**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 Authentifizierungsmoeglichkeiten 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

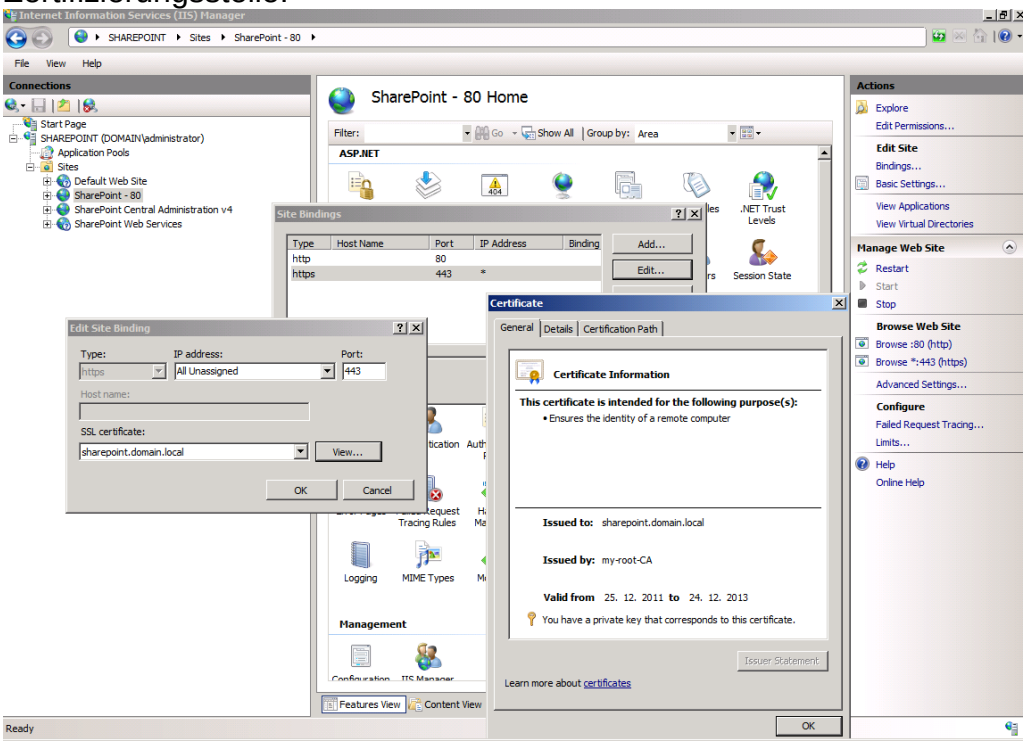
**Sharepoint und ADFS**

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

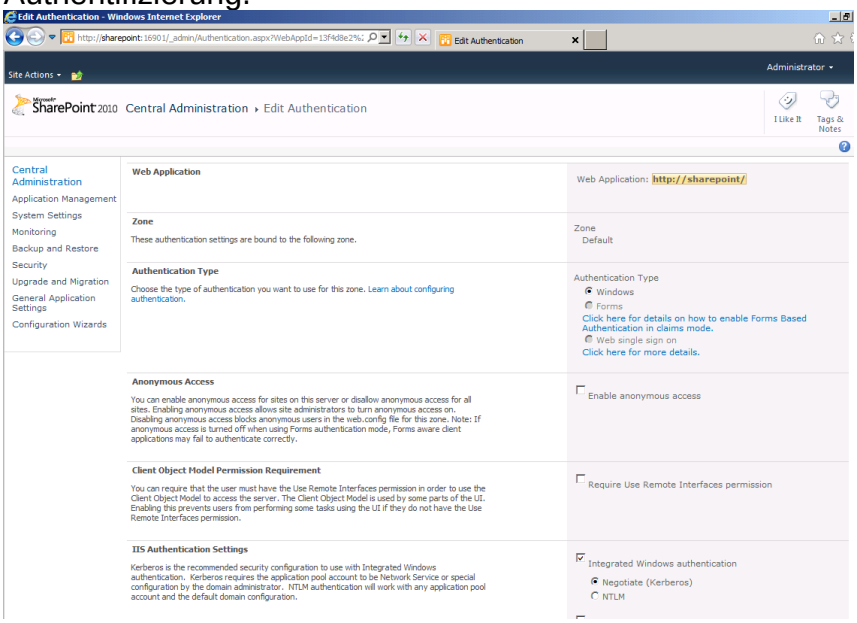
Standardmaessig existiert kein SSL Zertifikat auf dem Sharepoint Server. Idealerweise erstellt man ein Zertifikat fuer Webserverbindungen von einer internen Zertifizierungsstelle.



