Publishing Outlook Web Access with Microsoft Forefront TMG

Abstract

In this article, I will show you how to publish Exchange Server 2007 SP1 Outlook Web Access (OWA) with Microsoft Forefront TMG.

Let's begin

First, keep in mind that the information in this article are based on a beta version of Microsoft Forefront TMG and are subject to change.

A few weeks ago, Microsoft released Beta 3 of Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

One of the strength of Microsoft Forefront TMG is to publish internal network resources to the Internet through web access publishing rules. Microsoft Forefront TMG has built in capabilities to publish several Exchange Server functionalities like Outlook Web Access (OWA), Outlook Anywhere and Microsoft Exchange Active Sync.

To publish Outlook Web Access you must point the Default Gateway of the Exchange Client Access Server to the ISA Server internal interface IP address and you will need a webserver certificate on TMG server if you want to use HTTPS to HTTPS bridging. You must also create a webserver certificate for the public accessible name through which OWA should be reachable from the Internet.

Change FBA to basic authentication on Exchange Server

As a first step we have to change the Forms based Authentication (FBA) on Exchange Server site, because TMG also uses FBA and the settings enabled on TMG and Exchange will result in conflicts. To change OWA from FBA to Basic Authentication (used by TMG) start the Exchange Management Console, navigate to Server Configuration – Client Access – and click into the properties of the OWA settings and change FBA to Basic and Windows Authentication as you can see in the following screenshot.



Figure 1: Change authentication from FBA to Basic authentication

After we changed from forms based authentication to basic authentication at Exchange site, we must request a new certificate for the TMG web listener for the public DNS name which will be used to access Outlook Web Access from the Internet.

Important: The common name (CN) of the certificate must match the public DNS name used to access OWA. For example: If your public DNS name is OWA.IT-Training-Grote.de, the CN of the certificate must be the same.

With the Windows Server 2008 MMC Certificate Snap In it is possible to add additional information to the certificate request process. You will need these additional settings to create a certificate request with the custom CN as you can see in the following screenshot.

Certificate Enrollment		
Certificate Enrollment		
Request Certificates		
You can request the following types of (certificates. Select the certificates you want to request, and	then dick Enroll.
Computer	🔅 STATUS: Available	Details 🛞
Copy of Web Server	💓 STATUS: Available	Details®
🔥 More information is require	d to enroll for this certificate. Click here to configure settings	
Web Server	💓 STATUS: Available	Details®
A More information is require	d to enroll for this certificate. Click here to configure settings	
Show all templates		
Learn more about certificate types		
	Ent	oli Cancel

Figure 2: Request a new certificate

Click the link in the request certificate wizard and select the common name type and enter the CN you will need, in this case owa.it-training-grote.de and click Add.

ertificate Properties				×
	s Private Kev	Certification	Authority	
The subject of a certificate is the u enter information about the types in a certificate.	ser or computer of subject name	to which the and alternat	e certificate is issued tive name values that	l. You can at can be used
Subject of certificate				
The user or computer that is receiv	ing the certifica	te		
Subject name: Type:			CN=OWA.IT-TRAI	NING-GROTE.D
Value:	Add	>		
	< Rem	ove		
Alternative name:				
Type: Directory name				
Value:	٨dd	_ 1		
	Add			
	< Rem	ove		
Learn more about subject name				
		ОК	Cancel	Apply

Figure 3: Specify the CN for the public certificate

After the certificate has sucessfully created, you will see the result in the certificate Snap In.

