

## **Microsoft Sharepoint Server 2010 und Forefront TMG – Authentifizierungsoptionen**

Forefront TMG und Microsoft Sharepoint kommen mit einer Vielzahl von Authentifizierungsoptionen wie:

- NTLM
- Negotiate
- Kerberos (KCD)
- Basic Authentication
- FBA
- SSL Client Certificates
- SSO

Dieser Artikel beschreibt folgende Authentifizierungsmöglichkeiten in der Kombination Sharepoint / TMG:

- TMG Forms Based Authentication
- TMG Authentication mit Kerberos Constrained Delegation
- TMG SSL Client Certificate Authentication
- TMG keine Authentifizierung – Authentifizierung am Sharepoint Server

### **FBA**

Die Forms Based Authentication von Sharepoint Server 2010 ist ein Sonderfall in der Kombination mit Forefront TMG, da Forefront TMG standardmaessig durch den Assistenten ebenfalls eine FBA verwendet. Sharepoint Server 2010 hat als standardmaessigen Authentifizierungsprovider nur die Windows Authentication. Wie man das auf Sharepoint FBA aendern kann, steht zum Beispiel hier:

Configure Forms Based Authentication (FBA) with Sharepoint 2010

<http://blogs.technet.com/b/mahesm/archive/2010/04/07/configure-forms-based-authentication-fba-with-sharepoint-2010.aspx>

Weitere Infos findet man auch in einem Artikel von Frank Geisler und mir im Sharepoint Magazin (Ausgabe Januar 2011)

[www.sharepoint-magazin.de](http://www.sharepoint-magazin.de)

### **Sharepoint und ADFS**

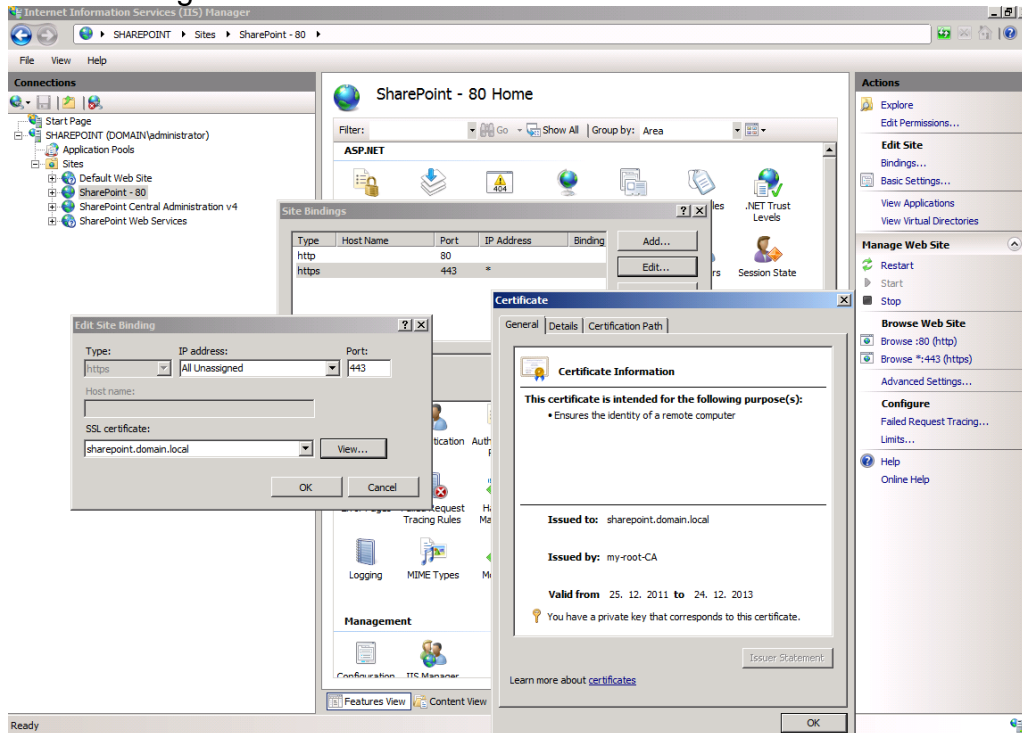
Ein weiterer "Spezialfall" ist die Verwendung von TMG+Sharepoint und ADFS. Wie das funktioniert zeigt Thorsten Pape eindrucksvoll in dieser Anleitung:

TMG + Sharepoint + ADFS!...

