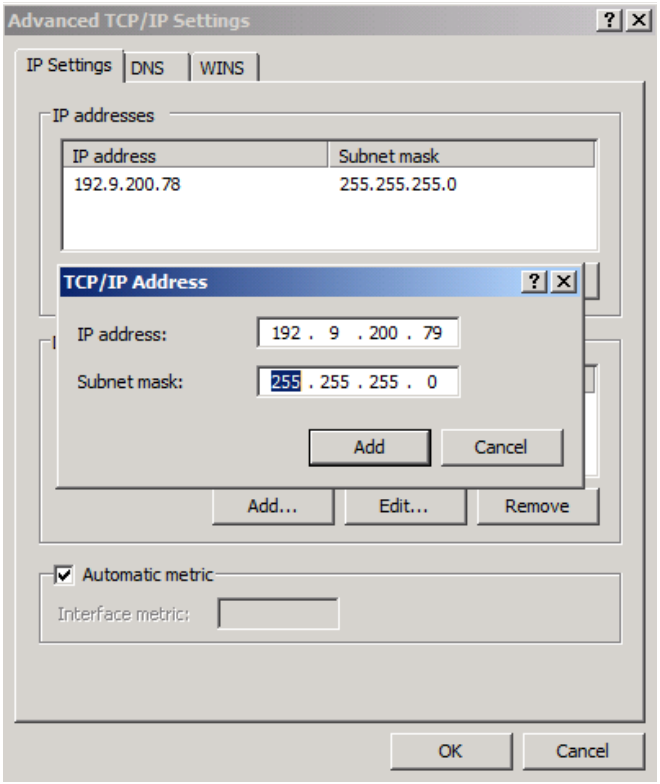
IIS 7.5 mit Exchange Server 2010 – OWA FBA Intern und Extern ueber Forefront TMG

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.



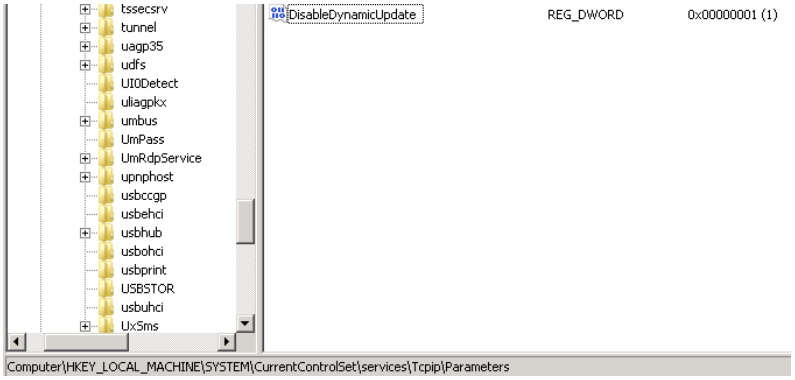
Um zu verhindern, dass alle IP-Adressen im DNS registriert werden, sondern nur die primaere IP-Adresse fuer den internen OWA Aufruf, muss ein Hotfix im System eingespielt werden (wenn das System Windows Server 2008 ist. Fuer Windows Server 2008 R2 existiert der Fix (noch) nicht):

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

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

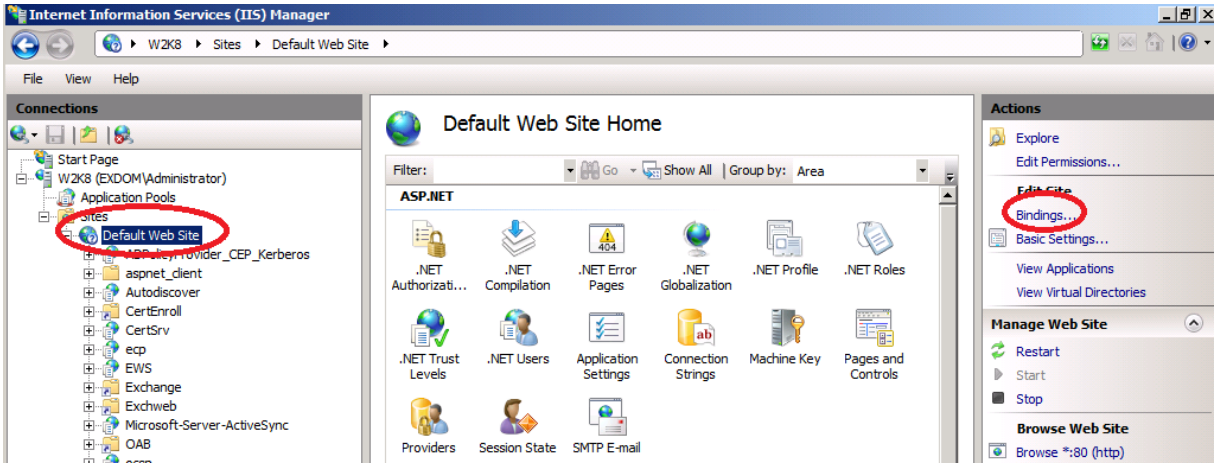
Netsh int ipv4 add address <Interface Name> <ip address> skipassource=true

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:

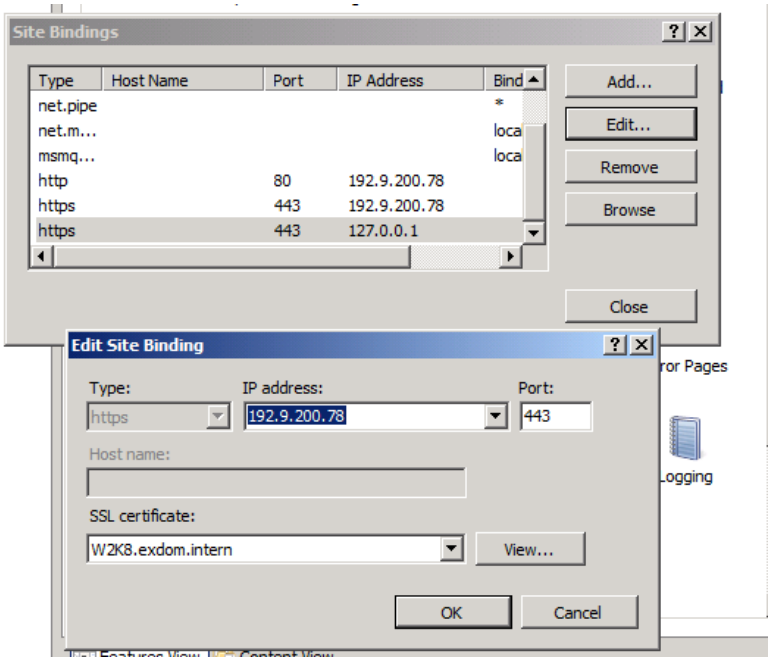


Anschliessend in der DNS-Verwaltung einen statischen A-Eintrag mit der IP-Adresse des DNS Servers erstellen (den dynamischen DNS Record vorher loeschen).

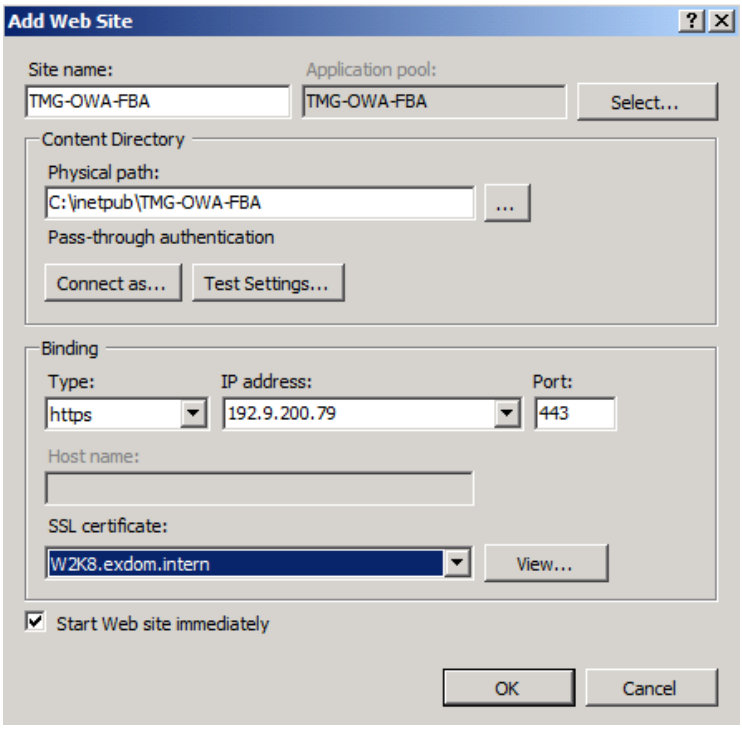
IP-Adresszuordnung auf der Default Web Site anpassen