Attention: If the certificate request process with the MMC was not successful, the problem might exist due to the reason, that the certificate request requires DCOM access which must be manually configured at the ISA/TMG Firewall. For additional information read the following Blog post from the ISA/TMG product team:

http://blogs.technet.com/isablog/archive/2007/05/16/rpc-filter-and-enable-strict-rpccompliance.aspx

🙀 Certificate Enrollment		
🙀 Certificate Enrollment		
Certificate Installation Results		
The following certificates have been	enrolled and installed on this computer.	
l√ Web Server	✓ STATUS: Succeeded	Details()
		Finish
		Finish

Figure 4: Certificate enrollment successful

Start the TMG Management console, navigate to the Firewall Policy node and create a new Exchange Web Client Access Publishing rule

🕮 Forefront TMG Bet	a					
File Action View	Help					
🗢 🔿 🖄 📊	🛛 🖬 🖻 🔿	ی چ	🔁 🕋 I	🚰 😼 🐴 🛵 🍕	🕻 📴 😭 📀 📀)
Microsoft Forefront Forefront TMG (Dashboard Monitoring	Threat Managemei TMG)	Forefi Threat I	ront Manage	ement Gateway	Beta	
Firewall Police	Refresh		wall Poli			
🧏 E-Mail Poli 🚏 Intrusion F ፩ Remote A	Export Firewall Pol Import Firewall Pol	icy icy		Name	Examples Action	Protocols
👍 Networkin	New All Tasks) 	Exchan Mail Se	ge Web Client Acces rver Publishing Rule.	s Publishing Rule	DNS
Update Ce	View	•	ShareP Web Si	oint Site Publishing R te Publishing Rule	ule	RDP (
	Help		Non-W Access	eb Server Protocol P Rule FTP allow	ublishing Rule	FTP
Figure 5: Create a new Ex	kchange Web Client	😑 💽 Access Pu	3 blishing R	Blocked Web Des	🚫 Deny	🖳 НТТР

A new wizard start which will guide you to the OWA publishing process. Enter a name for the new publishing rule.

New Exchange Publishing Ru	le Wizard	×
	Welcome to the New Exchange Publishing Rule Wizard	
	This wizard helps you publish Web client mail access on an Exchange server or server farm. Use this option to publish Microsoft Outlook Web Access, Outlook Mail Access, Outlook RPC over HTTP, or Exchange Active Sync.	
	Exchange Publishing rule name:	
MKMK 1	OWA Publishing	
KAKKAT	To continue, dick Next.	
(1) KAN		
	<back next=""> Cance</back>	el

Figure 6: Exchange Publishing rule name

Specify the correct Exchange version and the web client mail service you want to publish.

New Exchange Publishing Rule Wizard		×
Select Services Select the services that you are publi	shing on this mail server.	\uparrow
Exchange version:	Exchange Server 2007	•
Web client mail services:		
Outlook Web Access		
Cutlook Anywhere (RPC/HTTP(s))	
Publish additional folders on t	he Exchange Server for Outlook 2007 di	ents
🔲 Outlook Mobile Access		
Exchange ActiveSync		
	< Back Next >	Cancel

Figure 7: Publish OWA with Exchange Server 2007

We want to publish a single Website, so we select this option.

New Exchange 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 Forefront TMG load balance requests between a server farm (mirrored servers). Help about <u>publishing server farms</u>
< Back Next > Cancel

Figure 8: Publish a single Web site

Select SSL, so TMG will establish a secure connection with the Client Access Server (CAS).

New Exchange 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).
O 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 publishing over SSL, an appropriately named SSL server certificate must be installed on the published server, or on each server in the server farm.
< Back Next > Cancel

Figure 9: use SSL for connection to the published server

Enter the Internal Site name of the Client Access Server. This is the internal FQDN of the CAS server. The Internal Site name must match the Common Name (CN) of the certificate used on the Client Access Server.

New Exchange Publishing Rule Wizard				
Internal Publishing Details Specify the internal name of the Exchange site or server you are publishing.				
Internal site name: w2k8-ex2k7sp1.exchange.dom				
The internal site name is the name of the Web site you are publishing as it appears internally. Typically, this is the name internal users type into their browsers to reach the Web site.				
The internal site name must match the common or subject alternative name (SAN) on the certificate bound on the Web site that you are publishing.				
If Forefront TMG cannot resolve the internal site name, Forefront TMG can connect using the computer name or IP address of the server hosting the site.				
Use a computer name or IP address to connect to the published server				
Computer name or IP address: Browse				
< Back Next > Cancel				

Figure 10: Specify the internal site name

In the next step of the wizard, enter the public name which clients must use in their browsers to access the published Outlook Web Access Server through the Internet.

