Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Publishing Microsoft SharePoint 2010 with Forefront TMG and different authentication options - Part II

Abstract

This two part article series will explain how to use the different Microsoft SharePoint Server 2010 and Forefront TMG authentication options to securely publish Microsoft SharePoint Server 2010 with Forefront TMG to the Internet.

Let's begin

The first article started with an overview about authentication options in Microsoft SharePoint Server 2010 and Microsoft Forefront TMG. I gave you also an overview how to set the different authentication options in Microsoft SharePoint Server 2010 and we started publishing Microsoft SharePoint Server 2010 with the Standard publishing wizard of Forefront TMG and configured the SharePoint Server 2010 to listen on the HTTPS port. The second part of this article will explain how to change the authentication settings on the Forefront TMG Server to the following:

- KCD (Kerberos Constrained Delegation)
- SSL Client Certificate Authentication
- No Delegation / authentication at the TMG Server

Before we start with the different authentication options let us change the HTTPS to HTTP bridging of Forefront TMG to the SharePoint Server to HTTPS to HTTPS bridging. In the first article we requested a certificate from our internal Certification Authority for the SharePoint Server so now we can change the Bridging on the Forefront TMG Server as shown in the following screenshot.

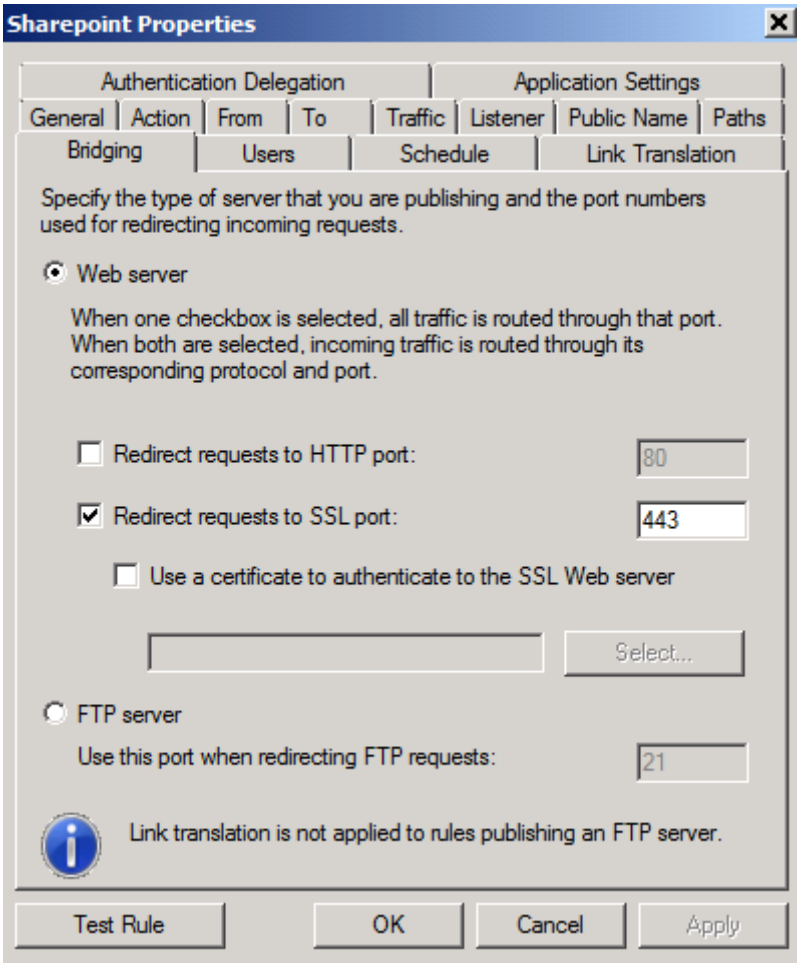

Figure 1: Change HTTP to HTTPS redirection

Kerberos Constrained Delegation

Kerberos Constrained Delegation (KCD) is a primary functionality of the Kerberos protocol introduced first in Windows Server 2000 domain environments for authenticating users, services and computers. If a published Web server like the SharePoint Server also needs to authenticate a user that sends a request to it and if the Forefront TMG computer cannot delegate authentication to the published Web server by passing user credentials to the published Web server or impersonating the user, the published Web server will request the user to provide credentials for a second time. ISA Server 2006 first introduces support for Kerberos constrained delegation to enable published Web servers to authenticate users by Kerberos after their identity has been verified by ISA Server using a non-Kerberos authentication method. When used in this way, Kerberos constrained delegation eliminates the need for requiring users to provide credentials twice. To get Kerberos Constrained Delegation to work, we must change the Authentication Delegation method to Kerberos Constrained Delegation in the Forefront TMG Management console for the SharePoint publishing rule. The Service Principal Name (SPN) is host/InternalDNSFQDN of the SharePoint Server.

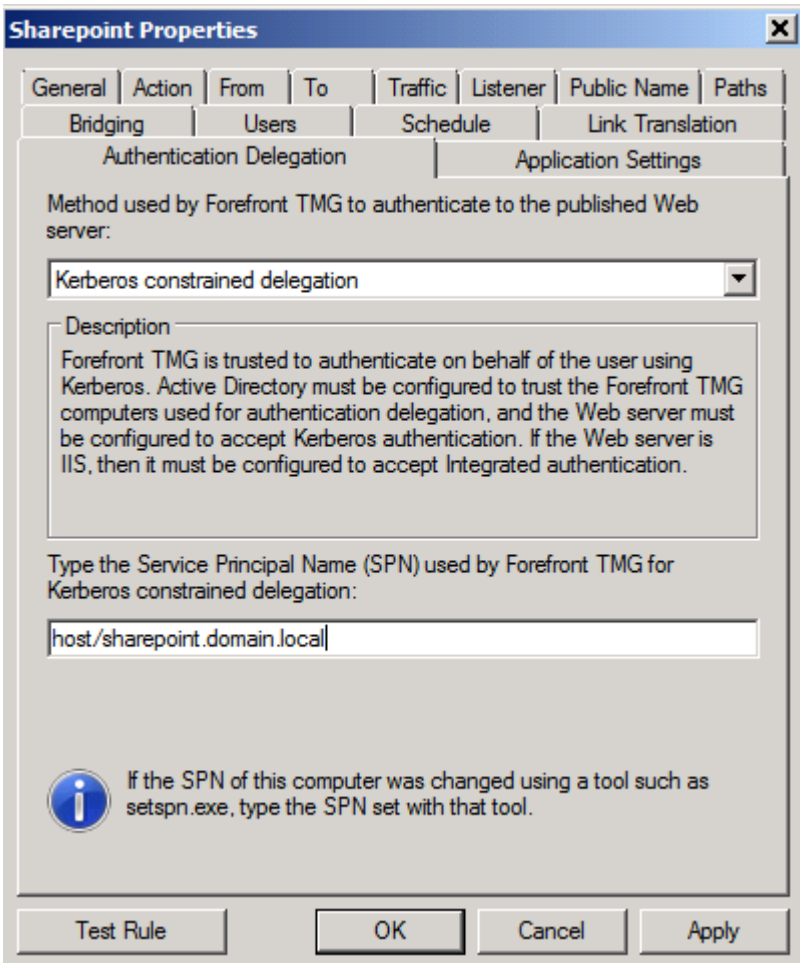

Figure 2: Using KCD

Next we must change the Client Authentication Method to HTTP-authentication with Integrated Authentication

