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 I

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 will start with an overview about authentication options in Microsoft SharePoint Server 2010 and Microsoft Forefront TMG. I will show you how to set the different authentication options in Microsoft SharePoint Server 2010 and we will start publishing Microsoft SharePoint Server 2010 with the Standard publishing wizard of Forefront TMG.

SharePoint Server 2010 comes with a lot of supported authentication mechanisms. The supported authentication mechanisms are:

Windows authentication
- NTLM
- Kerberos
- Anonymous
- Basic
- Digest

Forms based authentication
- LDAP
- Microsoft SQL Server database
- Third party application and role provider

Using Forms based authentication in Microsoft SharePoint Server 2010 is primary done at the Microsoft SharePoint Server 2010. It is not the Forms Based Authentication provided by Microsoft Forefront TMG. If you want to learn more about how to enable Sharepoint Server 2010 for FBA, read the following article.

SAML token-based authentication

SAML (Security Assertion Markup Language) is an open Standard based on XML for exchanging authorization data and authentication data between different domains/realms.

- ADFS 2.0
- LDAP
- Third party Identity provider

Using SAML based authentication with SharePoint Server 2010 and Microsoft Forefront TMG is out of the scope of this article. If you want to use ADFS 2.0 based claims authentication you should have a look into Microsoft Forefront UAG which comes with a lot of enhancements for publishing Microsoft SharePoint 2010. Forefront UAG comes with integrated support for publishing internal resources based on ADFS 2.0.

To configure the different SharePoint authentication options we must use the SharePoint 2010 Central Administration Website and edit the Authentication settings for a Web Application.