<http://blog.forefront-tmg.de/?p=562>

## SSL fuer den internen Sharepoint Server

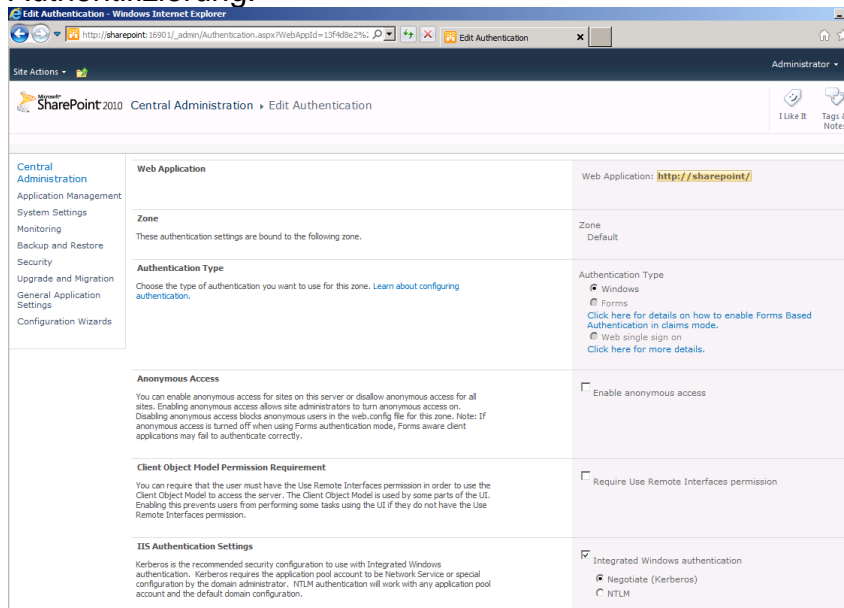
Standardmaessig existiert kein SSL Zertifikat auf dem Sharepoint Server. Idealerweise erstellt man ein Zertifikat fuer Webserverbindungen von einer internen Zertifizierungsstelle.



Das Zertifikat muss den internen DNS FQDN des Sharepoint Servers enthalten, wie der Name auch in der Sharepoint TMG Publishing Regel verwendet wird. Das Zertifikat muss auf die Sharepoint Webseite gebunden werden.

## Authentifizierung am Sharepoint

Standardmaessig unterstuetzt der Sharepoint Server die Windows integrierte Authentifizierung.



Fuer eine neue Sharepoint Website kann die Claims Based Authentication verwendet werden.

**Create New Web Application**

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

OK Cancel

**Authentication**

Select the authentication for this web application.

[Learn about authentication.](#)

Claims Based Authentication  
 Classic Mode Authentication

**IIS Web Site**

Choose between using an existing IIS web site or create a new one to serve the Microsoft SharePoint Foundation application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

Use an existing IIS web site  
Default Web Site

Create a new IIS web site

Name  
SharePoint - 22911

Port  
22911

Host Header

Path  
C:\inetpub\wwwroot\wss\VirtualDirecto

**Security Configuration**

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

Yes  
 No

Use Secure Sockets Layer (SSL)

Yes  
 No

... und somit auch die Forms Based Authentication fuer die Sharepoint Site

**Create New Web Application**

**Claims Authentication Types**

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

Trusted Identity Provider Authentication enables federated users in this Web application. This authentication is Claims token based and the user is redirected to a login form for authentication.

[Learn about configuring authentication.](#)

Enable Windows Authentication

Integrated Windows authentication  
NTLM

Basic authentication (credentials are sent in clear text)

Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

ASP.NET Role manager name

Trusted Identity provider

There are no trusted identity providers defined.

Sign In Page URL

## TMG Publishing

Weitere Informationen zur Sharepoint Veröffentlichung ueber ISA/TMG:

<http://technet.microsoft.com/en-us/library/cc984488.aspx>

<http://www.isaserver.org/tutorials/How-to-Publish-Microsoft-Sharepoint-Service-ISA-Server-2006.html>

Der Klassische Wizard


Kein SSL vom TMG zum internen Sharepoint Server

**New SharePoint Publishing Rule Wizard**

**Server Connection Security**  
Choose the type of connections Forefront TMG will establish with the published Web server or server farm.

Use SSL to connect to the published Web server or server farm  
Forefront TMG will connect to the published Web server or server farm using HTTPS (recommended).

Use non-secured connections to connect the published Web server or server farm  
Forefront TMG will connect to the published Web server or server farm using HTTP.

 When Forefront TMG authenticates to the published server on behalf of the client, user credentials may be sent over the network in clear text. Authentication using SSL will help protect client credentials.

