IIS 7.5 mit Exchange Server 2010 – OWA FBA Intern und Extern ueber Forefront TMG

Interne Exchange Benutzer sollen Outlook Web Access mit Formularbasierter Authentifizierung (FBA) verwenden. Aber auch Benutzer aus dem Internet sollen OWA mit FBA verwenden. Hier wird die FBA von Forefront TMG generiert und wenn Intern und Extern FBA aktiv ist, bekommen Benutzer aus dem Internet eine doppelte FBA Anmeldung. Um das Problem zu loesen kann man mit zwei virtuellen Verzeichnissen im IIS arbeiten. Das eine virtuelle Verzeichnis verwendet FBA fuer Aufrufe von OWA (OutlookWebApp) intern, das andere Vdir verwendet Basic Authentication. Forefront TMG wird so konfiguriert, dass auf das virtuelle Verzeichnis mit Basic Authentication umgeleitet wird.

Zweite IP-Adresse

Zuerst wird eine zweite IP Adresse auf dem Exchange Server 2010 benoetigt, welche fuer das neue virtuelle Verzeichnis eingerichtet wird.

Advar	nced TCP/IP Settings		? ×	
IP Se	ettings DNS WINS			
	P addresses			
	IP address	Subnet mask		
	192.9.200.78	255.255.255.0		
	TCP/IP Address		?×	
	IP address:	192 . 9 . 200 . 79		
	Subnet mask:	255 . 255 . 255 . 0		
		Add Ca	ancel	
	A	dd Edit	Remove	
Automatic metric Interface metric:				
		ОК	Cancel	

Um zu verhindern, dass alle IP-Adressen im DNS registriert werden, sondern nur die primaere IP-Adresse fuer den internen OWA Aufruf, muss ein Hotfix im System eingespielt werden (wenn das System Windows Server 2008 ist. Fuer Windows Server 2008 R2 existiert der Fix (noch) nicht):

http://support.microsoft.com/kb/975808/en-us

Danach kann mit NETSH festgelegt werden, welche IP-Adresse NICHT im DNS registriert werden soll:

Netsh int ipv4 add address <Interface Name> <ip address> skipassource=true

Auf einem Windows Server 2008 R2 ist die derzeit einzig mir bekannte Moeglichkeit, die dynamische DNS Registrierung auf dem Server auszuschalten und den A Record im DNS manuell anzulegen:



Anschliessend in der DNS-Verwaltung einen statischen A-Eintrag mit der IP-Adresse des DNS Servers erstellen (den dynamischen DNS Record vorher loeschen).

IP-Adresszuordnung auf der Default Web Site anpassen



	Host Name	Port	IP Address	Bind 🔺	Add
net.pipe				*	
net.m				loca	Edit
msmq				local	Remove
http		80	192.9.200.78		Kelliove
nttps		443	192.9.200.78		Browse
nttps		443	127.0.0.1		
<u>ا ا</u>				•	
					Close
Edit	Site Binding				? ×
					ror Pag
	ype:	IP address:		Port:	_
h	ttps 🔻	192.9.200.7	78	■ 443	
н	ost name:				
ШГ					Logging
	Cl. anntificantes				
	SL certificate:				
S S					

Neue Website erstellen und an die zweite IP binden

dd Web Site			?
Site name:	Application pool:		
TMG-OWA-FBA	TMG-OWA-FBA		Select
Content Directory			
Physical path:			
C:\inetpub\TMG-OWA-FBA			
Pass-through authenticatio	n		
Connect as Test Se	ttings		
-Binding			
Type: IP ad	dress:	Port:	
https 💌 192.	9.200.79	▼ 443	
Host name:			
SSL certificate:			
W2K8.exdom.intern		▼ View	
,			
Start Web site immediately	/		
		OK	Cancel
	l	UN	Cancer

Ein neues SSL Zertifikat ausstellen auf einen Namen, welcher vom Forefront TMG Server aufloesbar sein muss. Ggfs. auf dem TMG Server den Hostnamen in die HOSTS Datei eintragen. Das Zertifikat muss von einer vertrauenswuerdigen Zertifizierungsstelle (welcher auch der Forefront TMG vertraut) ausgestellt werden.

