



Spam-Filter und E-Mail-Kategorisierungsdienst

Installation und Konfiguration von expurgate.Inhouse

---

## **Installation und Konfiguration von eXpurgate.Inhouse**

<b>Prolog .....</b>	<b>4</b>
<b>Voraussetzung für den Betrieb von eXpurgate.Inhouse .....</b>	<b>4</b>
<b>Hinweise zu den Änderungen ab Version 2.0 .....</b>	<b>4</b>
<b>Das eXpurgate-Prinzip .....</b>	<b>5</b>
<b>1 Funktionsweisen von eXpurgate.Inhouse.....</b>	<b>6</b>
<b>1.1 eXpurgate als SMTP-Proxy</b>	<b>6</b>
<b>1.2 eXpurgate als Spam Assassin Server (Spamd)</b>	<b>6</b>
<b>1.3 eXpurgate als Sendmail Militer</b>	<b>7</b>
<b>2 Installation von eXpurgate.Inhouse.....</b>	<b>9</b>
<b>2.1 Installation von eXpurgate auf einem Windows-System</b>	<b>9</b>
2.1.1 Windows-Dienst Kommandos	16
2.1.2 Ändern des TCP-Ports bei Microsoft Exchange 5.5	16
2.1.3 Ändern des TCP-Ports bei Microsoft Exchange 2000 bzw. 2003	17
2.1.4 Testen, ob Exchange auf einem Port antwortet	19
<b>2.2 Installation von eXpurgate auf einem Unix-System</b>	<b>20</b>
2.2.1 eXpurgate unter Sun Solaris	20
<b>3 Konfiguration von eXpurgate.....</b>	<b>21</b>
<b>3.1 Allgemeine Kommandozeilen-Optionen</b>	<b>21</b>
<b>3.2 Optionen bei Nutzung des SMTP- oder SpamAssassin-Protokolls</b>	<b>23</b>
<b>3.3 SMTP-spezifische Optionen</b>	<b>24</b>
3.3.1 Verwendung mehrerer Zielsever und deren Priorisierung	25
3.3.2 XCLIENT-Erweiterung	25
<b>3.4 Logging-spezifische Optionen</b>	<b>26</b>
<b>3.5 Bedeutung der Logfile-Einträge</b>	<b>28</b>
<b>3.6 Verwendung des SOCKS-Protokolls</b>	<b>28</b>
<b>3.7 SSL/TLS zur Verschlüsselung der E-Mail-Übertragung</b>	<b>28</b>
<b>3.8 Hinzufügen von Received-Headern</b>	<b>29</b>
<b>3.9 Anpassen der SMTP-Mitteilungen</b>	<b>30</b>
<b>3.10 Die Konfigurationsdatei expurgate.xml</b>	<b>30</b>
<b>4 Testen der Funktion von eXpurgate .....</b>	<b>33</b>
<b>4.1 Grundlegende Tests Ihrer eXpurgate-Installation</b>	<b>33</b>

---

4.2	<i>Spezifische Optionen zum Testen von eXpurgate</i>	33
4.3	<i>Hinweise zum Testen der E-Mail-Kategorisierung von eXpurgate</i>	34
4.4	<i>Funktionsprüfung via Telnet</i>	35
5	<b>Einbinden von eXpurgate in ein bestehendes E-Mail-System .....</b>	<b>36</b>
5.1	<i>eXpurgate als SMTP-Forwarder</i>	36
5.1.1	Notwendige Änderungen an Postfix bei Verwendung von eXpurgate als Forwarder	38
5.2	<i>eXpurgate als Content_Filter in Postfix ("Sandwich")</i>	38
5.3	<i>eXpurgate in Postfix mit weiteren Content_Filtern, etwa einem Virens Scanner</i>	39
5.4	<i>Einbinden von eXpurgate in Exim</i>	40
5.5	<i>Verwendung von eXpurgate als SpamAssassin Spamd</i>	41
5.6	<i>Einbinden von eXpurgate in Qmail</i>	41
6	<b>Feintuning der E-Mail-Behandlung .....</b>	<b>42</b>
6.1	<i>Global wirkende Schalter</i>	42
6.2	<i>Benutzerspezifische Steuerung der eXpurgate-Checks: User Features</i>	42
6.3	<i>Steuerung in Abhängigkeit vom Absender</i>	44
6.3.1	Behandlung von E-Mails bestimmter Absenderadressen	44
6.3.2	Behandlung von E-Mails bestimmter Sender-IP-Adressen	45
6.4	<i>Freezing</i>	45
6.4.1	Voraussetzungen	46
6.4.2	Konfiguration	46
6.5	<i>Behandlung von Spam-E-Mails</i>	47
6.5.1	Systemweite Behandlung von Spam-E-Mails	48
6.5.2	Userspezifische Behandlung von Spam-E-Mails	48
6.5.3	Einstellen des Reject-Texts	48
6.6	<i>Behandlung von Viren-E-Mails</i>	49
6.7	<i>Erweiterte Optionen zur Behandlung einzelner E-Mail-Typen</i>	50
6.8	<i>Ausschalten der Signalisierung von E-Mails der Kategorie "dangerous"</i>	51
6.9	<i>Behandlung von "suspect" als "clean"</i>	51
6.10	<i>Behandlung von Bounce-E-Mails</i>	51
6.11	<i>Behandlung bestimmter "clean"-Subkategorien als Spam</i>	51
7	<b>Verwendung der eXpurgate-Statistiken .....</b>	<b>53</b>
Anhang	<b>.....</b>	<b>55</b>
	<i>Die eXpurgate E-Mail-Kategorien</i>	55
	<i>IP-Bereiche der eXpurgate-Server</i>	57
	<i>Lizenzen</i>	57

---

## Prolog

Mit der vorliegenden Dokumentation möchten wir Ihnen die Funktionsweise unseres Spamfilters bzw. E-Mail-Kategorisierungsdiensts eXpurgate.Inhouse anhand einiger Beispiele nahebringen. Neben einem Überblick soll es Ihnen insbesondere als Referenz für die Behandlung spezieller Szenarien und Wünsche dienen. Bitte erschrecken Sie nicht ob des Umfangs: für eine funktionsfähige Installation mit Standardparametern sollte der Installationsaufwand innerhalb einer Viertelstunde zu bewältigen sein. Bitte beachten Sie, dass sich dieses Dokument lediglich der eXpurgate.Inhouse-Lösung, also der Nutzung von eXpurgate in Kombination mit Ihrem bestehenden Mailserver zuwendet.

## Voraussetzung für den Betrieb von eXpurgate.Inhouse

**Damit eXpurgate.Inhouse eingehende E-Mails kategorisieren kann, ist es zwingend erforderlich, dass eXpurgate TCP-Verbindungen zu den Netzen**

**194.145.224.0/24**

**und**

**195.190.135.0/24**

**jeweils auf Port 55555 aufbauen kann.**

Bitte überprüfen und ändern Sie ggf. Ihre Firewall-Einstellungen.

## Hinweise zu den Änderungen ab Version 2.0

Mit dem Versionssprung von 1.3.x zu 2.x wurden einige grundlegende Änderungen eingeführt, die wir hier gebündelt zusammenfassen möchten. Details entnehmen Sie bitte den entsprechenden Kapiteln (siehe Verweise).

*Änderungen am Konfigurationsfile expurgate.xml (bitte die entsprechenden Abschnitte in Ihrer bisherigen Konfigurationsdatei ergänzen):*

- Neuer Abschnitt `<SmtpOutList>`: Hierin werden die SMTP-Relays konfiguriert, an die eXpurgate E-Mails nach dem Spam-Check weiterleitet. Es lassen sich mehrere Relays mit unterschiedlichen Prioritäten konfigurieren. Dieser Abschnitt muss vorhanden sein! Er darf allerdings leer bleiben, wenn ein SMTP-Relay – wie bisher – über die Kommandozeile angegeben wird (Kapitel 3.3.1: *Verwendung mehrerer Zielservers und deren Priorisierung*).
- Der Parameter `filterOnOffForUserInFile` ist entfallen. Er wurde durch die Parameter `noFreezingForAllUsers`, `noExpurgateForAllUsers` und `noVirusCheckForAllUsers` ersetzt. Darüber hinaus kann über den Parameter `userFeaturesDB` für einzelne User/Domains festgelegt werden, welche Scanning-Features aktiviert bzw. deaktiviert sein sollen (Kapitel 6.2: *Benutzerspezifische Steuerung der eXpurgate-Checks: User Features*).
- Parameter für die Konfiguration des neuen Features *Freezing* (siehe Kapitel 6.4 ff).
- Unterstützung der XCLIENT-Erweiterung (ab eXpurgate 2.0.5, siehe Kapitel 3.3.2).

**Kommandozeilen-Optionen:** Ab Version 2.0.5 muss `smtpouthost` immer angegeben werden. Zum Parameter `--logmailidalways` (ab Version 2.0.4) siehe Kapitel 3.4.

## Das eXpurgate-Prinzip

eXpurgate beruht auf einer von *eleven* entwickelten neuartigen Technologie zur Spam-Erkennung und E-Mail-Kategorisierung. eXpurgate überprüft E-Mails insbesondere auf das entscheidende Charakteristikum von Spam als Massensendung. Ein wesentlicher Bestandteil dieser Prüfung ist der so genannte *Bulkcheck*. eleven hat dafür einen Kontrollsummen-Algorithmus entwickelt, der es dem System erlaubt, mehrere E-Mails miteinander zu vergleichen, ohne deren textlichen Inhalt zu kennen. Dies geschieht durch Reduzierung der E-Mails auf einen nur wenige Bytes großen Code, der keinerlei Rückschlüsse auf ihren ursprünglichen Inhalt zulässt. Je häufiger eine gleiche oder ähnliche E-Mail zuvor empfangen wurde, desto höher ist die Wahrscheinlichkeit, dass es sich bei der gerade in der Prüfung befindlichen um Spam handelt. Die Identifizierung erfolgt ausschließlich über die kurze Kontrollsumme.

eXpurgate kombiniert dieses Test-Verfahren mit weiteren und ist somit in der Lage, eine E-Mail eindeutig als Spam oder andere Art von Massenmail (z. B. Newsletter) zu kategorisieren. Darüber hinaus erkennt eXpurgate auch gefährliche E-Mail-Inhalte und -Anhänge (Attachments) wie Viren und Würmer, bevor diese Systemveränderungen verursachen können. Durch die von eleven entwickelte selbstlernende *Bulkcheck*-Technologie verzögert sich die E-Mail-Zustellung beim Kunden in der Regel nur um Sekundenbruchteile, während die Vertraulichkeit durch die Verschlüsselung gewahrt wird. Zudem *reduziert* die Technologie im Gegensatz zu herkömmlichen Spam-Filtern das Auftreten von so genannten "*false positives*" (fälschlich als Spam erkannten E-Mails) auf ein absolutes Minimum.

Den klassifizierten E-Mails werden entsprechende Header hinzugefügt, die deren automatische Weiterverarbeitung ermöglichen. Nähere Informationen zu den Headern finden Sie im Anhang A dieses Dokuments; Hinweise zur Konfiguration Ihres E-Mail-Programms finden Sie auf unseren Support-Seiten im Internet unter [www.eleven.de/support/](http://www.eleven.de/support/)

# 1 Funktionsweisen von eXpurgate.Inhouse

eXpurgate arbeitet entweder als *SMTP-Proxy* (Relay), als *Spam Assassin Server* (Spamd) oder als *Sendmail Milter*. Diese unterschiedlichen Funktionsweisen möchten wir Ihnen im folgenden kurz vorstellen. Allen Konzepten gemein ist, dass sich eXpurgate lediglich um die Kategorisierung von E-Mails, nicht jedoch um deren Auslieferung an Benutzer kümmert. Daher ist für die Verwaltung von Benutzern bzw. E-Mail-Konten immer ein bereits vorhandener Mailserver erforderlich. Durch den geringen Ressourcen-Bedarf von eXpurgate ist für dessen Installation jedoch in der Regel keine separate Maschine erforderlich, sondern meist kann eXpurgate zusätzlich zur vorhandenen Mailserver-Software auf derselben Maschine mitinstalliert werden.

Alle folgenden Installationsarten basieren auf dem *Bulkcheck* als Grundprinzip von eXpurgate. Jede eingehende E-Mail wird von eXpurgate.Inhouse einer Analyse unterzogen, bei der ein kurzer Prüfwert SSL-verschlüsselt an die zentralen eXpurgate-Server übertragen wird. Die eXpurgate-Server sind redundant ausgelegt und auf mehrere Standorte verteilt, um eine höchstmögliche Verfügbarkeit zu gewährleisten. Für die Übermittlung der Prüfschlüssel ist es erforderlich, dass eXpurgate.Inhouse eine Verbindung nach außen zu den eXpurgate-Servern in den Netzen 194.145.224.0/24 und 195.190.135.0/24<sup>1</sup> auf Port 55555 aufbauen und von dort kommende Antworten annehmen kann. Sie müssen ggf. Ihre Firewall-Konfiguration entsprechend anpassen. Alternativ können Sie die Verbindungen auch mit Hilfe des SOCKS-Protokolls nach außen leiten. Die eXpurgate-Server bauen selbst aktiv keine eingehenden Verbindungen auf, sondern antworten lediglich auf Requests.

## 1.1 eXpurgate als SMTP-Proxy

Als *SMTP-Proxy* fungiert eXpurgate wie ein zusätzlicher, vorgeschalteter Mailserver: eXpurgate nimmt via SMTP (Simple Mail Transfer Protocol) eingehende E-Mails an, um sie kategorisiert via SMTP an den eigentlichen Mailserver weiter zu reichen. Die Weiterleitung erfolgt dabei an genau einen festgelegten Server, wobei Mechanismen wie DNS-MX-Einträge u. a. unberücksichtigt bleiben. eXpurgate nimmt also als Proxy eingehende E-Mails selbst an, um diese nach erfolgter Prüfung an den eigentlichen Mailserver durchzureichen.

## 1.2 eXpurgate als Spam Assassin Server (Spamd)

Als *Spam Assassin Server* nimmt eXpurgate hingegen nicht selbständig von außen eingehende E-Mails an. Stattdessen nimmt es auf einem definierten Port Anfragen bzw. E-Mails von einem Spam Assassin Client entgegen und beantwortet diese mit Hilfe des Spam Assassin Protokolls, je nachdem, ob es sich dabei um Spam handelt oder nicht. Darüber hinaus wird ein weiterer Header zurückgegeben, der die Kategorie der E-Mail enthält. Weitere Informationen finden Sie im *Spamd*-Konfigurationsbeispiel weiter unten (vgl. Kapitel 5.5) sowie unter [www.spamassassin.org](http://www.spamassassin.org).

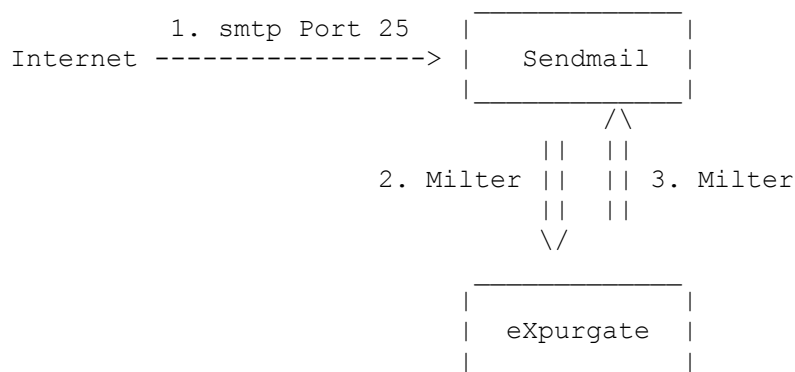
---

<sup>1</sup> Sie finden die verwendeten IP-Netze in der öffentlich einsehbaren Datenbank des RIPE als ELEVEN-NET und ELEVEN-NET2 dokumentiert (vgl. Anhang).

### 1.3 eXpurgate als Sendmail Milter

Als *Milter* (Mail Filtering API) für Sendmail arbeitet eXpurgate ähnlich wie als Spam Assassin Daemon, indem es sich des Milter-Protokolls bedient. Allerdings steht das Milter-Protokoll nur unter *Sendmail* (offiziell ab Version 8.12) zur Verfügung.

Die Arbeitsweise lässt sich dabei schematisch wie folgt darstellen:



Bitte beachten Sie, dass die im Abschnitt

#### 6.2: Benutzerspezifische Steuerung der eXpurgate-Checks: User Features

beschriebene Funktionalität nur bei Verwendung von eXpurgate als SMTP-Proxy (einschließlich Before-Queue-Content-Filter für Postfix) zur Verfügung steht, nicht jedoch bei Verwendung der Milter-Schnittstelle. Dies liegt darin begründet, dass die Spezifikation der Schnittstelle die Übergabe von empängerspezifischen Daten nicht zulässt.

Um eXpurgate als Milter in Sendmail einzubinden, muss Sendmail mit dem Feature, Milter-Programme anzusprechen, kompiliert sein. Um zu überprüfen, ob dieses Feature bei einem vorhandenen Sendmail-Binary zur Verfügung steht, können Sie folgende Kommandozeile benutzen:

```
sendmail -bt -d0.4 < /dev/null
```

Sie erhalten so, neben anderen Angaben zum installierten Sendmail-Programm, welche Optionen einkompiliert wurden (*Compiled with*). Der Output dürfte dem folgenden ähneln:

```
Compiled with: DNSMAP LOG MAP_REGEX MILTER MIME7TO8 MIME8TO7
```

Wenn in dieser Liste "Milter" mit ausgegeben wird, können Sie Ihr Sendmail mit Milter verwenden. Andernfalls müssen Sie Ihr Sendmail neu kompilieren, wobei in der Datei `devtools/Site/site.config.m4` folgender Eintrag existieren muss:

```
APPENDDEF(`confENVDEF', ` -DMILTER')
```

Anschließend muss Sendmail mit der Option `-c` neu kompiliert werden.<sup>2</sup>

Sendmail hat mehrere Möglichkeiten, ein Milter-Programm zu kontaktieren. Sie steuern dies durch einen **Konfigurationsstring**, in dem Sie das zu benutzende Protokoll, gefolgt von einem

<sup>2</sup> Die Option `-c` teilt dem Compiler mit, Änderungen in `site.config.m4` zu berücksichtigen. Auf sie kann verzichtet werden, wenn Sendmail zum ersten Mal kompiliert wird.

Doppelpunkt angeben. Folgende Protokolle stehen zur Verfügung:

Named Sockets	unix:/pfad/zum/kommunikations/file
	local:/pfad/zum/kommunikations/file
IP V4 Sockets	inet:port@hostname
IP V6 Sockets	inet6:port@hostname

Die gewählte Kommunikationsform muss für Sendmail und eXpurgate gleich sein. Für Sendmail müssen in der Datei 'sendmail.mc' folgende Einträge existieren:

```
INPUT_MAIL_FILTER(`eXpurgate', `S=<Kommunikationsstring>, F=, T=C:10m;S:5m;R:5m;E:5m')dnl
define(`confINPUT_MAIL_FILTERS',`eXpurgate')dnl
```

Dabei müssen Sie <Kommunikationsstring> mit Ihren Vorgaben ersetzen.