< Back   Next >   Cancel

HTML Form Authentication

**New Web Listener Definition Wizard**

**Authentication Settings**  
Select how clients will authenticate to Forefront TMG, and how Forefront TMG will validate their credentials.

Select how clients will provide credentials to Forefront TMG:  
HTML Form Authentication

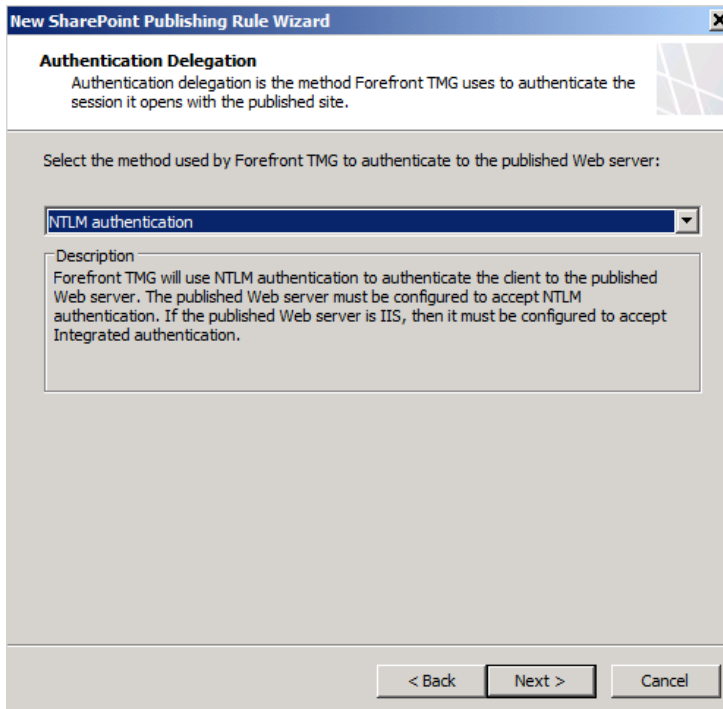
Collect additional delegation credentials in the form  
The logon form will include additional fields for user credentials. Forefront TMG will use the credentials for authentication to published servers.

Select how Forefront TMG will validate client credentials:

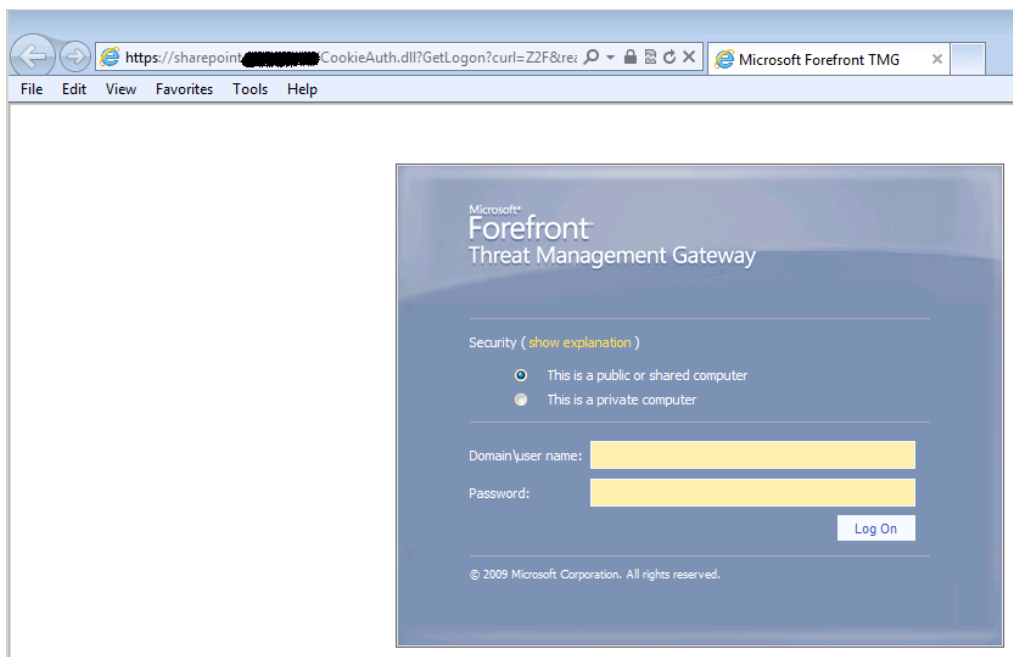
Windows (Active Directory)    RADIUS OTP  
 LDAP (Active Directory)    RSA SecurID  
 RADIUS