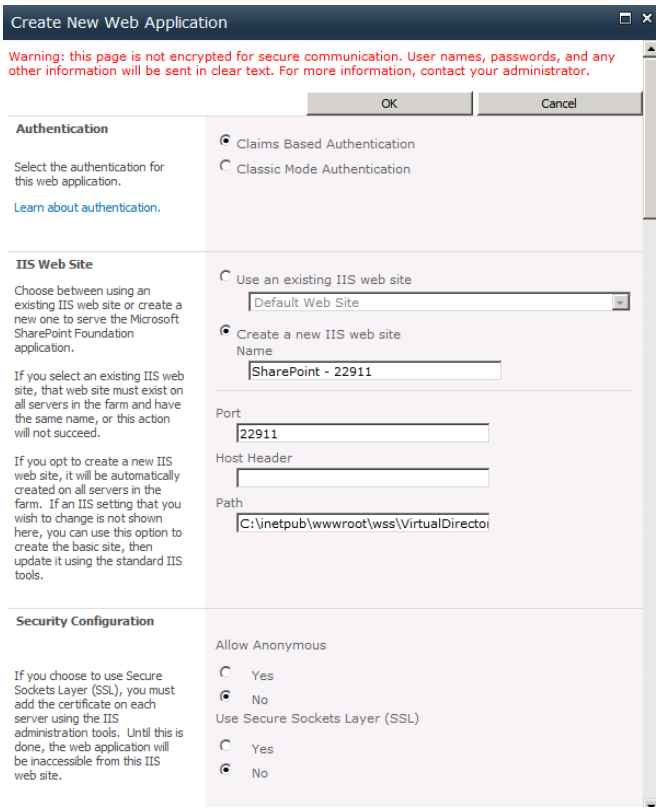

Das Zertifikat muss den internen DNS FQDN des Sharepoint Servers enthalten, wie der Name auch in der Sharepoint TMG Publishing Regel verwendet wird. Das Zertifikat muss auf die Sharepoint Webseite gebunden werden.

## Authentifizierung am Sharepoint

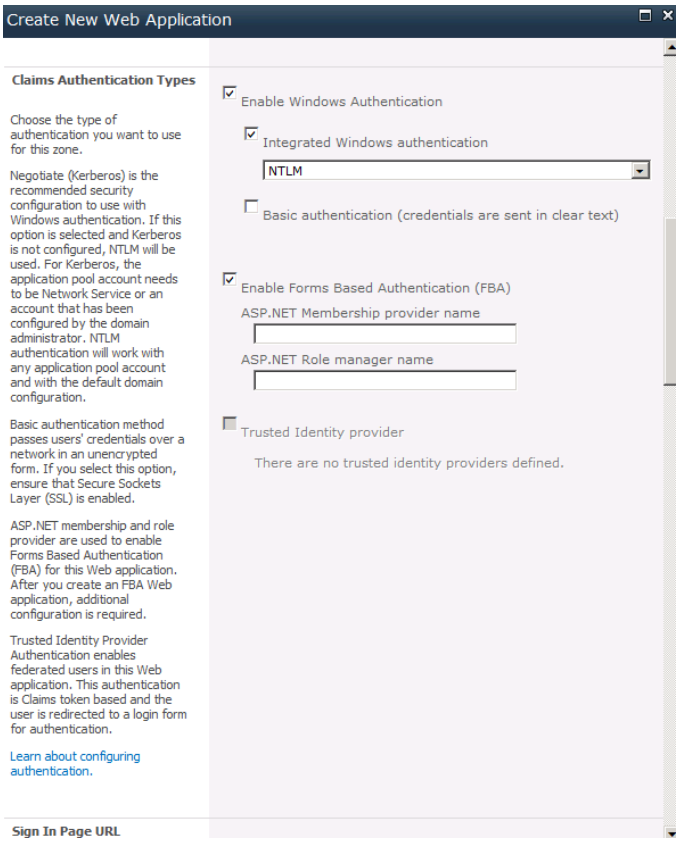
Standardmaessig unterstuetzt der Sharepoint Server die Windows integrierte Authentifizierung.