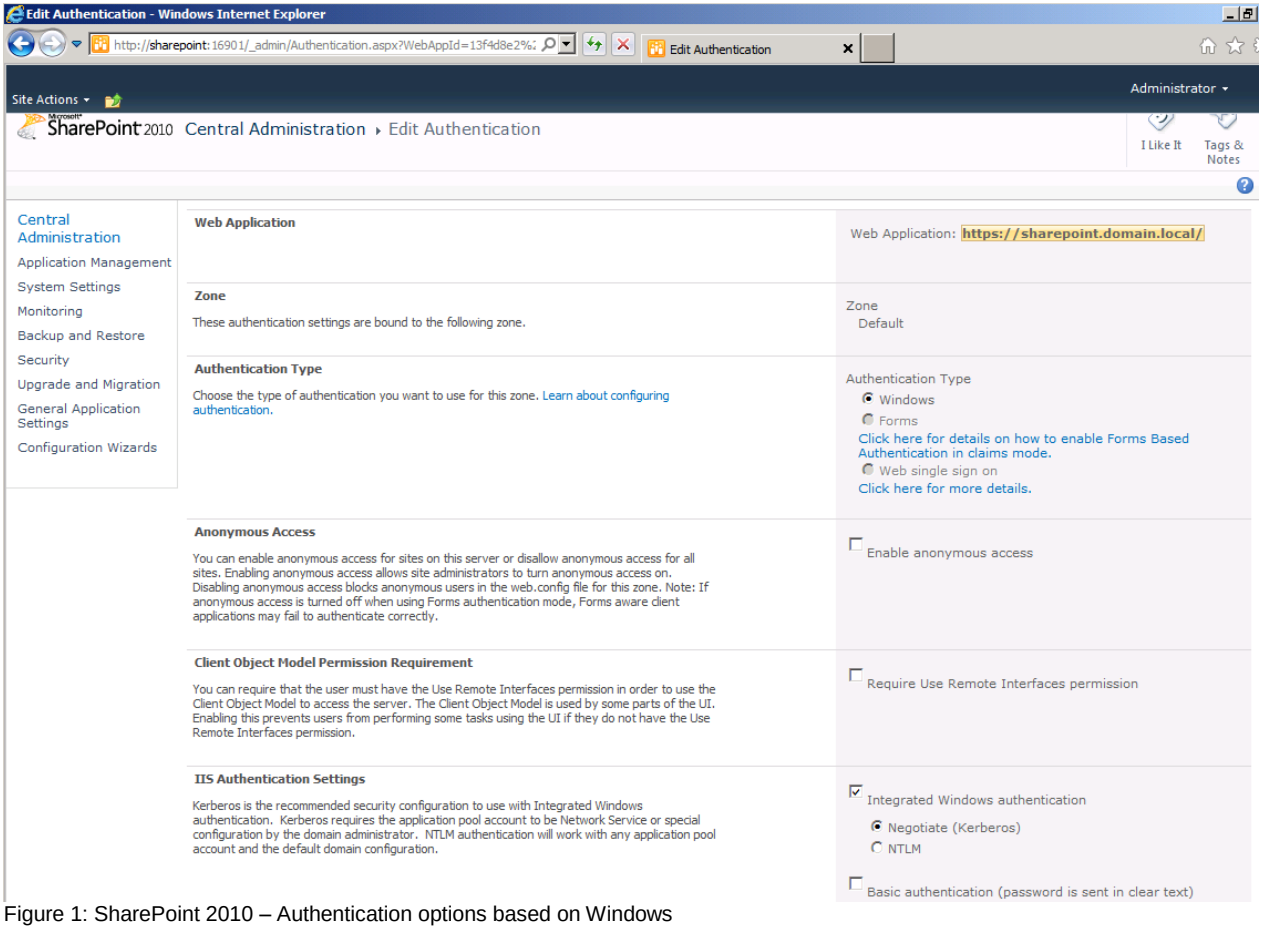

Figure 1: SharePoint 2010 – Authentication options based on Windows

If you create a new Web Application you are able to distinguish between claims based authentication and Classic Mode Authentication (Windows NTLM, Kerberos, Digest for example) as you can see in the following screenshot.