< Back   Next >   Cancel

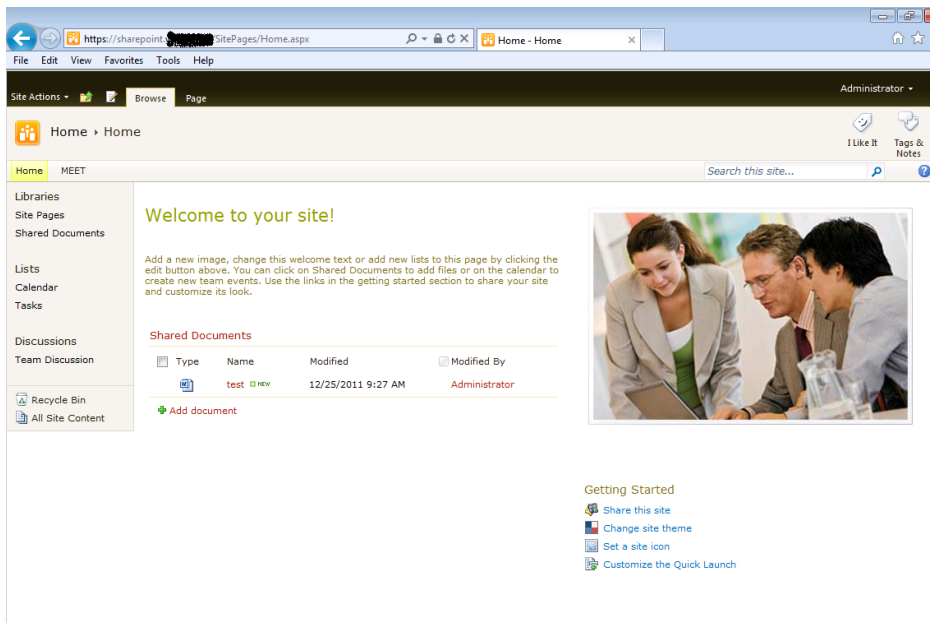
## NTLM Authentication



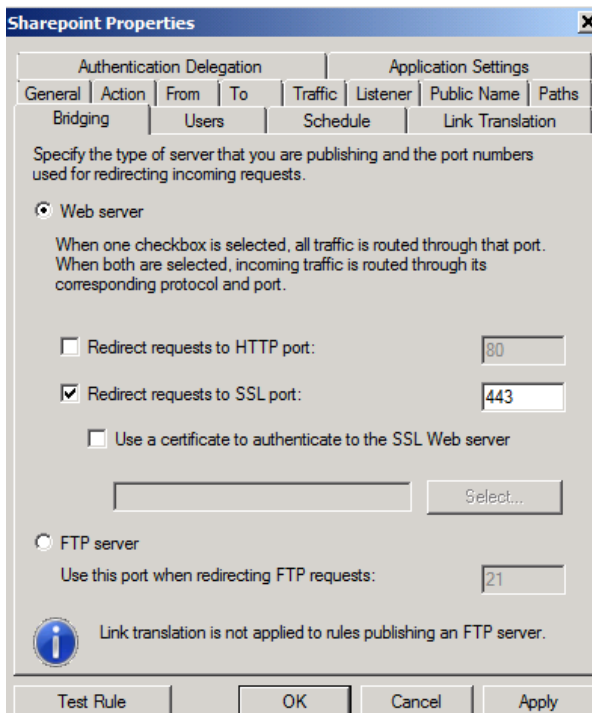
So sieht es am Client aus (FBA kommt von TMG)



## Alles prima



Aendern der Publishing Rule am TMG, dass der Sharepoint Server vom TMG aus per HTTPS erreichbar ist

