

HTTPS Inspection in Forefront TMG und IP-Ausnahmen

dieser Beitrag ergaenzt die Aussage des Microsoft TMG Support aus meinem Artikel:
<http://www.it-training-grote.de/blog/?p=2591>

In dem Artikel steht, dass man mit Forefront TMG keine Ausnahmen von der HTTPS Inspection fuer IP-Adressen machen kann.

Die Original Aussage des MS Support war:

“No, but if you know the certificate subject and SAN names used by those services, you can enter those in the exceptions.

TMG uses the subject and SAN attributes to determine if the upstream server is “exceptional” as well as how to build the spoof cert if it needs to. The primary reason IPs aren’t usable is that in the hosted cloud Internet of today, IP addresses do not represent anything even remotely like “identity” and identity is exactly the context in which certificate validation operates.”

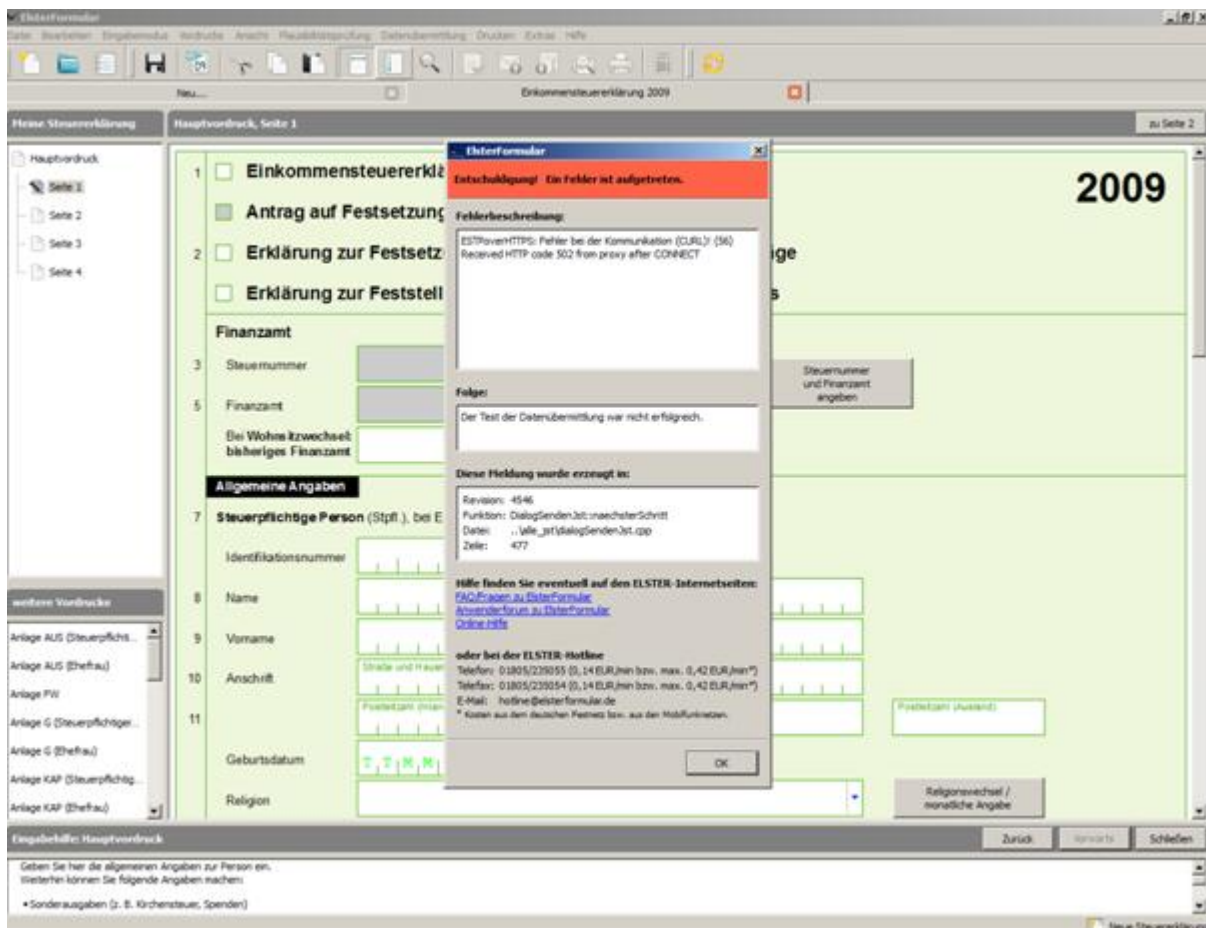
Dem scheint nicht so zu sein. In einem Posting in der deutschen ISA Server Newsgroup vom 30.04.2010 schreibt Alex111:

“Nachtrag: zum Glück erlaubt es TMG die IP wie folgt einzugeben. So hat es bei mir funktioniert: *.236.97.247”