New Exchange Publishing Rule Wizar	d X
Public Name Details Specify the public domain name (F published site.	QDN) or IP address users will type to reach the
Accept requests for: Only requests for this public name or IP	This domain name (type below):
Public name:	owa.it-training-grote.de
	Example: www.contoso.com
	< Back Next > Cancel

Figure 11: Specify the public name to access OWA

Create a new OWA Web listener. The web listener should use SSL due to security reasons.

New Web Listener Definition Wizard
Client Connection Security Select what type of connections this Web Listener will establish with clients.
Require SSL secured connections with clients Forefront TMG will publish servers only over HTTPS to the clients (recommended).
O Do not require SSL secured connections with clients Forefront TMG will publish servers over HTTP. Client credentials will be sent unencrypted to the Forefront TMG computer.
When publishing over SSL, an appropriately named SSL server certificate must be installed on the Forefront TMG computer.
< Back Next > Cancel

Figure 12: Require SSL for connections with clients

Now it is time to select the Network on which Microsoft TMG should listen for incoming network traffic for Outlook Web Access. Select the External network and if you only have one IP address bound to the external network interface of TMG you can leave the setting unchanged, else you must select the IP address in the Listener which should be used to publish Outlook Web Access.

New Web Listener Definition V	Vizard	×		
Web Listener IP Addresses Specify the Forefront TMG networks, and the IP addresses on those networks, that will listen for incoming Web requests.				
Listen for incoming Web reque	ests on these networks:			
Name	Selected IPs	▲		
🗹 🌑 External	<all addresses="" ip=""></all>			
Hannover	<all addresses="" ip=""></all>	-		
🗖 📥 Internal	<all addresses="" ip=""></all>			
🔲 📥 Local Host	<all addresses="" ip=""></all>	-		
		-		
	Select IP Addresses			
Forefront TMG will compre requesting the content sup	ess content sent to clients through this Web Listener if the opport compression.	lients		
	< Back Next > Ca	ancel		

Figure 13: Select the Web listener for external requests

As a next step choose the certificate which will be bound to the weblistener for accessing OWA through the Internet. You must select the certificate which you had created with the MMC.

Select Certificate

? <u>_ D ×</u>

Issued To 🔺	Validity	Issued By	Expirati	on Date	Friendly Name
owa.it-training	. Valid	exchange-W2K8-E	02.08.2	2011	
TMG	Valid	TMG	10.06.2	2010	Microsoft Exchange
☑ TMG	Valid	TMG	10.06.2	2010	Microsoft Exchange
Show only valid ce	rtificates				
Show only valid cere server Name	rtificates Details:	Certificate Store		Private Key	
Show only valid cere ertificate Installation Server Name	rtificates Details:	Certificate Store Correctly installed (Local Mach	hine,	Private Key Correctly insta	alled
Show only valid cere ertificate Installation Server Name	rtificates Details:	Certificate Store Correctly installed (Local Mad	hine,	Private Key Correctly insta	alled
Show only valid cere ertificate Installation Server Name TMG	rtificates Details:	Certificate Store Correctly installed (Local Mac	hine,	Private Key Correctly insta	alled

Figure 14: Select the certificate for public OWA access

Select Formas Based Authentication (FBA) with Windows authentication.

