How to publish Microsoft Sharepoint services with ISA Server 2006

Abstract

In this article, I will show you how to publish Microsoft Sharepoint services 3.0 with ISA Server 2006 Enterprise (two nodes).

Let's begin

Beginning with ISA Server 2006, Microsoft made publishing Microsoft Sharepoint Servers and Sharepoint services a little bit easier through a Sharepoint publishing wizard which guides you through the entire publishing process.

Installing Sharepoint services

As the first part we have to install Microsoft .NET Framework 3.0 or higher on the Server where we want to install Sharepoint services.

You can download the .NET Framework from the Microsoft website. I provided the link at the end of this article.

Installing the .NET Framework is very easy. Simply follow the installation wizards instructions.

🐻 Microsoft .NET Framework 3.0 Setup	
Download and Install Progress	. Framework
Downloading:	
Status: Calculating transfer rate	
Total Download Progress: 3 MB / 30 MB	
	Cancel

Figure 1: .NET Framework 3.0 installation

After the .NET Framework has been installed, start the installation of the Microsoft Sharepoint services 3.0. You can download the Sharepoint services for free from the Microsoft website. I provided the link at the end of this article.

For this example we choose the Standalone installation option. The typical installation option installs the Sharepoint services with a local MSDE (Microsoft SQL Server Desktop Engine) – Windows Internal Database. For advanced options choose the other setup option.



Figure 2: Standalone Setup option

After installing Sharepoint services 3.0 it should be possible to open the default Sharepoint Team site. It is now on to you to create custom Sharepoint sites which you want to use internal or with ISA Server publishing over the Internet.



Figure 3: .Default Sharepoint Services website

In this example I created a new Sharepoint website with the Blog template to publish a Blog about ISA Server.



Figure 4: New Team site

Specify the Title and the URL location for the Sharepoint Team Blog website.

🚈 New SharePoint Site - M	licrosoft Internet Explorer		_ 8 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorite	es <u>T</u> ools <u>H</u> elp		_
🕝 Back 🝷 🕘 👻 👔	🏠 🔎 Search 👷 Favorites 🔣 🍙 🌜 🚍		
Address 🙆 http://server3/_	layouts/newsbweb.aspx	💌 🔁 Go	Links »
	Team Site > Create > New SharePoint Site New SharePoint Site		
	Use this page to create a new site or workspace under this SharePoint site. You can specify	a title, Web site address, and access permissions. Create Cancel	
	Title and Description Type a title and description for your new site. The title will be displayed on each page in the site.	Title: ISASERVER Description:	
	Web Site Address Users can navigate to your site by typing the Web site address (URL) into their browser. You can enter the last part of the address. You should keep it short and easy to remember. For example, http://server3/sitename	URL name: http://server3/ lisaserver	
	Template Selection	Select a template: Collaboration Meetings Team Site Blank Site Document Workspace Wiki Site Slop	

Figure 5: Creating the Sharepoint Blog site

After successful creation of the Sharepoint Blog site, you can open the website by specifying the correct URL.



Figure 6: The new Sharepoint Blog site

Alternate Access mapping

Each Web application has a set of internal URLs which are used for accessing the internal website. A public URL is what user's type to get to the SharePoint site, and that URL is what appears in the links on the pages. If you try to open the published

Sharepoint site from outside the Internal network, you have to activate the Alternate access mapping feature for the Sharepoint website you want to publish through ISA Server.



Specify the external website URL in the Internet section on the Public Zone URLs.

🖉 Edit Public Zone URL	s - Microsoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vo	orites <u>T</u> ools <u>H</u> elp	4
🔇 Back 🝷 🕘 👻 🚺	🗈 🏠 🔎 Search 👷 Favorites 🛛 😥 🛃 🔜	
Address 🙆 http://server	3:17982/_admin/EditOutboundUrls.aspx?CollectionId=974f01e6%2D	06ce9%2D40bf%2Da191%2Dc61096aa616c
🔆 Central Adı	ministration	
Home Operations	Application Management	Site Actions 🔻
	Central Administration > Operations > Alternate Acce Edit Public Zone URLs	ess Mappings > Edit Public Zone URLs
View All Site Content		
Central Administration	Alternate Access Mapping Collection Select an Alternate Access Mapping Collection.	Alternate Access Mapping Collection: SharePoint - 80
 Operations 		
Application Management Recycle Bin	Public URLs Enter the public URL protocol, host, and port to use for this resource in any or all of the zones listed. The Default Zone URL must be defined. It will be used if needed where the public URL for the zone is blank and for administrative actions such as the URLs in Quota e-mail.	Default http://server3 Intranet Internet https://sps.it-training-grote.de Custom Extranet
		Save Delete Cancel

Figure 8: Edit Public Zone URLs

After that, the Sharepoint part is done and we have to configure ISA Server 2006.