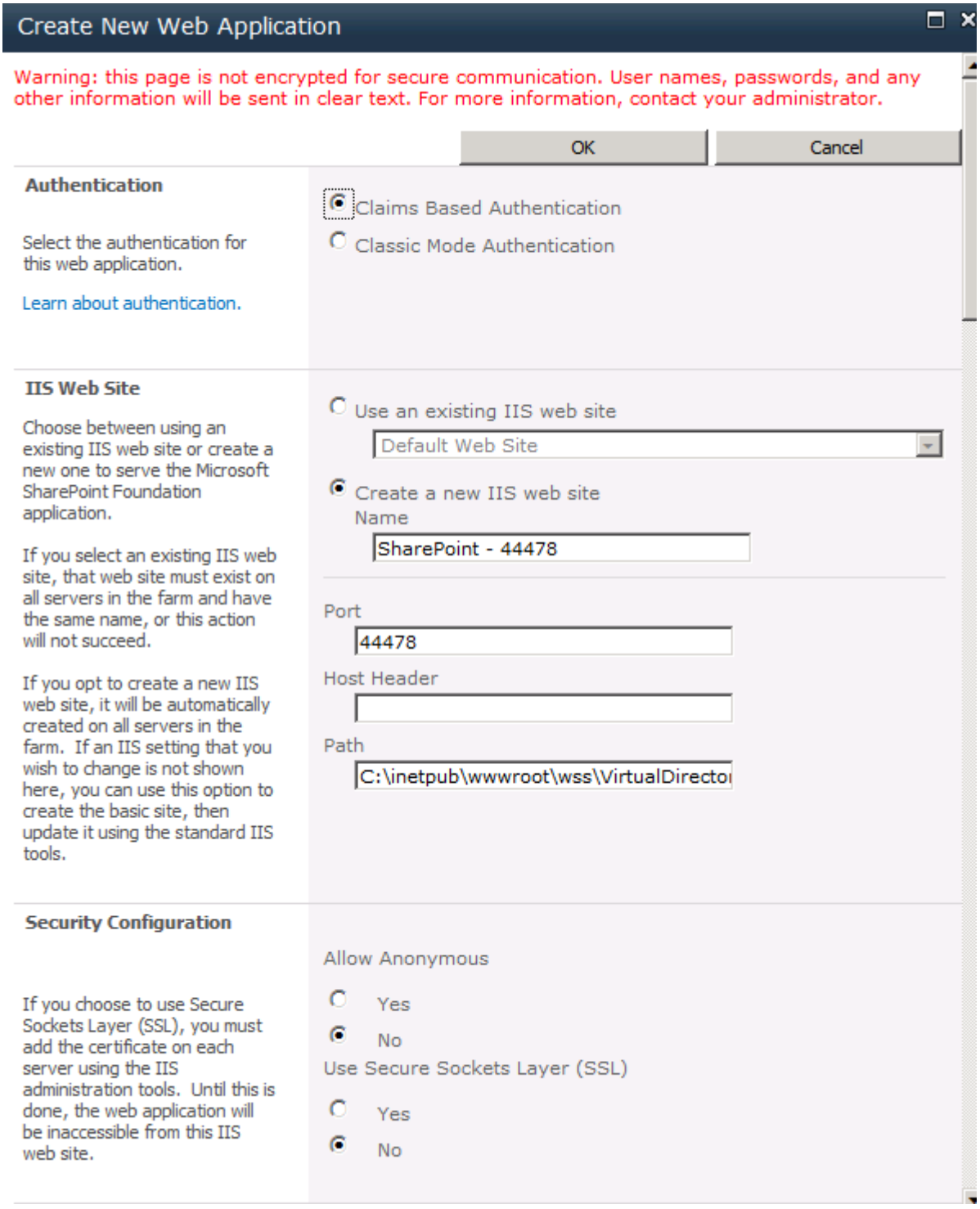

Figure 2: SharePoint 2010 – Claims based Authentication

If you decied to use Claims based Authentication we are able to select different Authentication providers like Forms Based Authentication (FBA) or Third Party Trust Providers if they has been registered and configured at the SharePoint Server 2010.

