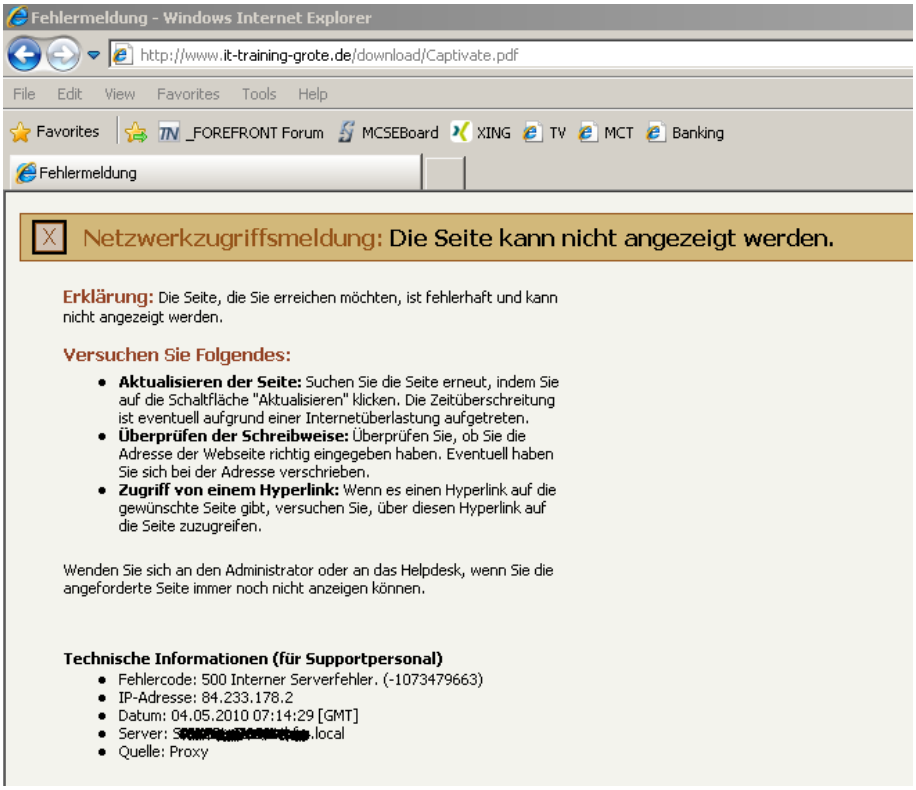
Forefront TMG - 0xc0040011 FWX_E_IS_BUSY

Nach der Implementierung von Forefront TMG kam es in unregelmaessigen Abstaenden, leider nicht reproduzierbar, zu folgender Fehlermeldung