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




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

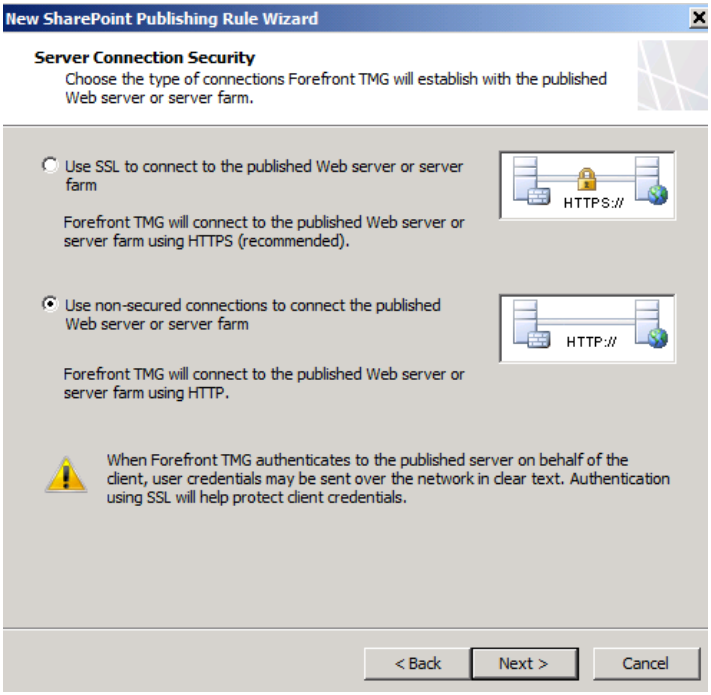


**TMG Publishing**

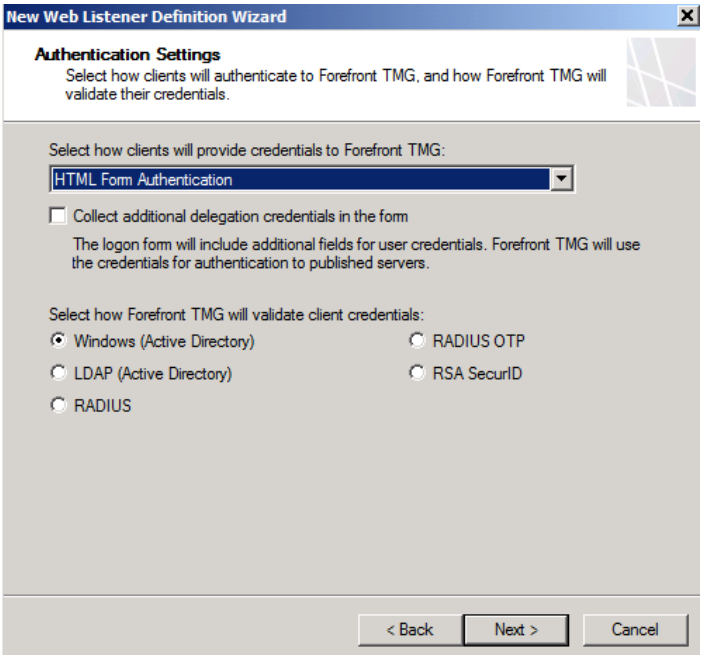
Weitere Informationen zur Sharepoint Veroeffentlichung ueber ISA/TMG:
http://technet.microsoft.com/en-us/library/cc984488.aspx
http://www.isaserver.org/tutorials/How-to-Publish-Microsoft-Sharepoint-Service-ISA-Server-2006.html

Der Klassische Wizard

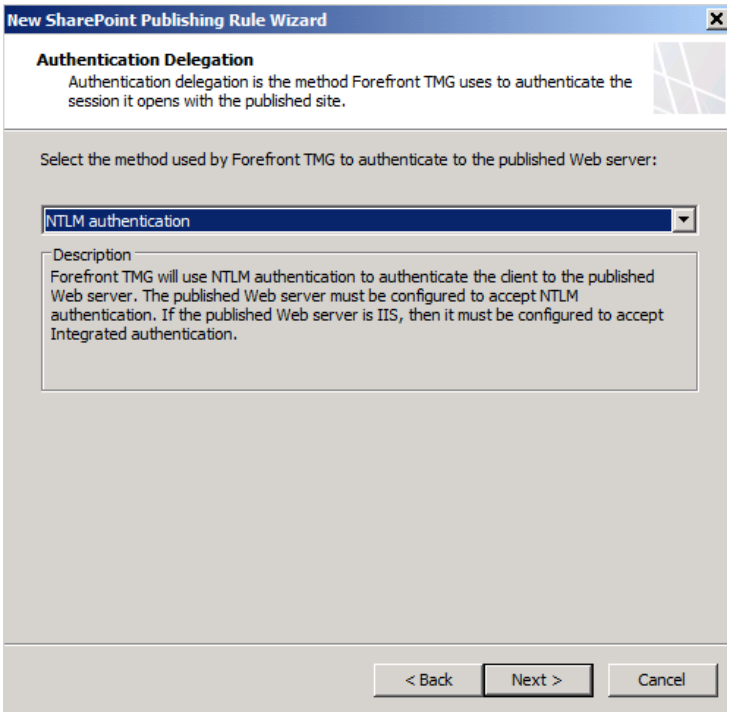
**Kein** SSL vom TMG zum internen Sharepoint Server