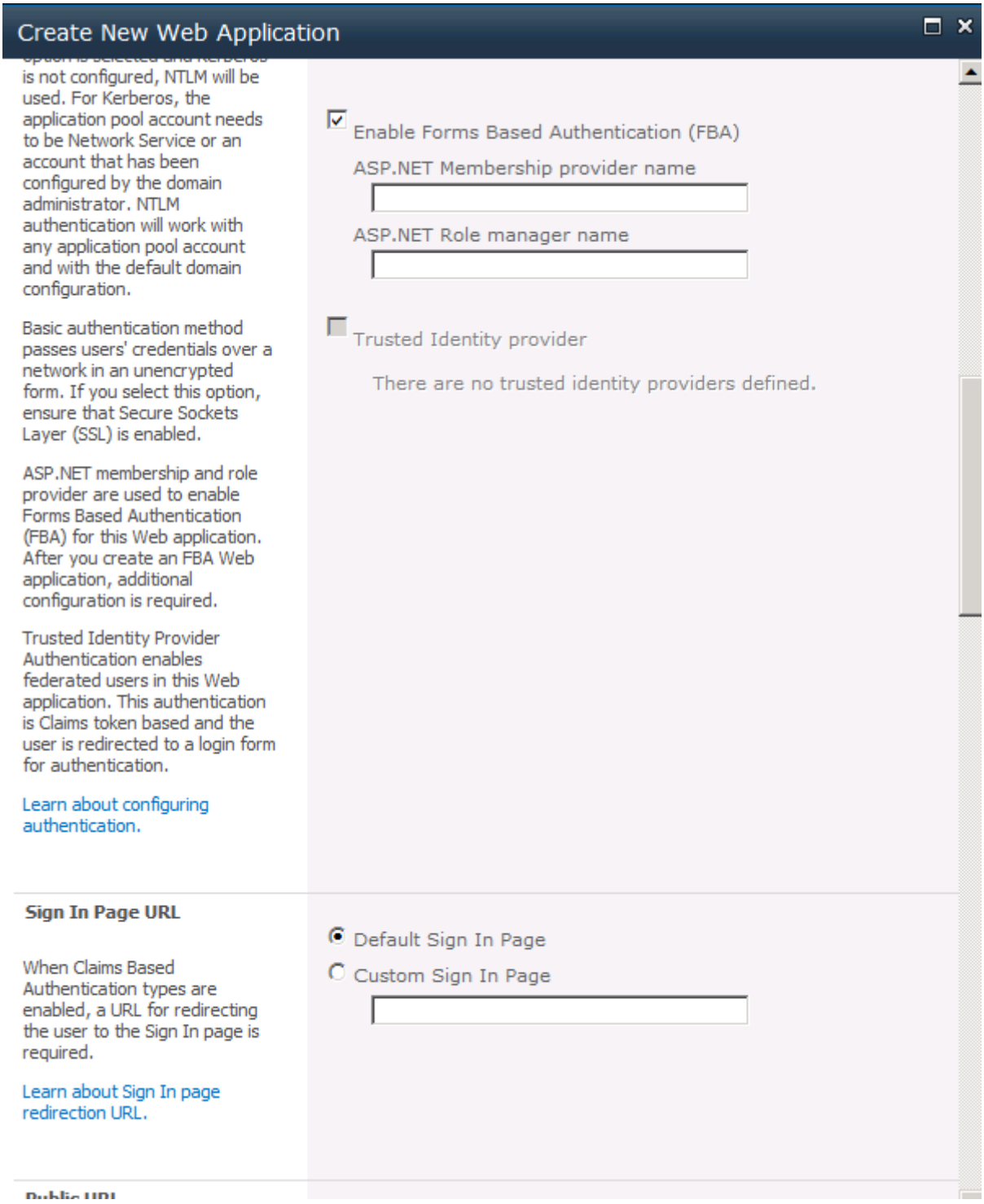

Figure 3: SharePoint 2010 – Enable Forms based Authentication

Creating the SharePoint publishing rule on Forefront TMG

Start the Forefront TMG Management console and create a new SharePoint Site Publishing Rule.

Give the SharePoint publishing rule a name like “Sharepoint publish”. We will publish a single Web site or load balancer.

The assistant use non secured connections to connect the published Web server or server farm. We will change this in article two to a secure HTTPS connection between the TMG Server and the published SharePoint server.

Enter the Internal site name of the SharePoint Server. We will use the internal DNS FQDN (Fully Qualified Domain Name) of the SharePoint Server.

In the public name details we will accept requests for the external DNS domain name from the Internet.

Create a new Web Listener. I will only give you the high level steps how to create the Weblistener:

- Require SSL secured connections with clients
- Listener External
- Select certificate
- HTML Form Authentication with Windows (Active Directory)
- No SSO

We use NTLM authentication as the wizard suggests.

SharePoint AAM configuration

Alternate Access Mapping (AAM) is used in SharePoint Server 2010 or in combination on Forefront TMG. AAM in Microsoft Sharepoint Server 2010 is used to map web requests from the Internet to correct web application and web sites of the internal SharePoint Server 2010.
If SharePoint AAM (Alternate Access Mapping) has not been configured at the Sharepoint Server or if you are not sure, select the second radio button.