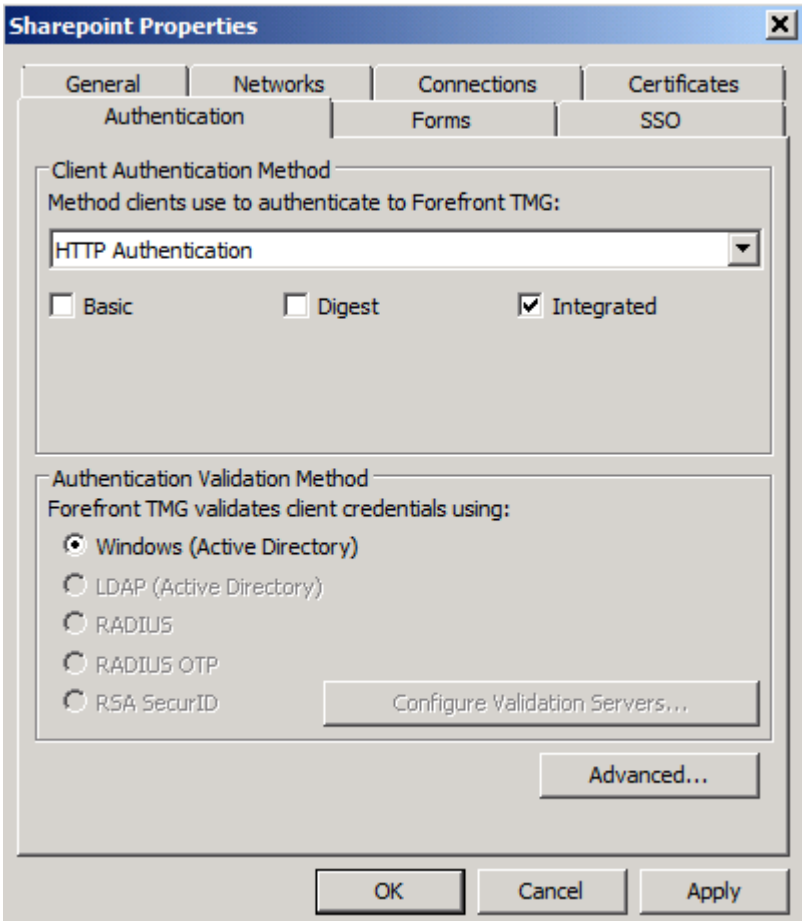

Figure 3: Integrated HTTP authentication

To get KCD (Kerberos Constrained Delegation) working, the Sharepoint Server must trust the Forefront TMG Server for Kerberos Delegation. Open the Active Directory User and Computers console, make sure that the “advanced Feature” view is activiated, navigate to the Forefront TMG computer account, select the Delegation tab and specify the SharePoint Server for the Service type HOST.