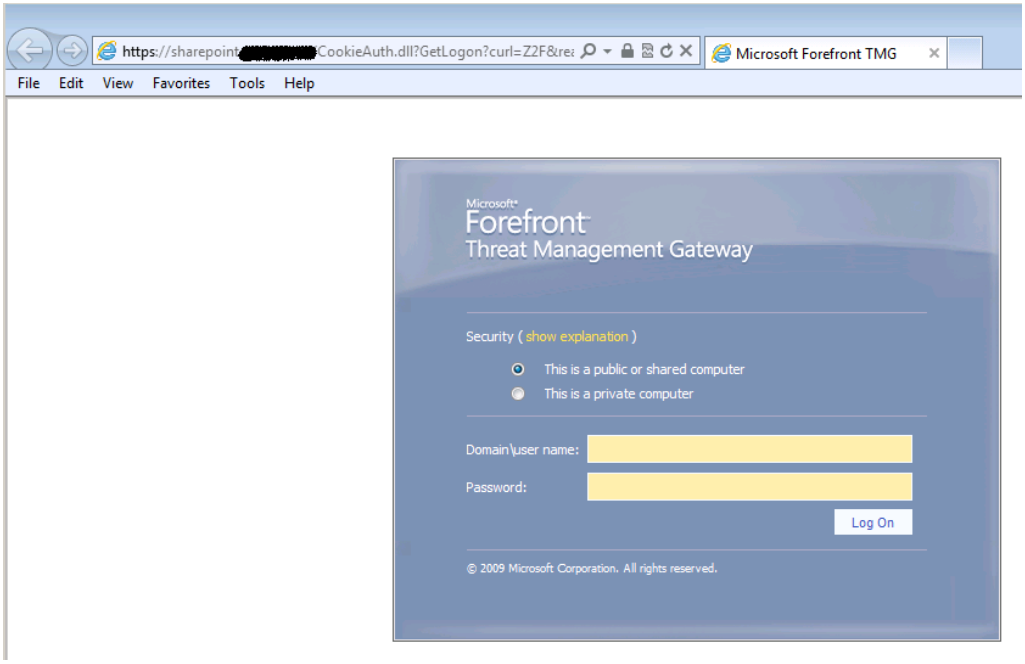

HTML Form Authentication



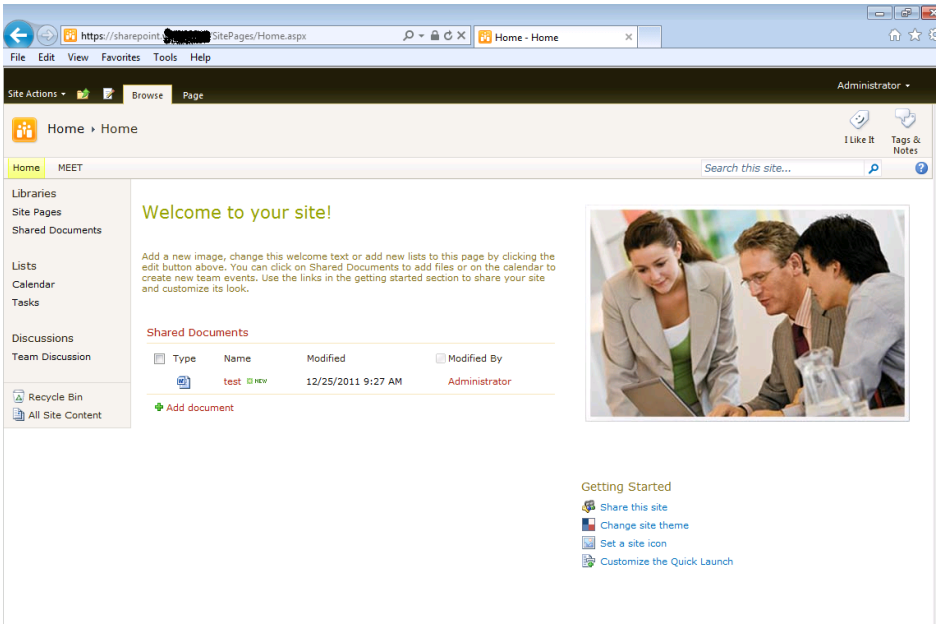
NTLM Authentication



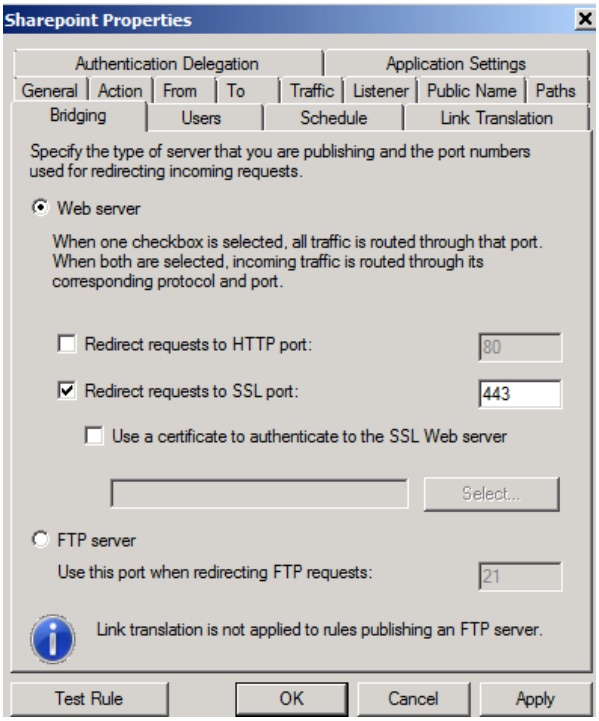

So sieht es am Client aus (FBA kommt von TMG)



