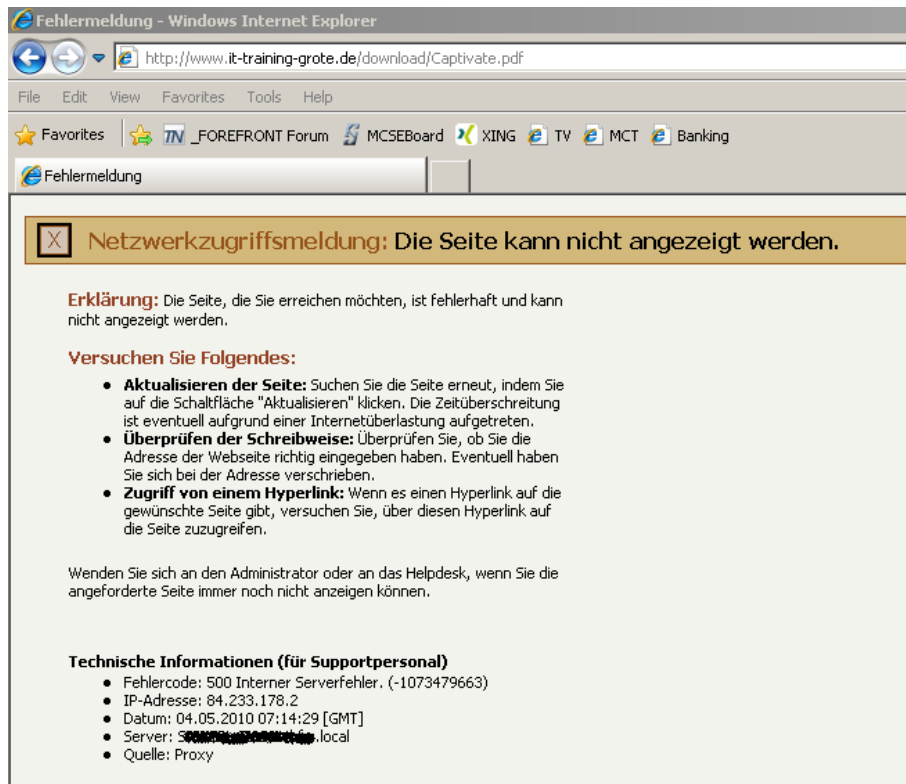


## Forefront TMG - 0xc0040011 FWX\_E\_IS\_BUSY

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



Die Fehlermeldung trat nur bei HTTP-Verbindungen auf. Alle anderen Verbindungen liefen ohne Probleme. Durch mehrfaches betätigen 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/ForefrontedgelA/thread/ee5fad65-76b2-42d9-bf72-8fce0254391a?outputAs=rss>

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

**Fehlgeschlagener Verbindungsversuch** SRV-BPL-TMG01 04.05.2010 08:26:54

**Protokolltyp:** Webproxy (Forward)  
**Status:** 0xc0040011 FWX\_E\_IS\_BUSY  
**Regel:** Alle: HTTP+HTTPS in das Internet  
**Quelle:** Ausbildung (10.84.51.147:1224)  
**Ziel:** Extern (pbtg.u.nuggad.net 94.198.59.132:80)  
**Anforderung:** GET http://94.198.59.132/rc/nuggn=1516487384  
**Filterinformationen:** Req ID: 0bbfee55; Compression: client=No, server=No, compress rate=0% decompress rate=0%

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

**Microsoft Network Monitor 3.3**

**Network Conversations (2948)**

Process Name	Conv ID	Source	Destination	Protocol Name	Description
psrv.exe	...	74.114.8.80	217.7.128.222	HTTP	HTTP-HTTP Payload, URL: ...
psrv.exe	...	217.7.128.222	74.114.8.80	TCP	TCP-Flags=... SrcPort=60593, DstPort=HTTP(80), PayloadLen=0, Seq=1729644930, Ack=40777009

**Frame Summary**

Process Name: psrv.exe, Conv ID: ..., Source: 74.114.8.80, Destination: 217.7.128.222, Protocol Name: HTTP, Description: HTTP-HTTP Payload, URL: ...