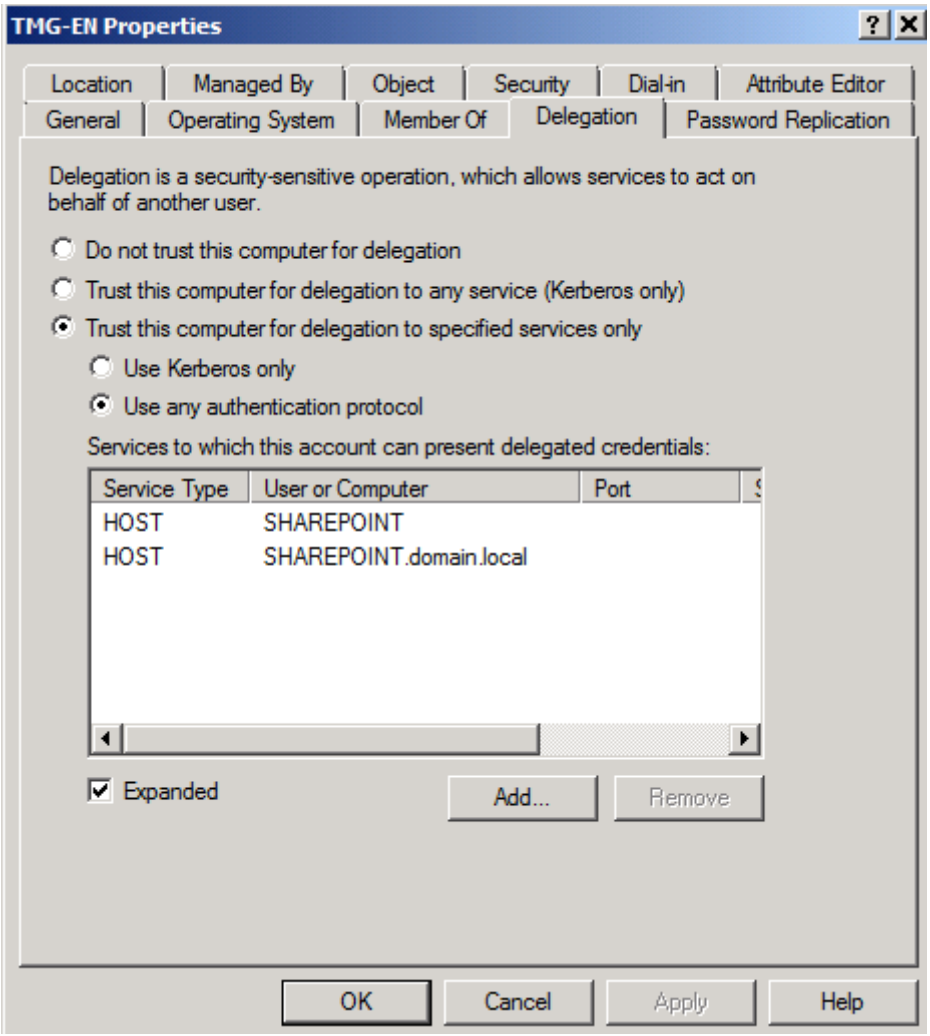

Figure 4: The Sharepoint Server trusts Forefront TMG for delegation

SSL Client Certificate authentication

Now we want to change the authentication between the Forefront TMG Server and the client to SSL Client Certificate Authentication. First, we need to change the allowed Client Authentication Method to SSL Client Certificate Authentication. If the client is not able to authenticate with the SSL client certificate you can use different fallback authentication methods like Basic, Digest and Integrated.

