

KASPERSKY LAB

Kaspersky[®] Anti-Spam 3.0

KASPERSKY® ANTI-SPAM 3.0

Handbuch für Administratoren

© Kaspersky Lab

<http://www.kaspersky.de>

Redaktionsschluss: Oktober 2006

Inhalt

KAPITEL 1. KASPERSKY® ANTI-SPAM 3.0	6
1.1. Was ist neue in der Version 3.0	7
1.2. Lizenzierungspolitik	9
1.3. Hardware- und Softwarevoraussetzungen	9
1.4. Lieferumfang	10
1.4.1. Lizenzvereinbarung	11
1.4.2. Registrationskarte	11
1.5. Service für registrierte Benutzer	11
1.6. Textgestaltung	12
KAPITEL 2. ARCHITEKTUR VON KASPERSKY ANTI-SPAM UND SPAM- FILTERUNGSGRUNDSÄTZE	14
2.1. Produktbestand	14
2.2. Erkennungstechnologie	18
2.2.1. Analyse der formellen Anzeichen	18
2.2.2. Inhaltsfilterung	18
2.2.3. Überprüfen mit Hilfe der externe Dienste	19
2.2.4. Urgent Detection System Technologie	20
2.3. Erkennungsergebnisse und E-Mail-Handhabung	21
2.4. Inhaltsfilterung-Datenbanken	22
2.5. Filterungsrichtlinien	23
2.6. Verwaltungszentrale	23
2.7. Monitoring	24
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-SPAM	26
3.1. Vorbereitung der Installation	26
3.2. Installation von Kaspersky Anti-Spam	27
3.3. Zugangseinstellungen für die Verwaltungszentrale	28
3.4. Lizenzschlüssel installieren	29
3.5. Kaspersky Anti-Spam in den Mailserver integrieren	30
3.6. Einstellungen von Updates der Inhalt-Datenbanken und Benutzung des UDS-Dienstes	32
KAPITEL 4. VERWALTUNG VON SPAMFILTERUNGSSERVER	33

4.1. Starten und Verwalten der Komponente von Kaspersky Anti-Spam	33
4.2. Verwaltungszentrale von Kaspersky Anti-Spam	34
4.3. Verwaltung von Filterungsrichtlinien	35
4.3.1. Allgemeine Filterungsrichtlinie	36
4.3.1.1. Abschnitt <i>General</i>	38
4.3.1.2. Abschnitt <i>DNS & SPF Checks</i>	40
4.3.1.3. Abschnitt <i>Headers Checks</i>	41
4.3.1.4. Abschnitt <i>Eastern Encodings</i>	43
4.3.1.5. Abschnitt <i>Obscene Content</i>	43
4.3.2. Verwaltung der "weißen" und "schwarzen" Listen	44
4.3.3. Verwaltung von Listen der benutzten DNSBL-Diensten	46
4.3.4. Verwaltung von Liste der geschützten Domänen	48
4.3.5. Gruppenverwaltung	49
4.3.6. Verwaltung von Gruppen-Filterungsrichtlinien	52
4.3.7. Aktionen an den E-Mails	53
4.4. Inhaltsfilterung-Datenbanken updaten	56
4.4.1. Update-Parameter einstellen	56
4.4.2. Update starten	59
4.5. Einstellungen von Spamfilterung-Server	60
4.5.1. Allgemeine Filterungsserver-Parameter	61
4.5.2. Parameter des Master-Filterungsprozesses	62
4.5.3. Parameter der Filterungsprozesse	63
4.5.4. Spamerkennungsparameter	64
4.5.5. Einstellungen von Clientmodulen	66
4.5.6. Benachrichtigung über E-Mailablehnung	67
4.6. Einstellungen der Verwaltungszentrale	69
4.7. Verwaltung von Lizenzschlüsseln	70
4.7.1. Informationen über den Lizenzschlüssel ansehen	71
4.7.2. Neuen Lizenzschlüssel installieren	72
4.7.3. Lizenzschlüssel entfernen	73
4.8. Monitoring des Filterungsservers	73
4.8.1. Allgemeine Informationen über Produktzustand	73
4.8.1.1. Detaillierte Information über Filterungsserver-Kernel	75
4.8.1.2. Detaillierte Information über Updatemodul	76
4.8.1.3. Detaillierte Information über Lizenzierungsmodul	78
4.8.2. Meldungen und Berichte des Monitoringsystems	79
4.9. Statistik von Kaspersky Anti-Spam	80
KAPITEL 5. KASPERSKY ANTI-SPAM DEINSTALLIEREN	82