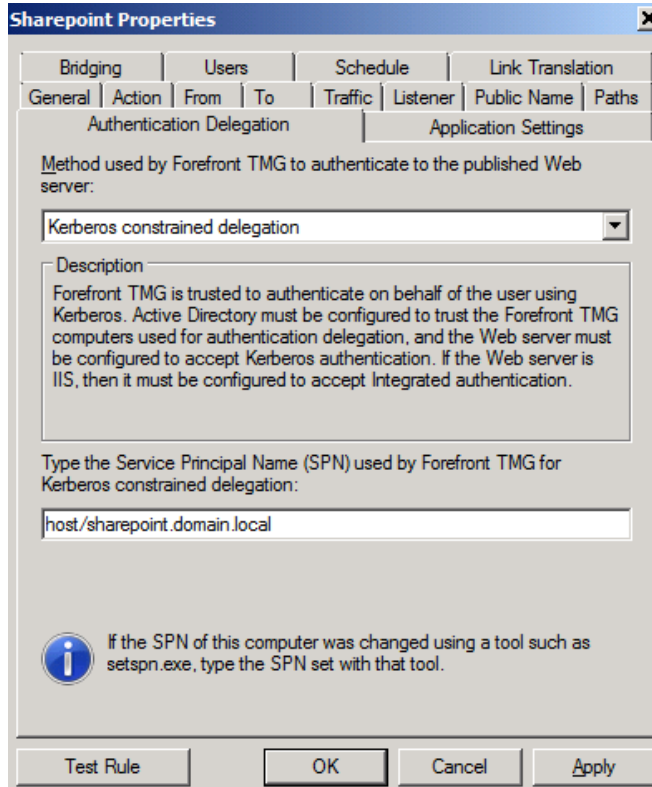


**Anmerkung:** Dazu muss am Sharepoint Server ein Webserver Zertifikat von einer Trusted CA ausgestellt werden, welcher den internen DNS FQDN des Sharepoint Servers enthaelt und im IIS muss das Binding fuer die Sharepoint Sites um HTTPS erweitert werden.

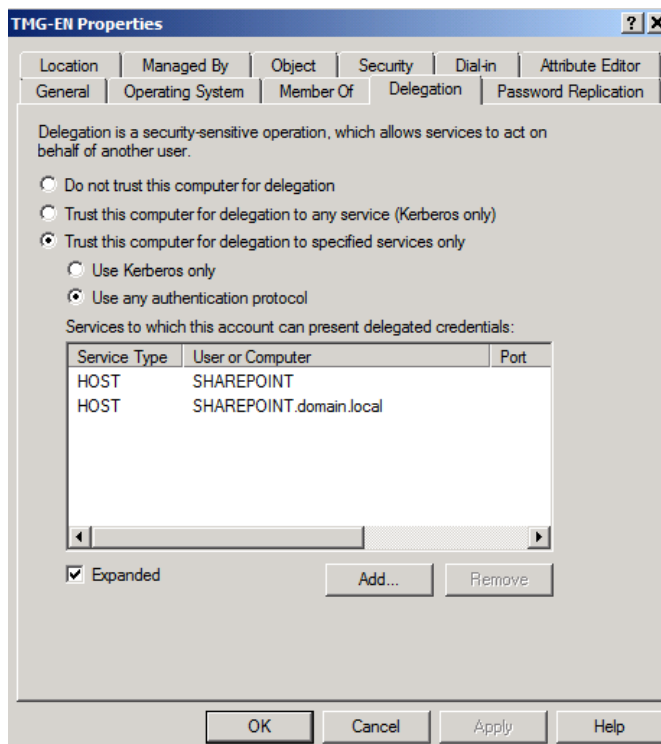
## Forefront TMG und Sharepoint Publishing ohne FBA