Alles prima




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

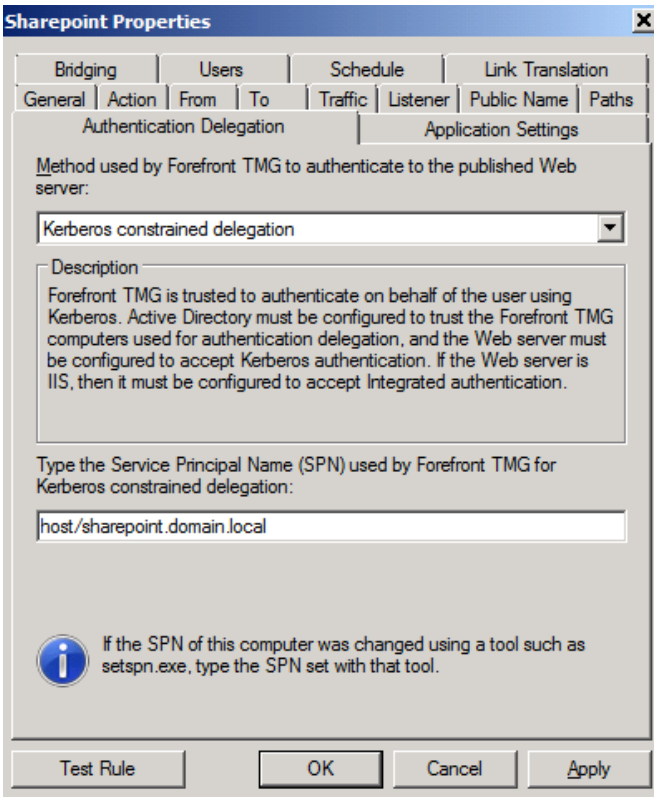



**Anmerkung**: Dazu muss am Sharepoint Server ein Webserver Zertifikat von einer Trusted CA ausgestellt werden, welcher den internen DNS FQDN des Sharepoint Servers enthaelt und im IIS muss das Binding fuer die Sharepoint Sites um HTTPS erweitert werden.

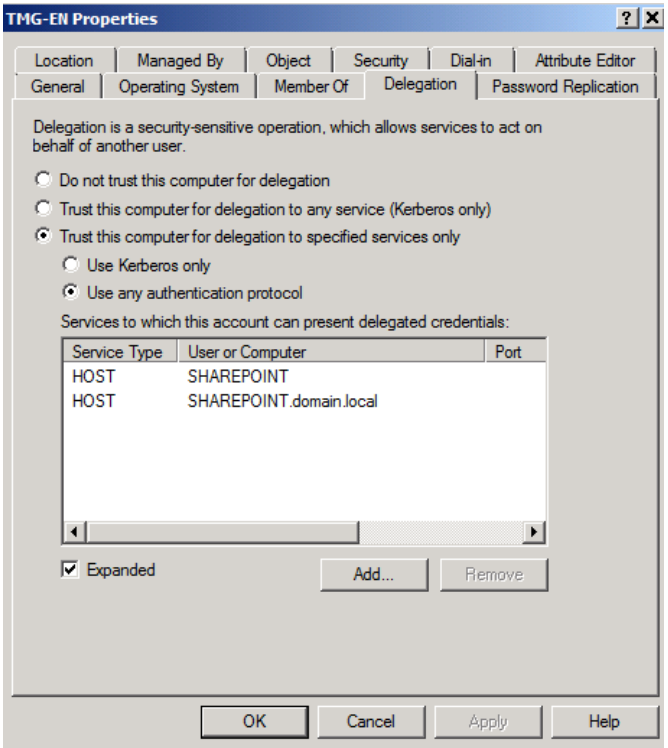
**Forefront TMG und Sharepoint Publishing ohne FBA**