### Beispiel:

```
INPUT_MAIL_FILTER(`eXpurgate', `S=local:/var/run/sendmail/eXpurgate.sock,
F=, T=C:10m;S:5m;R:5m;E:5m')dnl
```

Um eXpurgate als Militer zu starten, muss die Kommandozeile wie folgt aussehen:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml --servermode
--milter <Kommunikationsstring>
```

wobei <Kommunikationsstring> wieder mit dem gleichen String wie oben zu ersetzen ist.

### Beispiel:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml -servermode
--milter local:/var/run/sendmail/eXpurgate.sock
```



## 2 Installation von eXpurgate.Inhouse

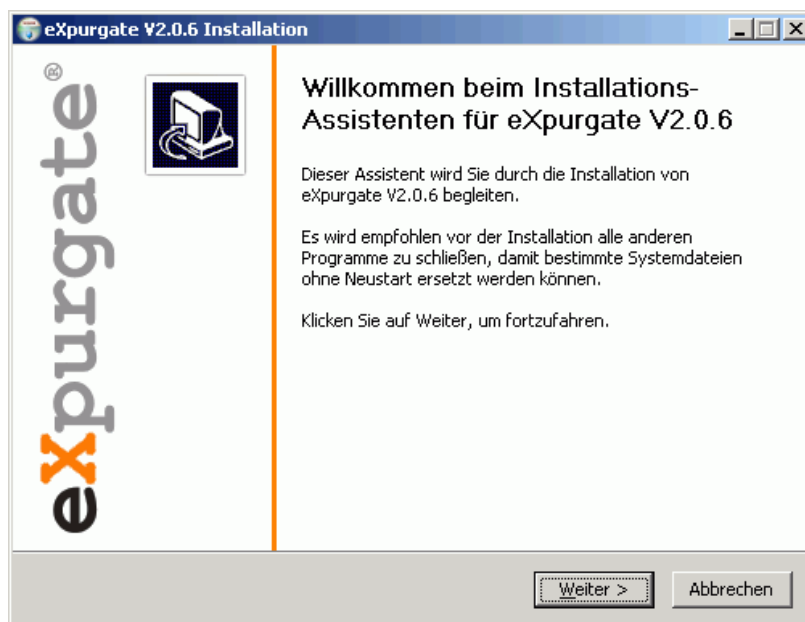
Im folgenden Abschnitt möchten wir Ihnen die Installation von eXpurgate.Inhouse auf einem Windows- bzw. Unix-System vorstellen. Beide Teile sind jeweils auf das Betriebssystem zugeschnitten, so dass Sie lediglich den Abschnitt, der sich ihrem Betriebssystem zuwendet, zu beachten brauchen. In beiden Fällen sollten Sie jedoch den darauf folgenden Abschnitt über die Konfiguration von eXpurgate beachten: da diese weitgehend unabhängig vom zugrundeliegenden Betriebssystem ist, behandeln wir sie in einem eigenen Kapitel.

Grundsätzlich haben wir bei der Entwicklung von eXpurgate darauf geachtet, Ihnen den Einstieg so leicht wie möglich zu machen. Deshalb brauchen Sie, falls überhaupt, nur sehr wenige Änderungen an den Grundeinstellungen vorzunehmen.

### 2.1 Installation von eXpurgate auf einem Windows-System

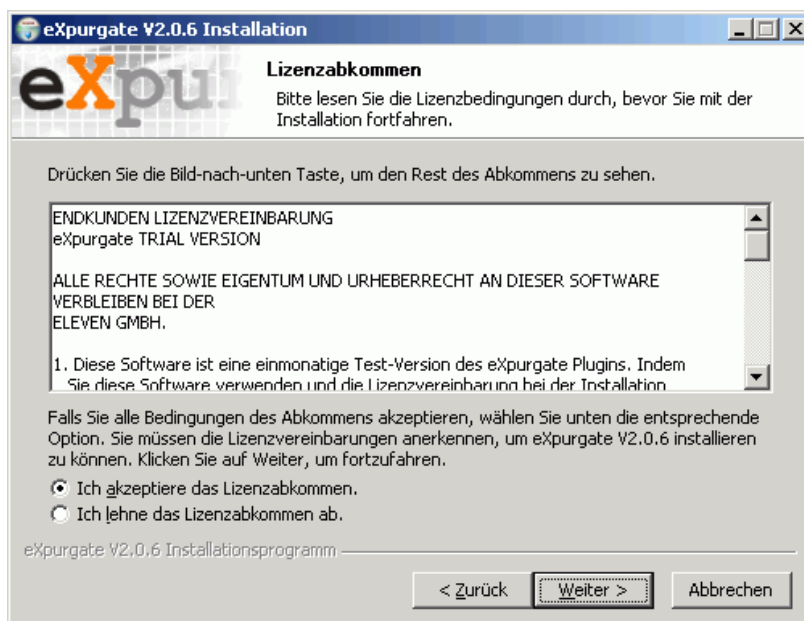
Wenn Sie eXpurgate unter Microsoft Windows installieren, werden die notwendigen Parameter bereits während des Installationsvorgangs abgefragt und eXpurgate anschließend als Dienst installiert und gestartet.<sup>3</sup>

Um die Installation zu starten, doppelklicken Sie bitte auf die eXpurgate-Installationsdatei (z. B. expurgate-V2\_0\_5\_WindowsNT\_x86.exe). Es erscheint der Installations-Assistent, der Sie durch die weitere Installation leitet.

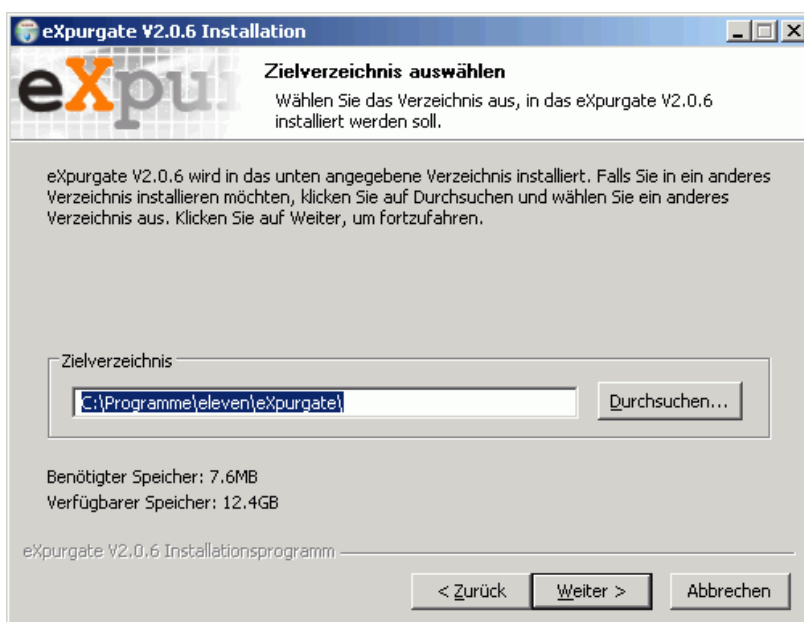


Klicken Sie auf *Weiter*, um mit der eigentlichen Installation zu beginnen.

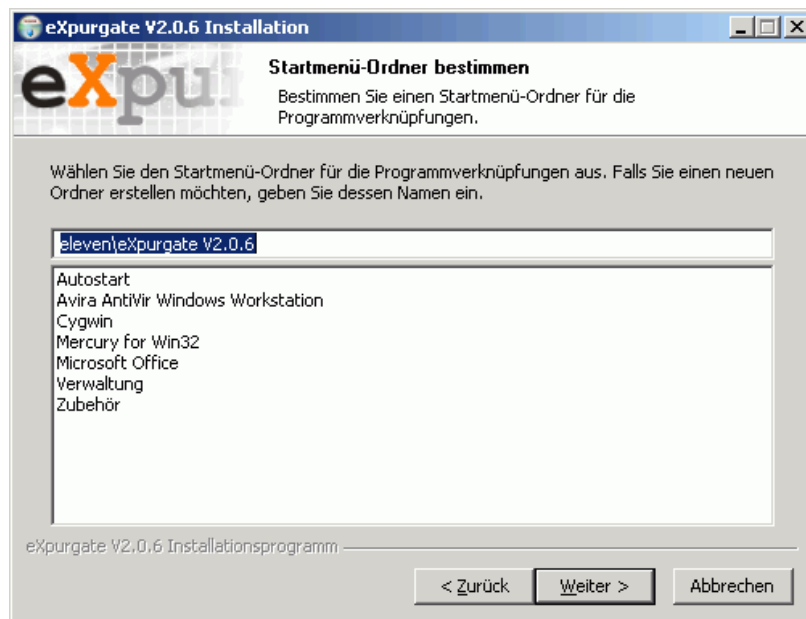
<sup>3</sup> Sie können diese Basisinstallation jederzeit wiederholen, indem Sie den Installer erneut aufrufen oder den Menüpunkt für das eXpurgate-Setup im Windows-Startmenü auswählen. Achtung: Da dabei die Datei eXpurgate.xml überschrieben wird, gehen sämtliche Änderungen einer vorherigen Installation verloren.



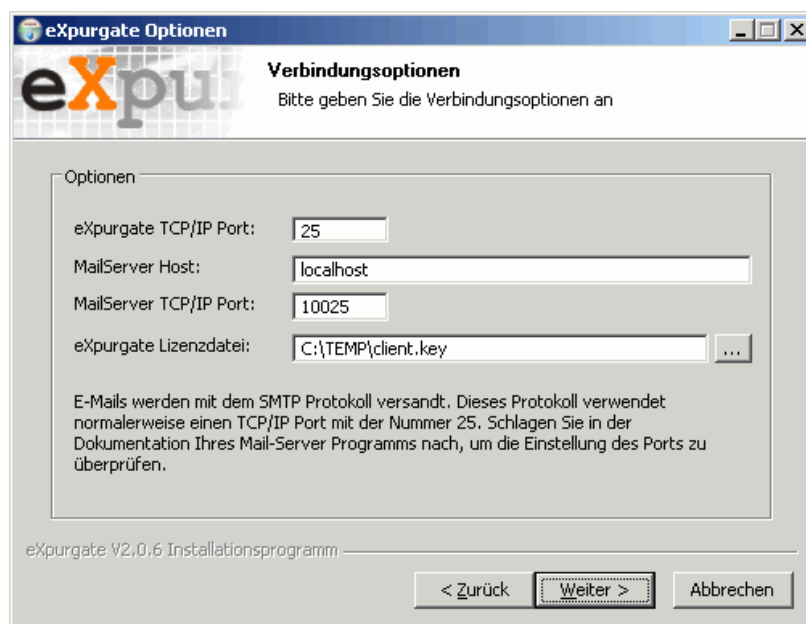
Bitte lesen Sie die Lizenzbedingungen aufmerksam durch. Klicken Sie in das Feld vor "Ich akzeptiere das Lizenzabkommen", danach auf *Weiter*.



Wählen Sie nun das Verzeichnis aus, in das eXpurgate installiert werden soll. Die Voreinstellung entspricht dem Verzeichnis *eleven\exPurgate* unterhalb Ihres Programmverzeichnisses (z. B. C:\Programme\eleven\exPurgate). Sie können dieses jedoch beliebig an Ihre Installationsvorgaben anpassen.



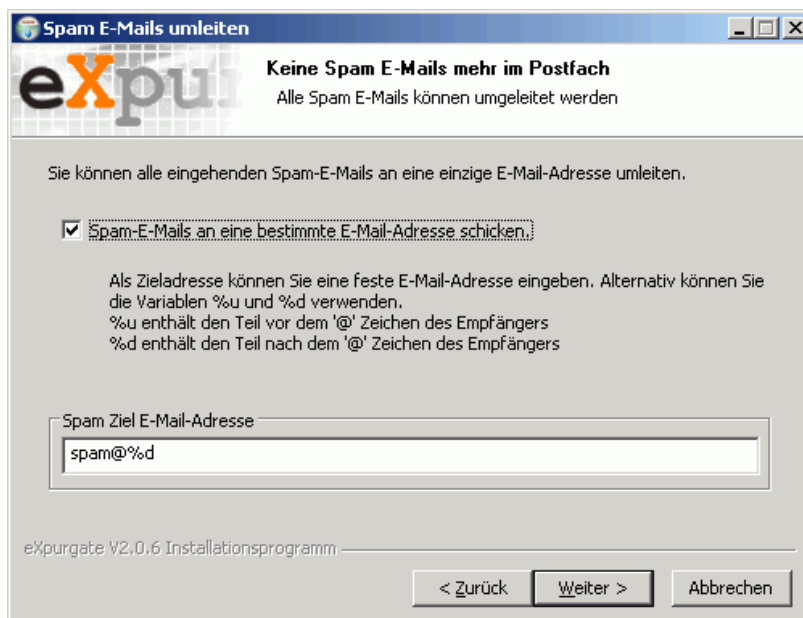
Geben Sie an, an welcher Stelle eXpurgate im Windows-Startmenü gelistet werden soll und klicken Sie auf *Weiter*.



Unter den Verbindungsoptionen müssen Sie angeben, auf welchem Port eXpurgate eingehende E-Mails annehmen soll (default: 25). Als *Mailserver Host* und *Mailserver TCP/IP Port* geben Sie an, unter welcher Adresse und welchem Port eXpurgate Ihren bestehenden Mailserver erreichen kann. Sollen eXpurgate und der bestehende Server auf demselben Rechner laufen, müssen Sie dessen Port in einen bislang unbenutzten ändern. Andernfalls tragen Sie hier den Namen der anderen Maschine und den Port des Mailers darauf ein.

Nachdem Sie die den Pfad zur eXpurgate Lizenzdatei angegeben und die Einträge mit einem

Klick auf *Weiter* bestätigen haben, versucht eXpurgate Ihren bereits vorhandenen Mailserver auf dem soeben angegebenen Port anzusprechen. Ist dieser erreichbar, gelangen Sie mit einem Klick auf *Weiter* zum nächsten Fenster *Spam E-Mails umleiten*.<sup>4</sup>



Im Fenster *Spam E-Mails umleiten* können Sie festlegen, ob alle Spam-E-Mails an eine einzige E-Mail-Adresse umgeleitet werden sollen. Wenn Sie diese Option nutzen möchten, schalten Sie sie mit einem Häkchen vor *Spam-E-Mails an eine bestimmte E-Mail Adresse schicken* ein. Geben Sie dann auch das Ziel dieser E-Mails ein. Die Vorgabe spam@%d leitet somit alle E-Mails, die Spam enthalten, an die E-Mail-Adresse "spam" innerhalb Ihrer Domain (z. B. spam@meine-domain) weiter.

Dieses Verfahren ermöglicht es Ihnen, alle eingehenden, als Spam klassifizierten E-Mails in ein gesondertes Postfach zu leiten. Somit bekommt die Vielzahl Ihrer Nutzer die unerwünschten E-Mails gar nicht zu sehen, während diese zentral im Spam-Postfach weiterverarbeitet werden können.

**Bitte achten Sie unbedingt darauf, dass die hier angegebene E-Mail-Adresse auch wirklich existiert bzw. legen Sie diese ggf. jetzt an, da Sie sonst möglicherweise die dann nicht zustellbaren E-Mails mit einer Fehlermeldung zurückschicken würden. Auf diese Weise würden Sie eher zu einer weiteren Verschärfung als zur Lösung der Spam-Problematik beitragen.**

Klicken Sie auf *Weiter*.

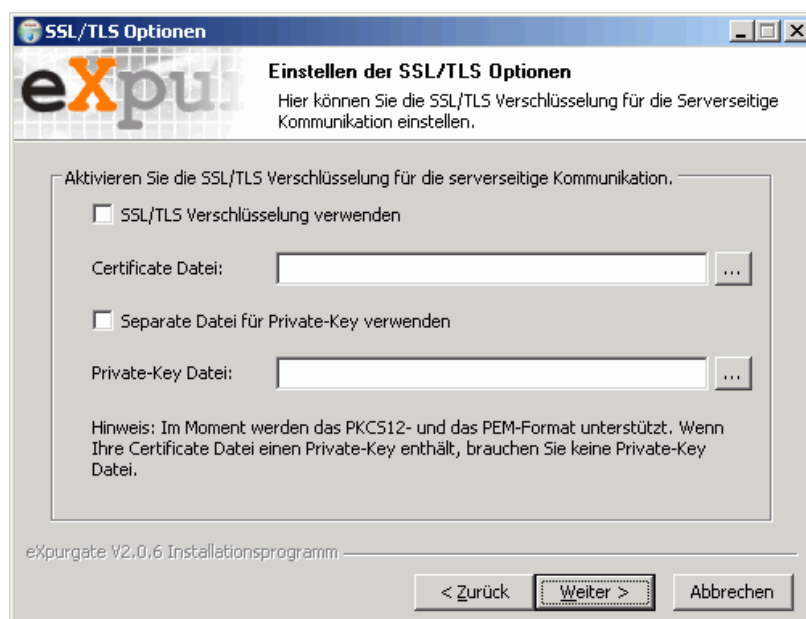
<sup>4</sup> Falls der angegebene Mailserver nicht erreichbar ist, teilt eXpurgate Ihnen das mit der Meldung "Kann den angegebenen Mailserver nicht auf dem angegebenen Port erreichen" mit. Bestätigen Sie diese mit einem Klick auf OK, um zum vorigen Fenster zurückzugelangen. Prüfen Sie bitte Ihre Angaben bzw. stellen Sie sicher, dass eXpurgate den angegebenen Server erreichen kann. Klicken Sie auf *Weiter*, um die Prüfung erneut vorzunehmen.



Mit der Option *Umschreiben der Betreffzeile* können Sie für kategorisierte Massen-E-Mails deren Betreffzeile (Subject) umschreiben lassen. Auf diese Weise erhalten Sie schnell einen Überblick, um welchen E-Mail-Typ es sich handelt und ob es lohnend oder gar gefährlich wäre, die E-Mail(s) zu öffnen. Dieses Verfahren eignet sich besonders dann, wenn die E-Mails nach der Klassifizierung durch eXpurgate manuell geprüft werden sollen.

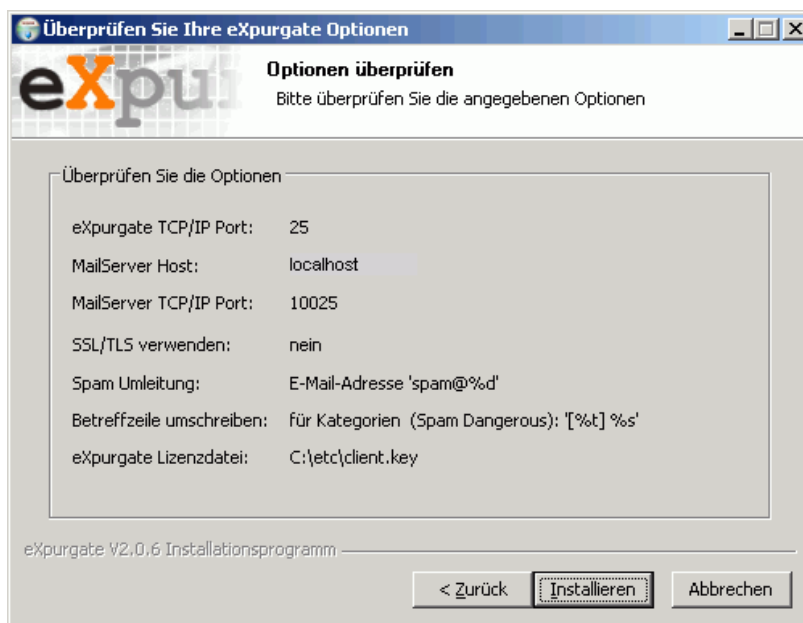
Sie können für die Typen *Spam*, *Bulk* und/oder *Dangerous* (gefährlich) festlegen, nach welchem Schema die Betreffzeile umgeschrieben werden soll. Die Voreinstellung *[%t] %s* bewirkt beispielsweise, dass die Betreffzeile einer eingehenden Spam-E-Mail mit dem Betreff "*Hi Allen, make money fast*" umgeschrieben wird zu "*[spam] Hi Allen, make money fast*" und somit schneller (aus-) zu sortieren ist.

Klicken Sie auf *Weiter*, um zu den SSL/TLS-Optionen zu gelangen. Diese dienen der sicheren Verschlüsselung des Übertragungswegs zwischen geeigneten Servern. Falls Sie dieses vergleichsweise neue und eher seltene Verfahren nicht verwenden, sollten Sie hier keine Änderungen vornehmen und auf *Weiter* klicken.

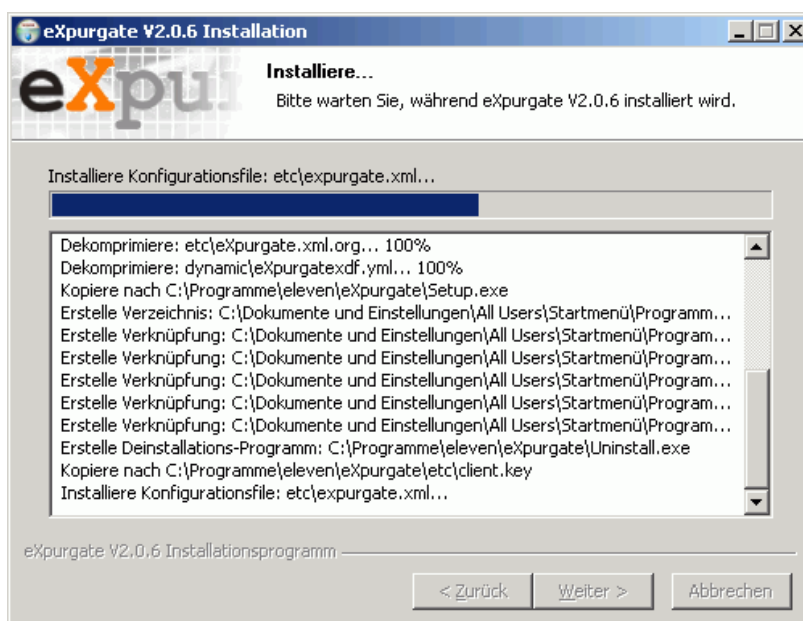


Nähere Informationen zum SSL/TLS-Verfahren erhalten Sie im entsprechenden Abschnitt weiter unten in dieser Dokumentation (vgl. 3.7, S. 28). Für die "normale", im Internet übliche E-Mail-Übertragung mittels SMTP und das Funktionieren von eXpurgate ist diese Option *nicht* erforderlich, kann also in den meisten Fällen deaktiviert bleiben.