**Frame Details**

```

Frame: Number = 1037, Captured Frame Length = 1514, Media
[+] Decode As [ ] Columns [ ] Prot Off: 0 (0x00) Frame Off: 0 (0x00)
[Ethernet: Etype = Internet IP (IPv4), DestinationAddress:
[IPv4: Src = 74.114.8.80, Dst = 217.7.128.222, Next Proto
[0000 00 15 17 80 2F FA 00 90 7F 40 ... 7F 00
[000A AC 28 08 00 45 00 05 DC 35 9A ... 1E ..
[0014 40 00 37 06 5B DA 4A 72 08 50 0 ... 7. [0J
[001E D9 07 80 D2 00 5C B1 F3 0D 0 ... B. P.1
[0028 F7 19 67 15 8A 62 50 10 1C 18 ... -09. bP
  
```

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:

```
Administrator: Eingabeaufforderung
eichnisdienst löschen
/EnumTrustAnchors -- Einem Namen zugeordnete Datensätze auflisten
/EnumDirectoryPartitions -- Verzeichnispartitionen auflisten
/DirectoryPartitionInfo -- Informationen zu Verzeichnispartition abrufen
/CreateDirectoryPartition -- Verzeichnispartition erstellen
/DeleteDirectoryPartition -- Verzeichnispartition löschen
/EnlistDirectoryPartition -- DNS-Server zu Partitionsreplizierungsbereich hin
zufigen
/UnenlistDirectoryPartition -- DNS-Server von Replizierungsbereich entfernen
/CreateBuiltInDirectoryPartitions -- Vordefinierte Partitionen erstellen
/ExportSettings -- Einstellungen in DnsSettings.txt im Datenbankver
zeichnis des DNS-Servers ausgeben
/OfflineSign -- Offlinesignierte Zonendateien, einschließlich Sc
hlüsselgenerierung/-löschung

<Befehlsparameter>:
  DnsCmd <Befehlsname> /? -- Hilfeinfo zu bestimmten Befehl

C:\Users\Administrator.VERWALTUNG>dnsCmd /Config /EnableEDnsProbes 0

Registrierungseigenschaft EnableEDnsProbes wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

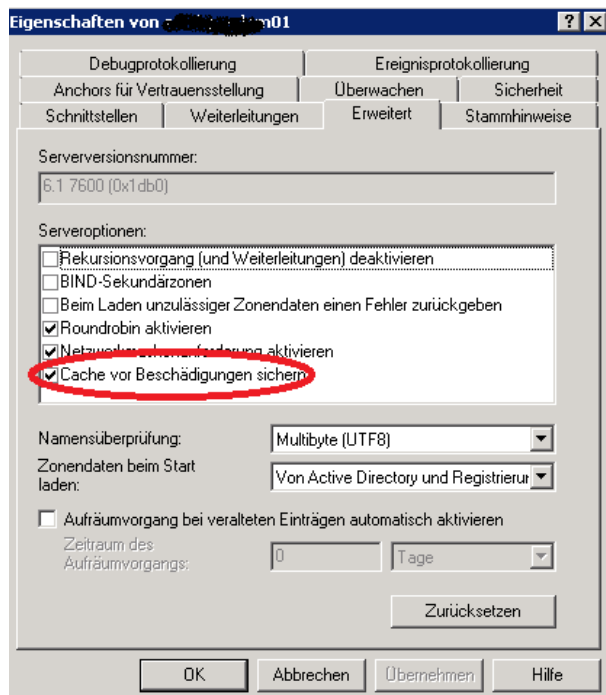
C:\Users\Administrator.VERWALTUNG>
```

Das löste 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 eingekreist können:  
Symptom: Sobald **einer** der Domänencontroller (egal aus welcher Domäne) gebootet wurde, konnte die Fehlermeldung „500 Interner Serverfehler“ reproduziert werden.

Zum Konstrukt: Beim Kunden sind drei Windows Domänen in einer Active Directory Gesamtstruktur 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 Beschädigung sichern“ nicht aktiviert und das auf keinem Domänen 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 Domänen Controller kann autark gebootet werden.