KAPITEL 6. HÄUFIGE FRAGEN	84
ANHANG A. ZUSÄTZLICHE INFORMATIONEN ÜBER KASPERSKY ANTI- SPAM.....	88
A.1. Anordnung der Dateien in den Verzeichnissen	88
A.2. Clientmodule der Mailserver.....	89
A.2.1. Zusammenarbeit des Clientmoduls mit dem Filterungsservers	89
A.2.2. Allgemeine Parameter der Clientmodule	90
A.2.3. kas-milter – Clientmodul für den Mailserver Sendmail	91
A.2.4. kas-pipe – Clientmodul für die Mailserver Postfix, Exim	93
A.2.5. kas-exim – Clientmodule für den Mailserver Exim.....	100
A.2.6. kas-qmail – Clientmodul für den Mailserver Qmail	103
A.2.7. kas-cgpro – Clientmodul für den Mailserver Communigate Pro.....	104
A.3. Konfigurationsdateien von Kaspersky Anti-Spam	107
A.3.1. Haupt-Konfigurationsdatei <i>filter.conf</i>	107
A.3.2. Konfigurationsdatei <i>kas-thttpd.conf</i>	112
A.4. Dienstprogramme von Kaspersky Anti-Spam	113
A.4.1. kas-htpasswd	113
A.4.2. kas-show-license.....	113
A.4.3. install-key	114
A.4.4. remove-key.....	115
A.4.5. kas-restart.....	116
A.4.6. mkprofiles	117
A.4.7. sfmonitoring	118
A.4.8. sfupdates	119
A.5. Exta-Header des Filterungsmoduls.....	120
A.6. Einstellungen des <i>cron</i> -Dienstes.....	123
ANHANG B. WIE KANN SPAM AN DIE ANALYTIK-GRUPPE VERSCHICKT WERDEN.....	126
ANHANG C. DAS UNTERNEHMEN	128
C.1. Weitere Produkte und Services von Kaspersky Lab	129
C.2. Kontaktinformationen.....	133
ANHANG D. ANWENDUNGEN DER FERMDANBIETER.....	134

KAPITEL 1. KASPERSKY®

ANTI-SPAM 3.0

Kaspersky® Anti-Spam 3.0 (weiter auch *Kaspersky Anti-Spam* oder Produkt genannt) ist ein Programmkomplex, der das Filtern der elektronischen Post durchführt und als Ziel hat, die Benutzer des E-Mail-Systems von dem Massenversand - Spam zu schützen.

Anhand von vordefinierten Richtlinien, bearbeitet Kaspersky Anti-Spam die Nachricht, das heißt: entweder stellt die Nachricht dem Benutzer unverändert zu, blockt sie, generiert eine Benachrichtigung darüber, dass die Nachricht nicht angenommen werden kann, verändert oder ergänzt die Betreffzeile, und führt andere von dem Administrator festgelegte Aktionen durch.

Jede Nachricht wird auf typische Merkmale des unerwünschten Werbe-Massenversand untersucht.