Creating certificates

The next step is to create a Webserver certificate for the ISA Server Sharepoint Listener. The Common Name (CN) of the certificate must match the FQDN you use on the Internet to access the website. For normal use you should use certificates from your internal CA or a commercial certificate. For this article we will be using self signed certificates with the help of the SELFSSL tool from the IIS 6 Resource Kit. You can download the IIS 6 Resource Kit for free from the Microsoft website. I provided the link at the end of this article.

Installing IIS 6 Resource Kit

InstallShield Wizard	
	Preparing to Install IIS 6.0 Resource Kit Tools Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
	Configuring Windows Installer
	[Cancel]

Figure 9: Installing IIS 6 Resource Kit

SELF SSL is a command line tool to create a certificate.



Figure 10: Using SELFSSL

SELFSSL has several options for creating certificates. Executing SELFSSL with /? will show you the available options.

Attention: Keep special attention by the /V: parameter. The /V: parameter specifies the lifetime of the certificate in days!

After creating the certificate, you have to ways to bring the certificate to the other ISA Server node which is already a member in an ISA NLB cluster:

- 1) Export the certificate with private key from the first node
- 2) Create a new certificate with the same settings on the second node.

🚡 Console1 - [Console Root\Cert	ificates (Local Computer)\Personal'	\Certificates]			_ 8 ×
🚡 Eile Action View Favorites	<u>W</u> indow <u>H</u> elp				_ & ×
← → 🔁 🖬 👗 🗈 🗙	🗗 🖳 😫				
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name
🖻 🗐 Certificates (Local Computer)	8 RootCA	RootCA	2/23/2013	<all></all>	<none></none>
📮 🖳 Personal	🔤 server.domaene.internal	RootCA	2/22/2009	Client Authentication	DC
	SPS.it-training-grote.de	SPS.it-training-grote.de	8/18/2010	Server Authentication	<none></none>
Trusted Root Certification	📟 we	RootCA	2/22/2010	Server Authentication	SSL-SQL
Enterprise Trust	📟 web	RootCA	2/22/2010	Server Authentication	SSL-SQL
Intermediate Certification					
🗄 🖳 Trusted Publishers					
🗄 💼 Untrusted Certificates					
😟 🕀 📄 Third-Party Root Certifica					
🗄 💼 Trusted People					
🗄 💼 Certificate Enrollment Rec					
	1				
Figure 11: Certificate MMC					

For the example in this article we export the certificate from the first node, move it to the second node and import it into the local computer certificate store.

Import PFX file on the second ISA node.

Certificate Import Wizard	×
Password	
To maintain security, the private key was protected with a password.	
Time the ensured for the enjoyed law	
rype the password for the private key.	
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
< <u>B</u> ack <u>N</u> ext > Cancel	

Figure 12: Import the PFX file into the local computer certificate store

Attention: Because we are using a self signed certificate, we have to import the self signed certificate also into the Trusted Root Authority store on both ISA server nodes.

The Sharepoint Publishing on ISA

Open the ISA MMC and create a new Sharepoint publishing rule with the help of the wizard.

Name the rule.

Select Publish a single website or Load balancer.

New SharePoint Publishing Rule Wizard
Publishing Type Select if this rule will publish a single Web site or external load balancer, a Web server farm, or multiple Web sites.
 Publish a single Web site or load balancer Use this option to publish a single Web site, or to publish a load balancer in front of several servers. Help about <u>publishing a single Web site or load balancer</u> Publish a server farm of load balanced Web servers Use this option to have ISA Server load balance requests between a server farm (mirrored servers). Help about <u>publishing server farms</u> Publish <u>multiple</u> Web sites Use this option to publish more than one Web site. A new rule will be created for each a server farm and the publish more than one Web site.
Help about <u>publishing multiple Web sites</u> < Back

Figure 13: Publish a single website or Load Balancer

In this example we are not using SSL from the ISA Server to the Sharpoint services Server.