Die Bindings der Default Webseite auf die explizite IP Adresse setzen

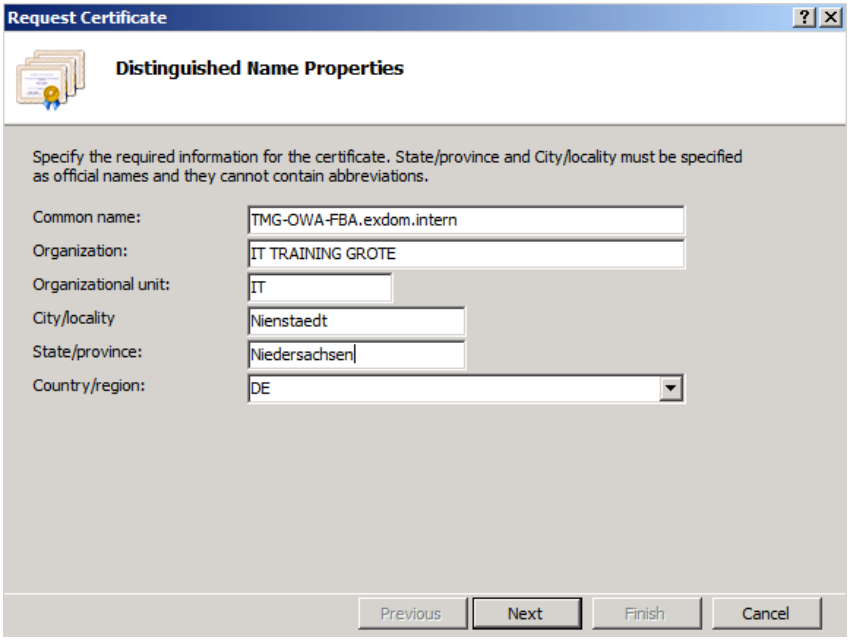


Neue Website erstellen und an die zweite IP binden

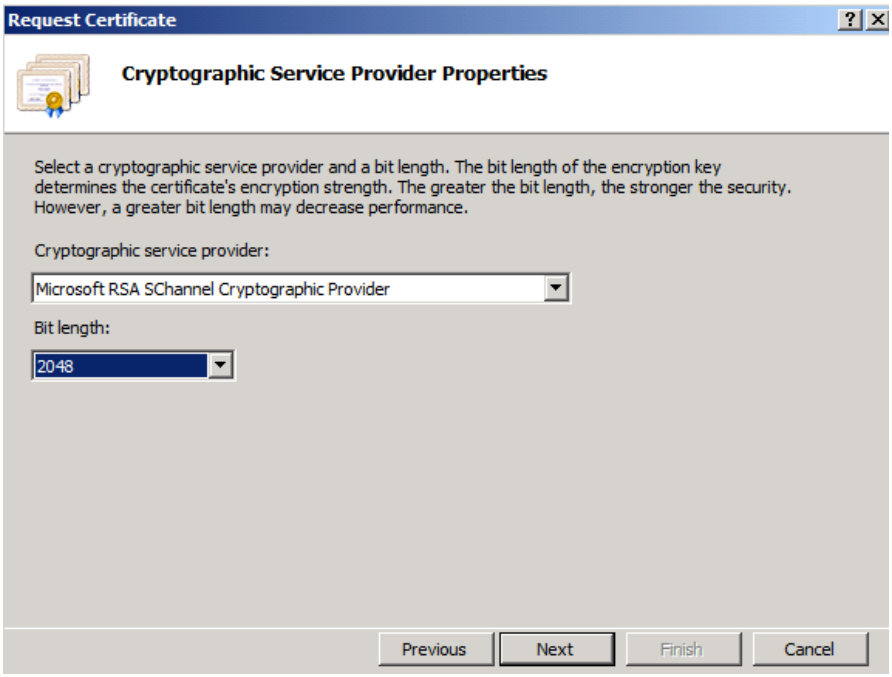


Ein neues SSL Zertifikat ausstellen auf einen Namen, welcher vom Forefront TMG Server aufloesbar sein muss. Ggfs. auf dem TMG Server den Hostnamen in die HOSTS Datei eintragen. Das Zertifikat muss von einer vertrauenswuerdigen Zertifizierungsstelle (welcher auch der Forefront TMG vertraut) ausgestellt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