Als erstes, werden unterschiedliche E-Mail-Parameter untersucht: Absender- und Empfängeradresse (envelope), Grösse der Nachricht, wie auch die Headers der E-Mail (Überschripte *From* und *To* eingeschlossen). Außerdem, führt *Kaspersky Anti-Spam* folgende Untersuchungen während der Analyse durch:

- Überprüfung der Absenderadresse (E-Mail und/oder IP-Adresse) mit Hilfe der Schwarz- und Weißlisten;
- Vorhandensein der IP-Adresse des Absenders in diesem oder jenem der DNS-based real time black hole list (DNSBL);



DNSBL (DNS based black hole list) – IP-Adressen-Datenbank der Mailserver, von welchen Massenversand ausgeführt wird. Solche Mailserver nehmen die Nachrichten von allen an und versenden diese an jemanden weiter. Das Benutzen von DNSBL gibt Ihnen die Möglichkeit das Annehmen der Nachrichten von so einem Server automatisch zu verbieten. Richtlinien der Listenerstellung sind bei den Service unterschiedlich. Bitte legen Sie die Richtlinien sorgfältig durch, bevor Sie diesen Service zur Filterung der Nachrichten benutzen.

- Vorhandensein des DNS-Eintrags über den Absender-Server (reverse DNS lookup);
- Überprüfung der IP-Adresse des Absenders auf Übereinsimmung mit der für die Domäne erlaubten Adressen mit Hilfe der Sender Policy Framework Technologie (SPF);

- Überprüfung der Adressen und Links zu Webseiten, die im E-Mail-Text enthalten sind, mit Hilfe des Dienstes Spam URI Realtime Blocklists (SURBL).

Als Zweites, wird Inhaltsfilterung benutzt, das heißt, es werden Inhalt einer E-Mail (einschließlich E-Mail-Header *Subject*) und eingefügte Dateien¹ analysiert. Dabei werden linguistische Algorithmen benutzt, die auf dem Vergleichen der Nachricht mit Muster-E-Mail und auf der Suche charakteristische Begriffe (Wörter und Wortverbindungen) basieren.

Kaspersky Anti-Spam führt auch Untersuchung der grafischen Dateien durch und vergleicht diese mit den Signaturen von bekannten Spam-Nachrichten. Ergebnisse des Vergleichs werden brücksichtigt beim Entscheiden, ob E-Mail zum Spam gehört.

E-Mails, in den Anzeichen der unerwünschten Korrespondenz gefunden werden, werden der Filterung-Richtlinie entsprechend behandelt (s. Pkt. 2.3 auf S. 21).

Filterung-Richtlinie wird mit Hilfe der Verwaltungszentrale vom Administrator eingestellt (s. Pkt.2.6 auf S.23).

1.1. Was ist neue in der Version 3.0

Kaspersky Anti-Spam 3.0 behältet alle Vorteile der Vorgängerversion bei, enthält aber auch eine Reihe von Verbesserungen und Erweiterungen:

1. Neue Version des Filterungskerns Spamtest.

Neue Version des Filterungskerns Spamtest, welcher zum Inhalt von Kaspersky Anti-Spam 3.0 gehört, besitzt folgende Eigenschaften:

- Erhöhte Produktivität und Arbeitsstabilität;
- niedrige Anforderungen an die Grösse des Arbeitsspeichers;
- niedriger Netzwerkverkehr über das Internet (Updates der Datenbasen der Inhaltsfilterung).

2. Verbesserte Filterungsmethoden.

Praktisch alle Methoden der Spamerkennung, die in Vorgängerversion benutzt wurden, wurden verbessert; unter Anderen:

¹ Es werden Einlagen folgender Formaten untersucht Plain text, HTML, Microsoft Word, RTF (Details s. Pkt. 2.2.2 auf S.18).

- Es wurden Auswertungs-Algorithmen der HTML-Objekte in E-Mail verbessert (erhöht Bekämpfungseffektivität der Spammer-Tricks, die auf das Umgehen der Filterungssysteme ausgerichtet sind);
- Analysesystem der E-Mail-Header wurde erweitert und verbessert;
- Analysesystem der grafischen Einlagen (GSG) wurde verbessert;
- Die Benutzung der Dienste Sender Policy Framework (SPF) und Spam URL Realtime Blocklists (SURBL) wurde hinzugefügt.
- das Benutzen des eigenen Dienstes Urgent Detection System (UDS) wurde eingeschaltet, dies erlaubt die Daten über Spam-Arten in Echtzeit zu erhalten.