Zum Abschluss der Installation werden Ihre Angaben zusammengefasst. Bitte kontrollieren und korrigieren Sie sie falls nötig. Klicken Sie danach auf *Installieren*.



Nun wird eXpurgate gemäß Ihren Vorgaben auf Ihrem Rechner installiert, als Windows-Dienst hinzugefügt und gestartet.

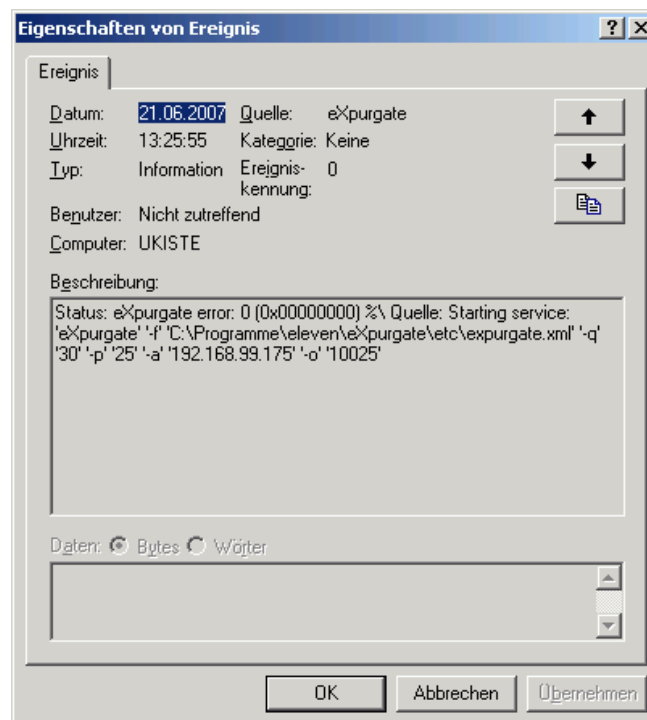


Am Ende der Installation wird noch die Verbindung zu den eXpurgate-Servern (exDBs) bei eleven geprüft. Wenn die Installation erfolgreich war, gelangen Sie zum letzten Bild.



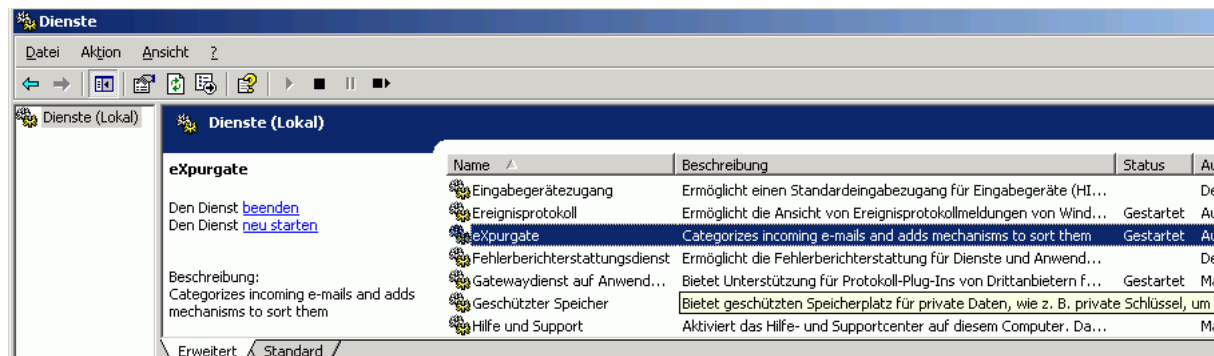
Zum Beenden des Installationsassistenten klicken Sie bitte auf *Fertig stellen*. Ihr eXpurgate ist nun betriebsbereit installiert.

eXpurgate protokolliert seine Starts samt der verwendeten Kommandozeilenoptionen in der Windows-Ereignisanzeige (Event Log, zu finden via Start/ Programme/ Verwaltung/ Ereignisanzeige). Hier erhalten Sie auch erste Hinweise auf etwaige Fehler.



## 2.1.1 Windows-Dienst Kommandos

eXpurgate wird unter Microsoft Windows als Dienst installiert, sodass eXpurgate automatisch - ohne Benutzeranmeldung - nach einem Systemstart gestartet wird. Sie können dies unter Start/ Programme/ Verwaltung/ Dienste überprüfen.



Für die Steuerung von eXpurgate als Windows-Dienst stehen Ihnen auf der Kommandozeile die folgenden Parameter zur Verfügung:

install	Installiert eXpurgate als Windows-Dienst ohne ihn zu starten. Die Start-Parameter müssen folgend angegeben werden
remove	Deinstalliert eXpurgate als Windows-Dienst
start	Startet den bereits installierten eXpurgate-Dienst
stop	Beendet den installierten eXpurgate-Dienst
isinstalled	Überprüft, ob eXpurgate als Dienst installiert wurde
isrunning	Überprüft, ob eXpurgate gegenwärtig als Dienst läuft
getpath	Gibt den Pfad zurück, unter dem der Dienst installiert wurde
getparameter	Gibt die Parameter zurück, mit denen der Dienst gestartet wird
setparameter	Setzt neue Startparameter (analog zu "install")

## 2.1.2 Ändern des TCP-Ports bei Microsoft Exchange 5.5

Wenn Sie eXpurgate mit Microsoft Exchange 5.5 auf demselben Server einsetzen wollen, müssen Sie dafür sorgen, dass Exchange Mails auf einem anderen Port als 25 entgegennimmt.<sup>5</sup> Der SMTP-Connector von Exchange 5.5 übernimmt dabei den Port, an den er sich bindet, aus der Datei `services`, die Sie unterhalb Ihres Windows-Verzeichnisses (%SystemRoot% bzw. C:\WINNT) in `system32\drivers\etc` finden. Diese können Sie z. B. wie folgt editieren:

```
notepad %SystemRoot%\system32\drivers\etc\services
```

Der Datei `services` liegt folgendes Schema zugrunde:

```
# <Dienstname> <Portnummer>/<Protokoll> [Alias...] [#<Kommentar>]
[...]
smtp                25/tcp             mail                #Simple Mail Transfer Protocol
```

<sup>5</sup> Wenn Sie eXpurgate und Exchange auf verschiedenen Rechnern einsetzen wollen, ist diese Änderung nicht erforderlich, da sich dann nicht zwei Serverprogramme denselben Port 25 teilen müssen.



Ändern Sie bitte den Wert hinter smtp (default: 25/tcp) auf den Zahlenwert eines neuen, freien Ports, auf dem Ihr Exchange nun Mails entgegennehmen soll, wie z. B. 10025. Entsprechend müsste der geänderte Eintrag in der Datei `services` wie folgt aussehen:

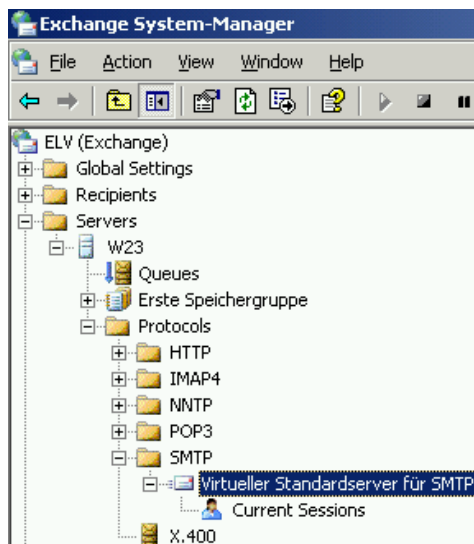
```
smtp          10025/tcp      mail          #Simple Mail Transfer Protocol
```

Anschließend muss der Dienst neu gestartet werden, damit die Änderung wirksam werden kann. Sie können dies mit Hilfe von `telnet` testen (vgl. 2.1.4).

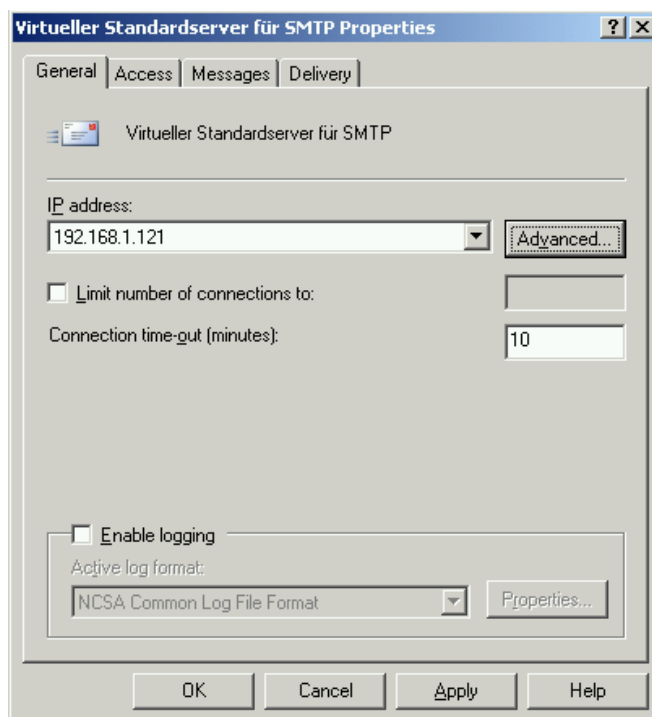
### 2.1.3 Ändern des TCP-Ports bei Microsoft Exchange 2000 bzw. 2003

Die Möglichkeit zum Ändern des Ports, auf dem Exchange Mails von außen entgegennimmt, ist bei Exchange 2000 bzw. 2003 bereits vorgesehen, so dass es dafür eine Option innerhalb des Programms gibt. Um diese zu erreichen, gehen Sie bitte wie folgt vor:

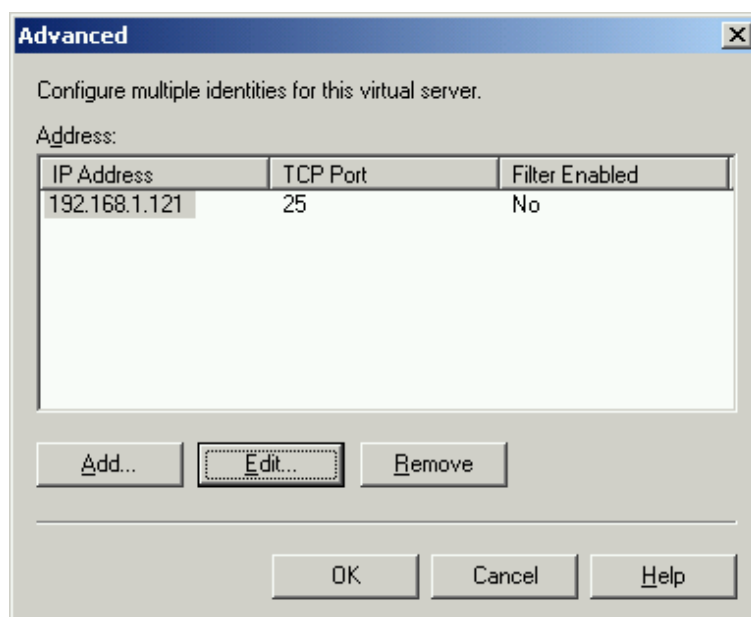
- Öffnen Sie den Exchange-System-Manager (i.d.R. im Startmenü unter Programme/Microsoft Exchange/System-Manager).
- Klicken Sie im System-Manager auf Server, dann auf den betreffenden Server und unter /Protokolle/SMTP mit der rechten Maustaste auf Virtueller Standardserver für SMTP, um im dann aufgehenden Menü auf Eigenschaften zu klicken.



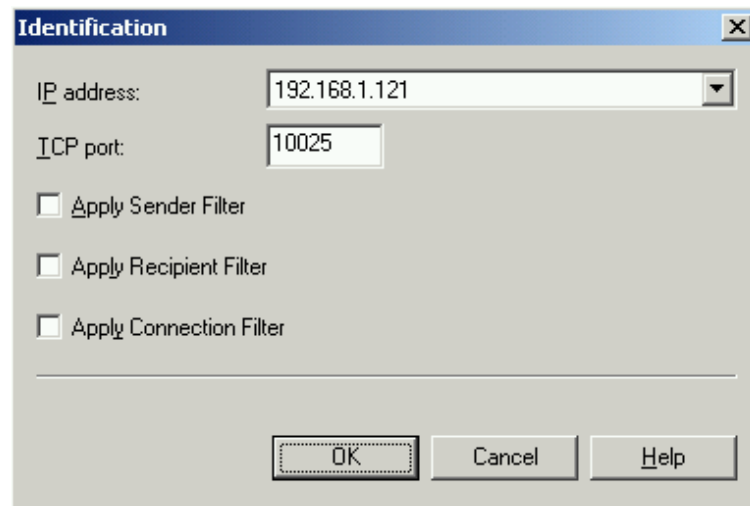
Wählen Sie auf der Registerkarte "General" die IP-Adresse des Servers aus und klicken Sie dann auf `Erweitert`.



Klicken Sie auf Bearbeiten, um die Eigenschaften dieses Virtuellen Servers bearbeiten zu können.



Hier können Sie unter TCP Anschluss den Port ändern, auf dem Ihr Exchange eingehende E-Mails entgegennehmen soll. Tragen Sie dort einen anderen, bislang ungenutzten Port, wie z. B. 10025 ein und bestätigen Sie dies mit OK.



Mit einem weiteren OK gelangen Sie zurück zum Exchange System-Manager. Halten Sie nun den Virtuellen Server an, um ihn anschließend neu zu starten. Nun sollte Ihr Exchange auf Port 10025 ansprechbar sein. Lesen Sie bitte den folgenden Abschnitt, um zu testen, ob die Änderung erfolgreich war.

#### 2.1.4 Testen, ob Exchange auf einem Port antwortet

Wenn Sie testen möchten, ob Ihr Exchange Server die Änderung des Ports übernommen hat, können Sie dies mit Hilfe von `telnet` testen. Öffnen Sie dazu eine Kommandozeile und geben Sie folgendes ein:

```
telnet 192.168.1.121 10025
```

 (Dabei verwenden Sie statt 192.168.1.121 die IP-Adresse Ihres Exchange-Servers, wobei 10025 dem neuen TCP-Port entspricht.)

Ihr Exchange sollte Sie nach erfolgreicher Änderung und Neustart des Virtuellen SMTP-Servers etwa wie folgt begrüßen:

```
220 W23.intern Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready
```

Beenden Sie den SMTP-Dialog mit Exchange durch die Eingabe von `quit`. Wenn dieser Test erfolgreich war, können Sie eXpurgate nun auf Port 25 starten, damit dieses eingehende Mails nach der Klassifizierung an Exchange weiterleiten kann.

## 2.2 Installation von eXpurgate auf einem Unix-System

Wenn Sie eXpurgate unter einem Unix-Derivat nutzen wollen, kopieren Sie bitte das für Ihre Plattform bestimmte Archiv in das Root-Verzeichnis '/' und entpacken Sie es dort (z. B. mit: `"tar -xzf eXpurgate-1_1_1_Linux_i686.tar.gz"`). eXpurgate wird dadurch in das vorbereitete Verzeichnis `/usr/local/eleven` installiert.<sup>6</sup>

eXpurgate benötigt für den Betrieb die zentrale Konfigurationsdatei `expurgate.xml` im Verzeichnis `etc` unterhalb des Installationsverzeichnisses. Da diese bei einem Update durch eine neuere Version überschrieben würde, liegt sie ab der Version 1.3.29 nur noch unter dem Namen `expurgate.xml-orig` bei. Sie können diese kopieren oder umbenennen, um so eine funktionierende `expurgate.xml`-Datei zu erhalten. Diese können Sie editieren, um Ihre gewünschten Einstellungen vorzunehmen.

Anschließend müssen Sie noch manuell ein für Ihr System spezifisches Initscript starten. Im Verzeichnis `etc/init.d` unterhalb des eXpurgate-Verzeichnisses finden Sie einige Beispieldateien für verschiedene Distributionen. Bitte wechseln Sie in das zu Ihrem System passende Unterverzeichnis und beachten Sie die weiteren Hinweise im Script `expurgate`.

Damit eXpurgate ordnungsgemäß funktionieren kann, müssen Sie nun noch Ihre Lizenzdatei einspielen. Diese wird per Voreinstellung als `client.key` im Verzeichnis `etc` unterhalb des eXpurgate-Verzeichnisses erwartet. Bei Bedarf können Sie jedoch deren Namen und Pfad über den Parameter `license file` in der zentralen Konfigurationsdatei `expurgate.xml` Ihren Wünschen anpassen. Informationen zu Ihrer Lizenz erhalten Sie durch Aufruf von `"./expurgate --testshowlicence --configfile ../etc/expurgate.xml"` im eXpurgate-Programmverzeichnis.

Damit ist die Grundinstallation abgeschlossen – im folgenden Abschnitt erfahren Sie, wie Sie eXpurgate an Ihr System anpassen und starten können.

### 2.2.1 eXpurgate unter Sun Solaris

Das Betriebssystem Sun Solaris weist Besonderheiten auf, die unter gewissen Umständen einige Anpassungen des Betriebssystems erforderlich machen. Je nach Versionsnummer sind die folgenden Patches, jeweils für die Sparc-Plattform, erforderlich:<sup>7</sup>

Solaris 10	Kein Patch nötig	
Solaris 9	111711-16 (oder neuer)	32-bit Shared library Patch for C++
	112963-30 (oder neuer)	Linker Patch (32-bit)

Die erforderlichen Patches bekommen Sie unter folgendem Link:

<http://developers.sun.com/prodtech/cc/downloads/patches/index.html>

<sup>6</sup> Falls Sie ein anderes Installations-Verzeichnis (z. B. `/opt/expurgate`) bevorzugen, müssen Sie den eXpurgate-Installationspfad in der Datei `expurgate.xml` (s. u.) anpassen.

<sup>7</sup> Für die x86-Plattform bieten wir nur Solaris 10, für das keine Patches erforderlich sind.

### 3 Konfiguration von eXpurgate

Nachdem wir uns im vorigen Teil der Grund-Installation von eXpurgate.Inhouse auf Ihrem System zugewendet haben, möchten wir Ihnen im folgenden die Konfigurationsoptionen vorstellen, mit denen Sie das Verhalten von eXpurgate beeinflussen.

Die Konfiguration von eXpurgate erfolgt einerseits durch Parameter, die dem Programm beim Start übergeben werden (Kommandozeilen-Optionen) und andererseits durch die Konfigurationsdatei `expurgate.xml`. Beide Teile finden Sie in den entsprechenden Kapiteln dieses Dokuments erklärt.

#### 3.1 Allgemeine Kommandozeilen-Optionen

Mit Hilfe der folgenden Kommandozeilen-Optionen steuern Sie eXpurgates Betrieb. Diese sind weitgehend unabhängig vom verwendeten Betriebssystem. Eine Übersicht der möglichen Optionen erhalten Sie auch, wenn Sie `expurgate --help` eingeben. Jeweils in Klammern geben wir die in älteren eXpurgate-Versionen verwendeten kurzen Optionen wieder: diese sind derzeit noch alternativ gültig, werden aber in zukünftigen Versionen nicht mehr unterstützt. Bitte berücksichtigen Sie, dass die langen Optionen jeweils mit zwei vorangestellten Bindestrichen angegeben werden müssen, die kurzen hingegen nur mit einem.