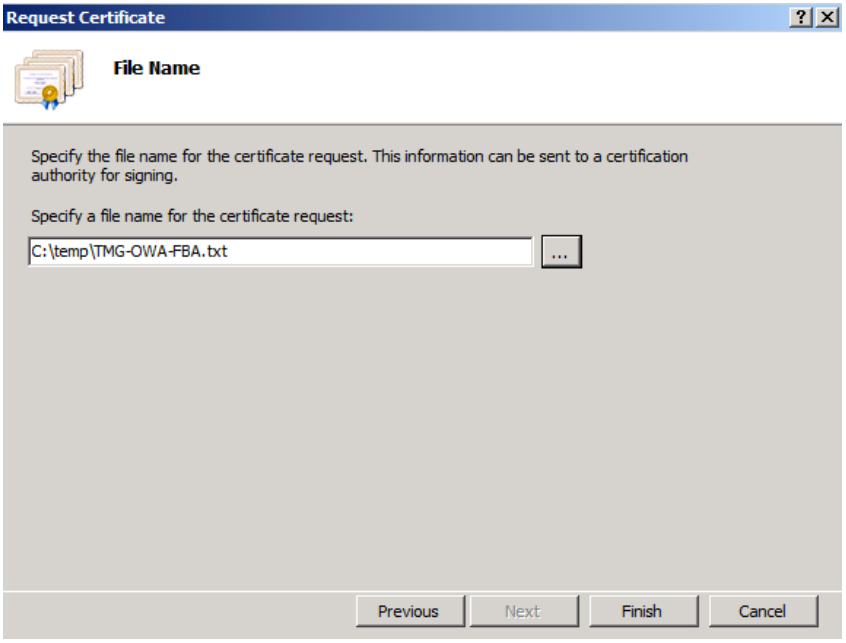
Zertifikatanforderung stellen



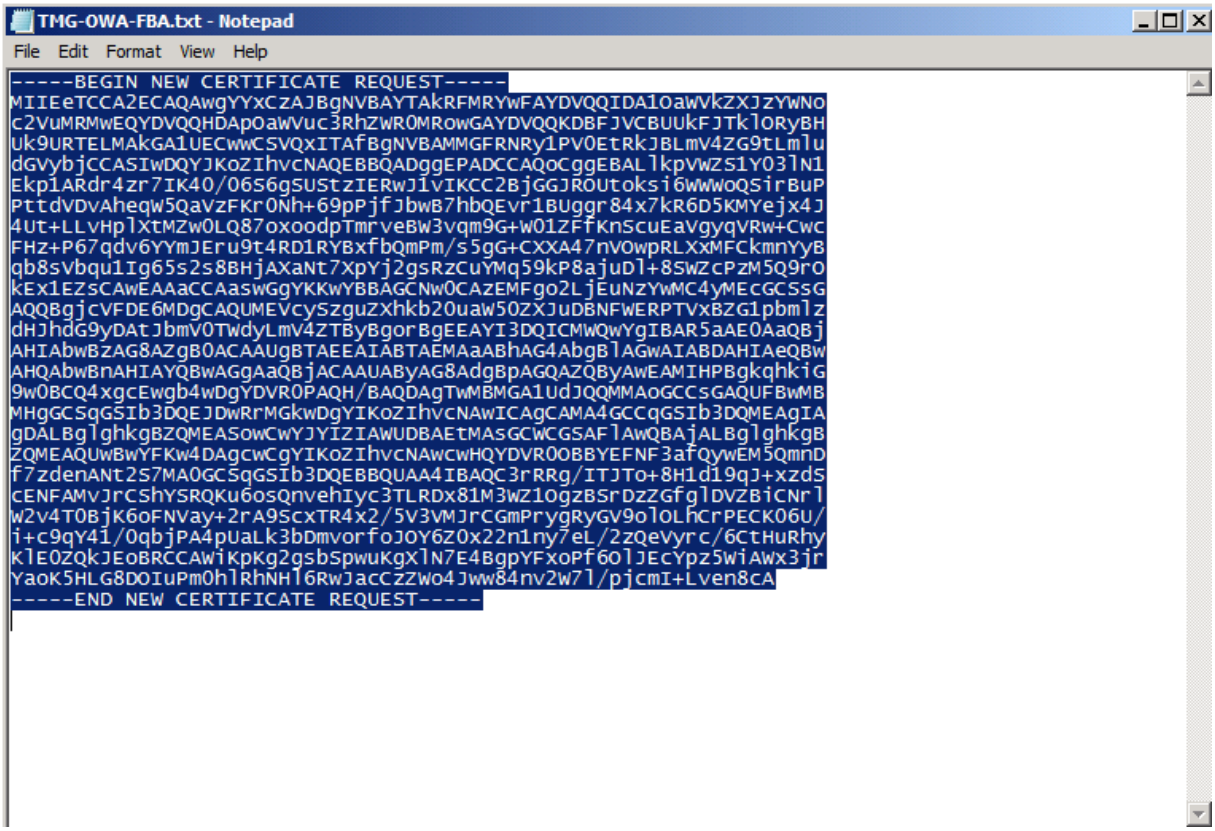
CSP und Schluessellaenge auswaehlen



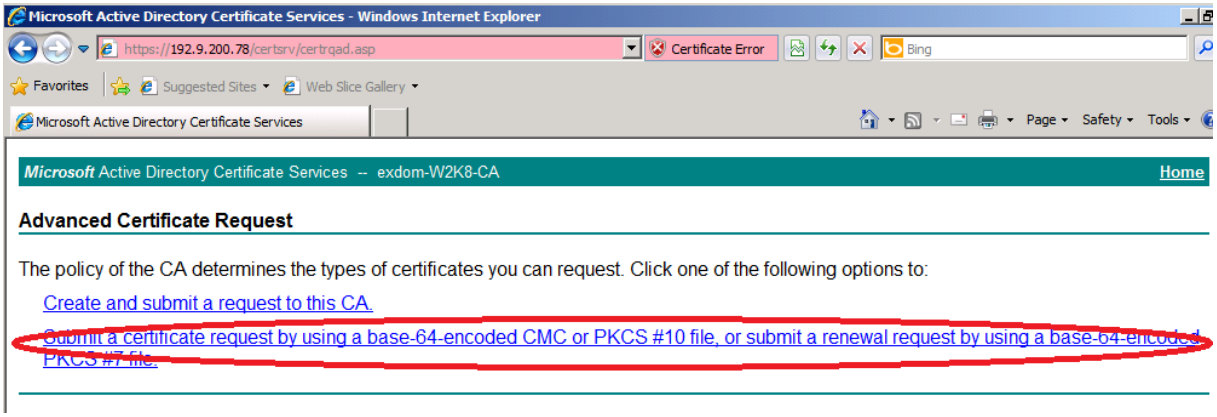
Signing Request Datei erstellen



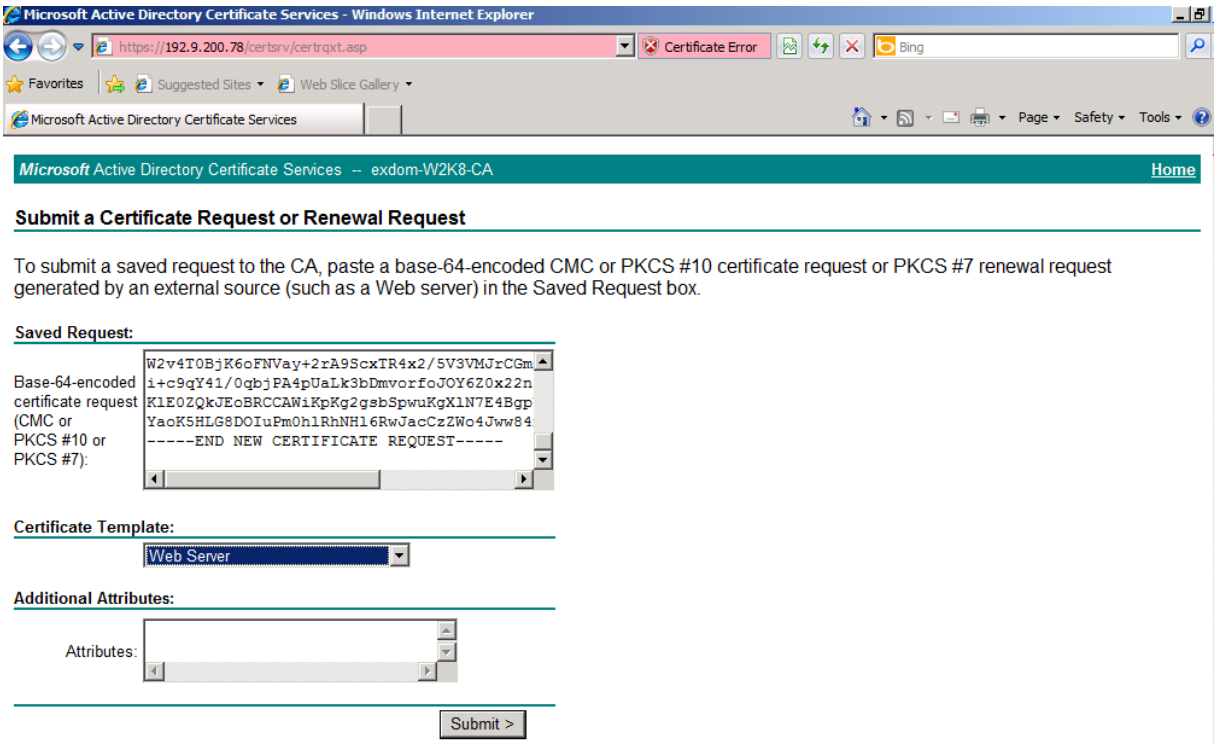
Inhalt der Anforderungsdatei in die Zwischenablage kopieren