Verwendung von Kerberos Constrained Delegation

**Achtung**: Setzt TMG Domaenenmitgliedschaft voraus!

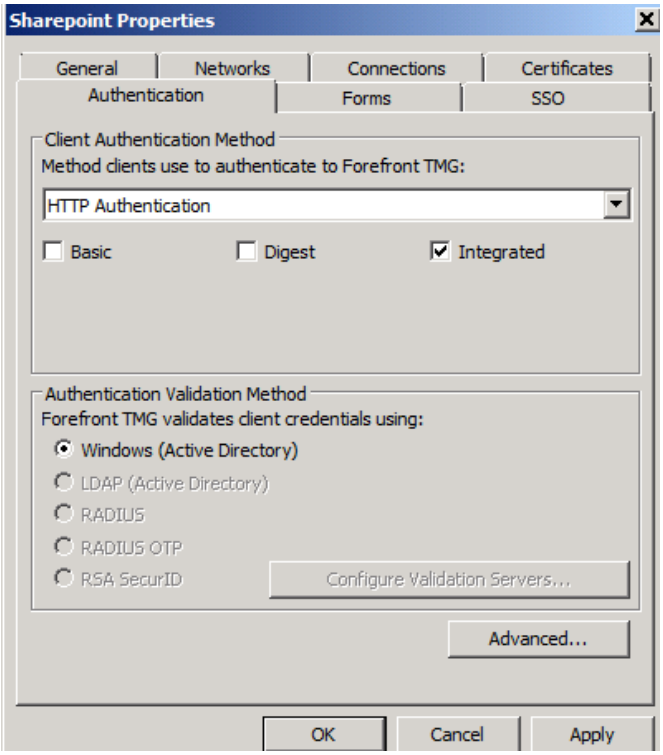



TMG im AD fuer Kerberos Delegation zum Sharepoint Server erlauben

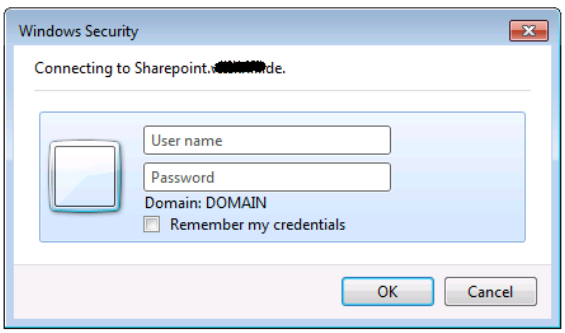


**Aendern des TMG Listeners fuer integrierte Authentifizierung ueber HTTP**

**Achtung**: Setzt TMG Domaenenmitgliedschaft voraus!

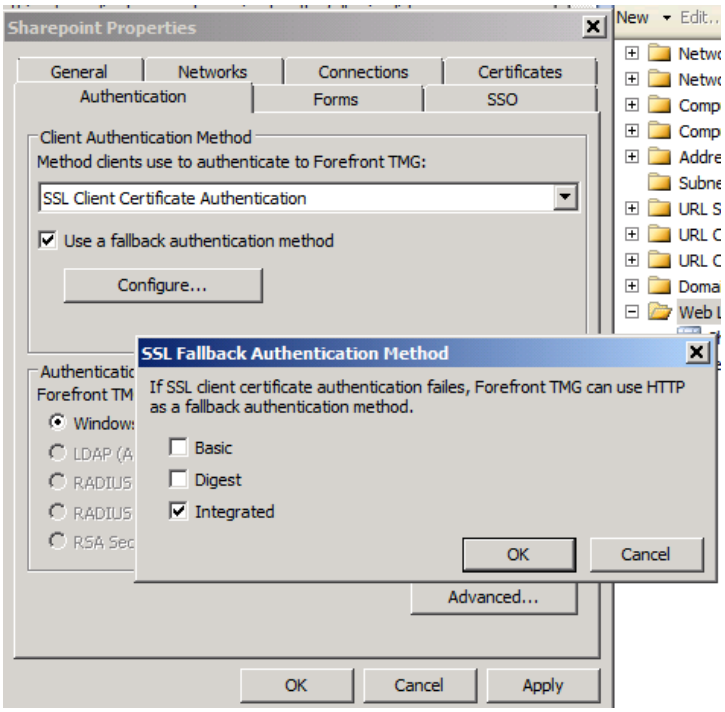