<code>help (h)</code>	Gibt die möglichen Optionen aus
<code>version (v)</code>	Gibt die Programm-Version aus
<code>shortversion (V)</code>	Gibt die Programm-Version in kurzer Form aus
<code>configfile &lt;configfile&gt; (f)</code>	Spezifiziert das Konfigurationsfile (default: <code>expurgate.xml</code> )
<code>connectiontimeout &lt;secs&gt; (m)</code>	Maximalzeit für eine Verbindung in Sekunden, 0 für unendlich (default: 300)
<code>datatimeout &lt;secs&gt;</code>	Gibt an, wie lange eXpurgate maximal auf Daten von der Gegenseite wartet oder wie lange versucht wird, Daten an die Gegenseite zu senden (in Sekunden). Wird der Wert überschritten, so wird die Verbindung mit einem temporären Fehler geschlossen. (0 für unendlich, default: 0)
<code>servermode (s)</code>	Servermode: startet dieses Programm im Hintergrund als <i>daemon</i>
<code>spamd (r)</code>	Wenn dieser Parameter angegeben wird, kommuniziert eXpurgate nicht über das SMTP-Protokoll sondern als <i>Spamd</i> über das Spam Assassin Protokoll. Für eine erfolgreiche Klassifizierung wird im Header des Spam Assassin-Protokolls die Zeile 'Sender:<Absender>' benötigt - als <Absender> ist damit der im SMTP-Dialog verwendete MAIL-FROM-Part des Mail-Envelopes gemeint
<code>pidfile &lt;pidfile&gt; (P)</code>	Schreibt in die angegebene Datei die Prozess-Nummer des startenden eXpurgate Servers
<code>milster &lt;socketIdent&gt; (M)</code>	Verwendet statt SMTP das Sendmail-Milster-Protokoll und <socketIdent> für die Kommunikation mit Sendmail (vgl. 1.3)
<code>milvertimeout &lt;seconds&gt; (T)</code>	libmilster MTA Verbindungs-Timeout (30)
<code>testexit &lt;numofmails&gt; (Y)</code>	Nur zu Testzwecken: Nach der mit <numofmails> angegebenen Anzahl verarbeiteter E-Mails beendet sich eXpurgate (0)
<code>exdbproxy &lt;port&gt; (N)</code>	Startet ausschließlich einen exDB-Proxy auf dem angegebenen Port
<code>uid &lt;userid&gt;</code>	Wechselt nach dem erfolgreichen Start zur mit userid (numerisch oder namentlich) angegebenen Userid
<code>gid &lt;groupid&gt;</code>	Wechselt nach dem erfolgreichen Start zur mit groupid

(numerisch oder namentlich) angegebenen Groupid

## 3.2 Optionen bei Nutzung des SMTP- oder SpamAssassin-Protokolls

<code>ipaddress &lt;ip/hostname&gt; (i)</code>	Die IP-Adresse oder der Hostname, auf dem Verbindungen angenommen werden sollen (default: 0.0.0.0)
<code>bindport &lt;port&gt; (p)</code>	Bindet auf die Server Port-Nummer (default: 11011)
<code>socketqueuesize &lt;size&gt; (q)</code>	Wenn Verbindungsanfragen schneller erfolgen als vom Betriebssystem abgearbeitet werden können, ist dies die Zahl der maximalen Verbindungen, die gepuffert werden (default: 5)
<code>mrtgfile &lt;path&gt; (g)</code>	<p>MRTG Debug-Datei Pfad + Datei-Präfix</p> <p>Wenn angegeben, werden zwei Dateien erzeugt, in denen Laufzeitinformationen stehen, die von MRTG (Multi Router Traffic Grapher) verarbeitet werden können.</p> <p>Die Angabe wird als Dateiname mit Pfad verstanden, an den '_proc.mrtg' für das erste und '_times.mrtg' für die zweite Datei angehängt werden. Die Dateien werden alle 60 Sekunden aktualisiert.</p> <p>In der Datei '_proc_mrtg' stehen die folgenden Werte:</p> <ul style="list-style-type: none"><li>- Anzahl der verarbeiteten Mails</li><li>- Aktive Verbindungen</li><li>- Uptime des Programms in Sekunden</li><li>- Beschreibung</li></ul> <p>In der Datei 'times_mrtg' stehen die folgenden Werte:</p> <ul style="list-style-type: none"><li>- Verbrauchte Prozessor-Zeit im Verhältnis zur vergangenen Zeit in Prozent</li><li>- Häufigkeit des Überschreitens der maximal erlaubten Anzahl von Prozessen</li><li>- Uptime des Programms in Sekunden</li><li>- Beschreibung</li></ul>
<code>maxprocesses &lt;maxproc&gt; (x)</code>	Maximale Anzahl von laufenden Prozessen, 0 für unendlich viele. (default: 50)
<code>blockip &lt;iplist&gt; (b)</code>	<p>Eine kommaseparierte Liste von IP-Adressen bzw. Netzen mit Netzmaske, die keine Verbindungen zu diesem Programm aufbauen dürfen. Alternativ können Sie Namen und Pfad einer Datei mit IP-Adressen angeben</p> <p>Beispiel von einer Liste aus IP Adressen:</p> <p>192.168.1.100, 192.168.2.0/24, 192.168.3.0/255.255.255.0</p>
<code>permitip &lt;iplist&gt; (c)</code>	Eine kommaseparierte Liste von IP-Adressen bzw. -Netzen mit Netzmaske, die eine Verbindung aufbauen dürfen. Ist dieser Parameter gesetzt, dürfen Verbindungen nur von Rechnern aufgebaut werden, deren IP-Adressen zu den angegebenen passen. Ist eine Adresse als Parameter sowohl für 'b' als auch für 'c' angegeben, darf diese keine Verbindungen aufbauen (d. h. 'b' bindet stärker als 'c')

### 3.3 SMTP-spezifische Optionen

<code>smtpouthost &lt;ip/hostname&gt; (a)</code>	Spezifiziert die Adresse des Mailservers für die Weiterleitung (default: localhost). Falls Sie mehrere Zielserver verwenden möchten, beachten Sie bitte den folgenden Abschnitt. Der <code>smtpouthost</code> <b>muss</b> angegeben werden, damit eXpurgate startet.
<code>smtpoutport &lt;port&gt; (o)</code>	Gibt die Port-Nummer an, auf dem der mit 'a' angegebene Server E-Mails entgegen nimmt (default: 10024)
<code>helohostname &lt;hostname&gt; (n)</code>	Hostname, der beim HELO ausgegeben werden soll (default: localhost)
<code>smtpwelcomemsg &lt;message&gt; (w)</code>	SMTP-Willkommensnachricht, die bei einem Connect ausgegeben wird (default: <i>XXX - eXpurgate 2.0.7 (August 13, 2007 11:00:00), eleven GmbH, Berlin/Germany</i> )
<code>allowrelaydomain &lt;List&gt; (k)</code>	Wenn angegeben, nimmt das Programm nur Mails für die angegebenen Domains an (kommaseparierte Liste oder Dateiname). Kann bzw. sollte mit der Option 'j' ergänzt werden
<code>allowrelayip &lt;IPList&gt; (j)</code>	Gibt - wenn 'k' gesetzt wurde - eine Liste von IP-Adressen oder eine Datei an, von denen aus an alle Domains E-Mails versendet werden darf. Ohne die Option 'k' hat diese Option keine Wirkung
<code>smtpmaxrcpts &lt;maxRcpt&gt; (R)</code>	Legt die maximale Anzahl von Empfängern für eine E-Mail fest. Wenn diese Anzahl überschritten wird, wird jeder weitere Empfänger abgelehnt (default: 250)
<code>validatesmtpenv (u)</code>	Der Empfänger, der im SMTP Envelope spezifiziert wurde, wird "on-the-fly" auf dem Ziel-Mailserver geprüft, bevor der Rest der E-Mail verarbeitet wird. Diese Option ist mittlerweile obsolet, da die Envelope-Überprüfung mittlerweile per default eingeschaltet ist. Sie kann mittels <code>dontvalidatesmtpenv</code> deaktiviert werden.
<code>dontvalidatesmtpenv</code>	Das mittlerweile voreingestellte Überprüfen der Envelope-Daten kann mit Hilfe dieser Option deaktiviert werden. Dies ist vor allem bei nacheinandergeschalteten Instanzen eines Mailservers, bei denen bereits der erste die Envelope-Daten geprüft hat, sinnvoll. Das Durchreichen an eine nachgelagerte Instanz ist nicht nur überflüssig, sondern es könnte zudem sein, dass die zweite Instanz mit knapperen Timeout-Parametern konfiguriert ist, da sie normalerweise alle Mails von localhost in kurzer Zeit erhält.
<code>passgiventhelo (U)</code>	Bewirkt, dass der mit dem HELO-Befehl angegebene Hostname an den Ziel-Mailserver durchgereicht wird. Sonst wird der mit der Option '-n' angegebene Hostname (default: localhost) übergeben
<code>noanglebrackets (B)</code>	Verhindert, dass um die im SMTP-Envelope angegebene E-Mail-Adresse spitze Klammern (" <code>&lt;</code> " und " <code>&gt;</code> ", sogenannte "angle brackets") gesetzt werden.
<code>smtpshortreply (S)</code>	Mit dieser Option gibt eXpurgate für positive SMTP-Antworten nur OK zurück. Diese Option ist hilfreich, falls Ihr Mailer die SMTP-Antworten von eXpurgate nicht versteht.
<code>allowpercenthack</code>	Ermöglicht die Verwendung von E-Mail-Adressen in der Form <code>user%nextdomain.dom@mydomain.dom</code>
<code>allowquotinghack</code>	Ermöglicht die Verwendung von E-Mail-Adressen in der Form <code>"user@nextdomain.dom"@mydomain.dom</code>
<code>allowbangpathhack</code>	Ermöglicht die Verwendung von E-Mail-Adressen der Form <code>nextdomain.com!user@mydomain.com</code>
	Ist die Option <code>allowrelaydomain</code> gesetzt, werden die mit den drei vorstehenden hack-Optionen beschriebenen Adress-Varianten automatisch geblockt und können mit diesen Optionen explizit wieder zugelassen werden.
<code>allowxforwardip &lt;iplist&gt;</code>	Speziell im Betrieb mit Postfix gibt diese Option IP-Adressen von Servern an, die den Postfix-Befehl <code>XFORWARD ADDR=w.x.y.z</code> verwenden dürfen, um so einer nachgelagerten Instanz die IP-Adresse eines einliefernden Servers zu übermitteln.
<code>allowxclientip</code>	Verwendung der XCLIENT-Erweiterung. Siehe Kapitel 3.3.2



### 3.3.1 Verwendung mehrerer Zielsever und deren Priorisierung

Im Gegensatz zu den eXpurgate-Versionen 1.x besteht ab eXpurgate 2.0 die Möglichkeit, mehrere Zielsever anzugeben und diese zu priorisieren.

Zur Zustellung bzw. Weiterleitung von E-Mails wird eXpurgate immer versuchen, an den höchstpriorisierten Zielsever auszuliefern. Sollte dahin keine Verbindung zustandekommen, wird eXpurgate den Verbindungsversuch mit dem Ziel-MTA der nächstniedrigeren Priorität fortsetzen. Sind mehrere Ziel-MTAs mit gleicher Priorität angegeben, wird jeweils einer von ihnen zufällig ausgewählt.

Auch wenn Sie lediglich *einen* Zielsever verwenden, müssen Sie diesen (seit eXpurgate 2.0.5) mit der Kommandozeilenoption `--smtpouthost` für den Namen bzw. die IP-Adresse (und gegebenenfalls `--smtpoutport` für den Port) angeben *oder* in der `expurgate.xml` eintragen.

Wollen Sie hingegen mehrere Zielsever verwenden, müssen Sie diese in der Konfigurationsdatei `expurgate.xml` im Abschnitt `SmtOutList` nach folgendem Schema eintragen:

```
<host name="Hostname" port="Portnummer" priority="Priorität"/>
```

Die Bedeutung der einzelnen Parameter können Sie der folgenden Übersicht entnehmen:<sup>8</sup>

hostname	Name des Zielsevers oder dessen IP-Adresse. Löst ein Name auf mehrere IP-Adressen auf, werden alle zugehörigen IP-Adressen mit gleicher Portnummer und Priorität behandelt
port	Gibt die Portnummer des MTAs auf dem Zielsever an
priority	Gibt die Priorität des Hosts als Zahl mit umgekehrter Rangordnung an. Analog zu MX-Einträgen im DNS steht hier die höchste Zahl für die niedrigste Priorität. Es gilt also: je niedriger die Zahl, desto wichtiger der Server

Im folgenden finden Sie ein Beispiel, wie Sie mehrere Server unterschiedlich priorisieren können:

```
<SmtOutList>
<host name="server1a.dom" port="25" priority="10"/>
<host name="192.168.1.125" port="25" priority="10"/>
<host name="backup.dom" port="25" priority="50"/>
</SmtOutList>
```

### 3.3.2 XCLIENT-Erweiterung

Ab eXpurgate 2.0.5 wird die **XCLIENT Extension** für SMTP unterstützt. Hierbei handelt es sich um eine Erweiterung des SMTP-Protokolls, mit der sich Access-Control Anfragen bei mehrstufigen MTA-Filter-Ketten durchreichen lassen.<sup>9</sup>

Auf der Senderseite (d. h., eXpurgate liefert an das Relay aus) wird XCLIENT automatisch verwendet, sobald das Relay diese Extension im SMTP-Dialog mitteilt.

<sup>8</sup> Wenn Sie beide Möglichkeiten parallel verwenden, wird stets der via Kommandozeile angegebene Server am höchsten priorisiert. Wir empfehlen jedoch der Übersichtlichkeit wegen, die beiden Varianten nicht zu mischen.

<sup>9</sup> Siehe [www.postfix.org/XCLIENT\\_README.html](http://www.postfix.org/XCLIENT_README.html)

Auf der Empfängerseite ist die Kommandozeilen-Option `--allowxclientip`, gefolgt von einer Liste von IP-Adressen bzw. Netzen, dafür verantwortlich. Ist diese Option aktiv, akzeptiert eXpurgate von den aufgelisteten IP-Adressen das XCLIENT-Kommando und leitet es auch weiter.

### 3.4 Logging-spezifische Optionen

Wenn Sie die Logging-Funktionalität von eXpurgate nutzen möchten, müssen Sie diese explizit einschalten. Sie können wahlweise in eine oder mehrere Dateien oder nach STDOUT loggen. Mit den folgenden Parametern legen Sie fest, *wohin* geloggt werden soll, während Sie mit den Informationsprioritäten (s. u.) angeben, *welche* Informationen geloggt werden sollen (Loglevel).

```
logstderr <prio>--<prio>[;...] (E) Protokolliert Informationen in den
                                definierten Prioritätsbereichen ("von ...
                                bis ...") auf STDERR. Diese Option kann
                                nicht in Verbindung mit der Option '-s'
                                genutzt werden
logfile <prio>--<prio>:<file> (F) Protokolliert Informationen eines
                                definierten Prioritätsbereichs in eine
                                angegebene Datei. Sie können auch mehrere
                                Log-Dateien schreiben lassen. Dazu
                                wiederholen Sie die Angaben zu <prio>-
                                <prio>:<file>, und zwar nach einem
                                Semikolon als Trennzeichen (siehe Beispiel
                                unten)
```

#### Informationsprioritäten (absteigend gelistet)

EMERG	Fehler, die beim Start von eXpurgate auftreten
ALERT	Schwere Laufzeitfehler, die zum Abbruch der zu verarbeitenden E-Mail führen
CRIT	Laufzeitfehler, die nicht zum Abbruch der zu verarbeitenden E-Mail führen
ERR	Verbindungsfehler, wenn die Kommunikation mit den eXpurgate-Servern und Weiterleitung der E-Mail nicht möglich ist
WARNING	Allgemeine Warnungen, die auf mögliche Fehlerquellen hindeuten
NOTICE	Informationen zur aktuellen E-Mail wie z. B. Absender und Typ
INFO	Mehr Informationen zur aktuellen E-Mail wie z. B. Antworten des Empfangs-Mailservers
DEBUG	Debug-Informationen, insbesondere zum Transfer-Protokoll

So bewirkt das nachfolgende **Beispiel**

```
--logfile EMERG-ERR:/var/log/expurgate-errors.log
```

dass alle Meldungen der Prioritäten EMERG, ALERT, CRIT und ERR ("von EMERG bis ERR") in die Datei `expurgate-errors.log` im Verzeichnis `/var/log` geloggt werden. Sie können auch mehrere Dateien für verschiedene Prioritäten angeben – per Semikolon getrennt – und auf diese Weise steuern, welche Meldungen in welche Dateien geschrieben werden sollen:

```
--logfile EMERG-ERR:/var/log/expurgate-err.log;NOTICE-
INFO:/var/log/expurgate.log
```

Sie können eine Liste von Prioritäten und Dateien angeben, um unterschiedliche Prioritäten in verschiedene Dateien zu schreiben. Wollen Sie nur Informationen *zu einem* Typ loggen, müssen Sie den gewünschten Typ doppelt angeben. Um z. B. nur den Typ NOTICE zu loggen, könnten Sie dies wie folgt erreichen:

```
--logfile NOTICE-NOTICE:/var/log/expurgate-notice.log
```

Unter Unix stehen Ihnen *zusätzlich* die folgenden Optionen zur Verfügung:

```
logsyslog <facility>.<prio>--<prio> (L)   Übergibt Informationen, in einem
                                         definierten Prioritätsbereich mit der
                                         angegebenen Facility an den Unix Syslog
                                         Daemon (Vgl. Unix Syslogfacilities).
                                         Weitere Facilities können durch ein Semi-
                                         kolon getrennt angegeben werden
logconsole <prio>--<prio>[;...] (O) Loggt Informationen in den definierten
                                         Prioritätsbereichen auf die Systemkonsole
                                         via '/dev/console'
```

Die nutzbaren Unix Syslogfacilities sind: AUTHPRIV, CRON, DAEMON, FTP, KERN, LOCAL0-7, LPR, MAIL, NEWS, SYSLOG, USER und UUCP. Wenn Sie mehr über die Unix Syslogfacilities wissen möchten, schlagen Sie bitte in Ihrer Unix Dokumentation unter syslog(3) nach.

### Option logmailidalways

Die (mit eXpurgate 2.0.4 eingeführte) Kommandozeilen-Option "--logmailidalways" sorgt dafür, dass jede Logmeldung zusätzlich als Präfix die ID der gerade verarbeiteten Mail erhält.<sup>10</sup> Die Logmeldung selbst bleibt unverändert.

#### Beispiel:

```
[2007-04-04 16:16:46.950490] eXpurgate[6425.3084928704] [NOTICE] Process  
handle connect from [127.0.0.1/32:35697]
```

wird mit der Option --logmailidalways zu

```
[2007-04-04 16:16:46.950490] eXpurgate[6425.3084928704] [NOTICE]  
ID:070404161646-191946C0-559B8336 Process handle connect from  
[127.0.0.1/32:35697]
```

Dadurch kann man leichter nach den Meldungen für eine individuelle Email "greppen".

## 3.5 Bedeutung der Logfile-Einträge

Eine Übersicht über die Bedeutung der einzelnen Logfile-Einträge finden Sie im Support-Bereich unter [www.eleven.de/support](http://www.eleven.de/support).

## 3.6 Verwendung des SOCKS-Protokolls

Mit Hilfe des SOCKS-Protokolls ist es möglich, die eXpurgate-Verbindungen aus dem internen Netz zu den eXpurgate-Servern über einen entsprechenden Proxy nach außen zu tunneln. eXpurgate unterstützt die SOCKS-Versionen 4 und 5. Um das SOCKS-Protokoll zu verwenden, müssen Sie es in der zentralen Konfigurationsdatei expurgate.xml aktivieren, indem Sie den Parameter 'usesocks="1"' setzen. Dort können Sie außerdem einstellen, welche Protokollversion und welchen Server-Port Sie verwenden, sowie etwa benötigte Daten zur Authentifizierung am SOCKS-Server festlegen. Weitere Hinweise zur Konfiguration der SOCKS-Funktionalität finden Sie in der Konfigurationsdatei expurgate.xml selbst.

## 3.7 SSL/TLS zur Verschlüsselung der E-Mail-Übertragung

Die TLS-Funktion von eXpurgate verhält sich konform mit RFC 2487, d. h. auf der Serverseite wird automatisch STARTTLS als SMTP-Extension als Antwort auf "EHLO" bekanntgegeben und die TLS-Aushandlung begonnen, wenn das STARTTLS-Kommando vom Client gesendet wird.