3. Ein grundsätzlich neues Interface.

Kaspersky Anti-Spam 3.0 benutzt eine Verwaltungszentrale, diese erlaubt Ihnen:

- Produkteinstellungen vornehmen: Filterungsrichtlinien, Aktionen an den Nachrichten, Produktivitätsparameter u.s.w.;
- Produktlizenzen verwalten: Lizenzschlüssel installieren, Information über aktuellen Lizenzschlüssel ansehen;
- Monitoring des Produktzustands durchführen und Statistik ansehen.

4. Bequemes Einstellen der Filterungsrichtlinien.

In der Version 3.0 **Einstellung der Filterungsrichtlinien** wird mit dem intuitiv zu bedienenden Interface der Verwaltungszentrale durchgeführt, dieses gibt Ihnen folgende Vorteile:

- Einfache Administration: bequemes Interface hat eine minimale Auswahl der Werkzeuge für Systemadministration und bietet dabei breite Möglichkeiten für die Adaptation des Systems zu den konkreten Betriebsbedingungen;
- Eigene Einstellungen für Benutzergruppen: für jede Gruppe können unabhängig von den Anderen die Methoden der Untersuchung ein- oder ausgeschaltet werden, es können auch an den Nachrichten vorzunehmende Aktionen definiert werden.

5. Verbesserte Mittel für Integration des Produktes und für die Anpassung in die Infrastruktur:

- Wurden überarbeitet und verbessert die Module der Zusammenarbeit mit Sendmail und Communicate Pro Server;

- Ein Neues System der Zustellung der Updates für Inhaltsfilterung-Datenbanken wurde ausgearbeitet;
- Alle Einstellungen wurden in eine gemeinsame Konfigurationsdatei zusammengefügt, dies vereinfacht die Systemeinstellungen und Administration.

1.2. Lizenzierungspolitik

Lizenzierungspolitik von Kaspersky Anti-Spam 3.0 bietet die Begrenzung für die Nutzung der Anwendung hinsichtlich folgender Merkmale:

- Umfang des E-Mail-Verkehrs;
- Anzahl der geschützten Postfächer.

Die genannten Begrenzungen werden nur für Nachrichten gelten, die den Benutzern der geschützten Domänen adressiert sind. Eine Liste der Domänen, E-Mail-Verkehr deren vom Produkt gefiltert wird, wird in dem Verwaltungszentrale erstellt (s. Pkt. 4.3.4 auf S. 48). Nachrichten, welche den Benutzern aus anderen Domänen adressiert sind, werden nicht gefiltert.



Erstellen Sie eine Liste der geschützten Domänen bevor Sie anfangen Kaspersky Anti-Spam zu benutzen.

1.3. Hardware- und Softwarevoraussetzungen

Für die Arbeit von Kaspersky Anti-Spam sind folgende Systemvoraussetzungen erforderlich:

- Intel Pentium III Prozessor mit Taktfrequenz nicht niedriger, als 500 MHz.
- Mindestens 512 MB Arbeitsspeicher.
- Eines der folgenden Betriebssysteme:
 - RedHat Linux 9.0.
 - Fedora Core 3.
 - RedHat Enterprise Linux Advanced Server 3.
 - SuSe Linux Enterprise Server 9.0.
 - SuSe Linux Professional 9.2.
 - Mandrakelinux version 10.1.

- Debian GNU/Linux 3.1.
- FreeBSD 4.10.
- FreeBSD 5.4 .
- Eines der folgenden E-Mail Server:
 - Sendmail 8.13.5 mit Militer API Unterstützung.
 - Postfix 2.2.2.
 - Qmail 1.03.
 - Exim 4.50.
 - Communigate Pro 4.3.7.
- Installierte Werkzeuge *bzip2* und *which*.
- Perl-Interpreter.

1.4. Lieferumfang

Das Softwareprodukt kann bei unseren Vertriebspartnern (als Hardcopy) oder in einem Online-Shop (z.B. www.kaspersky.com/de, Abschnitt **E-Store**) erworben werden.