Ergebnis am Client aus dem Internet

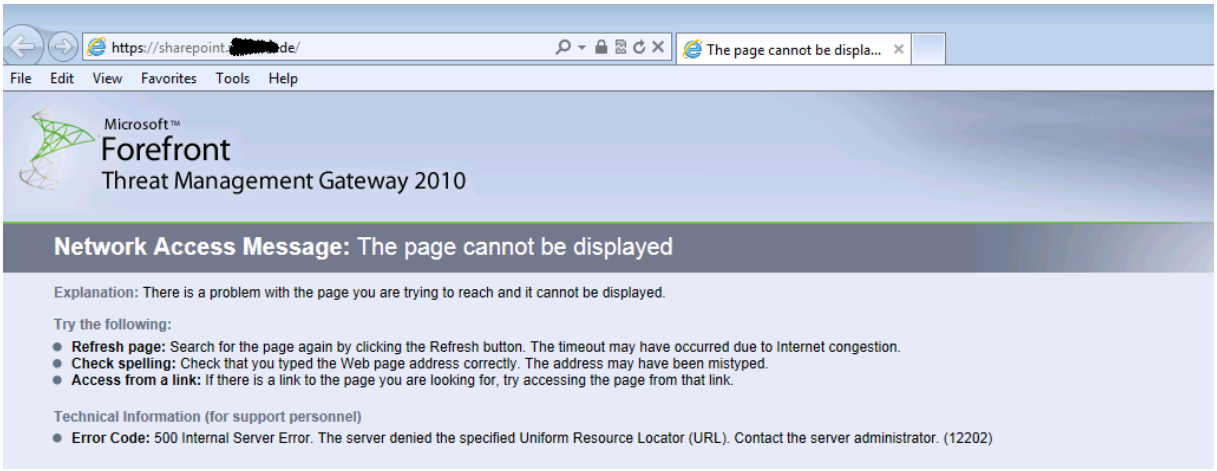



SSL Client Certificate Authentication

**Achtung**: Setzt TMG Domaenenmitgliedschaft voraus!
Fuer Clients ohne Zertifikat kann ein Fallback auf Kennwort basierte Authentifizierung verwendet werden.

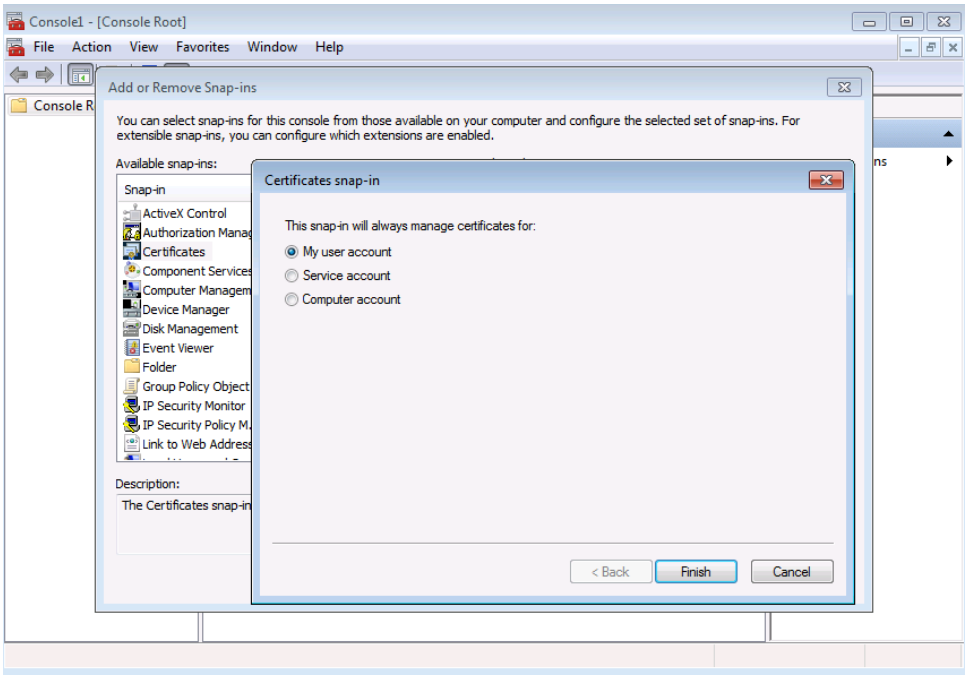



Fehlermeldung am Client wenn **kein** Fallback im TMG Listener konfiguriert ist und der Benutzer kein Zertifikat zur Authentifizierung hat