Auf der Client-Seite setzt eXpurgate ein STARTTLS ab, wenn diese Extension vom Server angekündigt wird. D. h., STARTTLS wird immer versucht, wenn die Gegenseite dies unterstützt, aber niemals zwingend verlangt.

Die Unterstützung von TLS in eXpurgate beschränkt sich darauf, dass der Transport mittels STARTTLS verschlüsselt wird. Dafür wird ein Private- und Public-Key (oder ein self-signed

---

<sup>10</sup> Das gilt natürlich nur für Logmeldungen, die mit der Verarbeitung von Mails zu tun haben.

Zertifikat) benötigt.<sup>11</sup>

eXpurgate aktiviert TLS automatisch, sobald ein Private- und Public-Key (Zertifikat) angegeben ist. Das kann entweder über die Kommandozeilen-Option (`--usetls`) oder über die Konfigurationsdatei `expurgate.xml` erfolgen, wobei die Kommandozeilen-Option den Vorrang hat.

Der Private- und Public-Key müssen zu PKCS (Public Key Cryptography Standards) konform sein und in einem der folgenden File-Formate vorliegen:

DER	ASN1-DER-encoded ist kompatibel mit PKCS#1 RSAPrivateKey
PEM	Ein base64-encodetes DER-Format mit zusätzlichen Kopf- und Fußzeilen
PFX	Bei PFX-Dateien handelt es sich um X.509-Zertifikats-Dateien (self-signed). Dieses Format ist kompatibel mit PKCS#12 (Personal Information Exchange Syntax Standard)

Wenn der angegebene Private-Key mit einem Passwort verschlüsselt ist, wird eXpurgate dieses beim Programmstart abfragen. Wenn man aber die Option "Passwort in einer Datei speichern/merken" einschaltet (durch `--tlspasswordfile`), dann speichert eXpurgate Passwörter (verschlüsselt) in der angegebenen Datei. eXpurgate wird dann beim nächsten Start nicht mehr nach dem Passwort fragen.

Im Allgemeinen erfolgt die Passwortabfrage unter Windows (auch wenn eXpurgate als Service läuft) über eine Dialogbox und unter Unix über die Konsole.<sup>12</sup>

## Kommandozeilen-Optionen

```
--usetls "<privatekey file>,<certificate file>"
```

oder

```
--usetls <self-signed certificate file z.B. PFX/X.509 file>
--tlspasswordfile <file>
```

Wenn Sie kein Passwort angeben (weder über die Kommandozeile noch in der `expurgate.xml`), können Passwörter nicht gespeichert werden: Sie müssen dann bei jedem eXpurgate-Start das Passwort des Private-Keys erneut eingeben. Weitere Hinweise zu Aktivierung von TLS finden Sie in der zentralen Konfigurationsdatei `expurgate.xml`.

## 3.8 Hinzufügen von Received-Headern

Im SMTP-Modus kann eXpurgate eingehenden E-Mails jeweils Received-Zeilen hinzufügen, die Sie mit Hilfe des Parameters `received-header` selbst konfigurieren können. Die Optionen entnehmen Sie bitte dem Kommentar und Beispiel in der `expurgate.xml`-Datei.

<sup>11</sup> Bitte beachten Sie: Zertifikatsverwaltung und Authentifizierung werden nicht unterstützt, d. h. eine host-basierte Authentifizierung wird nicht durchgeführt; Public Keys der Gegenseite werden nicht überprüft und die TLS-Aushandlung ist rein kooperativ.

<sup>12</sup> Wenn eXpurgate unter Unix automatisch gestartet wird, wird die Passwortabfrage problematisch bzw. nicht möglich sein. Sie können dies beheben, indem Sie eXpurgate zumindest einmal von der Konsole aus starten und die Speicherung von Passwörtern mit Hilfe von `--tlspasswordfile <file>` zulassen. Auf diese Weise können Sie auch etwaige Probleme eXpurgates als Dienst unter Windows beheben.

### 3.9 Anpassen der SMTP-Mitteilungen

Alle Antworten eines empfangenden SMTP-Servers an einen E-Mail-Sender bestehen aus einer Zahl und einem erklärenden Text (z. B.: 220 OK). Mit eXpurgate.Inhouse ist es nun möglich, die Standard-SMTP-Meldungen durch eigene zu ersetzen.

Um diese Funktion zu nutzen, müssen Sie zunächst eine Konfigurationsdatei für die Zuordnung zwischen der originalen und der wunschgemäßen anlegen. Diese muss als Textdatei mit folgendem Aufbau existieren:

```
<SMTP-Mitteilungscode>: Der neu anzuzeigende Text mit möglichen  
%VARIABLEN%
```

Dabei brauchen Sie nicht alle Mitteilungs-Codes neu zu definieren, sondern nur diejenigen, die geändert werden sollen. Eine einzeilige Datei mit der Angabe "OK: Alles klar!" wäre somit zulässig. Eine Beispieldatei mit allen möglichen Mitteilungs-Codes und den zugehörigen Variablen finden Sie als SMTPMessages.txt im Verzeichnis etc unterhalb des eXpurgate-Programmverzeichnis.

Nachdem Sie die Konfigurationsdatei erstellt haben, müssen Sie diese für die Benutzung durch eXpurgate aktivieren, indem Sie in der zentralen Konfigurationsdatei `expurgate.xml` folgende Zeile hinzufügen:

```
<setConstString name="smtpMessageFile" value="<pfad/zu/Ihrer/Datei>" />
```

Einige Mitteilungstexte enthalten %VARIABLEN%, die jeweils beim Aufruf ausgewertet werden.

### 3.10 Die Konfigurationsdatei expurgate.xml

Die Datei `expurgate.xml` ist die eXpurgate-Konfigurationsdatei im XML-Format. Um diese Datei zu editieren, empfiehlt sich ein XML- oder HTML-Editor, Sie können aber auch einen beliebigen Texteditor wie z. B. den Windows Editor (notepad) oder vi verwenden. Kommentare und Konfigurationsbeispiele sind immer zwischen `<!--` und `-->` eingeschlossen. Im folgenden werden die wichtigsten Konfigurationsabschnitte erläutert. Weitere Hinweise in englischer Sprache finden Sie in der Datei selbst.

#### eXpurgate-Installationspfad

Der von eXpurgate verwendete Programmpfad wird als `installpath`, ähnlich wie in der folgenden Zeile, angegeben:

```
<setconststring name="installpath" value="/usr/local/eleven"/>
```

Diese Zeile definiert das Verzeichnis in dem Ihr eXpurgate installiert wurde. Falls Sie das vorgegebene Verzeichnis ändern wollen, müssen Sie obige Zeile entsprechend anpassen.<sup>13</sup>

#### Pfad zur DynamicEngine

Bei der DynamicEngine handelt es sich um eine Art "Nachbrenner" für die Bearbeitung von

---

<sup>13</sup> Bei der Windows-Version wird der Pfad z. B. so angegeben: "C:/Programme/eleven/expurgate". Sollten Sie dies manuell anpassen, beachten Sie bitte, dass Sie hier Slashes (/) statt der sonst üblichen Backslashes (\) als Pfadtrenner verwenden müssen.

E-Mails, die insbesondere bei neuartigen Spam-Wellen ("Image-Only" Spams bspw.) eine deutliche Erhöhung der Erkennungsleistung mit sich bringt. Bei Aktivierung dieser Option (mit der Anweisung `useDynamicEngine`) wird ein zusätzliches, für eXpurgate schreibbares Verzeichnis benötigt, in dem administrative Dateien und Laufzeitinformationen für die DynamicEngine abgelegt werden.

```
<setconststring name="dynamicenginepath" value="${installpath}/dynamic"/>
```

Die Standard-Einstellung ist ein Verzeichnis mit Namen `dynamic` unterhalb des `installpath`.

## Sprache für Laufzeit-Fehlermeldungen einstellen

```
<setstring name="language" value="en"/>
```

In dieser Zeile können Sie die Sprache definieren, die eXpurgate für User-Laufzeitfehler verwendet: neben Englisch (en = default) steht derzeit noch Deutsch (de) zur Auswahl. Die folgenden Laufzeitfehler werden bei ihrem Auftreten für Ihre Nutzer sichtbar:

```
die eXpurgate-Lizenz ist abgelaufen
der Viruschecker konnte nicht kontaktiert
werden, somit die E-Mail nicht gecheckt
werden
sonstige
```

## Konfiguration der eXpurgate-Header

Damit eXpurgate das Subject der klassifizierten E-Mails umschreiben kann, müssen Sie einige Eintragungen innerhalb der Datei `expurgate.xml` vornehmen. Um E-Mails der Typen Spam, Bulk, Dangerous und/oder Virus bereits in deren Subject zu kennzeichnen, müssen Sie die folgenden Zeilen gemäß Ihren Wünschen anpassen.

```
<setconststring name="setSpamSubject" value=""/>
<setconststring name="setBulkSubject" value=""/>
<setconststring name="setDangerousSubject" value=""/>
<setconststring name="setDangerousVirusSubject" value=""/>
```

Dabei wird jeweils das Subject anhand des als `value=""` zwischen den Anführungszeichen angegebenen Texts umgeschrieben. Lassen Sie `value` leer, wird das Subject nicht verändert. Folgende Variablen können verwendet werden, um den Text dynamisch zu verändern.

<code>%u</code>	Entspricht dem Teil der E-Mailadresse vor dem '@' Zeichen, also dem Usernamen (E-Mail-Account)
<code>%d</code>	Entspricht dem Teil der E-Mailadresse nach dem '@' Zeichen, also dem Domainnamen
<code>%s</code>	Entspricht der ursprünglichen Betreffzeile
<code>%t</code>	Entspricht dem Namen der eXpurgate-Kategorie (clean, spam, bulk, dangerous)
<code>%v</code>	Name eines erkannten Virus'

Wenn beispielsweise das Subject einer als Spam erkannten E-Mail mit dem Betreff "*Hallo*" an Markus Mueller in "*spam an markus.mueller@domain.de Hallo*" umgeschrieben werden soll, muss die Konfiguration wie folgt aussehen:

```
<setconststring name="setSpamSubject" value="%t an %u@d %s"/>
```

## Behandlung von bulk.advertising und bulk.porn

Wenn Sie wünschen, dass E-Mails vom Typ *bulk.advertising* und *bulk.porn* als *spam* behandelt werden sollen, können Sie dies mit folgender Zeile festlegen:<sup>14</sup>

```
<setconstinteger name="handleBulkSubsLikeSpam" value="1"/>
```

Falls Sie diese Gleichbehandlung nicht wünschen, setzen Sie `value` bitte auf den Wert "0" statt "1".

## Weiterleitung von Massen-E-Mails an einen zentralen Account

Wenn Sie alle kategorisierten Massen-E-Mails an einen zentralen Account weiterleiten wollen, müssen Sie die beiden folgenden Zeilen anpassen. Sie können diese Option jedoch nur nutzen, wenn Sie eXpurgate als SMTP-Proxy oder Milter einsetzen.

```
<setconstinteger name="sendSpamMailsToOneAccount" value="0"/>
```

Wenn Sie in dieser Zeile den Wert "0" auf "1" setzen, werden alle E-Mails, die zur Kategorie Spam gehören, gezielt an eine bestimmte E-Mail-Adresse umgeleitet. Dabei ist es irrelevant, an wen die E-Mail ursprünglich adressiert war: alle E-Mails der Kategorie Spam werden dann an diese Adresse geleitet. Wenn Sie dies wünschen **müssen** Sie auch die folgende Zeile anpassen.

```
<setstring name="spamMailbox" value=""/>
```

Wenn Sie die Weiterleitung wünschen, müssen Sie auch den Parameter `spamMailbox` anpassen, indem Sie als `value` eine Ziel-Adresse eintragen. Beachten Sie dabei bitte, dass die angegebene E-Mail-Adresse auch tatsächlich auf Ihrem Server aktiviert ist.

## Unterstützung von GTUBE

eXpurgate unterstützt seit Version 2.0.5 den GTUBE-Test<sup>15</sup> des SpamAssassin. Dazu muss in der `expurgate.xml` die folgende Zeile eingefügt werden, und zwar im Abschnitt `<mailCheck/>`:

```
<setconstinteger name="obeyGTUBE" value="1"/>
```

Beachten Sie jedoch, dass die GTUBE-Unterstützung auf einem Produktivsystem nicht dauerhaft eingeschaltet werden sollte, da eXpurgate hiermit mehr Ressourcen benötigt.

---

<sup>14</sup> Eine Beschreibung der E-Mail-Kategorien finden Sie im Anhang.

<sup>15</sup> Siehe auch <http://spamassassin.apache.org/gtube/>



## 4 Testen der Funktion von eXpurgate

Im folgenden zeigen wir Ihnen, wie Sie mittels Kommandozeilenoptionen Ihre frische eXpurgate-Installation testen können. Es folgen einige Anmerkungen, wie Sie den Live-Betrieb simulieren können.

### 4.1 Grundlegende Tests Ihrer eXpurgate-Installation

Falls Sie eXpurgate unter Windows einsetzen, wurden die beiden wichtigsten Tests bereits während der Installation durchgeführt. Sie können diese jedoch jederzeit manuell ausführen. Wenn Sie eXpurgate unter Unix einsetzen, werden diese Tests nicht automatisiert durchgeführt. Im folgenden zeigen wir Ihnen, wie Sie die Erreichbarkeit der eXpurgate-Server und Ihres bestehenden Mailservers testen können.

#### Verfügbarkeit der eXpurgate-Server testen

```
expurgate --configfile etc/expurgate.xml --testexdb
```

Da in der Datei expurgate.xml die zu verwendenden eXpurgate-Server angegeben sind, muss der Name bzw. Pfad dieser Datei angegeben werden.

Wenn eine Verbindung nicht hergestellt werden konnte, wird "ERROR: [...]" ausgegeben. Konnte eine Verbindung hergestellt werden, lautet die Meldung "CONNECT: [...]", gefolgt von den Antwortzeiten.

#### Erreichbarkeit Ihres Mailservers testen

```
expurgate --testsmtpcheckdest --smtpouthost localhost --smtpoutport 10025
```

Testet die Verfügbarkeit des anderen Mailservers auf localhost mit Port 10025.

### 4.2 Spezifische Optionen zum Testen von eXpurgate

Folgende Optionen stehen Ihnen zum Test der eXpurgate-Installation zur Verfügung. Ihnen gemein ist, dass sie jeweils den angegebenen Test durchführen, *ohne eXpurgate zu starten*.

testconfig (t)	Testet die angegebenen Parameter
testexdb (Z)	Testet die Verbindung zu einem der im Konfigurationsfile angegebenen eXpurgate-Server.
testexdb <eXdbServer> (W)	Testet den angegebenen eXpurgate Server auf Erreichbarkeit
testshowlicence (l)	Gibt Informationen zum in der Konfigurationsdatei angegebenen Lizenzfile aus
testshowlicencefile <lizenzfile> (z)	Gibt Informationen zum angegebenen Lizenzfile aus
testsmtpcheckdest (C)	Prüft, ob der für die SMTP-Weiterleitung angegebene Mailserver erreichbar ist

### 4.3 Hinweise zum Testen der E-Mail-Kategorisierung von eXpurgate

eXpurgate verzichtet vollkommen auf herkömmliche Verfahren zur Spam-Erkennung wie beispielsweise aufwendige Phrasenuntersuchungen ("viagra", "make money" etc.) und/oder die Überprüfung von IP-Adressen über Realtime Blackhole Lists (RBLs). Stattdessen prüft eXpurgate vor allem das Hauptmerkmal von Spam als *Massen*-E-Mail.

Zu diesem Zweck bildet eXpurgate für jede E-Mail einen Schlüssel, der es dem System erlaubt, in Rückgriff auf die eXpurgate-Datenbank (exDB) verschiedene E-Mails hinsichtlich Ihrer Ähnlichkeit zu prüfen. In Kombination mit weiteren Tests erlaubt dieses Verfahren, Spam zweifelsfrei zu identifizieren und reduziert gleichzeitig die Gefahr der fehlerhaften Markierung individueller E-Mails auf ein absolutes Minimum.

Vor diesem Hintergrund kann eXpurgate jedoch nur *aktuelle* und *unveränderte* E-Mails als Spam erkennen. eXpurgate hält aus Geschwindigkeitsgründen immer nur einen sehr aktuellen Datenbestand vor. Folglich kann die Erkennungsrate mittels archivierter Spam-E-Mails nur unzureichend beurteilt werden. Darüber hinaus muss bei einem Test darauf geachtet werden, dass eXpurgate Spams unbedingt in unveränderter Form - so wie sie ursprünglich verschickt wurden - zugeführt werden. Deshalb kann die Erkennung auch nicht durch das Weiterleiten eines kompletten E-Mail-Verzeichnisses getestet werden: Einerseits sind die einzelnen E-Mails meist veraltet und andererseits werden diese beim Speichern meist mit zusätzlichen Informationen Ihres E-Mail-Programms angereichert. Gleichzeitig bewirkt das Einfügen einer gespeicherten E-Mail in eine neue, dass der Header der ursprünglichen zum Body der neuen wird. Die dann zu prüfende E-Mail und die aus ihr resultierende Prüfsumme würden so massiv verändert.

Für den Test Ihres Setups finden Sie Testmails der unterschiedlichen Kategorien im Verzeichnis "mails" unterhalb Ihres eXpurgate-Installationsverzeichnisses. Diese können Sie z. B. nutzen, um Filter- bzw. Weiterleitungsregeln für die einzelnen Typen zu testen. Bitte achten Sie darauf, dass Sie diese E-Mails eXpurgate möglichst unverändert zuführen.

Die beste und einzig aussagekräftige Art, eXpurgate zu beurteilen, besteht unseres Erachtens darin, eXpurgate den echten und aktuellen Mailverkehr zuzuführen. Dieses bietet Ihnen nicht nur die Möglichkeit, sich von der hohen Erkennungsrate sondern gleichzeitig auch von der im Verfahren begründeten sehr niedrigen False-Positive-Rate zu überzeugen.

## 4.4 Funktionsprüfung via Telnet

Um die Funktion Ihres eXpurgate zu testen, können Sie mittels `telnet` den folgenden Dialog eines sendenden Rechners mit ihrem eXpurgate simulieren. Sie benötigen dazu lediglich eine Kommandozeile.<sup>16</sup> Im folgenden Beispiel sind die manuellen Eingaben durch Fettung hervorgehoben.

```
telnet localhost 25

220 localhost ESMTP - eXpurgate 2.0.7 (August 13, 2007 11:00:00), eleven
GmbH

helo localhost

250 localhost Hello localhost [127.0.0.1/32]

mail from: <postmaster@localhost>

250 <postmaster@localhost> is syntactically correct

rcpt to: <postmaster@localhost>

250 <postmaster@localhost> is syntactically correct

data

354 Enter message, ending with "." on a line by itself

dies ist ein Test
.
250 OK localhost id=040511124439-0360-156D8029 [[OK id=1BNUkb-0000KF-8f]]

quit

221 localhost closing connection
```

Die Eingabe der Nachricht wird mit einem einzelnen Punkt in einer ansonsten leeren Zeile abgeschlossen. eXpurgate nimmt daraufhin Verbindung zu den Servern von eleven auf, um die Klassifizierung der E-Mail vorzunehmen. Wenn diese erfolgreich war, quittiert eXpurgate dies mit dem Code 250 OK und einer ID (ähnlich der abgebildeten).

---

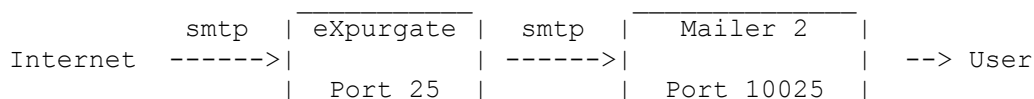
<sup>16</sup> Wenn Sie Microsoft Windows als Betriebssystem verwenden, erreichen Sie die Kommandozeile via Start → Ausführen, indem Sie `cmd` eintippen und die Eingabetaste drücken.

## 5 Einbinden von eXpurgate in ein bestehendes E-Mail-System

Im folgenden finden Sie Hinweise, wie Sie eXpurgate in Ihr bestehendes Mail-System einbinden. Bitte haben Sie Verständnis, falls Ihr Mail-System nicht aufgeführt sein sollte: Wir sind stets bemüht, mit unserer Dokumentation die tatsächliche Verbreitung bei unseren Kunden wider zu spiegeln, können dabei aber nicht jedes System erfassen.