Verwendung von Kerberos Constrained Delegation

**Achtung:** Setzt TMG Domaenenmitgliedschaft voraus!

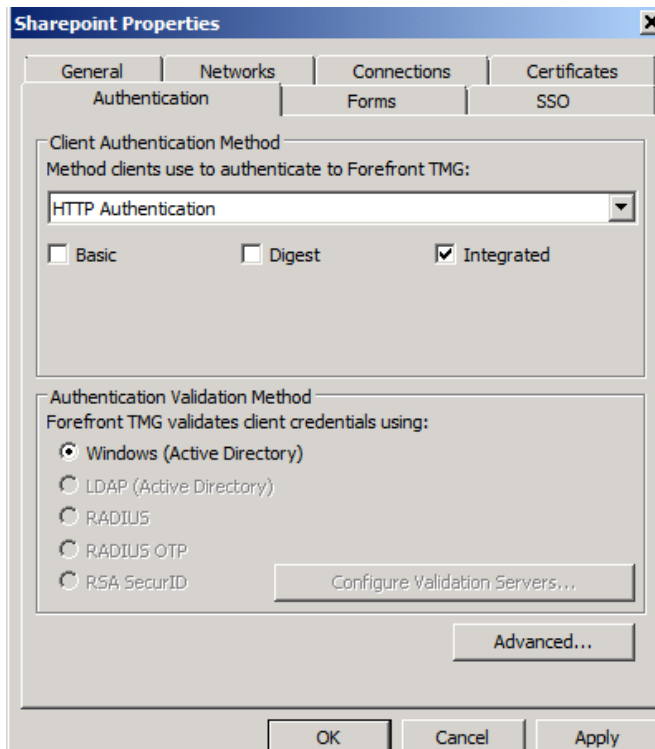


TMG im AD fuer Kerberos Delegation zum Sharepoint Server erlauben

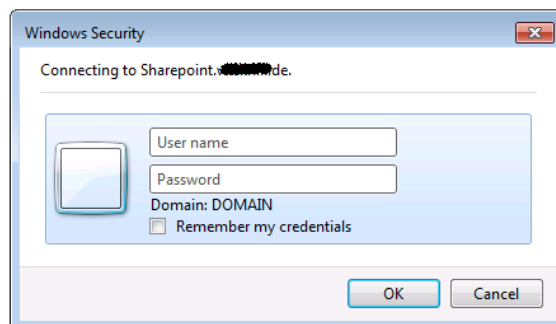
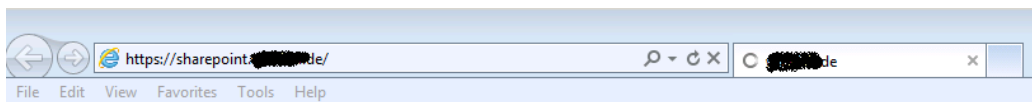


## Aendern des TMG Listeners fuer integrierte Authentifizierung ueber HTTP

**Achtung:** Setzt TMG Domaenenmitgliedschaft voraus!



Ergebnis am Client aus dem Internet

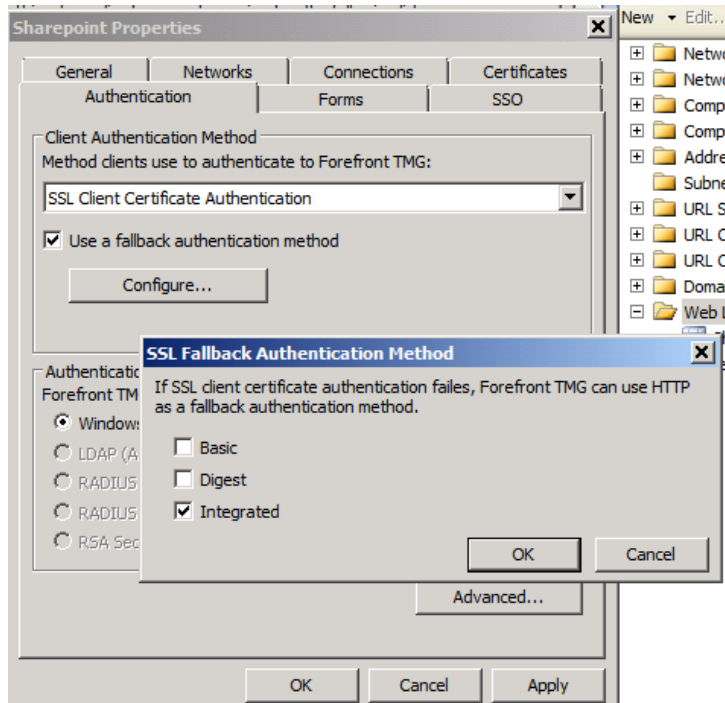




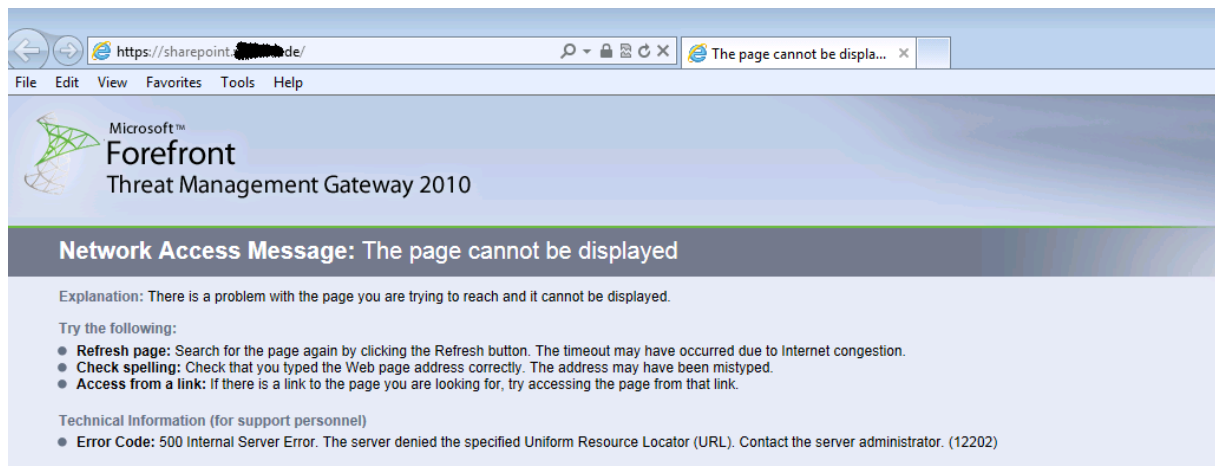
## SSL Client Certificate Authentication

**Achtung:** Setzt TMG Domaenenmitgliedschaft voraus!

Fuer Clients ohne Zertifikat kann ein Fallback auf Kennwort basierte Authentifizierung verwendet werden.