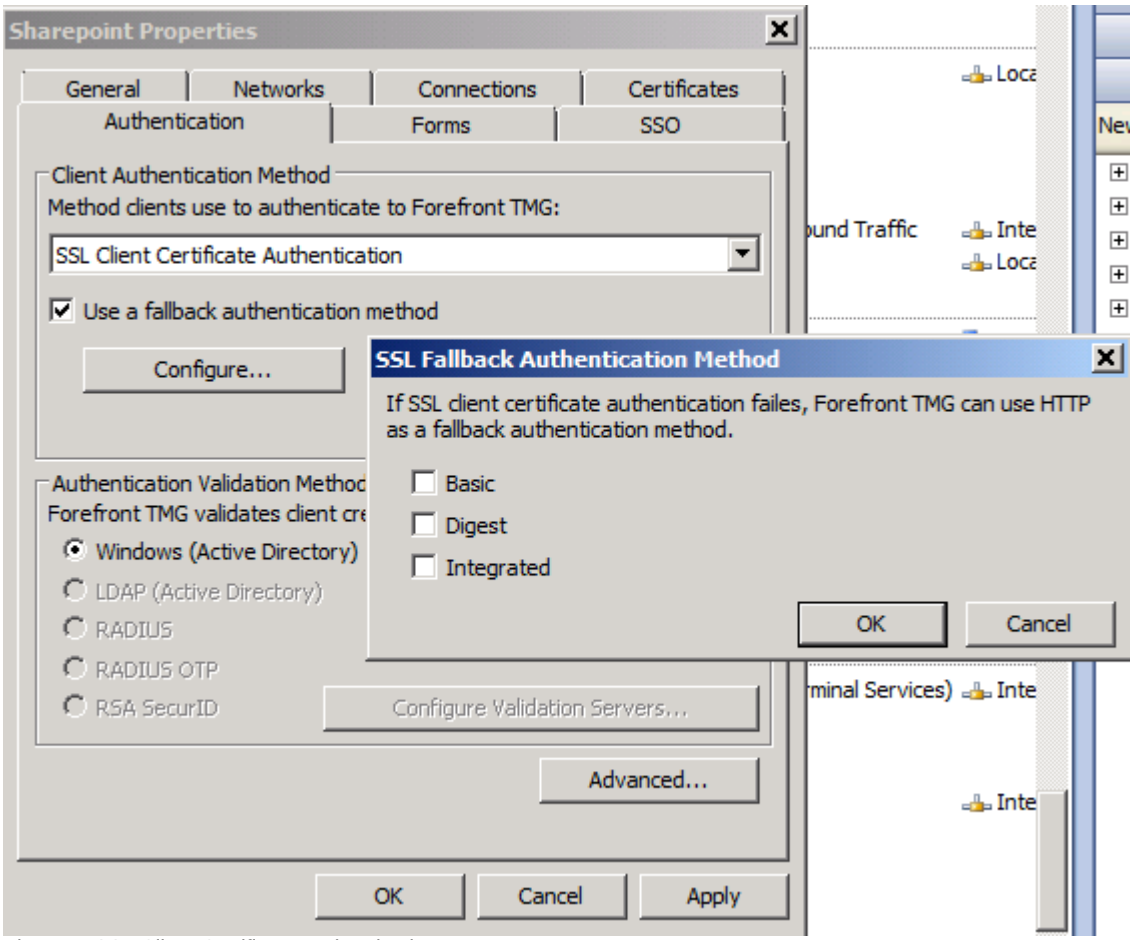

Figure 5: SSL Client Certificate Authentication

Next the client which must access the SharePoint Server from the Internet must have a user certificate installed into the local certificate store of the user account. There are some ways how to enroll the certificate to the client. If you have a large number of clients you can use the certificate auto enrollment with Active Directory and Group Policies, if you only have a few clients, we are able to request the certificate manually. Start an empty MMC, add the certificate Snap In for the local current user account and request a user certificate based on the certificate templates provided by your internal Certification Authority (CA).