### 5.1 eXpurgate als SMTP-Forwarder

Als SMTP-Forwarder bzw. -Proxy kommuniziert eXpurgate mit dem bestehenden Mailserver nach folgendem Schema:



Um eXpurgate zu starten, wechseln Sie bitte zunächst in das eXpurgate-Verzeichnis (z. B. `cd \programme\eleven\expurgate` unter Windows oder `cd /usr/local/eleven/bin` unter Unix) und rufen Sie es (in einer Zeile) wie folgt auf:

```
./expurgate --configfile ../etc/expurgate.xml --bindport 25
--smtpoutport 10025 --servermode
```

eXpurgate wird somit als Daemon (`--servermode`) mit dem Konfigurationsfile (`--configfile`) `expurgate.xml` im Unterverzeichnis `etc` gestartet.

eXpurgate "lauscht" dann auf Port 25 und sendet eingehende E-Mails an einen zweiten Mailer auf Port 10025 des lokalen Rechners. Um diese Ports zu nutzen, können Sie eXpurgate nicht ohne root- bzw. Administrator-Rechte starten. Mit Hilfe von `--uid` bzw. `--gid` können Sie eXpurgate anweisen, seine userid bzw. groupid nach dem Start zu ändern.

Folgendes Schema verdeutlicht den Ablauf des SMTP-Dialogs während der Einlieferung einer E-Mail bei eXpurgate:

Sender	eXpurgate	Mailer 2
Connect----->		
<-----Welcome (220)		
HELO----->		
<-----Hello (250)		
MAIL FROM----->		
	Connect----->	
	<-----Welcome (220)	
	HELO----->	
	<-----Hello (250)	
	MAIL FROM----->	
	<-----OK (250)	
<-----OK (250)		
RCPT TO----->		
	RCPT TO----->	
	<-----OK (250)	
....		
<-----OK (250)		....
DATA----->		
<-----Enter message (354)		
Sending data----->		
....		
'.'----->		
	<b>eXpurgate e-mail check</b>	
	DATA----->	
	<-----Enter message (354)	
	Sending data----->	
	....	
	'.'----->	
	<-----OK (250)	
	-----disconnect-----	
<-----OK (250)		
-----disconnect-----		

eXpurgate sendet also dem einliefernden Mailserver erst nach erfolgreicher Prüfung und Weiterleitung an den Zielservers (hier: Mailer 2) eine Erfolgsmeldung (OK). Konnte die Prüfung nicht durchgeführt und/oder die E-Mail nicht an den Empfangsserver zugestellt werden, erhält der sendende Server eine Fehlermeldung.

### 5.1.1 Notwendige Änderungen an Postfix bei Verwendung von eXpurgate als Forwarder

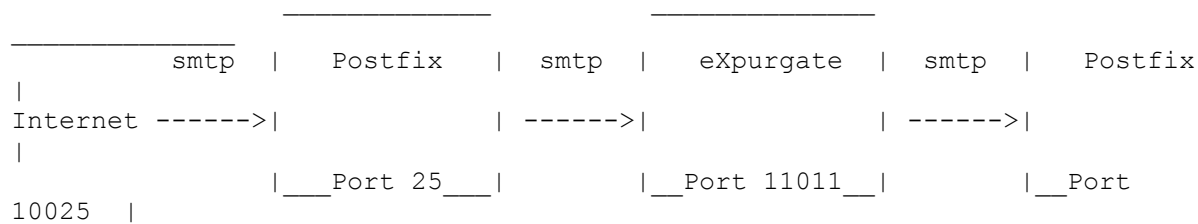
Ergänzend zu den Ausführungen des vorigen Kapitels sind bei Verwendung von Postfix einige Änderungen notwendig. Um Postfix auf einem anderen Port als 25 "lauschen" zu lassen, muss seine Konfigurationsdatei `master.cf` angepasst werden. Ersetzen Sie in dieser Datei in der Zeile, die mit "SMTP" beginnt, dieses "SMTP" durch die entsprechende Portnummer (z. B. 10025).

In der Konfigurationsdatei `main.cf` von Postfix muss in der Variable `my_networks` der Eintrag "127.0.0.0/8" entfernt werden. Das impliziert leider auch, dass von `localhost` keine E-Mails mehr an externe Empfänger verschickt werden können, sondern nur noch an die eigenen Domains.

Weiterhin muss eXpurgate die Startoption `--smtpouthost localhost` bekommen, da es sonst nicht auf 127.0.0.1 seine E-Mails einliefert, sondern mit der lokalen IP, die u. U. in `my_networks` steht, was dann zu einem Open Relay führen würde.

## 5.2 eXpurgate als Content\_Filter in Postfix ("Sandwich")

Die nachfolgend beschriebene "Sandwich"-Integration von eXpurgate in den Unix-Mailer Postfix ist ebenfalls möglich, doch empfehlen wir *grundsätzlich* die Konfiguration nach Kapitel 5.1/5.1.1. Die "Sandwich"-Konfiguration lässt sich schematisch wie folgt darstellen:



Postfix ermöglicht die Einbindung von eXpurgate über die Option `content_filter`. Hierfür müssen die folgenden Einträge in die jeweiligen postfix-Konfigurationsdateien (default im Verzeichnis `/etc/postfix`) hinzugefügt werden.

Fügen Sie in `main.cf` hinzu:

```
content_filter = smtp:localhost:11011
```

Damit definieren Sie für Postfix einen neuen Content-Filter, der eingehende Nachrichten via SMTP an Port 11011 auf localhost weiterleitet. Falls Sie mehrere Content-Filter einsetzen, können Sie diese mittels Kommata separieren.

Fügen Sie in `master.cf` hinzu (eine Zeile):

```
localhost:10025 inet n - n - - smtpd -o content_filter= -o
myhostname=localhost
```

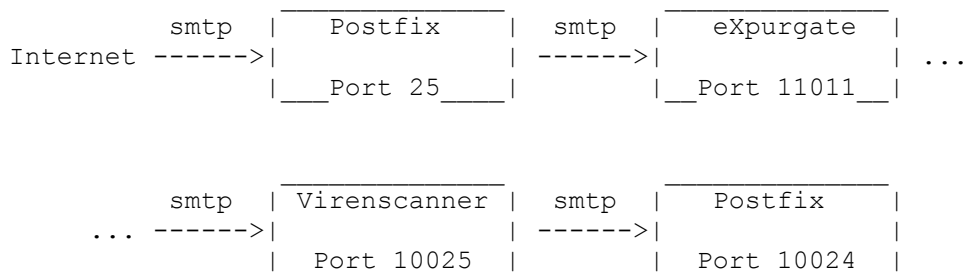
Dieser Eintrag definiert für Postfix eine weitere Aktion. Postfix "lauscht" nun auf TCP-Port 10025 auf eingehende SMTP-Verbindungen. Diese werden jedoch nicht an einen Content-Filter weitergeleitet.

Anschließend starten Sie eXpurgate als Daemon auf Port 11011 mit Port 10025 für die Weiterleitung an die zweite Postfix-Instanz (in einer Zeile).

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 11011 --smtpoutport 10025 --servermode
```

### 5.3 eXpurgate in Postfix mit weiteren Content\_Filtern, etwa einem Virenschanner

Die Einbindung von eXpurgate zusammen mit einem Virenschanner in Postfix erfolgt analog zu der bereits bekannten Konfiguration. Hier kommt allerdings mit dem Virenschanner ein weiterer Dienst hinzu, den es einzubinden gilt. Deren Kommunikation liegt folgendes Schema zugrunde:



Wenn eXpurgate unter Postfix zusammen mit einem Virenschanner benutzt werden soll, empfiehlt es sich, zuerst den Virenschanner und anschließend eXpurgate zu installieren und einzubinden. Ein Virenschanner installiert sich normalerweise auf Port 10025 als Postfix Content-Filter. Um eXpurgate hinzuzufügen, muss in der Postfix-Konfigurationsdatei `main.cf` der Content-Filter-Port für eXpurgate angepasst werden:

```
main.cf:
content_filter = smtp:localhost:11011
```

Dieser Eintrag definiert den Content-Filter für Postfix. Postfix sendet eingehende Nachrichten nun via SMTP-Protokoll weiter an eXpurgate auf Port 11011 auf localhost. eXpurgate muss nun die kategorisierte E-Mail an AntiVir weiterleiten, damit sie auf Viren und ähnliches geprüft werden kann. AntiVir wird die E-Mail anschließend wieder in das Postfix-System zurückleiten.

Um als Content-Filter für Postfix in der Kombination mit einem Virenschanner zu arbeiten, muss eXpurgate mit folgenden Parametern (in einer Zeile) gestartet werden:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
          --bindport 11011 --smtpoutport 10025 --servermode
```

Speziell für den Betrieb mit Postfix steht Ihnen die Kommandozeilen-Option `allowxforwardip` zur Verfügung, mit der Sie angeben können, von welchen IP-Adressen aus Server den Postfix-Befehl `XFORWARD ADDR=w.x.y.z` verwenden dürfen, um damit einer nachgelagerten Instanz die IP-Adresse eines von außen einliefernden Servers zu übermitteln.<sup>17</sup>

<sup>17</sup> Nähere Informationen zum XFORWARD-Kommando finden Sie in der postfix-Dokumentation, z.B. unter: [www.postfix.org/XFORWARD\\_README.html](http://www.postfix.org/XFORWARD_README.html)

## 5.4 Einbinden von eXpurgate in Exim

Um eXpurgate in Exim einzubinden, gibt es zwei Möglichkeiten. eXpurgate kann entweder als SMTP-Forwarder oder als Spam Assassin *Spamd* betrieben werden. Im ersten Fall wird Exim auf einem anderen Port als 25 gestartet. Dazu muss in der Exim-Konfiguration die Option `daemon_smtp_port` wie folgt auf z. B. Port 10125 gesetzt bzw. hinzugefügt werden.

```
daemon_smtp_port = 10125
```

Dies bewirkt, dass Exim nach einem Neustart E-Mails auf Port 10125 entgegennimmt. eXpurgate wird nun so gestartet, dass es auf Port 25 E-Mails annimmt und diese nach der Kategorisierung an Exim auf Port 10125 weiterleitet. Dazu muss eXpurgate mit folgenden Parametern (in einer Zeile) gestartet werden:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 25 --smtpdesport 10125 --servermode
```

Weitere Informationen zu eXpurgate als SMTP-Forwarder finden Sie in diesem Dokument.

Soll Exim die E-Mails mittels des SpamAssassin-Protokolls an eXpurgate übertragen, muss zunächst der Exim Sourcecode gepatcht und neu übersetzt werden. Den Patch bekommen Sie unter <http://duncanthrax.net/exiscan-acl/>. Seit Version 4.50 ist der Exiscan Patch in Exim enthalten.

Im Exim Konfigurationsfile `/etc/configure` müssen einige Optionen gesetzt werden. Im Abschnitt `MAIN CONFIGURATION SETTINGS`:

```
acl_smtp_data = acl_check_content
spamd_address = 127.0.0.1 783
```

Dies bewirkt, dass für jede eingehende E-Mail sogenannte Content-Checks bzw. Inhaltsüberprüfungen durchgeführt werden. Wobei `acl_check_content` eine neue Sektion in der Exim Konfigurationsdatei referenziert (s. u.). Die zweite Zeile gibt den zu kontaktierenden Spamd an.

Weiterhin müssen noch Einträge in der Exim-Konfigurationsdatei hinzugefügt werden, die angeben, was mit dem Ergebnis der Inhaltsprüfung passieren soll. Dazu müssen im Abschnitt `ACL CONFIGURATION` die folgenden Einträge existieren. Leider unterscheidet sich die Konfiguration von Exim-Versionen vor und ab Version 4.5.

### Für Exim-Versionen vor 4.5

```
begin acl
acl_check_content:
    warn message = X-purgate-Report: $spam_score - $spam_report
    spam = nobody:true
accept
```

### Für Exim-Versionen ab 4.5

```
begin acl
acl_check_content:
    warn message = X-purgate-Report: $spam_score - $spam_report
    spam = nobody:true
accept
```

Diese Zeilen bewirken, dass in jede E-Mail eine Header-Zeile mit dem Ergebnis der Kategorisierung eingetragen wird.

Um eXpurgate als *Spamd* zu starten, muss die Kommandozeile wie folgt aussehen:

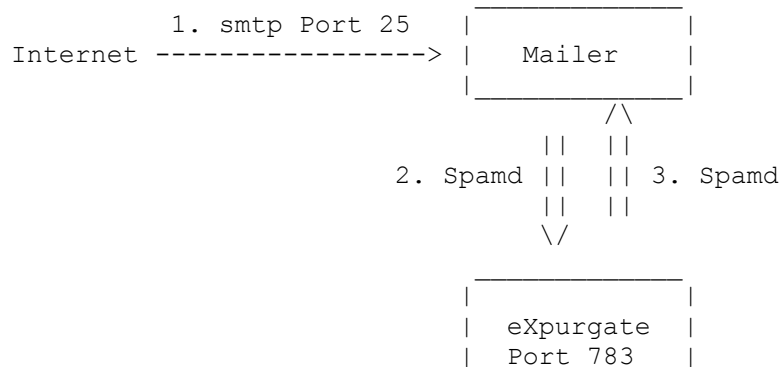
```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 783 --spamd --servermode
```



Weitere Informationen zum Betreiben von eXpurgate als *Spamd* finden Sie im folgenden Abschnitt.

## 5.5 Verwendung von eXpurgate als SpamAssassin Spamd

Als SpamAssassin Spamd kommuniziert eXpurgate mit dem Mailserver gemäß folgendem Schema:



eXpurgate kann als Spam Assassin *Spamd* mit folgender Kommandozeile gestartet werden:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml --bindport 783
--spamd --servermode
```

Testen kann man nun z. B. mit dem SpamAssassin-Client *spamc* aus dem SpamAssassin-Paket:

```
cat sample-spam.txt | spamc -R
100.0/10.0
X-purgate-Type: Spam
X-purgate-ID: 14123::040603215052-48E4-418BB983
```

Damit eXpurgate eine möglichst hohe Erkennungsrate erreicht, sollte im Spamd-Protokoll der Header 'Sender:' mit dem richtigen MAIL FROM aus dem E-Mail Envelope gesetzt werden.

eXpurgate unterstützt alle gängigen Spamd Befehle und antwortet auf einen Request mit "*Spam: True ; 1.0/1.0*", falls es sich bei der angefragten E-Mail um Spam handelt und mit "*Spam: False ; 0.0/1.0*" falls nicht. Zusätzlich gibt eXpurgate noch die Header '*X-purgate:*' und '*X-purgate-ID:*' zurück, die normalerweise von dem Mailer in den E-Mail-Header übernommen werden. Der Header '*X-purgate:*' enthält die der E-Mail zugeordnete Kategorie. Der Header '*X-purgate-ID:*' enthält eine eindeutige ID, mit der im Falle einer Fehlkategorisierung der Support von eleven unter [report@eleven.de](mailto:report@eleven.de) kontaktiert werden kann.

## 5.6 Einbinden von eXpurgate in Qmail

Informationen zum Einsatz von Qmail mit SpamAssassin finden Sie unter den folgenden Links. Sie können diese entsprechend auf den Einsatz mit eXpurgate anwenden.

[http://sylvestre.ledru.info/howto/howto\\_qmail\\_spamassassin.php](http://sylvestre.ledru.info/howto/howto_qmail_spamassassin.php)  
[www.magma.com.ni/~jorge/spamassassin.html](http://www.magma.com.ni/~jorge/spamassassin.html)  
[www.gbnet.net/~jrg/qmail/ifspamh/](http://www.gbnet.net/~jrg/qmail/ifspamh/)  
[www.pyics.net/lateral/stories/9.html](http://www.pyics.net/lateral/stories/9.html)

## 6 Feintuning der E-Mail-Behandlung

eXpurgate ermöglicht Ihnen, die Filterung pro E-Mail-Empfänger bzw. Domain zu steuern: Sie können die Filterung individuell ein- bzw. ausschalten und Spam-, Viren-, Outbreak- und Dangerous-E-Mails bereits während der Einlieferung zurückweisen (reject) oder löschen. Die dazu notwendigen Konfigurationsoptionen wollen wir Ihnen nachfolgend an einigen Beispielen vorstellen.

### 6.1 Global wirkende Schalter

Mit Hilfe der folgenden Optionen können Sie global, d. h. für alle an Ihre Installation angeschlossenen Benutzer, steuern, wie deren E-Mails behandelt werden sollen:

```
<setconstinteger name="noExpurgateForAllUsers" value="0"/>
<setconstinteger name="noFreezingForAllUsers" value="0"/>
<setconstinteger name="noVirusCheckForAllUsers" value="0"/>
```

Per Voreinstellung sind Spamcheck, Freezing und Virencheck für alle Benutzer eingeschaltet (d. h., "value" ist auf "0" gesetzt); Sie können diese aber auch explizit und unabhängig voneinander ausschalten, indem Sie für den entsprechenden "Schalter" hinter "value" den Wert 1 setzen. Diese Option ist i. d. R. nur dann sinnvoll, wenn Sie mit Hilfe der userspezifischen Regeln (*User Features*, s. u.) ein Feature lediglich für einzelne Benutzer einschalten wollen.

Grundsätzlich haben die nachfolgend beschriebenen userspezifischen Regeln Vorrang vor den globalen Schaltern. Wenn Sie also die Regeln geschickt setzen, können Sie sich ein wenig Arbeit ersparen, indem Sie die globale Regel als für die meisten User zutreffend definieren und nur für einige Ausnahmen userspezifische Regeln erstellen. Die Konfiguration wird dadurch für Sie übersichtlicher und Sie ersparen eXpurgate, bei jeder einkommenden E-Mail große Konfigurationsdateien abarbeiten zu müssen.<sup>18</sup>

### 6.2 Benutzerspezifische Steuerung der eXpurgate-Checks: User Features

Sie haben die Möglichkeit, für jeden Empfänger die Funktionen Spam-Check, Virus-Check und Freezing separat einzustellen – unabhängig von den bereits beschriebenen globalen Schaltern. Sie steuern das Verhalten durch die nachfolgend beschriebenen Parameter in der Konfigurationsdatei expurgate.xml. Um diese Funktionen nutzen zu können, ist es notwendig, dass eXpurgate im SMTP-Modus arbeitet – bei Betrieb als Milter oder spamd können die User Features *nicht* genutzt werden.

Die benutzerspezifischen Regeln legen Sie jeweils in Textdateien mit folgendem Aufbau fest:

E-Mail-Adresse bzw. Domain: Feature-Liste

<sup>18</sup> Grundsätzlich werden für jede eingehende E-Mail die userspezifischen Konfigurationsdateien neu geladen. Das ist normalerweise unproblematisch, da diese Dateien vom Betriebssystem zwischengespeichert werden. Sind die Dateien jedoch sehr groß, kann es sinnvoll sein, sie dauerhaft im Speicher zu halten. Mit der Option "preLoadAllDB" können Sie festlegen, dass eXpurgate die Dateien jeweils beim Start einliest und im Speicher hält. Allerdings erfordern Änderungen an der Liste dann jeweils einen Neustart eXpurgates.

**Beispiele:**

```
info@domain1.dom: expurgate
info@domain2.dom: freeze
```

Ignoriert werden dabei alle Zeilen, die leer sind, mit einem "#" beginnen, keinen Doppelpunkt oder keine gültige Aktion enthalten.

Um die userspezifische Steuerung zu aktivieren, geben Sie in der Konfigurationsdatei expurgate.xml unter

```
<setconststring name="userFeaturesDB" value=""/>
```

für value den Pfad und Namen der empfängerspezifischen Konfigurationsdatei ein. Dies könnte z. B. wie folgt aussehen:

```
<setconststring name="userFeaturesDB"
value="{installpath}/etc/userFeaturesDB"/>
```

Die Datei userFeaturesDB im Verzeichnis etc unterhalb des eXpurgate-Installationsverzeichnisses muss nach folgendem Schema aufgebaut sein:

```
E-Mail-Adresse: Feature [Feature]
```

Dabei kann "Feature" folgende Werte annehmen:

```
expurgate:      Spam-Check ist eingeschaltet.
noexpurgate:    Spam-Check ist ausgeschaltet.
viruscheck:     Virus-Check ist eingeschaltet.
noviruscheck:   Virus-Check ist ausgeschaltet.
freeze:         Freezing ist eingeschaltet.
nofreeze:       Freezing ist ausgeschaltet.
```

Mehrere Features pro Eintrag sind möglich. Die Features sind dann per Komma oder Leerzeichen voneinander zu trennen.