Wenn Sie das Produkt als Hardcopy erwerben, umfasst der Lieferumfang des Softwareprodukts folgende Komponenten:

- versiegelter Umschlag mit einer Installations-CD, welche die Dateien des Softwareprodukts enthält.
- Benutzerhandbuch.
- Lizenzschlüssel, auf einer separaten Diskette gespeichert ist.
- Registrierkarte (mit Lizenzschlüssel).
- Lizenzvereinbarung.



Bitte lesen Sie vor dem Öffnen des Umschlags mit der CD sorgfältig den Lizenzvereinbarung.

Beim Erwerb des Produkts in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Webseite. Die Distribution enthält neben dem eigentlichen Produkt auch das vorliegende Handbuch. Der Lizenzschlüssel ist entweder in der Distribution enthalten oder wird Ihnen nach Eingang der Bezahlung per E-Mail zugeschickt.

1.4.1. Lizenzvereinbarung

Die Lizenzvereinbarung ist eine rechtsgültige Vereinbarung zwischen Ihnen und Kaspersky Lab Ltd., in der festgelegt wird, zu welchen Bedingungen Sie das von Ihnen erworbene Softwareprodukt verwenden dürfen.

Bitte lesen Sie die Lizenzvereinbarung sorgfältig!

Wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen, können Sie die Packung mit Kaspersky Anti-Virus an den Händler zurückgeben, bei dem Sie diese erworben haben, und der Kaufbetrag des Produkts wird an Sie zurückerstattet. Voraussetzung dafür ist, dass der Umschlag mit der Installations-CD nicht geöffnet wurde.

Durch das Öffnen der versiegelten Packung mit der Installations-CD oder die Installation des Programms auf einem Computer akzeptieren Sie alle Bedingungen der Lizenzvereinbarung.

1.4.2. Registrationskarte

Bitte fñhlen Sie die Abreisskarte vollständig aus: Ihren Namen, E-Mail-Adresse, Telefonnummer, und senden Sie an den Händler, bei dem Sie das Produkt gekauft haben.

Wenn Ihre Postalische- / E-Mail-Adresse oder Telefonnummer sich ändern, bitte teilen Sie die neuen Angaben dem Händler mit, an den Sie die Abreisskarte der Registrationskarte gesendet haben.

Registrationskarte ist ein Dokument, auf Grund dessen Sie den Status des registrierten Benutzers unserer Firma erhalten. Das gibt Ihnen das Recht auf technischen Support während der Gültigkeit der Lizenz. Außerdem bekommen die registrierte Benutzer Nachrichten über das Erscheinen neuer Softwareprodukte von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab Ltd. abonniert haben).

1.5. Service für registrierte Benutzer

Kaspersky Lab Ltd. bietet seinen legalen Benutzern ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Anti-Virus ermöglichen.

Durch den Erwerb einer Lizenz werden Sie zum registrierten Programmbenutzer und können während der Gültigkeitsdauer Ihrer Lizenz folgende Leistungen in Anspruch nehmen:

- Nutzung neuer Versionen des betreffenden Softwareprodukts






- Beratung bei Fragen zu Installation, Konfiguration und Benutzung des betreffenden Softwareprodukts (per Telefon und E-Mail)
- Benachrichtigungen über das Erscheinen neuer Softwareprodukte von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab Ltd. abonniert haben).



Bitte lesen Sie vor dem Öffnen des Umschlags mit der CD sorgfältig den Lizenzvereinbarung.

1.6. Textgestaltung

Bestimmte Textteile dieser Dokumentation sind in Abhängigkeit von ihrer Bedeutung durch unterschiedliche Formatierungselemente hervorgehoben. Die Textgestaltung wird in folgender Tabelle erläutert.

Formatierung	Bedeutung
Fette Schrift	Namen von Menüs, Menüelementen, Dialogfenstern, Elementen von Dialogfenstern, usw.
 Hinweis.	Zusatzinformationen, Hinweise.
 Achtung!	Sehr wichtige Informationen.
 <i>Um diese Aktion durchzuführen,</i> <ol style="list-style-type: none"> 1. Schritt 1. 2. ... 	Beschreibung einer Folge von Schritten und möglichen Aktionen, die vom Benutzer durchgeführt werden.
 Aufgabe, Beispiel	Aufgabenstellung, Beispiel für die Realisierung der Optionen des Softwareprodukts.
 Lösung	Lösung der vorhergehenden Aufgabe.