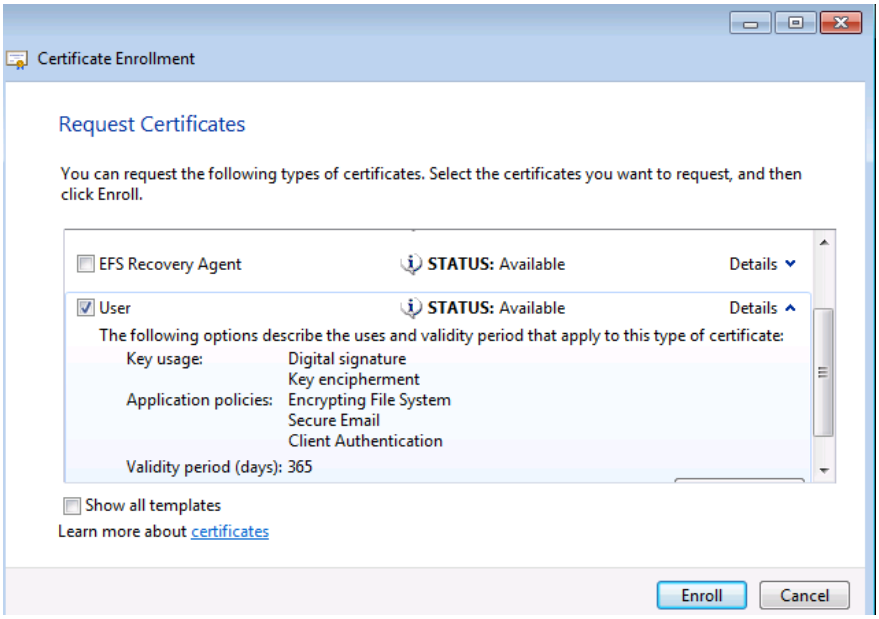


## Neues Zertifikat fuer den Benutzer

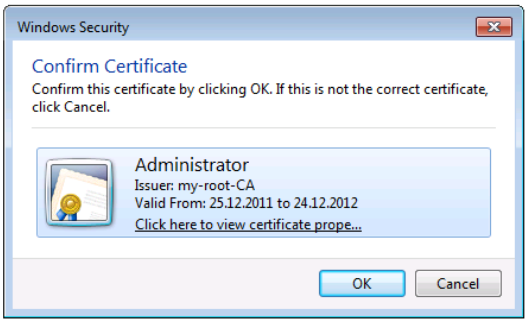
Als naechstes muss ein Benutzerzertifikat von der internen Zertifizierungsstelle fuer die Sharepoint Benutzer ausgestellt werden. Das Zertifikat MUSS fuer den Benutzer ausgestellt und in den lokalen Zertifikatspeicher des Benutzers importiert/angefordert werden.




Anforderung eines Zertifikats fuer den Benutzer

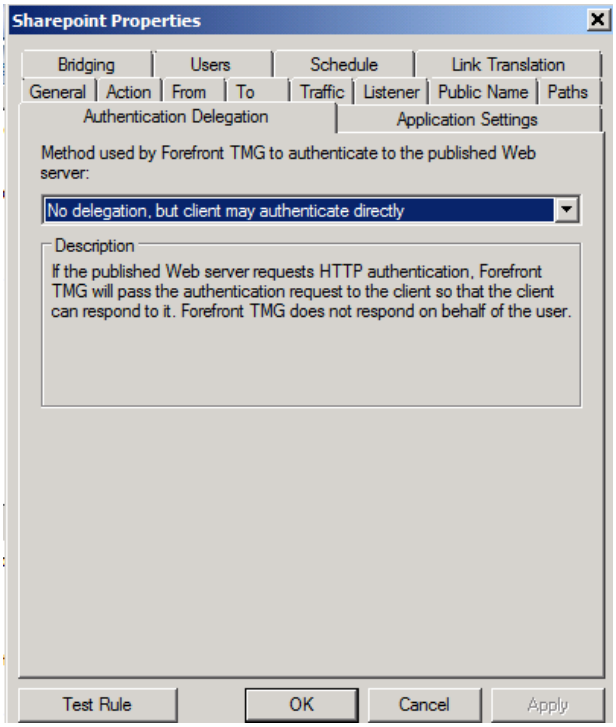


## Anmeldung an der Sharepoint Site mit Hilfe des Benutzer Zertifikats

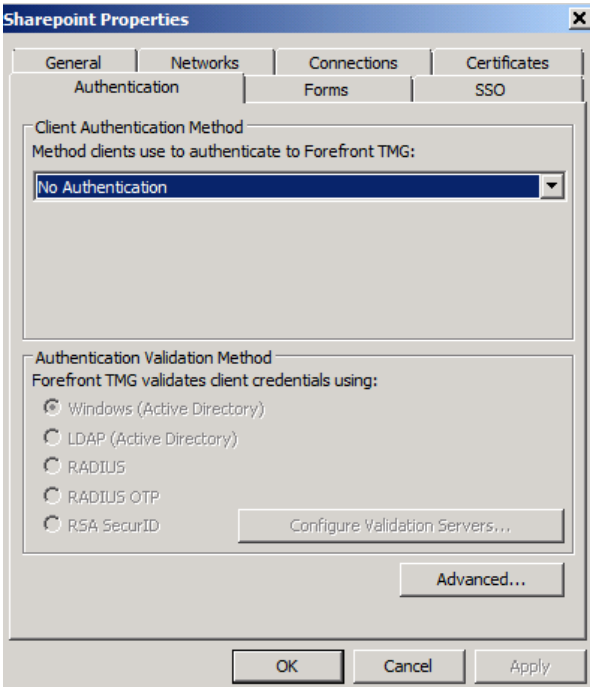




## Verlagerung der Authentifizierung lediglich auf den Sharepoint Server

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