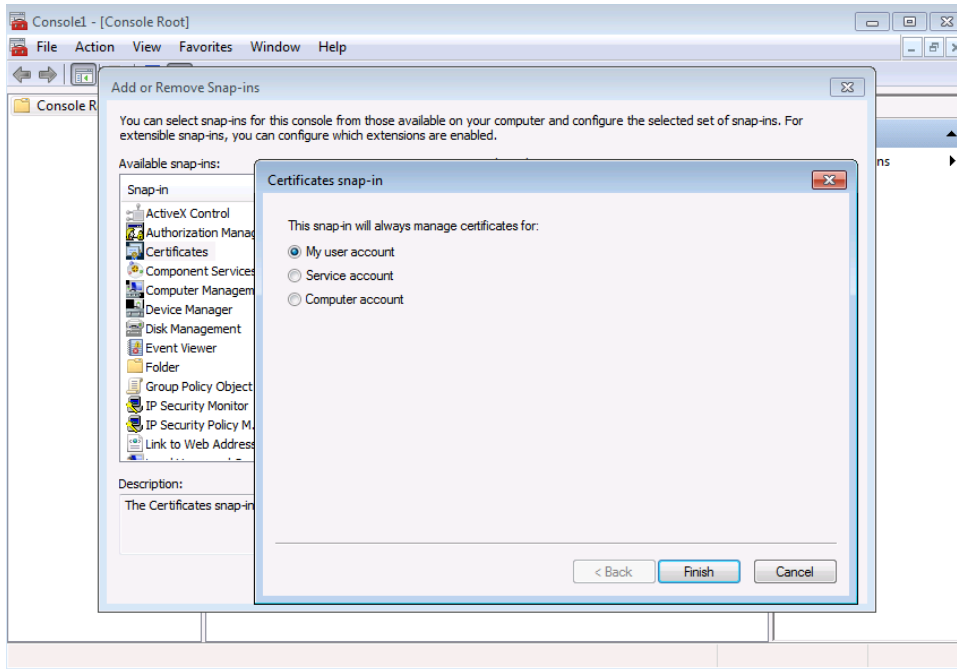


Fehlermeldung am Client wenn **kein** Fallback im TMG Listener konfiguriert ist und der Benutzer kein Zertifikat zur Authentifizierung hat