**Beispiele<sup>19</sup>:**

```
postmaster@domain1.dom: noexpurgate
chef@domain1.dom: noexpurgate
sales@domain1.dom: noexpurgate noviruscheck
domain2.dom: nofreeze
domain3.dom: noviruscheck
```

E-Mails an die Adressen "chef" und "postmaster" innerhalb der Domain "domain1.dom" würden hier ungefiltert zugestellt, jene für "sales" ungefiltert und ohne Virenprüfung. Weiterhin würden E-Mails an alle Adressen der Domain "domain2.dom" nicht durch Freezing verzögert, während alle an "domain3.dom" nicht auf Viren geprüft würden. Auf diese Weise können Sie auch einzelne Adressen für Domains von der Filterung ausnehmen, während Sie den Rest der Adressen für diese Domain filtern. Die userspezifischen Features werden dabei vor denen für die gesamte Domain ausgeführt, da eXpurgate jeweils absteigend nach dem Grad der Spezifizierung sortiert.

<sup>19</sup> Die Einträge in der userFeaturesDB sind als Ausnahmen zu den globalen Regeln zu verstehen. Es ist für den Betrieb von eXpurgate nicht nötig, User Features hier mit aufzunehmen, die von den globalen Einstellungen abgedeckt sind. Ist beispielsweise "Freezing" global ausgeschaltet ("noFreezingForAllUsers" value="1"), ist der value "nofreeze" in der userFeaturesDB redundant. Eine "doppelte Nennung" hat aber keine negativen Auswirkungen auf eXpurgate, abgesehen vielleicht von der durch zusätzliche Einträge verursachten Mehrgröße der Steuerungsdateien.

**Bitte beachten Sie, dass das Ausschalten der Filterung auch die in den folgenden Abschnitten vorgestellten Verfahrensweisen außer Kraft setzt. Wenn Sie beispielsweise für eine oder mehrere Adressen `noexpurgate` setzen, werden die in nachfolgend vorgestellten Regeln zur Behandlung bestimmter Absender bzw. Spam-E-Mails nicht angewandt.**

## 6.3 Steuerung in Abhängigkeit vom Absender

### 6.3.1 Behandlung von E-Mails bestimmter Absenderadressen

Mit Hilfe der Option `whiteBlackMailFromListFile` können Sie für bestimmte Absenderadressen angeben, dass deren E-Mails *immer*, d. h. *unabhängig vom Inhalt*, in einer vorbestimmten Weise behandelt werden sollen.<sup>20</sup> Dabei stehen Ihnen die Funktionen `spam`, `clean`, `delete`, `reject` und `tagAndDeliver` zur Verfügung. Um die Option zu nutzen, müssen Sie den Pfad und Namen einer Konfigurationsdatei in der `expurgate.xml`-Datei unter

```
<setconststring name="whiteBlackMailFromListFile" value=""/>
```

angeben. Dies könnte z. B. für `senderlist.txt` in `/usr/local/eleven/etc` wie folgt aussehen:

```
<setconststring name="whiteBlackMailFromListFile"
value="${installpath}/etc/senderlist.txt"/>
```

Für `value` können Sie die folgenden Aktionen verwenden:

<code>spam</code>	Alle E-Mails des Absenders werden als "spam" behandelt
<code>clean</code>	Alle E-Mails des Absenders werden als "clean" behandelt
<code>delete</code>	Alle E-Mails des Absenders werden gelöscht
<code>reject</code>	Alle E-Mails des Absenders werden zurückgewiesen. Dabei wird am Ende des SMTP-Dialogs jeweils 552 als Code mit einer Klartext-Meldung zurückgegeben. Den Text können Sie als "rejectText" für die einzelnen E-Mail-Typen selbst festlegen (siehe 6.5.3)
<code>tagAndDeliver</code>	Alle E-Mails des Absenders werden dem normalen Kategorisierungsprozess zugeführt und damit <i>abhängig</i> von ihrem Inhalt klassifiziert

So lassen sich beispielsweise eingehende E-Mails von Adressen bzw. Domains, von denen bislang massiv Spam-E-Mails versandt wurden, immer (d. h. *unabhängig* von ihrem tatsächlichen Inhalt) als "spam" deklarieren, während E-Mails von vertrauten Absendern bzw. Domains immer als "clean" markiert werden. Der Aufbau der Datei folgt dem bereits bekannten Schema und könnte z. B. so aussehen:

```
vertrautedomain.dom: clean
spammer@spamdomain.dom: spam
spammer@spamdomain2.dom: reject
wichtig@vertraut.dom: clean
```

E-Mail-Adressen von Domains, die nicht in dieser Liste aufgeführt sind, werden hinsichtlich ihres Inhalts kategorisiert. Grundsätzlich sollten Sie jedoch nur für besonders wichtige bzw. störende Absenderadressen Ausnahmen definieren, da Sie andernfalls Gefahr laufen, aufgrund dieser statischen Regeln unerwünschte Effekte zu erzielen.

<sup>20</sup> Bitte beachten Sie, dass `eXpurgate` für die Nutzung der o. g. Mechanismen via SMTP oder über das Milter-Protokoll angesprochen werden muss.

### 6.3.2 Behandlung von E-Mails bestimmter Sender-IP-Adressen

Analog zur Auswertung der angegebenen E-Mail-Adressen eines Absenders kann eXpurgate auch basierend auf der IP-Adresse eines einliefernden Servers bestimmte vordefinierte Aktionen einleiten. Mit Hilfe der Option `whiteBlackIPListFile` können Sie festlegen, dass E-Mails bestimmter einliefernder Hosts abhängig von deren IP-Adresse *immer* und damit *unabhängig vom Inhalt* als "spam" oder "clean" klassifiziert, zurückgewiesen, gelöscht oder klassifiziert zugestellt werden.

Um ausgehend von der IP-Adresse des sendenden Hosts zu filtern, müssen Sie als "value" für die Option `whiteBlackIPListFile` Pfad und Namen einer Datei mit den IP-Adressen angeben. Der Aufbau der Datei folgt dem im vorigen Abschnitt vorgestellten Schema: jeweils eine IP-Adresse pro Zeile. Dabei können Sie neben einzelnen IP-Adressen auch Netz-Bereiche anhand von Masken (z. B. 255.255.255.0) oder in CIDR-Notation (z. B. 192.168.1.0/24) angeben. Der Aufbau der Datei könnte also wie folgt aussehen:

```
10.11.12.13: clean
192.168.10.0/24: spam
172.16.0.0/255.255.252.0: nofilter
```

Neben den auf der E-Mail-Adresse des Senders basierenden Optionen steht Ihnen für die IP-basierenden zusätzlich die Option `nofilter` zur Verfügung. Damit können Sie z. B. die Filterung für lokale bzw. ausgehende E-Mails ausschalten, indem Sie die IP-Adresse(n) der lokalen Rechner bzw. Server eintragen.<sup>21</sup>

## 6.4 Freezing

Grundsätzlich kann eine Massen-E-Mail in der Anfangsphase ihres Versands noch nicht eindeutig als solche erkannt und klassifiziert werden. Die ersten E-Mails einer Spamwelle werden daher immer als "clean" klassifiziert. Sie können diesem Umstand begegnen und eXpurgates Erkennungsleistung verbessern, wenn E-Mails mit Verdachtsmomenten und (zunächst) geringer Verbreitung, aufgehalten bzw. eingefroren und später erneut geprüft und wieder aufgetaut werden.

Mit Hilfe des *Freezing* wird die Zustellung von "als Massenmail verdächtigen" E-Mails innerhalb eines frei wählbaren Zeitraums absichtlich verzögert. Derart verdächtige eingehende E-Mails werden zunächst angenommen, verbleiben aber bis zu einer eindeutigen Klassifizierung oder bis zum Ablauf eines von Ihnen definierten Zeitraums in einer Warteschlange. Während dieses Zeitraums wird für jede dieser E-Mails in festen Intervallen erneut bei den eXpurgate-Datenbank-Servern (exDBs) angefragt. Liegt dort inzwischen eine Klassifizierung für die betreffende(n) E-Mail(s) vor, wird diese jeweils gemäß der Regeln für die einzelnen E-Mailtypen zugestellt. Andernfalls verbleibt die Mail im Freezing und wird regelmäßig erneut geprüft.

Normale, individuelle E-Mails werden diesem Verfahren nicht unterworfen, sondern lediglich solche mit Verdachtsmomenten. Dabei handelt es sich grundsätzlich um einen kleinen Prozentsatz der gesamten E-Mail-Kommunikation. Aus diesen jedoch die später eindeutig als "spam" klassifizierten E-Mails herauszufiltern, stellt aber einen weiteren Faktor für die Erhöhung der Spam-Erkennungsrate dar.

<sup>21</sup> Im Milter-Modus entspricht die IP-Adresse der des einliefernden, nicht des Sendmail-Hosts. Im SMTP-Modus wird die IP-Adresse des einliefernden Servers verwendet, sofern nicht durch das XFORWARD-Kommando eine andere übermittelt wird.

### 6.4.1 Voraussetzungen

Bitte berücksichtigen Sie, dass zur Nutzung von *Freezing* eine besondere Lizenz erforderlich ist. Außerdem muss eXpurgate im SMTP- bzw. Proxy-Modus betrieben werden. Somit funktioniert *Freezing* nicht im Militer- oder SpamAssassin-Modus.

Die Aktivierung und Konfiguration von *Freezing* nehmen Sie bitte in der zentralen Konfigurationsdatei expurgate.xml vor. Im folgenden wollen wir Ihnen die wesentlichen Parameter kurz vorstellen. Nähere Hinweise entnehmen Sie bitte den Kommentaren im entsprechenden Abschnitt in der expurgate.xml.

### 6.4.2 Konfiguration

Um *Freezing* zu aktivieren, müssen Sie für den Parameter "freezingEnabled" in der folgenden Zeile den Wert "0" auf "1" (default: 0, deaktiviert) setzen:

```
<setconstinteger name="freezingEnabled" value="0"/>
```

Die maximale Zeit in Sekunden, um die eine E-Mail verzögert werden kann, können Sie mit Hilfe des Parameters maxFreezingTime einstellen (default: 3600, entsprechend einer Stunde):

```
<setconstinteger name="maxFreezingTime" value="3600"/>
```

Dabei können Sie mit Hilfe von maxNonBusinessHoursFreezingTime einstellen, wie lange E-Mails außerhalb der Geschäftszeiten maximal aufgehalten werden. So können Sie zu Zeiten, in denen normalerweise deutlich weniger bzw. keine relevante E-Mail-Kommunikation stattfindet, durch das Erhöhen des Intervalls die Erkennungsleistung weiter verbessern. Voreingestellt sind zwei Stunden (7200 Sekunden):

```
<setconstinteger name="maxNonBusinessHoursFreezingTime" value="7200"/>
```

Sie können die Zeit, die als "außerhalb der Geschäftszeiten" gewertet wird, mit Hilfe der Parameter nonBusinessHoursStart für den Beginn und nonBusinessHoursEnd für das Ende frei definieren. Der Wert wird als Ganzzahl in 24-Stunden-Schreibweise nach folgendem Verfahren kodiert:

Stunden\*10000 + Minuten\*100 + Sekunden. Normalerweise wird die Zeit zwischen 2:30 und 7:00 angegeben.<sup>22</sup>

```
<setconstinteger name="nonBusinessHoursStart" value="23000"/>
```

```
<setconstinteger name="nonBusinessHoursEnd" value="70000"/>
```

Der Parameter freezeCheckInterval erlaubt es, das Intervall für die erneute Anfrage der "eingefrorenen" E-Mails festzulegen; voreingestellt sind zehn Minuten (600 Sekunden). Somit wird für die betreffenden E-Mails alle zehn Minuten angefragt, ob unterdessen eine Klassifizierung vorliegt:

```
<setconstinteger name="freezeCheckInterval" value="600"/>
```

Der Parameter addFreezingHeader steuert die Generierung eines speziellen Freezing-Headers, mit dessen Hilfe einfach herauszufinden ist, wie lange eine E-Mail tatsächlich "eingefroren" war:

```
<setconstinteger name="addFreezingHeader" value="0"/>
```

Die möglichen Werte für value sind "0" (aus, default) und "1" (ein). Ist die Funktion eingeschaltet, wird die Header-Zeile x-purgate-freeze: <Anzahl Sekunden im Freezing> jeder E-Mail hinzugefügt, die eingefroren wurde.

<sup>22</sup> Sie können die Zahl auch ermitteln, indem Sie von üblichen Schreibweisen wie z. B. 8h 30min 00s oder 8:30:00 einfach die trennenden Zeichen weglassen: 83000

## Optionen für die Zustellung an den Mailserver

Da es passieren kann, dass der eigentliche Mailserver nach dem "Auftauen" nicht mehr erreichbar ist, können Sie mit Hilfe von "maxAttempts" und "intervalMinutes" angeben, wie oft maximal und in welchem Intervall eine erneute Zustellung versucht wird. Ist die Mail nicht zustellbar, wird die Zustellung entsprechend häufig und in den angegebenen Intervallen versucht:

```
<setconstinteger name="maxAttempts" value="12"/>
<setconstinteger name="intervalMinutes" value="5"/>
```

Misslingt die Zustellung dann immer noch, würde die E-Mail normalerweise gebount, also eine Unzustellbarkeitsmitteilung an den Absender generiert (s. u. "bounceHostAddress", "bounceState" und "bounceSpam"). Da es aber in aller Regel keine gute Idee ist, auf verdächtige oder gar als "spam" erkannte E-Mails Benachrichtigungen an den (vermeintlichen) Absender zu schicken, können Sie konfigurieren, ob dies erfolgen soll oder nicht. Wir raten dazu, keine Bounces zu versenden - insbesondere dann nicht, wenn die auslösende E-Mail "spam" ist.

Das globale Versenden von Bounces (durch eXpurgate!) können Sie mit Hilfe von bounceState ein- bzw. ausschalten:<sup>23</sup>

```
<setconstinteger name="bounceState" value="0"/>
```

Das Versenden von Bounces auf als "spam" klassifizierte E-Mails steuern Sie mittels "bounceSpam". Wir raten ausdrücklich davon ab, auf Spam-E-Mails Bounces zu versenden, da die vermeintlichen Absender meist gefälscht sind und man unnötig "die Falschen" belästigen würde. Daher ist das Bouncen von Spam-E-Mails standardmäßig deaktiviert.

```
<setconstinteger name="bounceSpam" value="0"/>
```

Als Arbeitsverzeichnis für das *Freezing* verwendet eXpurgate das Verzeichnis *spool* unterhalb des Installationsverzeichnisses. Dort werden neben den jeweils aus der Message-ID bestehenden üblichen Dateien mit den Endungen -D (Body) und -H (Header), zusätzliche Files mit den Endungen -C und -P angelegt. Diese werden zur Laufzeit dynamisch aktualisiert. Nach einem Neustart von eXpurgate werden sie neu eingelesen und das *Freezing* bzw. Auftauen aufgrund der gespeicherten Status-Informationen fortgesetzt. Nach erfolgreichem "Auftauen" und Versenden werden diese gelöscht.

Bitte beachten Sie auch die Hinweise zum Benutzerspezifischen Ein-/Ausschalten der Freezing-Funktion unter Punkt 6.2 "User Features" (Seite 42ff).

## 6.5 Behandlung von Spam-E-Mails

Mit Hilfe der folgenden Optionen können Sie festlegen, wie als Spam kategorisierte E-Mails behandelt werden sollen. Sie können deren Annahme verweigern (*reject*), sie löschen, an eine zentrale Adresse oder den ursprünglichen Empfänger weiterleiten sowie das Subject umschreiben lassen. Dabei können Sie die Regeln entweder systemweit für alle Empfänger oder jeweils pro User bzw. Domain festlegen.

---

<sup>23</sup> Sie können außerdem angeben, über welchen Host und Port Bounces versendet werden sollen und mit welchem HELO eXpurgate sich am Server meldet (vgl. expurgate.xml).

### 6.5.1 Systemweite Behandlung von Spam-E-Mails

Das systemweite Verhalten steuern Sie mit den Parametern "deleteSpamsGlobal", "rejectSpamsGlobal" bzw. "sendSpamMailsToOneAccount" - wenn Sie eine dieser Optionen aktivieren, wirkt sich diese auf alle Empfänger aus.

Wenn Sie alle eingehenden Spam-E-Mails (mit Ausnahme jener Empfänger, für die Sie die Option "nofilter" gesetzt haben) löschen möchten, sollten Sie die folgende Option auf den Wert "1" (default: 0) setzen.

```
<setconstinteger name="deleteSpamsGlobal" value="1"/>
```

Alternativ dazu können Sie einstellen, dass die Annahme von Spam-E-Mails verweigert wird, indem Sie rejectSpamsGlobal auf "1" setzen.

```
<setconstinteger name="rejectSpamsGlobal" value="0"/>
```

Der Sender von Spam erhält dabei die unter rejectText angegebene Meldung.

Sollten Sie sich dafür entscheiden, alle Spam-E-Mails an einen zentralen Account weiterzuleiten, können Sie diese Option mit Hilfe von "sendSpamMailsToOneAccount" einschalten, indem Sie value auf "1" setzen. Sie müssen anschließend mit dem Parameter "spamMailbox" angeben, an welche Adresse diese E-Mails weitergeleitet werden sollen.

```
<setconstinteger name="sendSpamMailsToOneAccount" value="0"/>
```

```
<setstring name="spamMailbox" value="spam%d"/>24
```

Für die Nutzung der systemweiten Spam-Regeln ist es erforderlich, dass eXpurgate entweder via SMTP oder via Milter angesprochen wird.

### 6.5.2 Userspezifische Behandlung von Spam-E-Mails

Mit Hilfe des Parameters

```
<setconststring name="spamActionsForUserInFile" value=
"${installpath}/etc/useractionlist.txt"/>
```

können Sie jeweils auf Userebene steuern, wie eingehende Spam-E-Mails behandelt werden. Sie können auf diese Weise E-Mails löschen, rejecten oder kategorisiert zustellen lassen. Dabei müssen Sie als "value" den Pfad und den Namen der Datei mit den userspezifischen Regeln angeben.

Der Aufbau für die userspezifische Konfigurationsdateien (im Beispiel useractionlist.txt) entspricht dem bekannten Schema:

```
user1@domain1: reject
user2@domain2: delete
domain3: tagAndDeliver
```

Dabei werden zunächst die einzelnen E-Mail-Adressen durchsucht. Kommt es dabei zu einem "Treffer", wird das angegebene Verfahren angewendet. Kommt es nicht zu einem "Treffer", werden die Einträge für die Domains ausgewertet.

### 6.5.3 Einstellen des Reject-Texts

Wenn eXpurgate eine E-Mail zurückweist (reject) erhält der sendende Server immer den Code 552 gefolgt von einer Fehlermeldung. Den Text der Fehlermeldung können Sie mittels des

---

<sup>24</sup> Eine Liste der verfügbaren Variablen finden Sie im Anhang.



Parameters "rejectText" selbst festlegen.

```
<setconststring name="rejectText" value="This e-mail is considered spam,  
the server is rejecting it."/>
```

Weitere Informationen finden Sie in der zentralen Konfigurationsdatei expurgate.xml.

## 6.6 Behandlung von Viren-E-Mails

**Für die Erkennung von Viren ist der - separat zu installierende und zu lizenzierende - Einsatz von AntiVir-SAVAPI erforderlich. Sie benötigen zudem einen speziellen eXpurgate-Lizenzkey, um eXpurgate für diese zusätzliche Funktion freizuschalten.<sup>25</sup>**

Analog zur Behandlung von Spam-E-Mails können auch E-Mails mit Viren global oder user-basiert rejected, umgeleitet oder gelöscht sowie deren Subjects umgeschrieben werden. Für die Zusammenarbeit mit AntiVir-SAVAPI sollten Sie diese zunächst installieren und als Dienst starten.