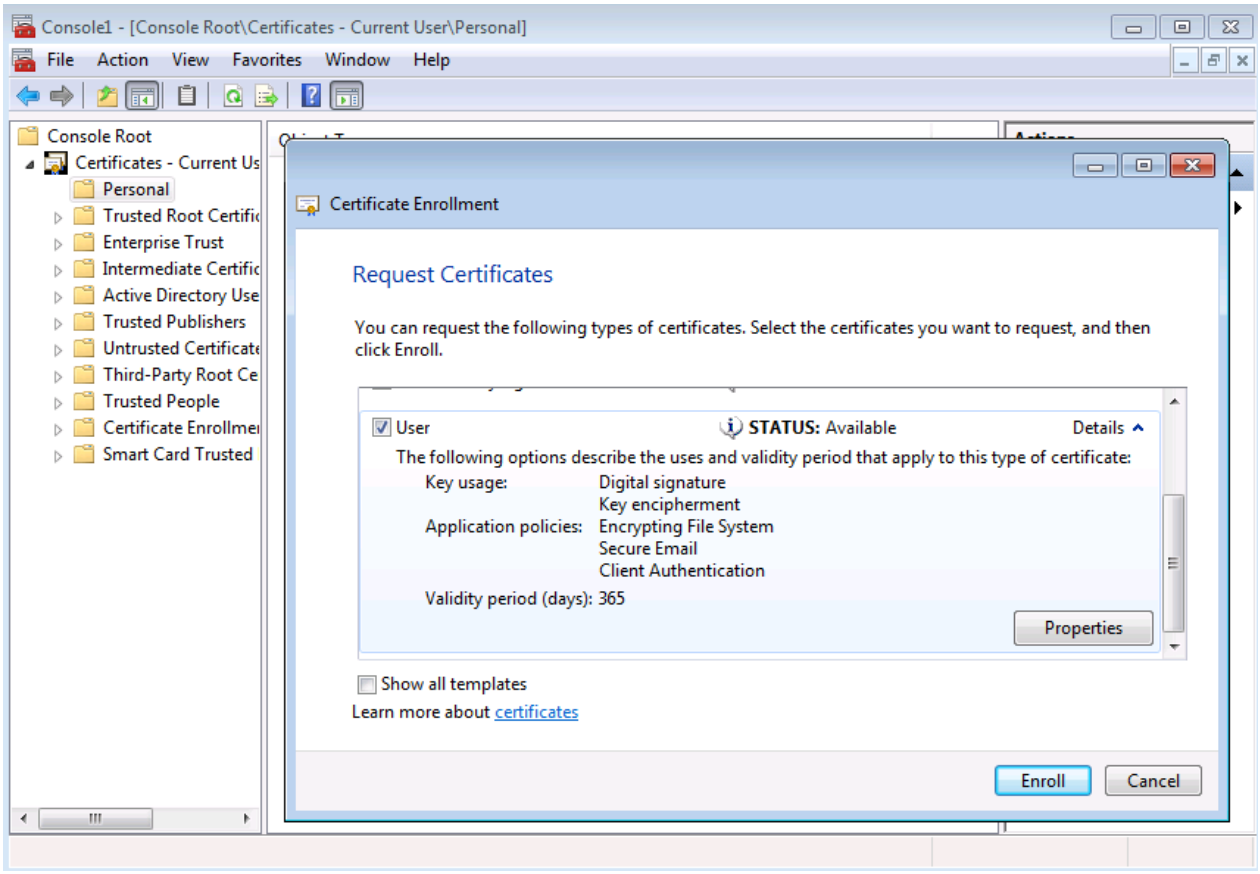

Figure 6: Request a certificate for SSL client certificate authentication

After the user account has received the correct certificate we are able to test the connection. Open the SharePoint website published by Forefront TMG and instead of entering the correct user name and password you now only have to select the issued certificate.
Please note: This is not two factor authentication. With only certificate authentication it is a secure way to only give known client access to the SharePoint Server but without entering an additional password/keyword like in traditional two Factor authentication.