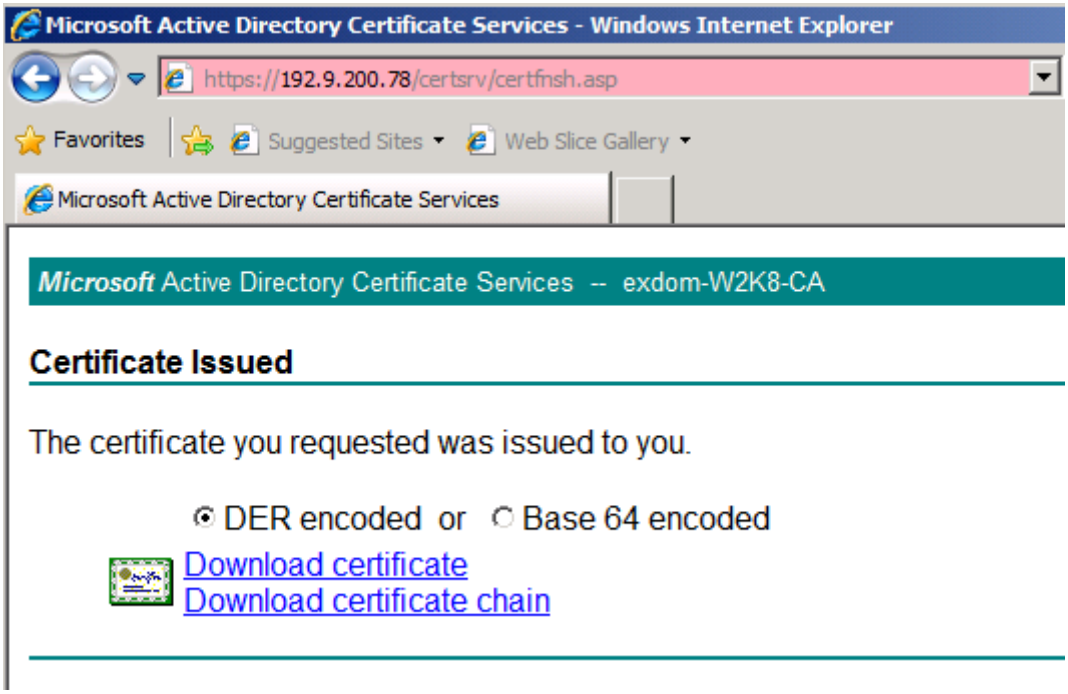
Advanced Certificate Request einreichen



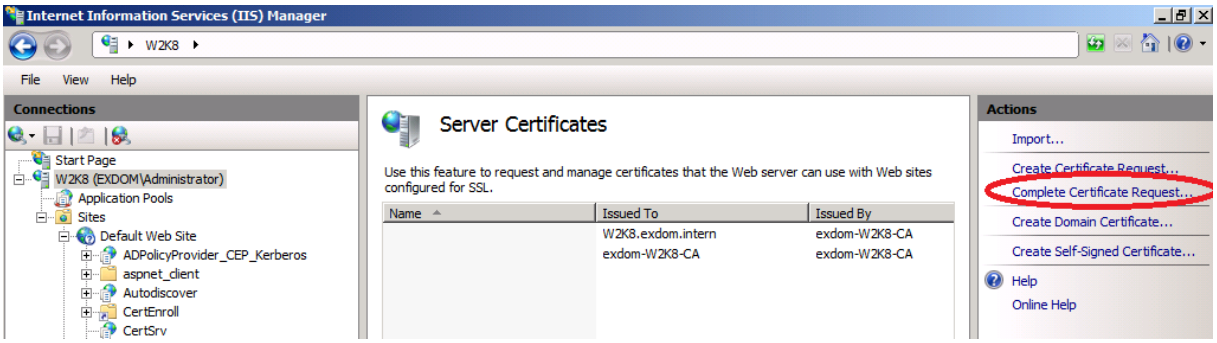
Zertifikatvorlage ist Webserver. CSR Request aus der Zwischenablage pasten