New Web Listener Definition Wizard		×
Authentication Settings Select how clients will authenticate to For validate their credentials.	refront TMG, and how Forefront TMG will	\mathbb{R}
Select how clients will provide credentials to	o Forefront TMG:	
HTML Form Authentication		
Collect additional delegation credentials	in the form	
The logon form will include additional fie the credentials for authentication to pub	lds for user credentials. Forefront TMG will lished servers.	use
Select how Forefront TMG will validate clier	nt credentials:	
Windows (Active Directory)	C RADIUS OTP	
C LDAP (Active Directory)	C RSA SecurID	
C RADIUS		
	< Back Next > 0	Cancel

Figure 15: Select Authentication method

Because we don't use SSO (Single Sign On), uncheck the SSO option.

New Web Listener Definition Wizard	×
Single Sign On Settings Single Sign On (SSO) allows users to authenticate once to Forefront TMG to access all published Web sites that use this Web listener.	
Enable SSO for Web sites published with this Web listener The SSO domain name specifies the published sites between which this Web listener will allow SSO to be applied.	
SSO domain name: Example: To enable SSO between sites 'portal.contoso.com' and 'sales.contoso.com', the SSO domain is .contoso.com	
< Back Next > Cancel	

Figure 16: Deactivate SSO

Click Finish and next.

As the Authentication Delegation method select Basic Authentication. Because Basic Authentication is used with SSL this is not a security problem.

New Exchange Publishing Rule Wizard	×
Authentication Delegation Authentication delegation is the method Forefront TMG uses to authenticate the session it opens with the published site.	\downarrow
Select the method used by Forefront TMG to authenticate to the published Web server:	
Basic authentication	•
Description Forefront TMG will use Basic authentication to authenticate the client to the published Wel server. The published Web server must be configured to accept Basic authentication.	D
< Back Next > Cance	

Figure 17: Authentication Delegation

After that, select the users and user groups which should be allowed to access Outlook Web Access through the Internet.

New Exchange Publishing Rule Wizard			×
User Sets You can apply the rule to requests from all specific user sets.	users. Or, you o	an limit access t	»
This rule applies to requests from the following	user sets:		
🚵 All Authenticated Users			Add
			Edit
			Remove
	< Back	Nexts	Cancel
	< DOCK	NEXT >	Cancer

Figure 18: Select users who should use OWA through TMG

Click Finish and Apply

After the wizard has successfully finished you can test your configuration. For this article I accessed the OWA website with my Windows 7 Netbook.

ℰ Microsoft Exchange - Outlook Web Access - V	/indows Internet Explorer	
🚱 🕞 🗢 🙋 https://owa.it-training-grote.d	e/CookieAuth.dll?GetLogon?reason=0&formdir=1&curl=Z2Fo 🔻 🔒 🛛 😽 🗙 🏷 Bing	• ٩
🖕 Favorites 🛛 👍 🖉 Suggested Sites 👻 🍘	Web Slice Gallery 🔻	
Hicrosoft Exchange - Outlook Web Access	🔐 🕶 🗟 👻 🖾 🖶 🕶	Page ▼ Safety ▼ Tools ▼ 🕢 ▼
		A
	Source to Microsoft Exchange Source Source	
		-
Done	Internet Protected Mode: Off	🖓 🔻 🔍 100% 👻 🖉
🚱 🌔 🚞 🖸		DE 😼 🎝 🕼 02.08.2009

Figure 19: Successfully connected to the OWA website through the Internet

Conclusion

In this article, I tried to show you how to publish Exchange Server 2007 Outlook Web Access with Microsoft Forefront TMG. As you have seen, publishing OWA with TMG is the same as in ISA Server 2006, so you shouldn't have problems to publish the required resources with TMG if you are familiar with the ISA Server 2006 Firewall.

Related links

Forefront Threat Management Gateway Beta 3 http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&displaylang=en Forefront TMG Beta 3 is Released http://blogs.technet.com/isablog/archive/2009/06/09/forefront-tmg-beta-3-isreleased.aspx What's new in Forefront TMG Beta 2 (Part 1) http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html Installing and configuring Microsoft Forefront TMG Beta 2 http://www.isaserver.org/tutorials/Installing-configuring-Microsoft-Forefront-TMG-Beta2.html