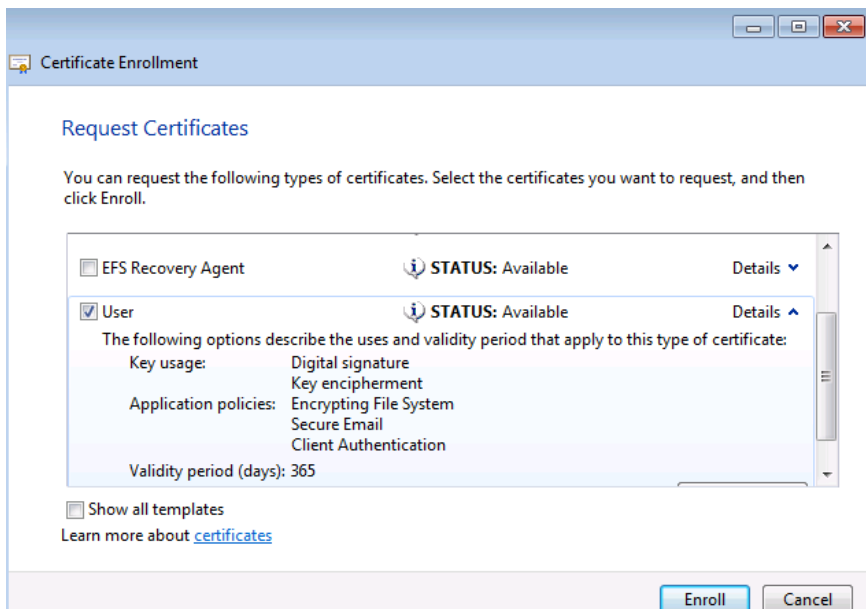


## Neues Zertifikat fuer den Benutzer

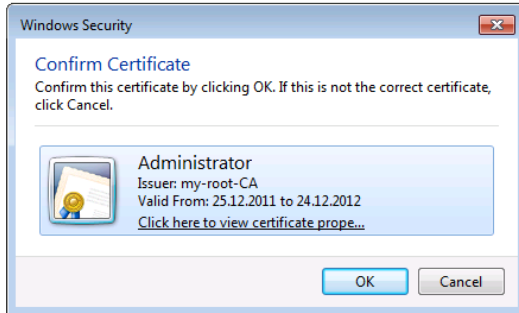
Als naechstes muss ein Benutzerzertifikat von der internen Zertifizierungsstelle fuer die Sharepoint Benutzer ausgestellt werden. Das Zertifikat MUSS fuer den Benutzer ausgestellt und in den lokalen Zertifikatspeicher des Benutzers importiert/angefordert werden.



## Anforderung eines Zertifikats fuer den Benutzer

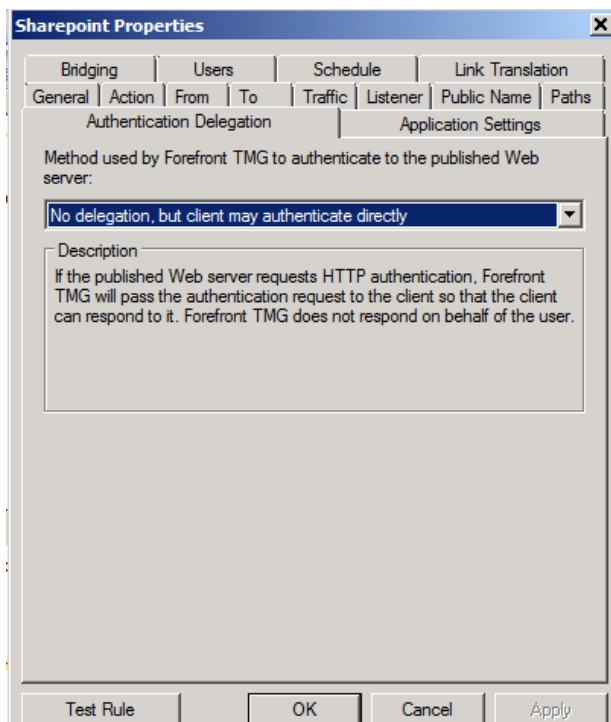


## Anmeldung an der Sharepoint Site mit Hilfe des Benutzer Zertifikats

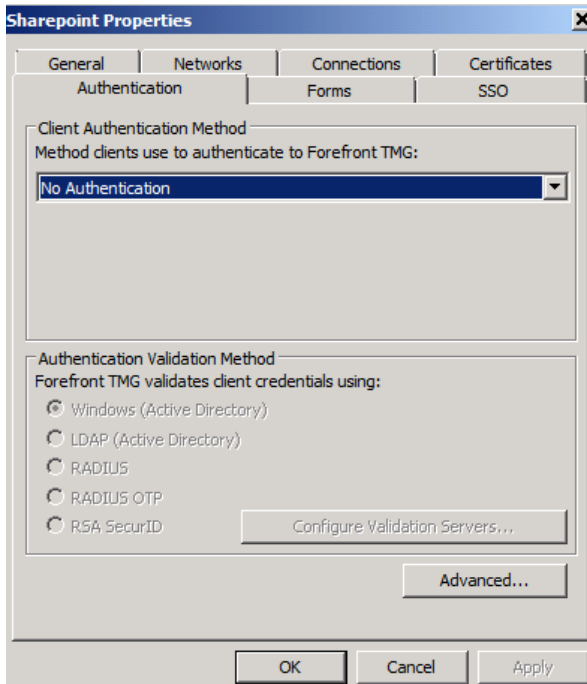


## Verlagerung der Authentifizierung lediglich auf den Sharepoint Server

In diesem Fall findet am Forefront TMG Server keine Praeauthentifizierung statt. Aenderung der Authentifizierungsdelegation auf „No delegation, but client may authenticate directly“.



## Aenderung des Sharepoint Listeners am Forefront TMG Server auf „No Authentication“



## Aenderung der Benutzerverifikation in der TMG Publishing Rule

Die Gruppe Sharepoint (welche eine AD Gruppe darstellt) muss durch den TMG Benutzersatz „Alle Benutzer“ ausgetauscht werden, da die Authentifizierung direkt am Sharepoint Server statt findet

