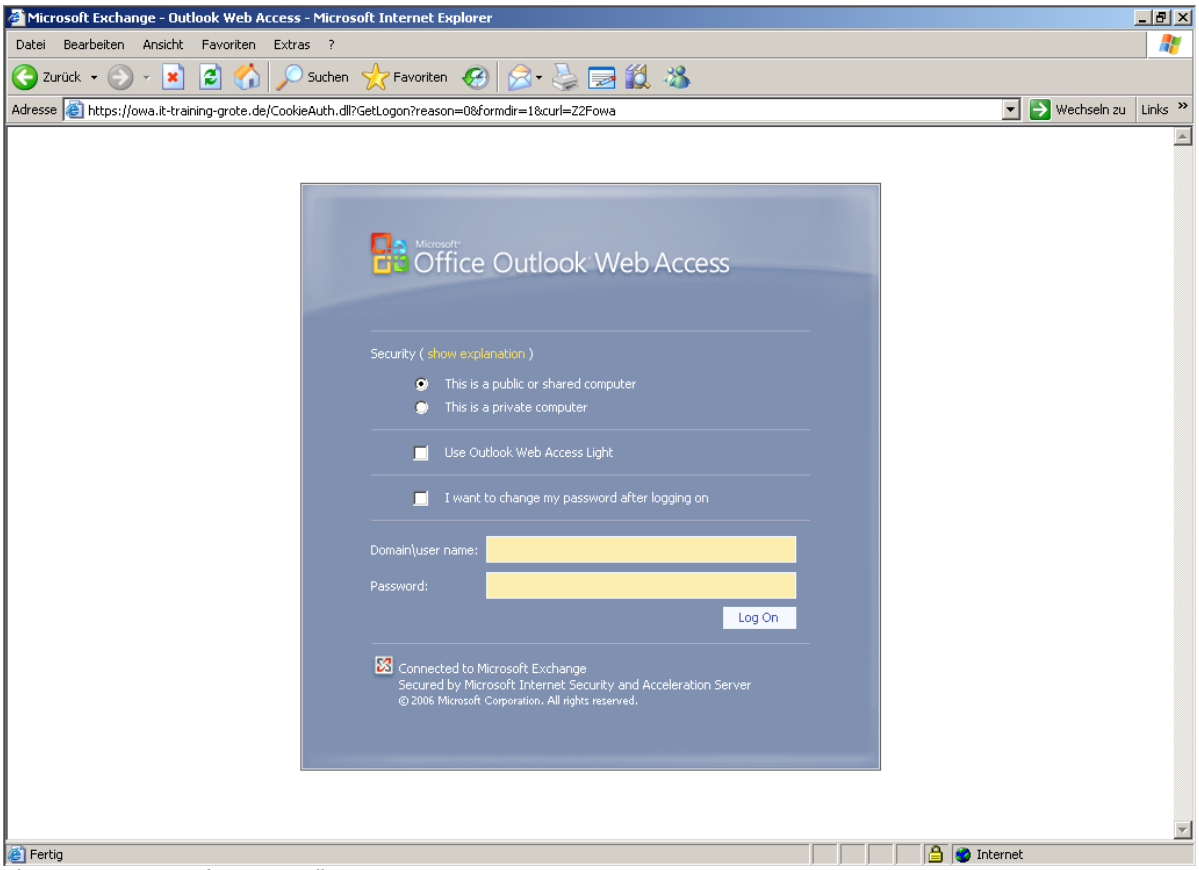

Figure 11 OWA FBA from a XP client

Conclusion

Exchange Server 2007 is a great product with several new functions. The changes in Outlook Web Access (OWA) are significantly. From the option to specify the language of Outlook Web Access during OWA logon to the option to specify different Out of Office messages for internal and external users to the option to block some file type from access through OWA. Outlook Web Access publishing with ISA Server 2006 is the ideal combination if you want to give your users secure access from anywhere in the world.

Related Links

Using ISA Server 2006 for Outlook Web Access
http://www.microsoft.com/technet/prodtechnol/exchange/E2k7Help/1a0bd5c6-fad7-49ec-9834-99be3fc115ed.mspx?mfr=true
What's New and Improved in ISA Server 2006
http://www.microsoft.com/isaserver/prodinfo/whatsnew.mspx
Exchange Server 2007 Beta 2 Technical Library
http://www.microsoft.com/technet/prodtechnol/exchange/2007/library/default.mspx
Exchange Server 2007 Beta 2 Product Overview
http://www.microsoft.com/exchange/preview/evaluation/overview.mspx