TMG2010 Exchange 2010 SMTP Filter

Die Mails werden über die Frontfirewall der Watchguard zum Exchange 2010 Edge Server in der DMZ zugestellt, der Edge gibt die Mail dann über das TMG weiter zum Exchange 2010 Hub/CAS/MBX im LAN.

Der Admin hatte keine Änderungen am Mail-Regelwerk oder dem SMTP Filter am TMG gemacht. Auch der Mail Admin hat keine Änderungen am Exchange gemacht.

Also wie aus dem Nichts stellt der Edge Server keine Mails mehr zum Hub Server zu und die Mail Queue auf dem Edge wächst und wächst.

Fehler der Queue: 500 5.5.1 Unrecognized command

Das SMTP Log sagt:

,,10.0.1.225:25,,,attempting to connect*
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,1,80.123.234.253:1231,10.0.1.225:25,+,,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,2,80.123.234.253:1231,10.0.1.225:25,<,"220 EX-MBX.intdomain.local Microsoft ESMTP MAIL Service ready at Tue, 7 Feb 2012 18:19:43 +0100",
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,3,80.123.234.253:1231,10.0.1.225:25,>,EHLO ex-edge.intdomain.local,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,4,80.123.234.253:1231,10.0.1.225:25,<,250- EX-MBX.intdomain.local Hello [80.123.234.253],
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,5,80.123.234.253:1231,10.0.1.225:25,<,250-SIZE,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,6,80.123.234.253:1231,10.0.1.225:25,<,250-PIPELINING,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,7,80.123.234.253:1231,10.0.1.225:25,<,250-DSN,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,8,80.123.234.253:1231,10.0.1.225:25,<,250-ENHANCEDSTATUSCODES,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,9,80.123.234.253:1231,10.0.1.225:25,<,250-STARTTLS,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,10,80.123.234.253:1231,10.0.1.225:25,<,250-X-ANONYMOUSTLS,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,11,80.123.234.253:1231,10.0.1.225:25,<,250-AUTH NTLM,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,12,80.123.234.253:1231,10.0.1.225:25,<,250-X-EXPS GSSAPI NTLM,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,13,80.123.234.253:1231,10.0.1.225:25,<,250-8BITMIME,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,14,80.123.234.253:1231,10.0.1.225:25,<,250-BINARYMIME,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,15,80.123.234.253:1231,10.0.1.225:25,<,250-CHUNKING,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,16,80.123.234.253:1231,10.0.1.225:25,<,250-XEXCH50,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,17,80.123.234.253:1231,10.0.1.225:25,<,250-XRDST,
2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,18,80.123.234.253:1231,10.0.1.225:25,<,250 XSHADOW,
*2012-02-07T17:19:44.550Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,19,80.123.234.253:1231,10.0.1.225:25,>,**X-ANONYMOUSTLS,***

*2012-02-07T17:19:44.565Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,20,80.123.234.253:1231,10.0.1.225:25,<,**500 5.5.1 Unrecognized command**,*
2012-02-07T17:19:44.565Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,21,80.123.234.253:1231,10.0.1.225:25,>,QUIT,
2012-02-07T17:19:44.581Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,22,80.123.234.253:1231,10.0.1.225:25,<,221 2.0.0 Service closing transmission channel,
2012-02-07T17:19:44.581Z,EdgeSync - Inbound to LAN,08CEB3D1DC574665,23,80.123.234.253:1231,10.0.1.225:25,-,,Local
---

Das 1. Komische: Im TMG Log sind KEINE Deny´s zu sehen. Der SMTP Verkehr wird normal erlaubt und nicht unterbrochen!

Nach einiger Suche habe ich den Blogeintrag von Jeff gefunden (http://www.expta.com/2008/03/how-to-add-smtp-verb-commands-to-isa.html). Dort und auch im TechNet (http://technet.microsoft.com/en-us/library/bb851514(EXCHG.80).aspx) wird ja gesagt, dass man entweder die SMTP-Verbs im SMTP Filter eintragen soll oder die SMTP/S Filter zu deaktivieren.

Wir haben dann erst mal X-ANONYMOUSTLS Verb im SMTP Filter als Verb eingetragen, allerdings war nirgendwo die Länge/Größe beschrieben.
Also haben wir den Wert von StartTLS übernommen und 10 Bytes eingetragen.

So hat sich dann auch die Fehlermeldung in der Mail Queue vom Edge Server verändert (421 5.5.2 Syntax error (command line too long))

SMTP Log:

,,10.0.1.225:25,,,attempting to connect*
2012-02-07T18:15:02.065Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,1,80.123.234.253:1533,10.0.1.225:25,+,,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,2,80.123.234.253:1533,10.0.1.225:25,<,"220 EX-MBX.indomain.local Microsoft ESMTP MAIL Service ready at Tue, 7 Feb 2012 19:15:01 +0100",
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,3,80.123.234.253:1533,10.0.1.225:25,>,EHLO ex-edge.indomain.local,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,4,80.123.234.253:1533,10.0.1.225:25,<,250-EX-MBX.indomain.local Hello [80.123.234.253],
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,5,80.123.234.253:1533,10.0.1.225:25,<,250-SIZE,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,6,80.123.234.253:1533,10.0.1.225:25,<,250-PIPELINING,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,7,80.123.234.253:1533,10.0.1.225:25,<,250-DSN,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,8,80.123.234.253:1533,10.0.1.225:25,<,250-ENHANCEDSTATUSCODES,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,9,80.123.234.253:1533,10.0.1.225:25,<,250-STARTTLS,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,10,80.123.234.253:1533,10.0.1.225:25,<,250-X-ANONYMOUSTLS,

2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,11,80.123.234.253:1533,10.0.1.225:25,<,250-AUTH NTLM,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,12,80.123.234.253:1533,10.0.1.225:25,<,250-X-EXPS GSSAPI NTLM,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,13,80.123.234.253:1533,10.0.1.225:25,<,250-8BITMIME,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,14,80.123.234.253:1533,10.0.1.225:25,<,250-BINARYMIME,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,15,80.123.234.253:1533,10.0.1.225:25,<,250-CHUNKING,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,16,80.123.234.253:1533,10.0.1.225:25,<,250-XEXCH50,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,17,80.123.234.253:1533,10.0.1.225:25,<,250-XRDST,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,18,80.123.234.253:1533,10.0.1.225:25,<,250 XSHADOW,
2012-02-07T18:15:02.081Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,19,80.123.234.253:1533,10.0.1.225:25,>,X-ANONYMOUSTLS,
2012-02-07T18:15:02.096Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,20,80.123.234.253:1533,10.0.1.225:25,<,421 5.5.2 Syntax error (command line too long),
2012-02-07T18:15:02.096Z,EdgeSync - Inbound to Ellerau,08CEB3D1DC5747BD,21,80.123.234.253:1533,10.0.1.225:25,>,QUIT,
---

und wir wussten, dass der TMG Server das Problem verursacht.
Allerdings wieder keine Fehlermeldung im TMG Log wie z.B. „0x80074e24 FWX_E_CONNECTION_KILLED“, NICHTS, nur zugelassenen Verbindungen per SMTP.

Wir haben jetzt temporaer den SMTP Filter auf dem TMG deaktiviert, so dass die Mails wieder zum HUB/MBX zugestellt werden.

Aber wie gesagt, das lief jetzt 2 Wochen fehlerfrei und auch vorher auf dem ISA war der SMTP Filter die ganze Zeit aktiv und mit Standard Einstellungen versehen, also kein extra „X-ANONYMOUSTLS” Verb.