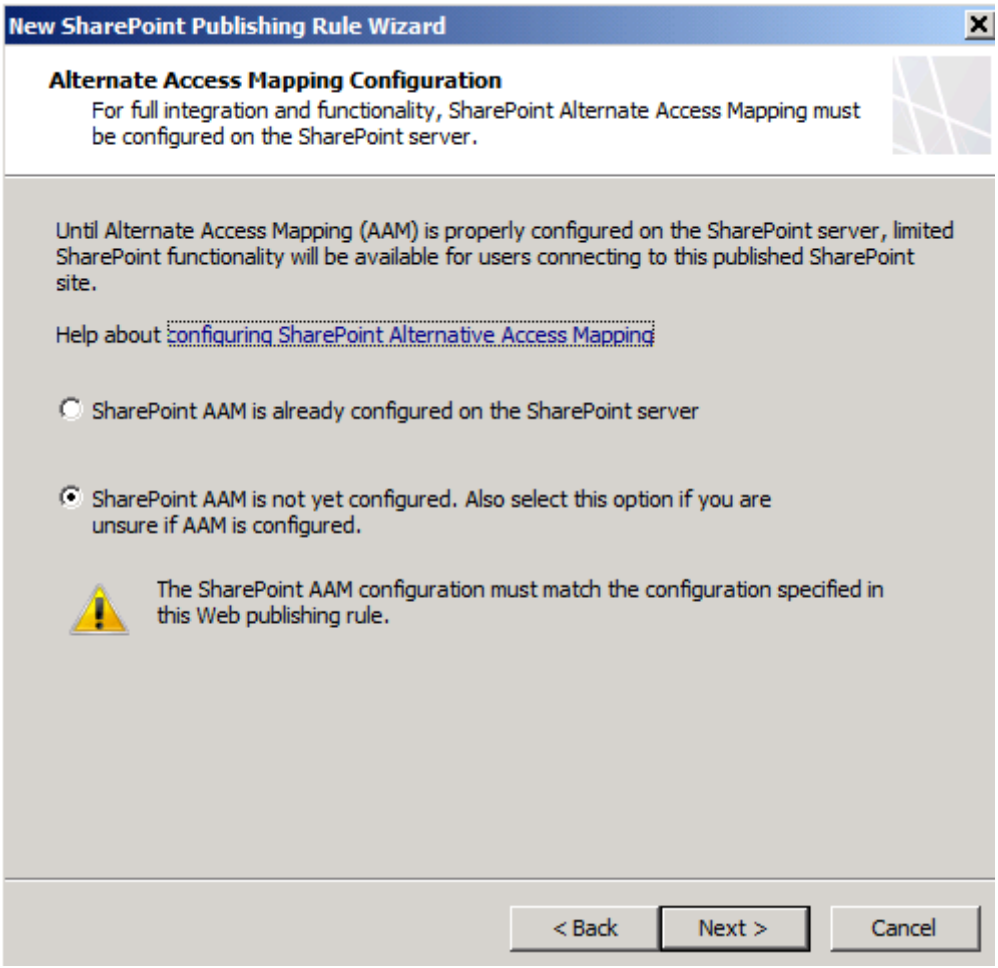

Figure 4: AAM configuration options

We remove the “Authenticated Users” user set from the wizard and use a new created user set in Forefront TMG, filled with a Active Directory user group which should be able to access the SharePoint Server over the Internet.

After the SharePoint publishing wizard has been finished and the TMG configuration change has been applied to the Forefront TMG storage we should test the connection with the Test Button in Forefront TMG or try to access the SharePoint Server from the Internet.

SSL on the SharePoint Server

As the last step in our first article we will enable the Sharepoint Server 2010 to listen on HTTPS requests.

First we have to request a new certificate from a internal Certification Authority (CA) or a self signed certificate. In our environment we will request a certificate from an internal Enterprise Certification Authority. We will use the certificate request wizard of the Internet Information Services (IIS) Manager, but it is also possible to request the certificate with the Certificate SnapIn.
Attention: The CN (Common Name) of the certificate must match the Internal Site Name in the TMG publishing rule – in this case the internal DNS FQDN.

After the certificate has been issued from the CA, we must change the bindings of the SharePoint Website in the Internet Information Services (IIS) Manager that IIS listens on Port 443 in addition to port 80 as shown in the following screenshot.