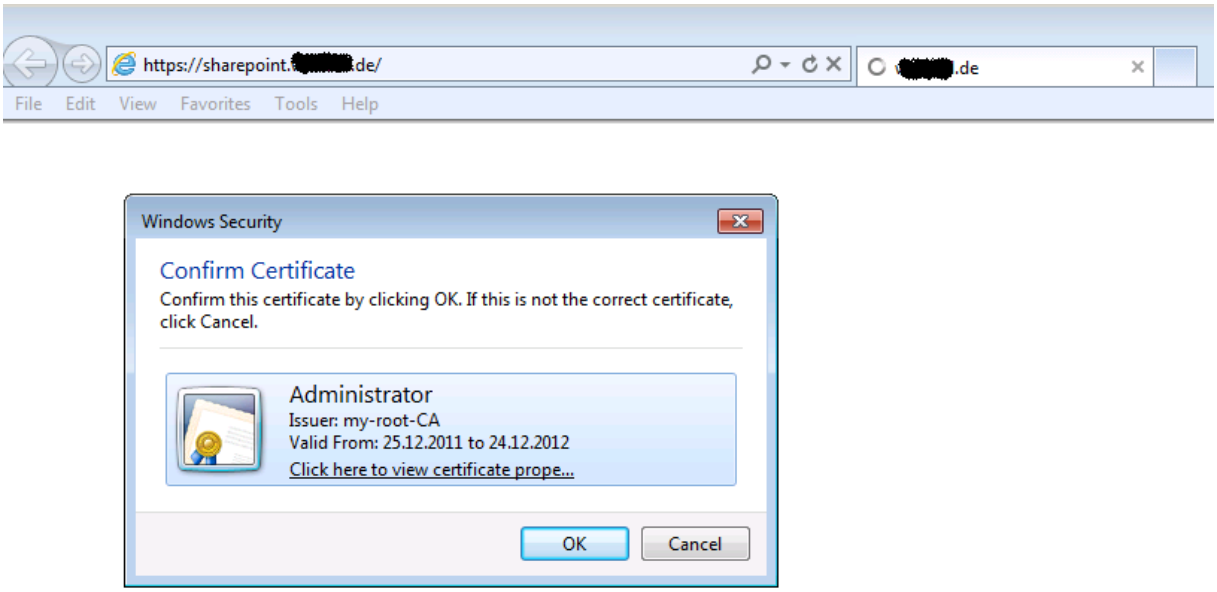

Figure 7: Test access to the Sharepoint Server with a client certificate

Enforce authentication only at the SharePoint Server

For some reasons it might be necessary to let only the SharePoint Server authenticate the client requests from the Internet. You can do this if you change the client Authentication method in the SharePoint Listener on Forefront TMG to “No Authentication”.

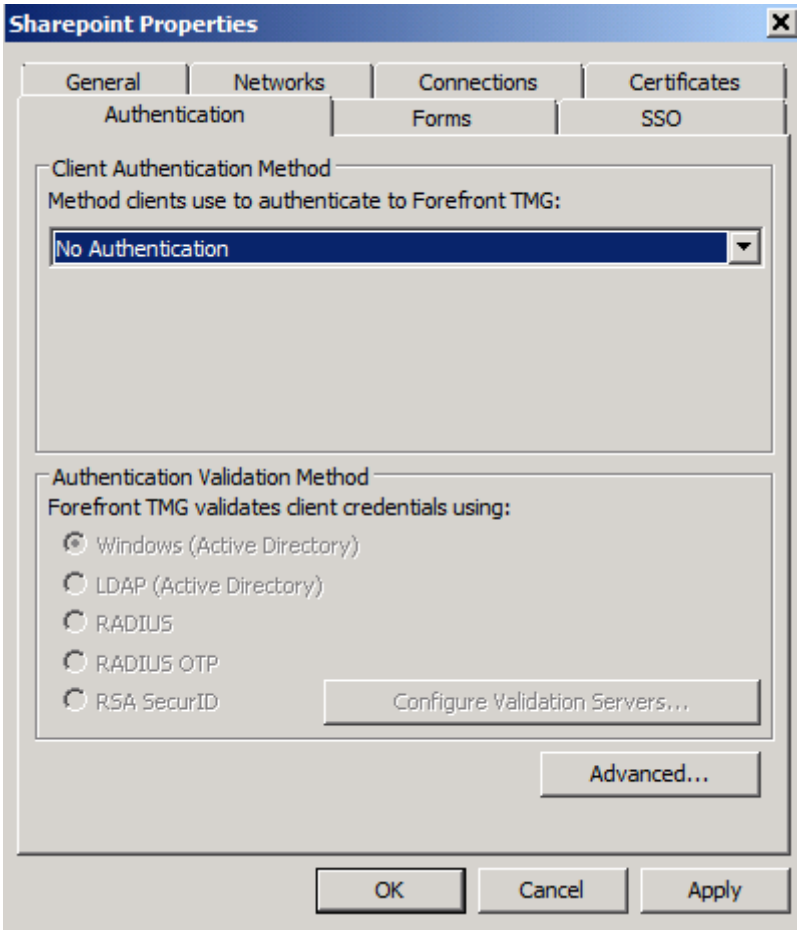

Figure 8: NO authentication at Forefront TMG

In addition we must change the Authentication Delegation to “No delegation, but client tmay authenticate directly” in the SharePoint publishing rule in the Forefront TMG console as shown in the following screenshot.