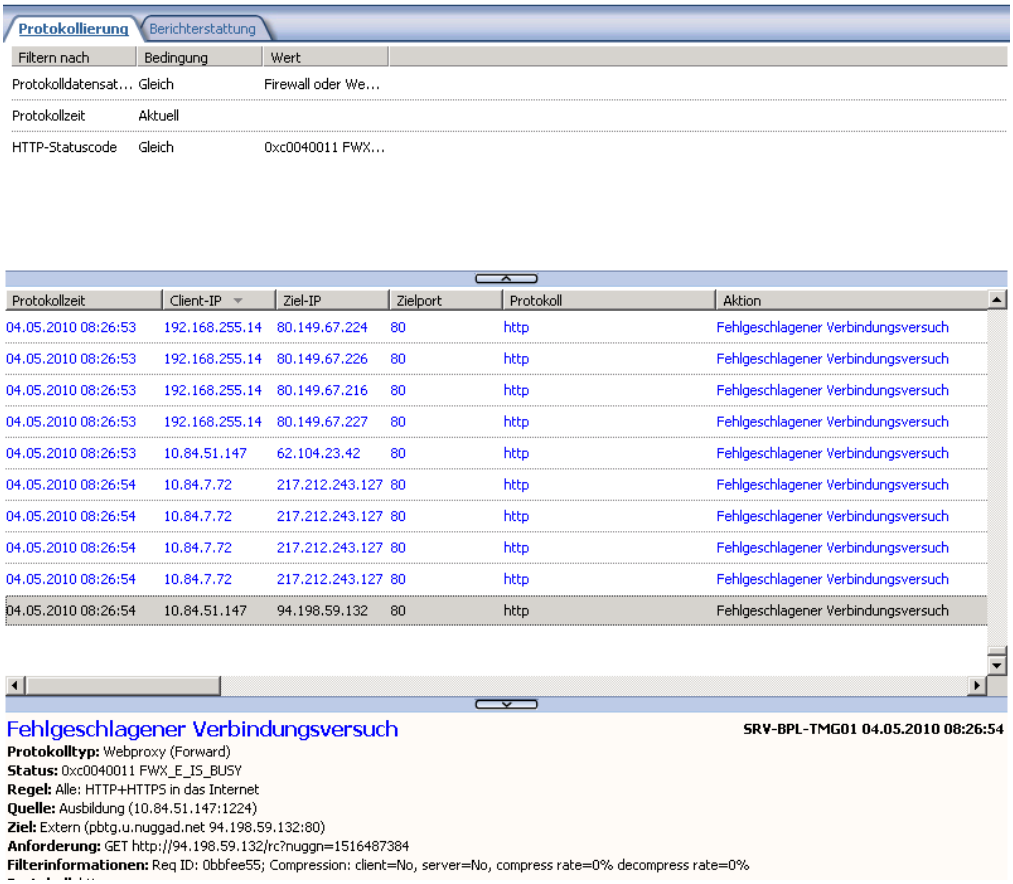


Die Fehlermeldung trat nur bei HTTP-Verbindungen auf. Alle anderen Verbindungen liefen ohne Probleme. Durch mehrfaches betaetigen der F5 Taste konnte die Webseite wieder dargestellt werden.

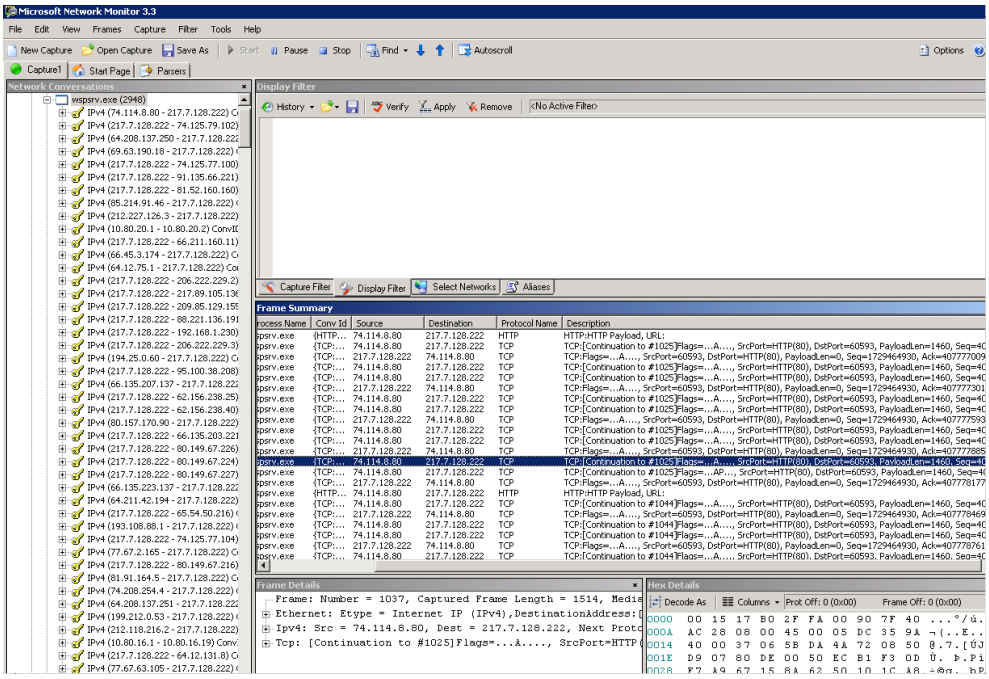
Google, aeeh Bing hat das gefunden:

0xc0040011 FWX_E_IS_BUSY
http://social.technet.microsoft.com/Forums/en/ForefrontedgeIA/thread/ee5fad65-76b2-42d9-bf72-8fce0254391a?outputAs=rss

Im Forefront TMG Log konnte man mit einem entsprechenden Filter folgendes sehen:



Also den Netzwerkmonitor angestartet und den Netzwerktraffic gesnifft. Dabei fiel mir erst mal nichts besonderes auf.



Auf den DNS Servern ist uns dann folgende Meldung aufgefallen:

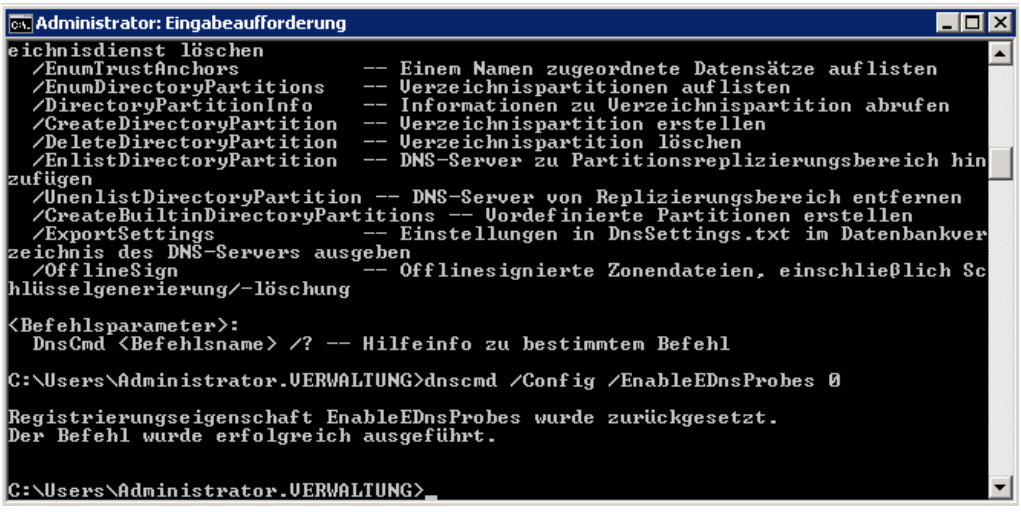
Danke Google, aeeh Bing habe ich dann folgendes gefunden:

http://support.microsoft.com/kb/828263/en-us
http://social.technet.microsoft.com/Forums/en-US/winserverPN/thread/7d0fc8f9-1c5c-428e-9f4f-887a162d0660

Der Artikel beschreibt eine Aenderung im DNS zur Unterstuetzung von EDNS, welcher nicht durch einige Firewalls durchgelassen wird, wenn UDP Pakete groesser 512 Byte blockiert werden.

Wir hatten beim Kunden paralell zur TMG Einfuehrung alle 12 Domaenencontroller von Windows Server 2008 64 Bit auf Windows Server 2008 R2 64 Bit ubgedatet und dabei wurde die neue Funktionaelitaet aktiviert.

Abhilfe war hier auf allen 12 Domaenencontrollern die EDNS Unterstuetzung zu deaktivieren:

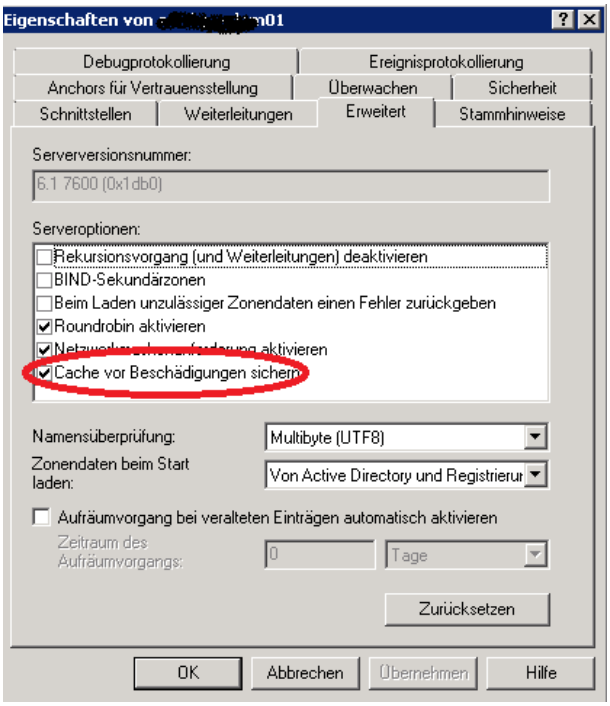


Das loeste das Problem der vielen Fehlermeldungen in der Ereignisanzeige des DNS Dienstes, aber noch nicht das Problem mit der Fehlermeldung „500 Interner Serverfehler“ ☹

Nach ewigem Suchen haben wir das Problem dann etwas einkreisen koennen: Symptom: Sobald **einer** der Domaenencontroller (egal aus welcher Domaene) gebootet wurde, konnte die Fehlermeldung „500 Interner Serverfehler“ reproduziert werden.

Zum Konstrukt: Beim Kunden sind drei Windows Domaenen in einer Active Directory Gesamtsruktur im Einsatz, welche durch zwei Forefront TMG Arrays getrennt sind.

Auch hier ergab nach einiger Recherche folgendes Ergebnis: In den Eigenschaften des DNS Server war die Option „Cache vor Beschaedigung sichern“ nicht aktiviert und das auf keinem Domaenen Controller. Scheinbar hat hier das Inplace Update von 2008 64 Bit auf 2008 R2 64 Bit diese Einstellung nicht uebernommen, denn standardmaessig ist die Einstellung aktiv!



Danach taucht die Fehlermeldung im Browser auch nicht mehr auf und jeder Domaenen Controller kann autark gebootet werden.