Um das Virenschanning via eXpurgate einzuschalten, muss in der Datei expurgate.xml "value" für den folgenden Parameter von "0" (default) auf "1" gesetzt werden:

```
<parameter name="ActivateVirusChecker" value="1"/>
```

Außerdem müssen Sie angeben, in welches Verzeichnis die von eXpurgate benötigten SAVAPI-Dateien installiert wurden, indem Sie die folgenden Zeilen in expurgate.xml Ihren Gegebenheiten anpassen:

```
<parameter name="AntiVir_windows_loadLibrary"  
value="C:/Programme/H+BEDV/AntiVir SAVAPI/SAVAPI.DLL"/>  
  
<parameter name="AntiVir_windows_AVEWIN32.DLL"  
value="C:/Programme/H+BEDV/AntiVir SAVAPI/AVEWIN32.DLL"/>  
  
<parameter name="AntiVir_windows_ANTIVIR.VDF"  
value="C:/Programme/H+BEDV/AntiVir SAVAPI/ANTIVIR.VDF"/>  
  
<parameter name="AntiVir_windows_HBEDV.KEY"  
value="C:/Programme/H+BEDV/AntiVir SAVAPI/HBEDV.KEY"/>
```

Zusätzlich können Sie mit dem Parameter scanEveryEmailForViruses festlegen, ob jede E-Mail (value=1) auf Viren untersucht werden soll oder nur E-Mails, denen Attachments angehängt sind (value=0, default). In der Praxis sollte es ausreichen, lediglich Attachments auf Viren zu untersuchen, da Sie damit einen Performance-Vorteil erhalten.

Nach einem Neustart eXpurgates kann dieses nun auch E-Mails mit Viren als "*dangerous.virus*" klassifizieren.

Bitte beachten Sie auch die Hinweise zum Benutzerspezifischen Ein-/Ausschalten der Virensan-Funktion unter Punkt 6.2 " User Features" (Seite 42ff).

---

<sup>25</sup> Sollten Sie bereits einen Virenschanner einsetzen, können Sie diesen leider nicht in der hier geschilderten Weise zusammen mit eXpurgate verwenden, da diese Funktion speziell auf AntiVir-SAVAPI basiert. Sie können Ihren bestehenden Virenschanner jedoch wie bisher verwenden, um Viren zu erkennen. Deren Erkennung hat dann jedoch keinen Einfluss auf die Klassifizierung durch eXpurgate als *dangerous.virus*. Sollte Ihr Virenschanner Echtzeit-Dateisystemschutz bieten, sollten Sie das eXpurgate-Spoolverzeichnis von der Prüfung ausnehmen.

## 6.7 Erweiterte Optionen zur Behandlung einzelner E-Mail-Typen

Grundsätzlich stehen Ihnen für die als spam, virus, virus-outbreak und dangerous klassifizierten E-Mails jeweils die globalen Optionen Löschen, Reject und Weiterleitung an eine zentrale Adresse, das Umschreiben des Subjects sowie user-spezifische Regeln zur Verfügung.

Die Behandlung von E-Mails dieser Typen steuern Sie jeweils im zugehörigen Abschnitt der Datei expurgate.xml. Die verfügbaren Optionen lehnen sich an die bereits im vorigen Abschnitt ausführlicher beschriebenen zur Behandlung von Spam-E-Mails an.

Die folgenden, globalen Optionen wirken sich jeweils auf alle Empfänger des Mailservers aus, während die userspezifischen die Steuerung auf der Grundlage einzelner Empfänger erlauben. Um diese Optionen zu aktivieren, müssen Sie jeweils den voreingestellten Wert (value) von "0" (disabled) auf "1" (enabled) setzen und eXpurgate neu starten.

delete<emailtype>Global  
reject<emailtype>Global

Löschen: eingehende Viren-E-Mails werden gelöscht  
Abweisen: E-Mails des betreffenden Typs, werden bei der Einlieferung mit einem 552-Fehler abgelehnt. Den Text, den der Sender angezeigt bekommt, können Sie unter <emailtype>RejectText einstellen (default: "This e-mail is <emailtype>, the server rejects it."). Diese Option steht nur zur Verfügung, wenn eXpurgate als SMTP-Proxy betrieben wird.

send<emailtype>MailsToOneAccount

Umleiten: E-Mails werden - unabhängig von der ursprünglichen Zieladresse - an eine zentrale Adresse geleitet, damit sie dort z. B. von einem Administrator kontrolliert werden können und nicht in User-Mailboxen gelangen. Die Umleitungsadresse können Sie unter "<emailtype>Mailbox" einstellen. Diese können Sie entweder statisch oder auch mit Hilfe der Variablen %u und %d abhängig vom ursprünglichen Empfänger (local part) bzw. der ursprüngliche Domain eintragen. Dabei sind auch Kombinationen aus festen und variablen Bestandteilen wie z. B. virus-%u@%d möglich.

Neben den globalen Regeln kann eXpurgate E-Mails auch anhand userbasierter Regeln verarbeiten. Die Regeln definieren Sie über die unter "<emailtype>ActionsForUserInFile" angegebene Datei mit dem bereits bekannten Schema. Sie können somit gezielt für einzelne Adressen bzw. Domains E-Mails der angegebenen Typen löschen (delete), zurückweisen (reject) oder markiert zustellen (tagAndDeliver).

Die Namen der Parameter für die E-Mail-Typen können Sie der folgenden Übersicht entnehmen.

E-Mail-Typ / Parameter	löschen	abweisen	umleiten	in Mailboxname	benutzerspezifische Regeln
<b>Spam</b>	deleteSpamsGlobal	rejectSpamsGlobal	sendSpamMailsToOneAccount	spamMailbox	spamActionsForUserInFile
<b>Virus</b>	deleteVirusesGlobal	rejectVirusesGlobal	sendVirusMailsToOneAccount	virusMailbox	virusActionsForUserInFile
<b>Virus-outbreak</b>	deleteOutbreakGlobal	rejectOutbreakGlobal	sendOutbreakMailsToOneAccount	outbreakMailbox	outbreakActionsForUserInFile
<b>dangerous</b>	deleteDangerousGlobal	rejectDangerousGlobal	sendDangerousMailsToOneAccount	dangerousMailbox	dangerousActionsForUserInFile
<b>bounce</b>	-	-	sendBouncesMailsToOneAccount	bouncesMailbox	-

## 6.8 Ausschalten der Signalisierung von E-Mails der Kategorie "dangerous"

E-Mails der `dangerous` - Subkategorien mit Ausnahme von `dangerous.virus`, `dangerous.virus-outbreak` und `dangerous.attachment` können Sie mit Hilfe der Option

```
< setconstinteger name="turnOffDangerousSubs" value="1" >
```

ausschalten. Somit werden E-Mails mit *potentiell* gefährlichem Inhalt nicht mehr als "dangerous" markiert. E-Mails mit definitiv gefährlichem Inhalt, wie z. B. angehängten Viren oder Würmern, werden hingegen auch weiterhin als "dangerous" markiert.

## 6.9 Behandlung von "suspect" als "clean"

Um E-Mails vom Typ "suspect" als "clean" zu markieren, können Sie für den Parameter

```
< setconstinteger name="handleSuspectAsClean" value="1" >
```

den Wert "1" setzen (default). Damit können Sie verhindern, dass E-Mails, die nicht eindeutig einer Kategorie zugeordnet werden konnten (und daher als "suspect" klassifiziert wurden), *fälschlich* als problematisch (im Sinne von "gefährlich") oder gar als "Spam" interpretiert werden.

## 6.10 Behandlung von Bounce-E-Mails

eXpurgate erkennt Bounce-E-Mails, d. h. E-Mails die von anderen Servern abgewiesen und an den (vermeintlichen) Absender zurückgeschickt werden und kann diese gesondert behandeln. Bounces können mit Hilfe des Parameters `sendBouncesMailsToOneAccount` an eine unter `bouncesMailbox` anzugebende zentrale Adresse weitergeleitet werden. Außerdem können Sie mit Hilfe von `setBouncesSubject` das Subject modifizieren.

Aufgrund der allgemeinen Nützlichkeit von Bounce-E-Mails, die normalerweise auf technische Probleme bei der Übertragung von E-Mails hinweisen, ist es nicht möglich, diese zu löschen oder abzulehnen - auch dann nicht, wenn sie sich z. B. während einer Wurmwelle als störend erweisen.

## 6.11 Behandlung bestimmter "clean"-Subkategorien als Spam

Falls Sie es wünschen, können Sie auch leere bzw. fast leere E-Mails als "Spam" markieren lassen. Bitte berücksichtigen Sie dabei, dass selbst leere E-Mails unter gewissen Umständen informativ sein können. Mit Hilfe der folgenden Optionen können Sie dafür sorgen, dass E-Mails der Typen "clean.empty" und "clean.emptybody" als "Spam" behandelt werden. Die einzelnen Kategorien unterscheiden sich dabei wie folgt:

`clean.empty`

E-Mails, die weder über ein Subject noch über einen Body verfügen und somit vollständig inhaltsleer sind. Allerdings kann in bestimmten Fällen (Debugging, Test einer neuen Installation) bereits der Empfang einer leeren E-Mail eine wichtige Information darstellen. Um E-Mails dieses

*clean.emptybody*

Typs als "Spam" zu behandeln, sollten Sie für "**handleEmptyLikeSpam**" den Wert 1 (default) setzen.

E-Mails, deren Body vollständig leer ist, aber deren Subject nicht leer ist. Um E-Mails dieser Kategorie als Spam zu behandeln, sollten Sie für

**"handleEmptyBodyLikeSpam"** den Wert 1 setzen (default: 0).

*clean.almostempty*

E-Mails, deren Body nur sehr wenig (bis zu 12 Zeichen) oder "unsichtbaren" Text enthält. Um diese als Spam zu behandeln, setzen Sie für "**handleAlmostEmptyLikeSpam**" den Wert 1.

## 7 Verwendung der eXpurgate-Statistiken

Die eXpurgate-Statistik-Funktion bietet Ihnen die Möglichkeit, sich einen statistischen Überblick über die Verteilung der einzelnen Mailtypen zu verschaffen. Dazu müssen Sie sich zunächst unter <https://www.eleven.de/settings/actions/customers/> mit Ihrem Usernamen und Passwort einloggen. Wählen Sie anschließend den Menüpunkt Statistiken aus, um den für die Statistik gewünschten Zeitraum anzugeben.

☐ Daten seit gestern anzeigen  
☒ Die letzte Woche anzeigen  
☐ Den letzten Monat anzeigen  
☐ Die letzten 3 Monate anzeigen  
☐ Maximum  
☐ Den spezifizierten Zeitraum anzeigen  
 Von  bis   
Format: JJJJ-MM-TT (z.B. 2004-12-31)

☐ Das Mailvolumen anzeigen

---

**Statistik erzeugt am: 15.2.2007 15:16:17 (Mailanzahl)**

[Download Excelfile](#)

Mailtypen	Anzahl	%	Durch. Anzahl pro Tag
<span style="color: green;">■</span> Clean	27.145	6.8	3393.1
<span style="color: red;">■</span> Spam	352.928	87.8	44116
<span style="color: brown;">■</span> Bulk	11.819	2.9	1477.4
<span style="color: black;">■</span> Bulk.Advertising	109	0.0	13.6
<span style="color: black;">■</span> Bulk.Porn	17	0.0	2.1
<span style="color: black;">■</span> Suspect	487	0.1	58.4
<span style="color: black;">■</span> Clean.Empty	55	0.0	6.9
<span style="color: black;">■</span> Clean.Almost-empty	0	0.0	0
<span style="color: black;">■</span> Clean.Empty-body	52	0.0	6.5
<span style="color: black;">■</span> Clean.Bounce	2.467	0.6	308.4
<span style="color: black;">■</span> Dangerous	0	0.0	0
<span style="color: purple;">■</span> Dangerous.Virus	5.370	1.3	671.3
<span style="color: black;">■</span> Dangerous.Attachment	23	0.0	2.9
<span style="color: black;">■</span> Dangerous.Code	29	0.0	3.6
<span style="color: black;">■</span> Dangerous.IFRAME	36	0.0	4.5
<span style="color: black;">■</span> Dangerous.Virus-Outbreak	1.472	0.4	184
<b>Total</b>	<b>401.989</b>		

**Anzahl derzeit aktiver Mailaccounts**

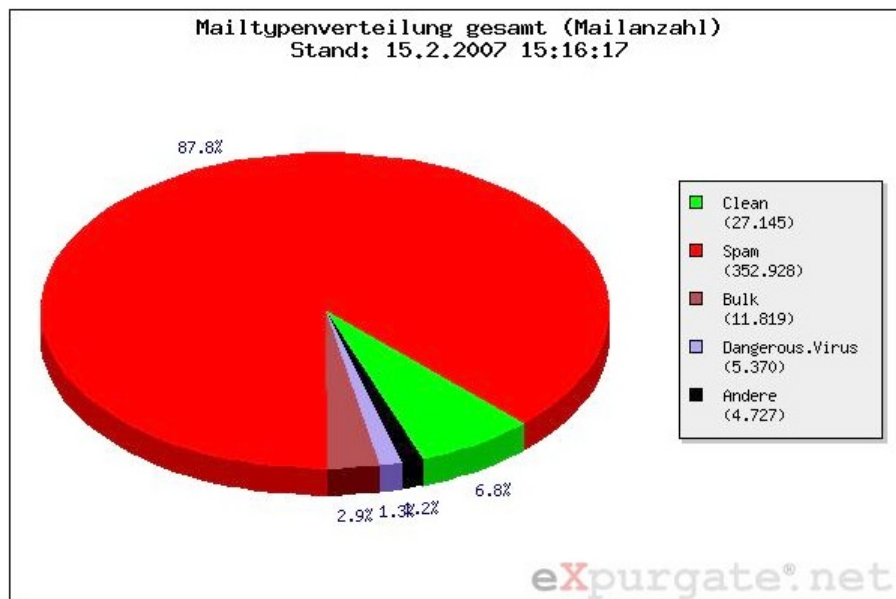
mit wenigen E-Mails	mit vielen E-Mails
2211	3100

Markieren Sie beispielsweise **"Die letzte Woche anzeigen"** und bestätigen Sie Ihre Auswahl mit einem Klick auf **"Submit Query"**,<sup>26</sup> um sich die Verteilung Ihrer E-Mails auf die verschiedenen Kategorien in der vergangenen Woche anzeigen zu lassen. Sie erhalten die Daten über die verarbeiteten E-Mails in drei Formen: tabellarisch, als Kuchen- und als Verlaufsdiagramm. Außerdem können Sie sich die Daten der tabellarischen Darstellung als Excel-Datei herunterladen, um diese für eigene Berechnungen bzw. Präsentationen zu nutzen.

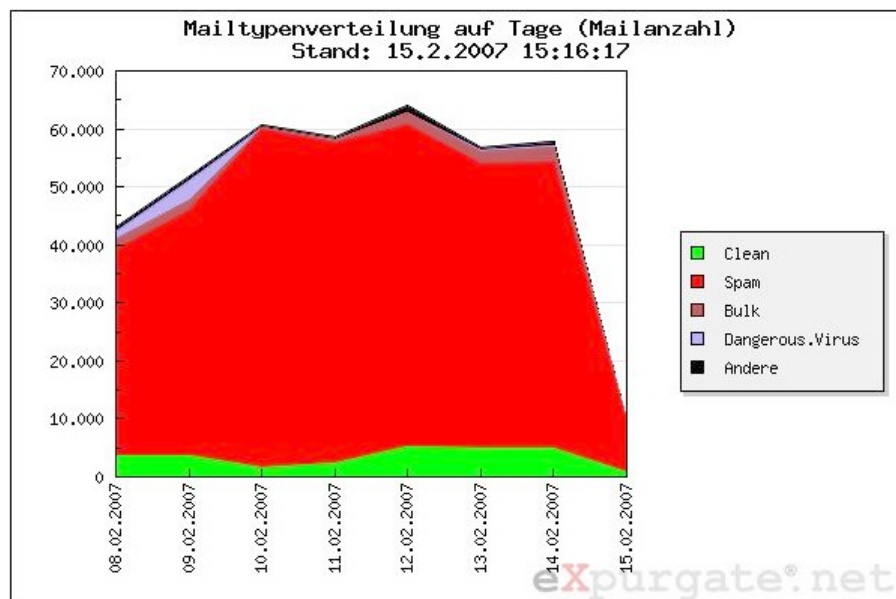
Den unterschiedlichen Darstellungsformen ist gemein, dass Sie jeweils die absolute Anzahl der einzelnen E-Mail-Typen und deren prozentualen Anteil bezogen auf alle E-Mails farbig darstellen. So erhalten Sie schnell einen Überblick darüber, wie hoch der Anteil "nützlicher" bzw. "cleaner" E-Mails im Verhältnis zu den weniger bzw. gar nicht erwünschten E-Mails ist.

<sup>26</sup> Bitte berücksichtigen Sie, dass die Abfrage und insbesondere deren grafische Aufbereitung je nach Mailvolumen bis zu einigen Minuten erfordern kann.

## Kuchendiagramm der E-Mail-Typen



## Verlaufsdigramm der E-Mail-Typen



## Anhang

### Die eXpurgate E-Mail-Kategorien

eXpurgate weist allen geprüften E-Mails eine der folgenden Kategorien zu:

clean	E-Mails, die keine verdächtigen Merkmale aufweisen
bulk	In Massen versendete E-Mails, wie z. B. Newsletter
spam	Eindeutig identifizierte Spam- und Phishing-E-Mails
suspect	E-Mails mit Verdachtsmomenten für "spam" oder "bulk"
dangerous	E-Mails, die u. U. gefährlichen ausführbaren Code oder entsprechende Attachments (Dateianhänge) enthalten
dangerous.attachment	E-Mails, die ein ausführbares Attachment (Dateianhang) enthalten
dangerous.code	E-Mails mit potentiell gefährlichem Inhalt, wie z.B. Links auf lokale Dateien
dangerous.iframe	E-Mails, die das iframe-Feature benutzen (Ein in einer E-Mail eingebettetes iframe könnte beispielsweise benutzt werden, um ein Script auszuführen, das Zugang zum lokalen Dateisystem hat und Dateien lesen oder löschen kann.)
dangerous.virus	E-Mails, die einen Virus enthalten (diese Kategorie steht nur dann zur Verfügung, wenn der optionale Virencheck aktiviert ist)
dangerous.virus-outbreak	E-Mails, die mit höchster Wahrscheinlichkeit einen neuen Virus enthalten (der aber aufgrund seiner Neuartigkeit von Virensclannern noch nicht als solcher erkannt werden kann; diese Kategorie steht nur dann zur Verfügung, wenn der optionale Virencheck aktiviert ist)
bulk.advertising	Werbemails, die kein typischer Spam, aber in der Regel unerwünscht sind
bulk.porn	E-Mails mit pornografischen Inhalten, die nicht "spam" sind (z. B. pornografische Newsletter)
clean.empty	E-Mails, die weder über ein Subject noch über einen Body verfügen und

<code>clean.emptybody</code>	somit völlig inhaltsleer sind E-Mails, deren Body leer und deren Subject nicht leer sind
<code>clean.bounce</code>	E-Mails, die wegen eines Zustellungsfehlers an den Absender zurück geschickt werden

*Weitere Kategorien sind in Planung.*

Die Kategorisierung einer E-Mail wird mit Hilfe zusätzlicher Einträge in deren Header vorgenommen. Anhand dieser Einträge können die von eXpurgate kategorisierten E-Mails mit jedem gängigem E-Mail-Programm durch die Einrichtung von Filtern in einer geeigneten Weise sortiert werden.



## IP-Bereiche der eXpurgate-Server

Gegenwärtig werden von der eleven GmbH die folgenden-Netze für die Erbringung des eXpurgate-Dienstes verwendet und sind wie folgt in der RIPE-Datenbank dokumentiert:

```
inetnum:      195.190.135.0 - 195.190.135.255
netname:      ELEVEN-NET
descr:        eleven GmbH
descr:        Germany
country:      DE
admin-c:      COLT2-RIPE
tech-c:       RR831-RIPE
status:       ASSIGNED PI
```

```
inetnum:      194.145.224.0 - 194.145.224.255
netname:      ELEVEN-NET2
descr:        eleven GmbH
country:      DE
org:          ORG-EA76-RIPE
admin-c:      RR831-RIPE
tech-c:       ERR11-RIPE
status:       ASSIGNED PI
```

## Lizenzen

eXpurgate verwendet die folgenden Lizenzen:

### ***OpenSSL***

Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit entwickelt wurde (siehe [www.openssl.org](http://www.openssl.org))

### ***Expat***

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002 Expat maintainers.

### ***Regex Lib***

Copyright (c) 1998-9 Dr. John Maddock



eleven – Gesellschaft zur Entwicklung und Vermarktung von Netzwerktechnologien mbH  
Hardenbergplatz 2 // 10623 Berlin // Germany  
fon: +49 30 / 52 00 56 - 0 // fax: +49 30 / 52 00 56 - 299  
e-mail: [info@eleven.de](mailto:info@eleven.de) // <http://www.eleven.de>