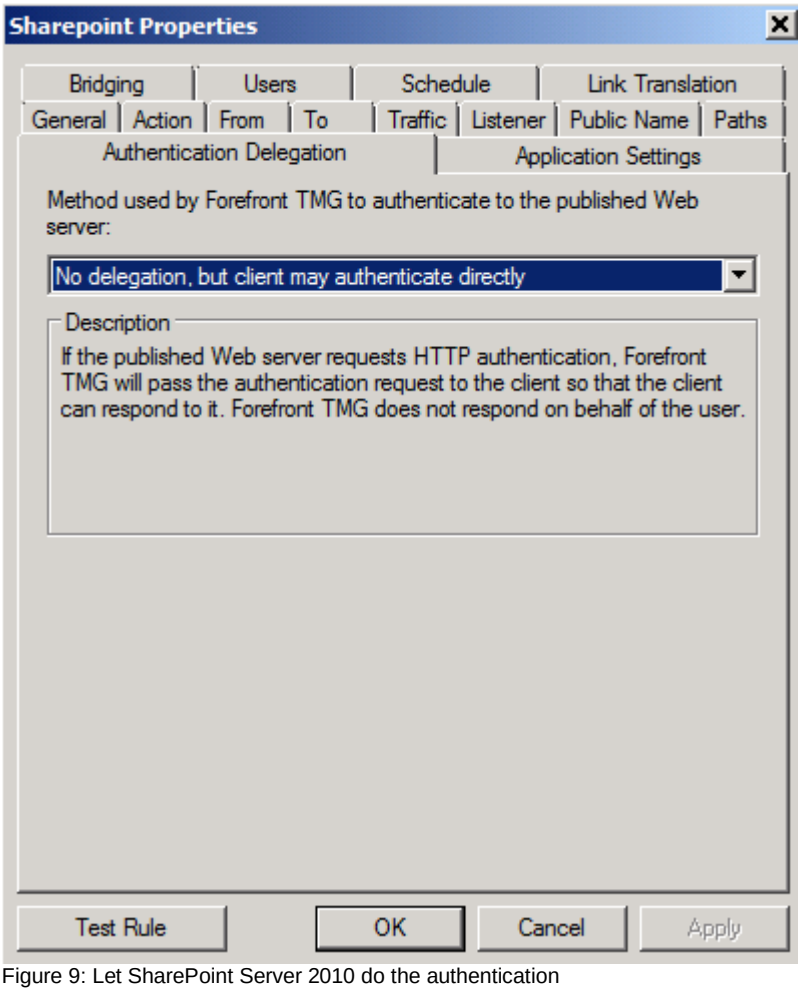

Figure 9: Let SharePoint Server 2010 do the authentication

Now, every authentication request will be forwarded to the Microsoft SharePoint Server 2010 without any pre authentication on the Forefront TMG Server.

Conclusion

In this second article about Microsoft SharePoint 2010 publishing we configured the different authentication options in Microsoft Forefront TMG to see this authentication options working together with Microsoft SharePoint Server 2010. Especially we talked about other Forefront TMG publishing options for Microsoft SharePoint Server 2010 like Kerberos Constrained Delegation (KCD), SSL Client certificate authentication and redirecting the authentication directly to the Microsoft SharePoint Server.

Related links

Kerberos Constrained Delegation in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794858.aspx
Plan authentication methods (SharePoint Server 2010)
http://technet.microsoft.com/en-us/library/cc262350.aspx
Using Kerberos for SharePoint Authentication
http://technet.microsoft.com/en-us/magazine/ee914605.aspx
Understanding SharePoint 2010 Claims Authentication
http://blogs.msdn.com/b/russmax/archive/2010/05/27/understanding-sharepoint-2010-claims-authentication.aspx
Legacy - Configuring SharePoint publishing

http://technet.microsoft.com/en-us/library/cc984488.aspx
Choosing Between Forefront TMG or Forefront UAG for Publishing Scenarios
http://blogs.technet.com/b/tomshinder/archive/2011/04/19/choosing-between-forefront-tmg-or-forefront-uag-for-publishing-scenarios.aspx
What every SharePoint administrator needs to know about Alternate Access Mappings (Part 1 of 3)
http://blogs.msdn.com/b/sharepoint/archive/2007/03/06/what-every-sharepoint-administrator-needs-to-know-about-alternate-access-mappings-part-1.aspx