Formatierung	Bedeutung
[Parameter] – Funktion des Parameters.	Befehlszeilenparameter.
Text von Meldungen Befehlszeilen	Text von Konfigurationsdateien, informativen Meldungen des Programms und Befehlszeilen.

KAPITEL 2. ARCHITEKTUR VON KASPERSKY ANTI-SPAM UND SPAM-FILTERUNGSGRUNDSÄTZE

Dieser Kapitel enthält Beschreibungen der Produktkomponenten und Spam-Filterungsgrundsätze, wie auch Beschreibung des Hauptwerkzeuges für Verwaltung und Einstellung von Kaspersky Anti-Spam – Verwaltungszentrale.

2.1. Produktbestand

Kaspersky Anti-Spam 3.0 ist ein System der Spamerkennung und Spamfilterung die mit dem Mailserver integriert wird. Kaspersky Anti-Spam 3.0 ist kein funktionstüchtiger Mailserver, der E-Mails empfangen, weiterleiten oder den Endbenutzern zustellen kann. Innere Aufbau von Kaspersky Anti-Spam ist auf der Abbildung 1 zu sehen.

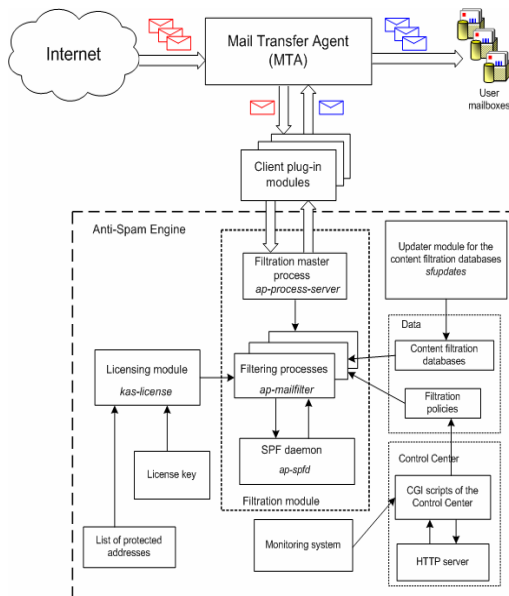


Abbildung 1. Architektur von Kaspersky Anti-Spam

Kaspersky Anti-Spam enthält folgende Bestandteile:

- **Clientmodule** – sind zum Integrieren des Produktes in den Mailserver bestimmt.
- **Filterungsserver** – eine Komponente, die Analyse der Nachrichten durchführt, diese klassifiziert und bearbeitet. Filterungsserver beinhaltet auch eine Reihe der Hilfsmodule, die seine Arbeit und Integration mit Mailserver gewährleisten:
 - Filterungsmodul – ein Modul, der Spamfilterung durchführt.
 - Lizenzverwaltungsmodul – Modul, welcher für Lizenzen- und Domänenlisten-Verwaltung bestimmt ist.
 - Inhaltsfilterung-Datenbanken – Datensatz, der vom Filterungsserver zur Klassifikation der E-Mails benutzt wird; Updates der Inhaltsfilterung-Datenbanken werden alle zwanzig Minuten zum Download bereitgestellt.
 - Update-Modul der Inhaltsfilterung-Datenbanken – ein System, das automatisches Herunterladen der Inhaltsfilterung-Datenbanken von dem Update-Server und deren Installation für weitere Verwendung vom Spamfilterung-Server gewährleistet.
 - Verwaltungszentrale – mit Hilfe dieses Web-Interface kann Systemadministrator die Einstellungen des Produkts ändern, wie auch Zustand und Arbeitsfähigkeit analysieren.
 - Monitoring-System – ein System, das erlaubt Zustand von Kaspersky Anti-Spam und seine einzelne Komponente zu überwachen, und dem Administrator warnen, wenn Störungen bei der Arbeit des Produktes auftreten.