New SharePoint Publishing Rule Wizard	×
Server Connection Security Choose the type of connections ISA Server will establish with the published Web server or server farm.	
C Use SSL to connect to the published Web server or server farm ISA Server 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 ISA Server will connect to the published Web server or server farm using HTTP.	
When ISA authenticates to the published server on behalf of the client, user credentials may be sent over the network in clear text. Authentication using will help protect client credentials.	SSL
Help about <u>server connection security</u>	
< <u>B</u> ack <u>N</u> ext > C	ancel

Figure 14: Use a non secured connection to connect to the SPS Server

If you want to use a secured connection from the ISA Server Enterprise array to the published Sharepoint Server, you must request a certificate for the Sharepoint Server and ISA Server must have the trusted Root CA certificate from the issuing CA.

As a next step specify the name of the internal site. The name you typed here, must match the common name of the certificate when you use HTTPS Bridging from ISA Server to the published Sharepoint Server.

New SharePoint Publishing Rul	e Wizard	×
Internal Publishing Details Specify the internal name of	of the SharePoint site you are publishing.	
Internal site name: The internal site name is the nar Typically, this is the name intern	server3 ne of the Web site you are publishing as it appears int al users type into their browsers to reach the Web site	ernally. a.
If ISA Server cannot resolve the computer name or IP address of	e internal site name, ISA Server can connect using the the server hosting the site. address to connect to the published server	
Computer name or IP address:	Brow	ise
	< <u>B</u> ack <u>N</u> ext >	Cancel

Figure 15: Specify the name of the internal site name

In the Public Name Details accept requests only for the domain name sps.it-training-grote.de.

New SharePoint Publishing Rule Wiza	rd	×
Public Name Details Specify the public domain name (Fo published site.	QDN) or IP address users will type to reach the	
<u>A</u> ccept requests for: Only requests for this public name or IP	This domain name (type below): address will be forwarded to the published site.	•
P <u>u</u> blic name:	sps.it-training-grote.de	
	Example: www.contoso.com	
	< <u>B</u> ack <u>N</u> ext > Ca	incel

Figure 16: Public Name details

Create a new Weblistener, name the Weblistener and select *Require SSL secured connections with clients*.

New Web Listener Definition Wizard	×
Client Connection Security Select what type of connections this Web Listener will establish with clients.	
Bequire SSL secured connections with clients ISA Server will publish servers only over HTTPS to the clients (recommended).	
Do not require SSL secured connections with clients ISA Server will publish servers over HTTP. Client credentials will be sent unencrypted to the ISA Server computer.	
When publishing over SSL, an appropriately named SSL server certificate n installed on the ISA Server computer.	nust be
Help about web listener client connections	
< <u>B</u> ack <u>N</u> ext >	Cancel

Figure 17: Use SSL for accessing the ISA Server from the client.

The Weblistener is the EXTERNAL network. If you have more than one IP address bound to the external network interface on ISA Server, select the IP address for the Sharepoint publishing manually to avoid problems with other Publishing rules.

ew Web Listener Definition Wizard		×
Web Listener IP Addresses Specify the ISA Server networks, an will listen for incoming Web requests.	d the IP addresses on those networks, that	
Listen for incoming Web requests on the	se networks:	
Name	Selected IPs	
🗹 🌑 External	<all addresses="" ip=""></all>	
🗖 📥 İnternal	<all addresses="" ip=""></all>	
🗖 📥 Local Host	<all addresses="" ip=""></all>	
🔲 👍 Quarantined VPN Clients	<all addresses="" ip=""></all>	T
		•
Sele	ect IP <u>A</u> ddresses	
ISA Server will compress content ser requesting the content support comp	nt to clients through this Web Listener if the cl ression.	ients
Help about <u>Web listener IP addresses</u>		
	< <u>B</u> ack <u>N</u> ext >	Cancel

Figure 18: Specify the External Weblistener

In the Listener SSL Certificates section, select the issued certificate.