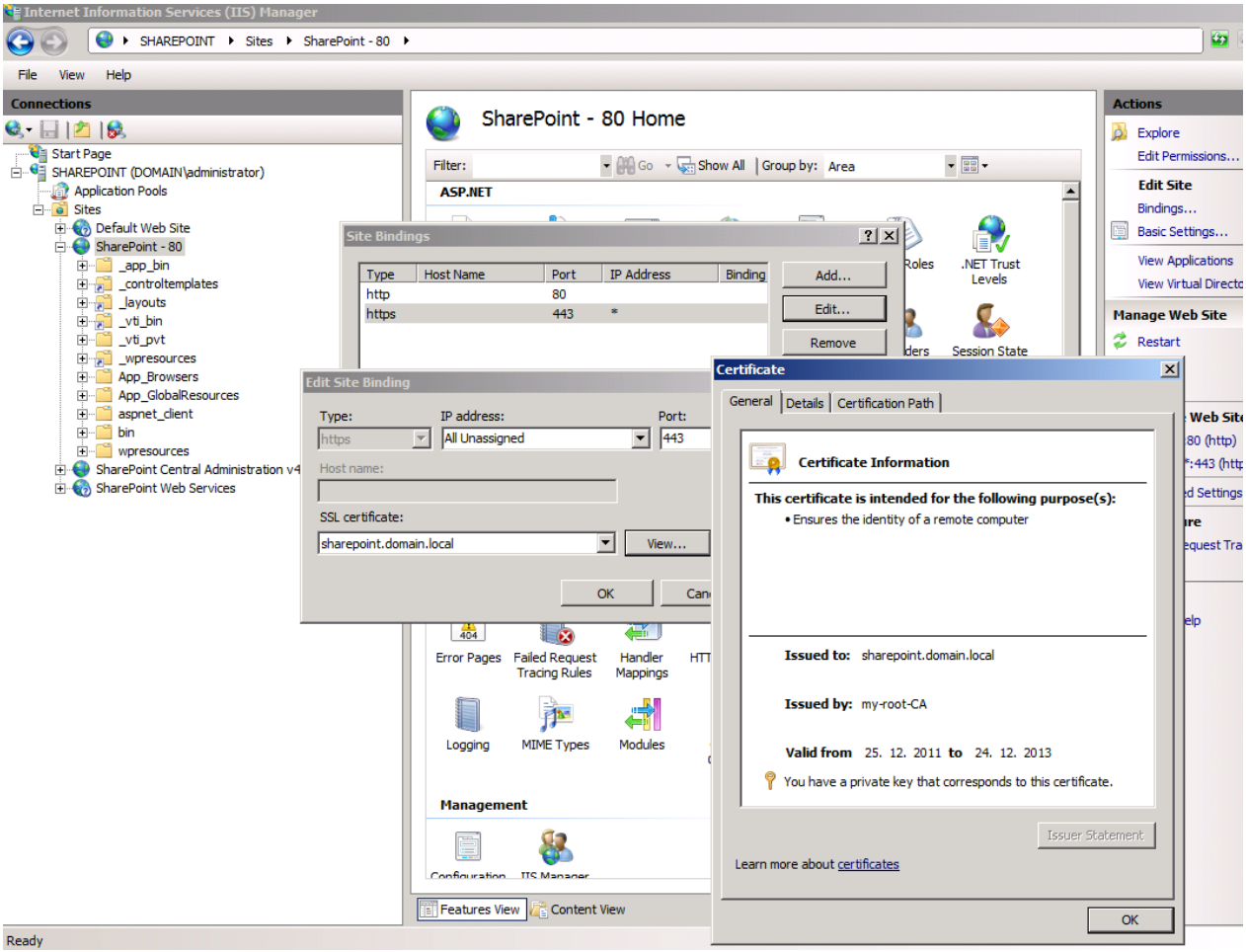

Figure 5: Certificate for HTTPS bindings on the IIS

Conclusion

In this first article we had a look into the different authentication options in Microsoft SharePoint Server 2010 and Microsoft Forefront TMG to see this authentication options working together. We also started with publishing Microsoft SharePoint Server 2010 with the default SharePoint publishing rule wizard in Forefront TMG. In the second article we will talk about other Forefront TMG publishing options for Microsoft SharePoint Server like Kerberos Constrained Delegation (KCD), SSL Client certificate authentication and redirecting the authentication directly to the Microsoft SharePoint Server.

Related links

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