Request Certificate					
Distinguished	I Name Properties				
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.					
Common name:	TMG-OWA-FBA.exdom.intern				
Organization:	IT TRAINING GROTE				
Organizational unit:	Π				
City/locality	Nienstaedt				
State/province:	Niedersachsen				
Country/region:	DE				
	Previous Next Finish Canc	el			

CSP und Schluessellaenge auswaehlen

Request Ce	rtificate				? ×
F	Cryptographic Service Pro	ovider Prope	erties		
Select a c determine However,	ryptographic service provider and a es the certificate's encryption strengt , a greater bit length may decrease p	bit length. The b th. The greater t performance.	it length of the he bit length, th	encryption key ne stronger the sec	curity.
Cryptogra	aphic service provider:				
Microsoft	RSA SChannel Cryptographic Provid	er	•		
Bit length	:				
2048	▼				
		Previous	Next	Finish	Cancel

Request Certificate				? X
File Name				
Specify the file name for the certificate reque authority for signing.	st. This informatio	n can be sent to a ce	rtification	
Specify a file name for the certificate request	:			
C:\temp\TMG-OWA-FBA.txt				
				1
	Previous	Next	Finish	Cancel

Inhalt der Anforderungsdatei in die Zwischenablage kopieren



Microsoft Active Directory Certificate Services - Windows	Internet Explorer
COO V Attps://192.9.200.78/certsrv/certrqad.asp	🔽 😵 Certificate Error 🛛 🗟 🐓 🗙 🕞 Bing
🔆 Favorites 🛛 🚔 🙋 Suggested Sites 🔹 🙋 Web Slice Gallery 🗣	
GMicrosoft Active Directory Certificate Services	🏠 👻 🗟 👻 🖃 👘 👻 Page 👻 Safety 👻 Tools 👻 🌘
Microsoft Active Directory Certificate Services - exdon Advanced Certificate Request	n-W2K8-CA <u>Home</u>
The policy of the CA determines the types of cer Create and submit a request to this CA.	tificates you can request. Click one of the following options to:
<u>Output a certificate request by using a base-</u> <u>PRCS #7 file.</u>	34-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded

Zertifikatvorlage ist Webserver. CSR Request aus der Zwischenablage pasten

Altor Services - Windows Internet Explorer - Windows Internet Explorer		_ 8				
🚱 🕞 🗢 🙋 https://192.9.200.78/certsrv/certrqxt.asp	💌 😵 Certificate Error 🛛 🚱 🍫 🗙 🔁 Bing	P				
🔆 Favorites 🛛 🚔 Suggested Sites 🔻 💋 Web Slice Gallery 👻						
Hicrosoft Active Directory Certificate Services	🏠 🔻 🔝 🤟 📑 🛻 🔹 Page + Safety + Ti	ools + 👔				
Microsoft Active Directory Certificate Services exdom-W2K8-CA		Home				
Submit a Certificate Request or Renewal Request						
To submit a saved request to the CA, paste a base-64-encoded (generated by an external source (such as a Web server) in the Sa Saved Request:	To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.					
W2v4T0BjK6oFNVay+2rA9ScxTR4x2/5V3VMjrCGm Base-64-encoded i+c9qY41/0gbjPA4pUaLk3bDmvorfoJOY620x22n cettificate request KIE02QkJEoBRCCAWiKpkg2gsbSpwukgXIN7E4Bgp (CMC or YaoK5HLG8DOIuPm0h1RhNH16RwJacCzZWo4Jww84 PKCS #7):						
Certificate Template:						
Web Server						

Services - Windows Internet Explorer				
🖕 Favorites 🛛 🚖 🙋 Suggested Sites 👻 🍘 Web Slice Gallery 👻				
Microsoft Active Directory Certificate Services				
Microsoft Active Directory Certificate Services exdom-W2K8-CA				
Certificate Issued				
The certificate you requested was issued to you.				
OER encoded or OBase 64 encoded				
Download certificate Download certificate chain				