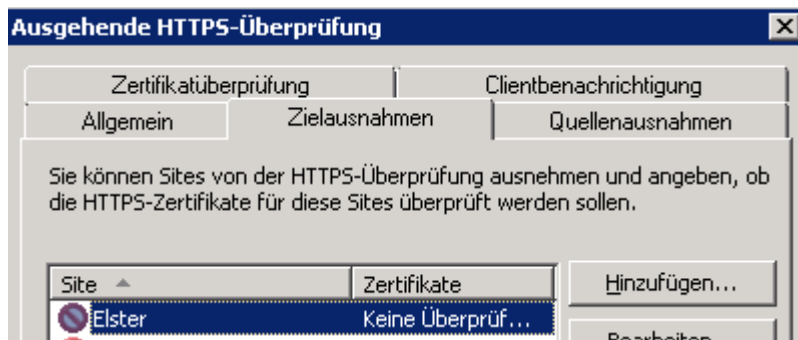
Quelle:

<http://www.it-training-grote.de/blog/?p=2906>

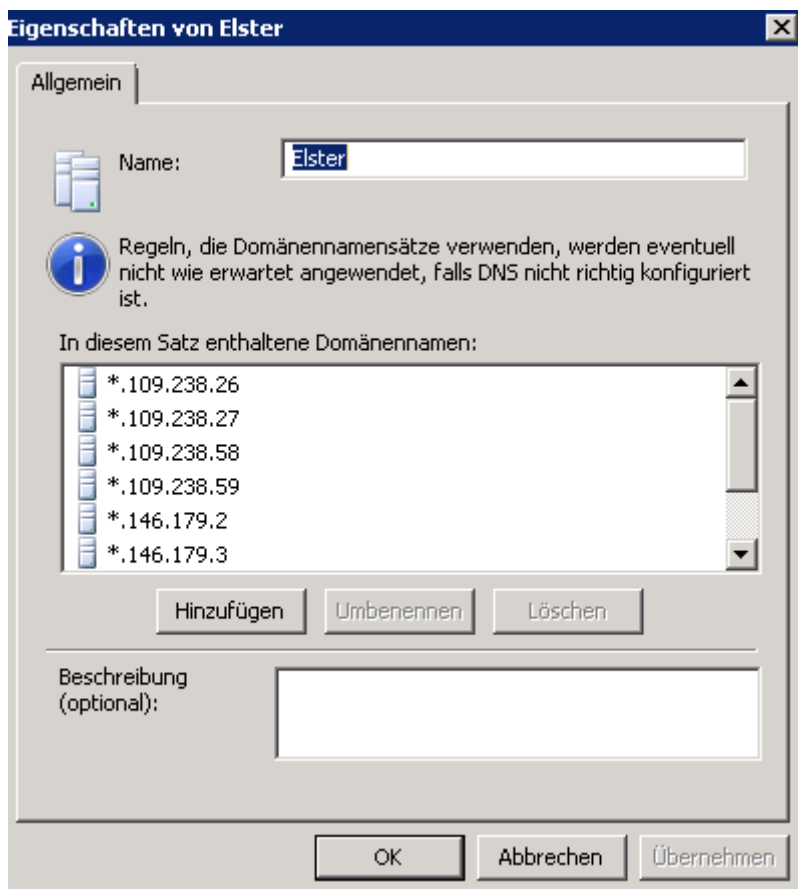
Ohne HTTPS Inspection Ausnahmen



Konfiguration der Ausnahmen der HTTPS-Ueberpruefung in Forefront TMG



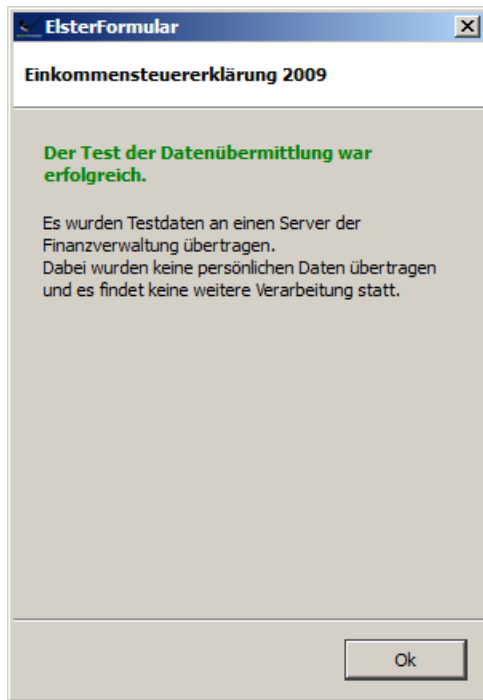
Konkret heissen die Ausnahmen von der HTTPS Ueberpruefung fuer Elster:



Quelle:

https://www.elster.de/elfo_faq.php?faqid=e13#e13

Mit HTTPS Inspection Ausnahmen



Wichtiger Hinweis:

Wenn am Forefront TMG Server Firewallregeln mit Benutzerauthentifizierung verwendet werden, muss man im Elsterformular bei den Proxy-Einstellungen den entsprechenden Windows Benutzernamen und das Kennwort hinterlegen UND nicht vergessen das Kontrollkästchen zur dauerhaften Speicherung des Kennworts zu aktivieren UND nicht vergessen, bei einer Windows Account Kennwortaenderung das Kennwort in den Elster Proxyeinstellungen ebenfalls anzupassen.