New W	/eb Listener Definiti	ion Wizard			×				
Listener SSL Certificates Select a certificate for each IP address, or specify a single certificate for this Web listener.									
œ	Use a single certificate for this Web Listener								
	SPS.it-training-grote.de			Select Certific	ate				
C Assign a certificate for each IP address									
	IP Address	Network	Server	Certificate					
				Selec <u>t</u> Certific	ate				
			< <u>B</u> ack	<u>N</u> ext >	Cancel				

Figure 19: Listener SSL certificate

As the Authentication option select HTML Form Authentication and Windows (Active Directory) as the Authentication provider.

New Web Listener Definition Wizard	×
Authentication Settings Select how clients will authenticate to IS their credentials.	A Server, and how ISA Server will validate
Select how clients will provide credentials t	o ISA Server:
HTML Form Authentication	
Collect additional delegation credentials	s in the form
The logon form will include additional fie credentials for authentication to publish	ilds for user credentials. ISA Server will use the ed servers.
Select how ISA Server will validate client c	redentials:
Mindows (Active Directory)	C RADIUS <u>O</u> TP
C LDAP (Active Directory)	C RSA SecurID
C RADIUS	
Help about authentication settings	
	< <u>B</u> ack <u>N</u> ext > Cancel

Figure 19: Select the Authentication method

Do not enable SSO.

For the example in this article we select NTLM as the Authentication model.

New SharePoint Publishing Rule Wizard
Authentication Delegation Authentication delegation is the method ISA Server uses to authenticate the session it opens with the published site.
Select the method used by ISA Server to authenticate to the published Web server:
NTLM authentication
Description ISA Server will use NTLM authentication to authenticate the client to the published Web server. The published Web server must be configured to accept NTLM authentication. If the published Web server is IIS, then it must be configured to accept Integrated authentication.
Help about authentication delegation
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 20: Specify Authentication method

Because we activated the Alternate access mapping feature on the Microsoft Sharepoint 3.0 services before we start the ISA publishing wizard, we doesn't have to activate this feature and we can select *SharePoint AAM is already configured on the SharePoint server*.

New SharePoint Publishing Rule Wizard
Alternate Access Mapping Configuration For full integration and functionality, SharePoint Alternate Access Mapping must be configured on the SharePoint server.
Until Alternate Access Mapping (AAM) is properly configured on the SharePoint server, limited SharePoint functionality will be available for users connecting to this published SharePoint site. Help about <u>configuring SharePoint Alternative Access Mapping</u>
SharePoint AAM is already configured on the SharePoint server
unsure if AAM is configured.
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 21: Alternate Access Mapping configuration

ISA Server 2006 can limit who can access the published server. It is possible to limit access to specific users or user groups. For this article we select the predefined *All Authenticated Users* set.

New SharePoint Publishing Rule Wizard	×
User Sets You can apply the rule to requests from all users. Or, you can limit acces specific user sets.	ss to
This rule applies to requests from the following user sets:	
All Authenticated Users	<u>A</u> dd
	Edit
	<u>R</u> emove
< Back Next >	Cancel

Figure 22: Specify User Sets

After ISA Server publishing has finished, you can try to access the published website, and if everything is configured correctly, you should see a website like this in the following picture.



Figure 23: The published website through ISA Server

Conclusion

In this article I showed you how to publish Microsoft Sharepoint services 3.0 through two ISA Server 2006 Enterprise servers. With the help of ISA Server 2006 it is very easy to publish a Sharepoint Server with the built in Sharepoint publishing wizard which will take the most work for you. The only thing you have to configure on the Sharepoint Server is to activate the Alternate Access Mapping feature.

Related links

Secure Application Publishing http://technet.microsoft.com/en-us/library/bb794854.aspx ISA Server 2006 overview http://www.isaserver.org/articles/isa-server-2006-overview.html Microsoft .NET Framework 3.0 Download http://www.microsoft.com/downloads/details.aspx?FamilyID=10cc340b-f857-4a14-83f5-25634c3bf043&DisplayLang=de Microsoft Sharepoint Services 3.0 Download http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=D51730 B5-48FC-4CA2-B454-8DC2CAF93951 IIS 6 Resource Kit download http://www.microsoft.com/downloads/details.aspx?familyid=56FC92EE-A71A-4C73-B628-ADE629C89499