Zertifikatrequest im IIS abschliessen

Hanager (IIS) Manager					
				🗾 🖸 🖂 🟠 I 🕖 🝷	
File View Help					
Connections Start Page W2K8 (SkDOM \Administrator) Application Pools	Server Ce Use this feature to reque configured for SSL.	rtificates	server can use with Web sites	Actions Import Create Certificate Request Complete Certificate Request	
Sites	Name 🔺	Issued To	Issued By	Create Domain Certificate	
🗄 豰 Default Web Site		W2K8.exdom.intern	exdom-W2K8-CA	Create Domain Certificate	
ADPolicyProvider_CEP_Kerberos		exdom-W2K8-CA	exdom-W2K8-CA	Create Self-Signed Certificate	
aspnet_client B				Help Online Help	
CER File angeben		<u>? ×</u>			
Specify Certificate Authority Res	ponse				
Complete a previously created certificate request by ret authority's response.	rieving the file that contains th	ne certificate			
File name containing the certification authority's respons	e:1				
C: \temp \certnew.cer					

OK Cancel

Friendly name: TMG-OWA-FBA.Exdom.intern

	W2K8.exdom.intern			
	The concrete of the concrete o	exdom-W2K8-CA		
	exdom-W2K8-CA	exdom-W2K8-CA		
-OWA-FBA.Exdom.intern	IMG-OWA-FBA.exdom.intern	exdom-W2K8-CA		
Certificate				
	1			
General De	tails Certification Path			
	Certificate Information			
This certificate is intended for the following purpose(s):				
This ce	Foruse the identity of a semate computer			
• E	insures the identity of a remote comp	uter		
• E	insures the identity of a remote comp	uter		
• E	insures the identity of a remote comp	uter		
• •	insures the identity of a remote comp	uter		
• •	insures the identity of a remote comp	uter		
• E	insures the identity of a remote comp	uter		
• E	insures the identity of a remote comp	uter		
+E	insures the identity of a remote comp	uter		
•E	insures the identity of a remote comp	uter		
ins ce •E	sued to: TMG-OWA-FBA.exdom.int	tern		
	sued to: TMG-OWA-FBA.exdom.int	uter		
	sued to: TMG-OWA-FBA.exdom.inf sued by: exdom-W2K8-CA	tern		
Ins ce •E	sued to: TMG-OWA-FBA.exdom.int	tern		
Ins ce •E Is	sued to: TMG-OWA-FBA.exdom.inf sued to: TMG-OWA-FBA.exdom.inf sued by: exdom-W2K8-CA	tern 9. 2012		
Ins ce •E	sued to: TMG-OWA-FBA.exdom.int sued to: TMG-OWA-FBA.exdom.int sued by: exdom-W2K8-CA	tern 9, 2012		
Inis ce •E Is Is Va Ŷ Yo	sued to: TMG-OWA-FBA.exdom.int sued to: TMG-OWA-FBA.exdom.int sued by: exdom-W2K8-CA alid from 13. 09, 2010 to 12. 0 u have a private key that correspond	tern 9. 2012 Is to this certificate.		
Inis ce • E Is Is Va Yo	sued to: TMG-OWA-FBA.exdom.int sued to: TMG-OWA-FBA.exdom.int sued by: exdom-W2K8-CA hild from 13. 09. 2010 to 12. 0 u have a private key that correspond	tern 19. 2012 Is to this certificate.		
Inis ce •E Is Is Va Ŷ Yo	sued to: TMG-OWA-FBA.exdom.inf sued to: TMG-OWA-FBA.exdom.inf sued by: exdom-W2K8-CA slid from 13.09.2010 to 12.0 u have a private key that correspond	tern 9. 2012 Is to this certificate.		
Inis ce • E Is Is V2 Ŷ Yo	sued to: TMG-OWA-FBA.exdom.int sued to: TMG-OWA-FBA.exdom.int sued by: exdom-W2K8-CA alid from 13.09,2010 to 12.0 u have a private key that correspond	tern 9. 2012 Is to this certificate. Issuer Stateme		

Zertifikat der neuen Website zuordnen (Binden)