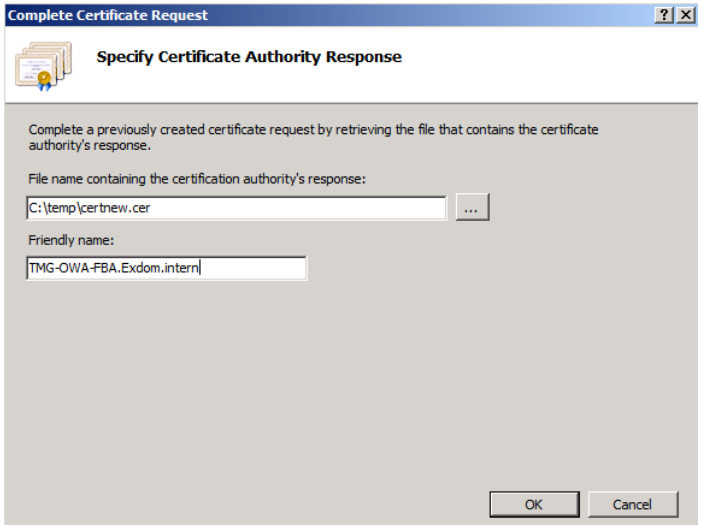
Zertifikat downloaden



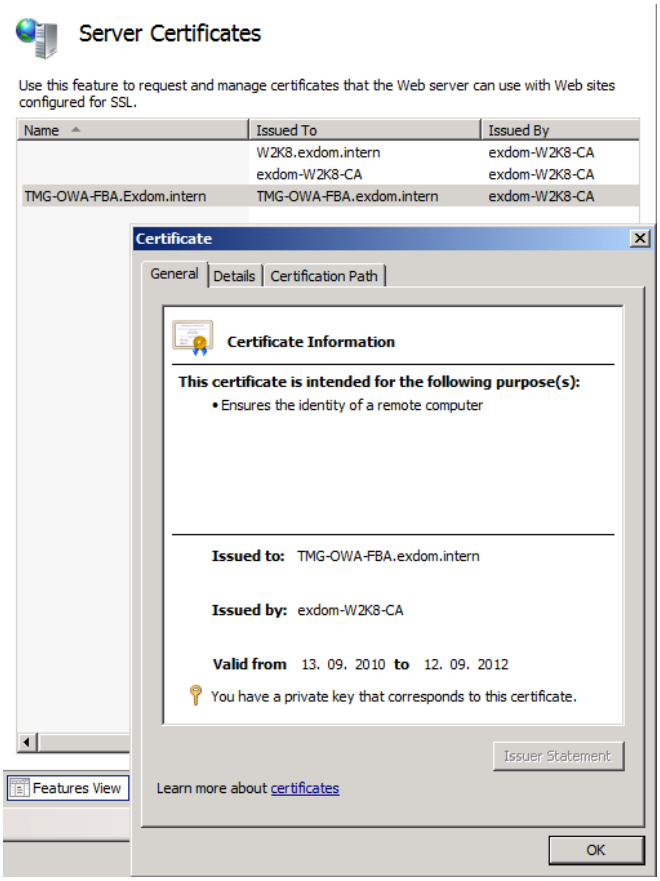
Zertifikatrequest im IIS abschliessen



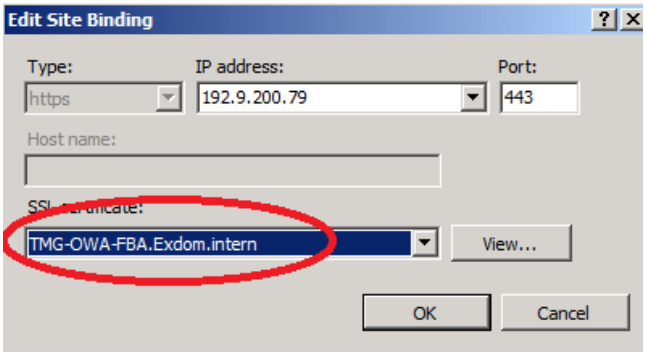
.CER File angeben



Fertig

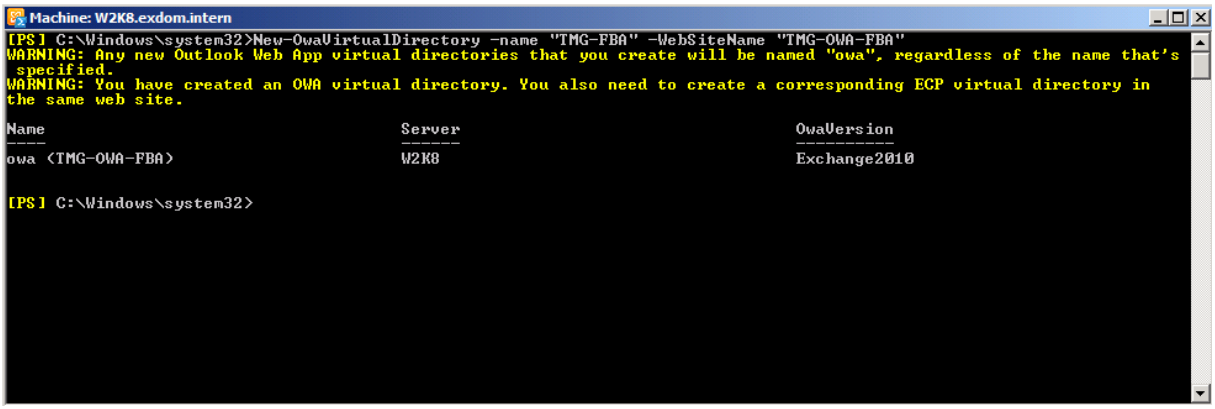


Zertifikat der neuen Website zuordnen (Binden)