Source: http://technet.microsoft.com/de-de/library/bb123752(EXCHG.140).aspx

🚱 Machine: W2K8.exdom.intern		
[PS] C:\Windows\system32>Net WARNING: Any new Outlook Wel specified. WARNING: You have created an the same web site.	w-OwaVirtualDirectory -name "TMG-FBA" b App virtual directories that you cr n OWA virtual directory. You also nee	Y -WebSiteName "TMG-OWA-FBA" eate will be named "owa", regardless of the name that's d to create a corresponding ECP virtual directory in
Name	Server	OwaVersion
owa (TMG-OWA-FBA)	W2K8	Exchange2010
[PS] C:\Windows\system32>		~

Neues ECP Virtual Directory

EPS 1	C:\Windows\system32>New-EcpVirtualDirectory -WebSiteNam	ws\system32>New-EcpVirtualDirectory -WebSiteName "TMG-OWA-FBA"					
Name	(TMC-000-FR0.)	Server					
EPS 1	C:\\/indows\system32>		•				

Ergebnis im IIS



Ergebnis in der EMC

Fuer OWA





owa (TMG-OWA-FBA) Properties								
Public Computer File Access Private Computer File Access Remote File Servers General Authentication Segmentation								
owa (TMG-OWA-FBA)								
Server: W2K8								
Web site: TMG-OWA-FBA								
Version: Exchange 2010								
Modified: Montag, 13. September 2010 07:53:04								
External URL:								
https://webmail.trainer.de								
OK Cancel Apply Help								

Das gleiche fuer das neue ECP Verzeichnis

ecp (TMG-OWA-FBA) Properties								
General Authentication								
ecp (TMG-OWA-FBA)								
Server:	W2K8							
Web site:	TMG-OWA-FBA							
Modified: Montag, 13. September 2010 07:55:39								
Internal URI								
	L .							
External UR	RL:							
https://web	bmail.trainer.de							
5	OK Cancel App	ly Help						

Authentication fuer das neue OWA und ECP Verzeichnis auf Basic Authentication stellen



BEMERKUNG:

Wenn ueber den Forefront TMG auch noch Exchange Active Sync gemacht werden soll und mit nur einem Listener gearbeitet wird, muss auf dem Exchange Server auch noch ein neues Exchange Active Sync Virtual Directory angelegt werden.

Auf Forefront TMG Seite

Auf Forefront TMG Seite muss jetzt in der Exchange Webclient Veroeffentlichungsregel auf der Registerkarte "Nach" der Exchange Server mit den neuen virtuellen Exchange Verzeichnissen angesprochen werden. Es muss also in der HOSTS Datei oder im DNS auf die neue IP-Adresse mit einem Namen verwiesen werden. Hierbei daran denken, dass der Common Name im Zertifikat enthalten sein muss, damit es zu keiner Zertifikat Fehlermeldung kommt.

Eigenschaften von Outlook WebApp									
Öffentlicher Name Linkübersetzung A Allgemein Aktio Diese <u>R</u> egel gilt für d	Pfac Authentifizi on Vo die veröffe	le Bridgin ierungsdelegieru n Nach ıntlichte Site:	g Ben ung Anwe Datenv	utzer Indungs Verkehr	Zeitplan seinstellungen Listener				
TMG-0WA-FBA.EXDOM.INTERN									
 Name oder IP-Adresse des Computers (erforderlich, wenn der interne Sitename unterschiedlich ist oder nicht aufgelöst werden kann): 									
				<u>D</u> urch	isuchen				
Ursprünglichen Hostheader anstelle des aktuellen Headers weiterleiten, der im Feld für den internen Sitenamen angegeben ist Anforderungen an die veröffentlichte Site weiterleiten Legen Sie fest, wie die Firewall Anforderungen an den									
veröffentlichten Server weiterleitet: <u>U</u> rsprung der Anforderungen scheint der Forefront TMG-Computer zu sein									
C Ursprung der Anforderungen scheint der ursprüngliche <u>C</u> lient zu sein									
Regel testen		OK	Abbrech	nen	0 <u>b</u> ernehmen				