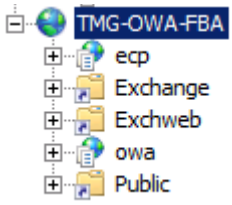
Neues OWA Virtual Directory erstellen

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



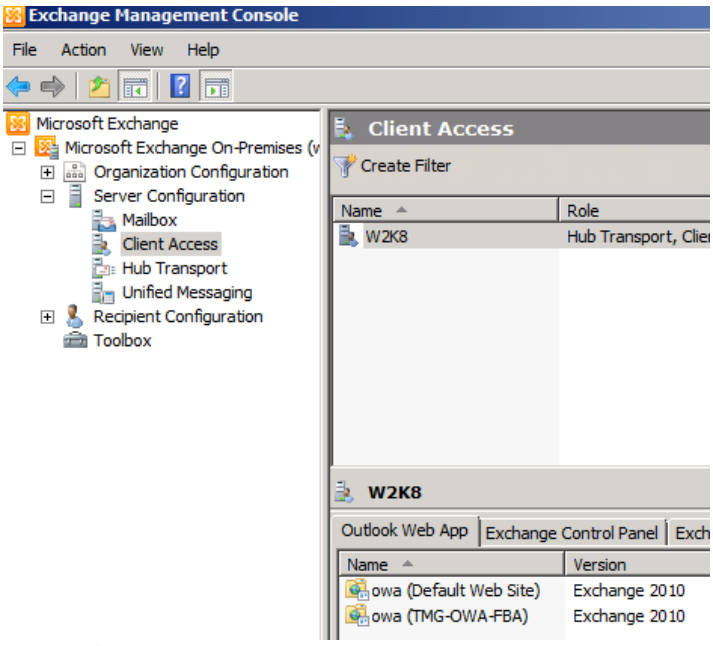
Neues ECP Virtual Directory

Ergebnis im IIS

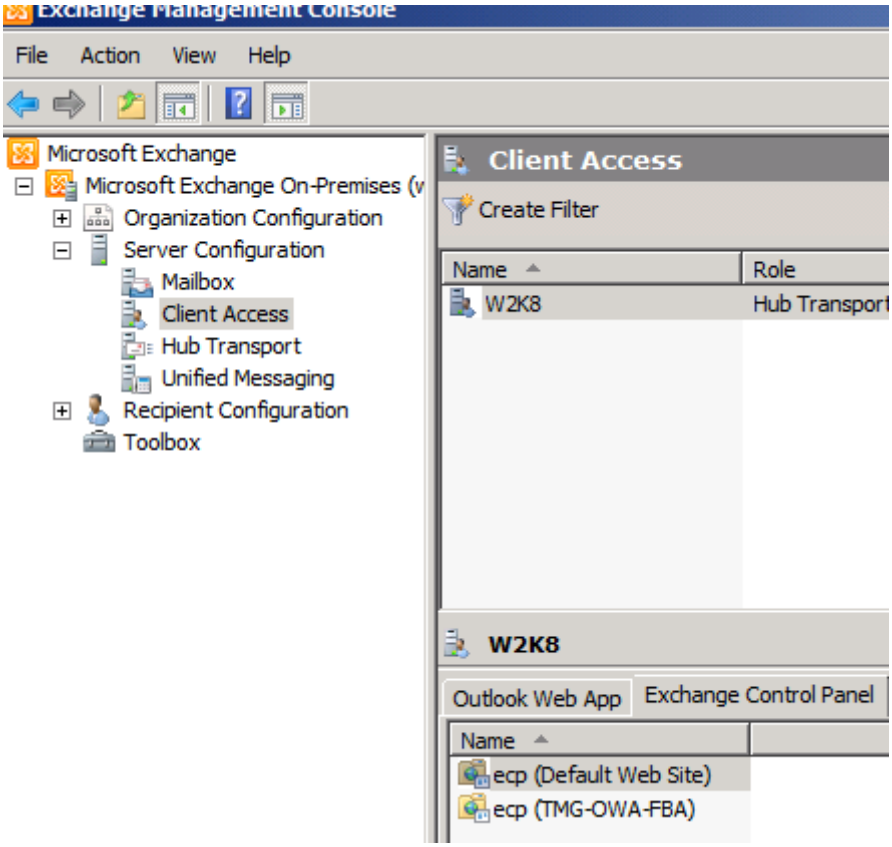


Ergebnis in der EMC

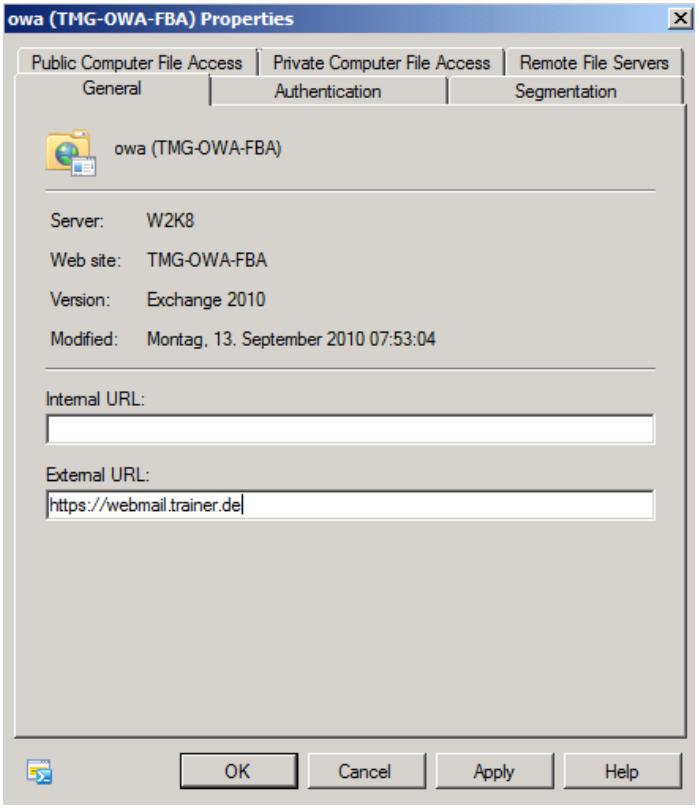
Fuer OWA



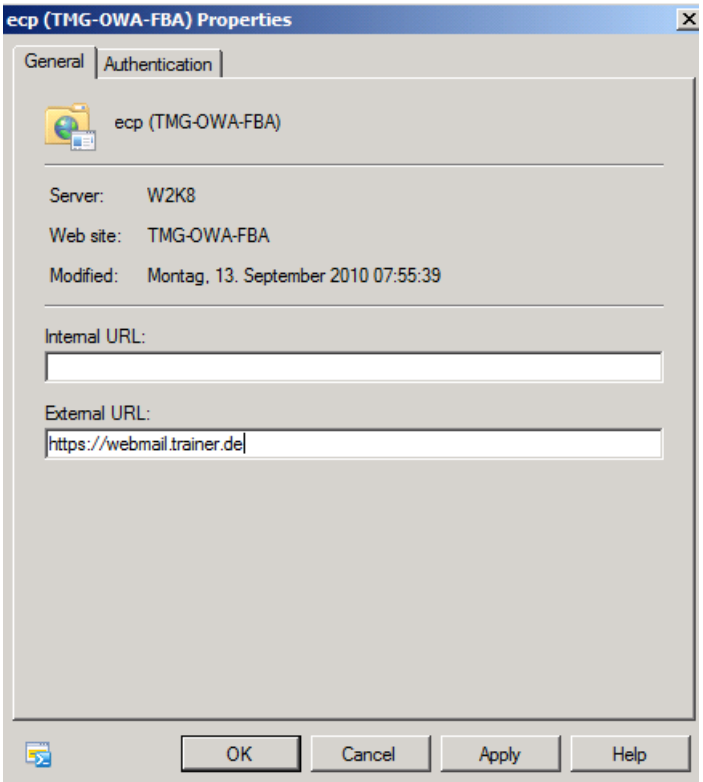
Fuer das ECP



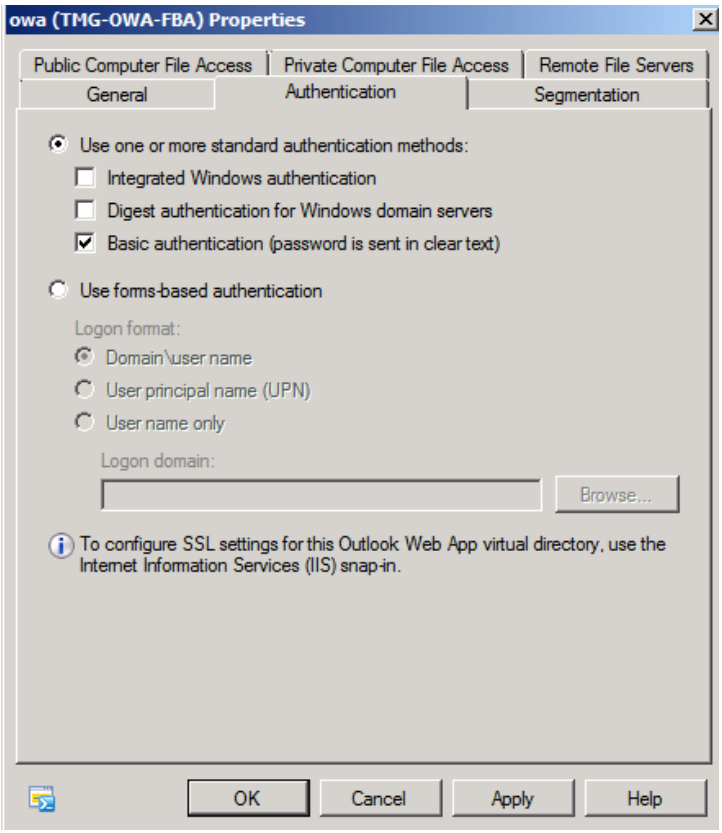
External URL anpassen. Die Internal URL kann leer bleiben



Das gleiche fuer das neue ECP Verzeichnis



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

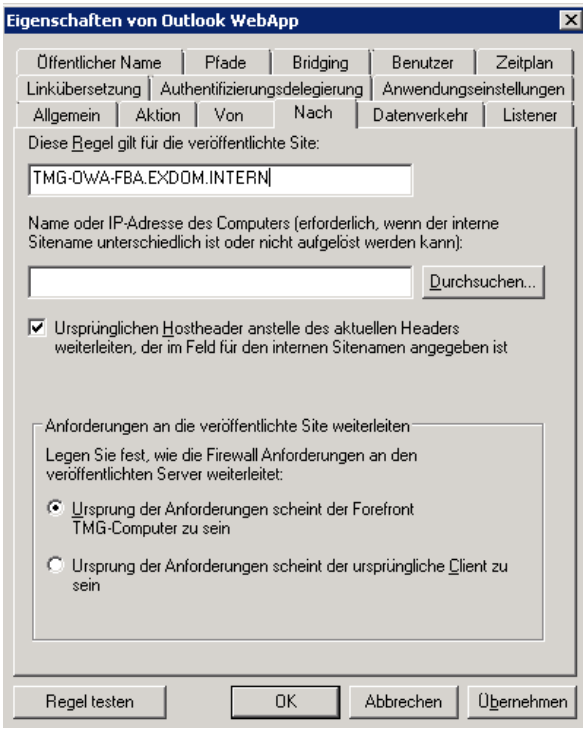


BEMERKUNG:

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
Pfade
Bridging
Benutzer
Zeitplan
Linkübersetzung
Authentifizierungsdelegierung
Anwendungseinstellungen
Allgemein
Aktion
Von
Nach
Datenverkehr
Listener
Diese Regel gilt für die veröffentlichte Site:
TMG-OWA-FBA.EXDOM.INTERN
Name oder IP-Adresse des Computers (erforderlich, wenn der interne Sitename unterschiedlich ist oder nicht aufgelöst werden kann):
Durchsuchen...
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:
Ursprung der Anforderungen scheint der Forefront TMG-Computer zu sein
Ursprung der Anforderungen scheint der ursprüngliche Client zu sein
Regel testen
OK
Abbrechen
Übernehmen