Clientmodule sind für die Integration von Kaspersky Anti-Spam in unterschiedliche Mailserver bestimmt. Jeder Clientmodul berücksichtigt Besonderheiten des konkreten Mailservers und ausgewählte Methode der Integration.

Zum Lieferumfang von Kaspersky Anti-Spam gehören Clientmodule für Mailserver Sendmail, Postfix, Exim, Qmail und Communicate Pro.

In der Regel, wird Clientmodul als Filter installiert und gewährleistet Empfang von dem Mailserver der Nachrichten, welche gefiltert werden sollen, wie auch darauf folgende Rückgabe der modifizierten E-Mails.

Die Module werden durch Mailserver gestartet. Ausnahme davon ist Sendmail, welcher keine Clientmodule startet. Mailserver kann mehrere Clientmodule starten, damit diese parallel die Nachrichten bearbeiten können. Details über Clientmodule und dessen Integration in den Mailserver s. Pkt. A.2 auf S. 89.

Unabhängig von Besonderheiten eines oder anderen Clientmodul wird die Zusammenarbeit mit Filterungsserver über Netzwerk- oder Lokalsocket, unter Benutzung eines internen Protokolls für Datenaustausch, ausgeführt.

Filterungsserver antwortet auf Anfragen der Clients, bekommt von Clients zum Untersuchen E-Mails und gibt die Ergebnisse zurück.

Wenn Standardverfahren für die Installation benutzt wird, werden Mailserver mit den integrierten Clientmodulen und Filterungsserver auf einem Computer installiert.

Es gibt auch Möglichkeit den Filterungsserver von Kaspersky Anti-Spam auf einem separaten Server zu installieren: in dem Fall werden die Daten zwischen Clientmodulen, die auf einem anderen Computer (Server) arbeiten, und dem Filterungsserver über TCP-Protokoll ausgetauscht.

Wenn Filterungsserver auf einem separaten Computer arbeitet, kann er gleichzeitig mehrere Mailserver bedienen, bei der Voraussetzung, dass Leistungsfähigkeit des Rechners für das Bearbeiten des gesamten E-Mail-Verkehrs ausreichend ist.

Bestandteile des Filterungsservers:

- Filterungsmodul, welcher das Untersuchen der E-Mails durchführt.
- Lizenzierungsmodul, welcher das Vorhandensein der gültigen Lizenzschlüssel-Datei, wie auch das Einhalten der in der Lizenz enthaltenen Begrenzungen überprüft.
- Hilfsprogramm für SPF-Anfragen.
- Ein Skript zum automatischen Downloaden und Kompilieren von Updates der Inhaltsfilterung-Datenbanken.
- Verwaltungszentrale.
- Hilfsprogramme und Skripte.

Hauptkomponente des Moduls ist Masterprozess der Filterung (*ap-process-server*), welche folgenden Aufgaben ausführt:

- Überwachung der Verbindungsanfragen des Clientmoduls an den Filterungsprozess;
- Das Starten der Filterungsprozesse, wenn keine freie Prozesse mehr gibt;
- Statusüberwachung der Prozesse;
- Beenden der Prozesse, wenn eine entsprechende Signale kommt (z. B., SIGHUP).

Beim beachtlichen E-Mailverkehr kann die Anzahl der Filterungsprozesse bis zu mehrere Dutzende steigen. Beim verringern der Last auf den Mailserver werden freie Filterungsprozesse beendet. Maximale und minimale Anzahl der gestarteten Filterungsprozesse wird in den Einstellungen des Filterungsservers definiert (s. Pkt. A.3.1 auf S. 107).

Filterungsprozess (ap-mailfilter) lädt beim Starten die Filterungsrichtlinien, wie auch die Inhaltsfilterung-Datenbanken. Nach dem die Verbindung mit dem Clientmodul, bekommt der Filterungsprozess die E-Mail-Header und den E-Mail-Körper; analysiert sie und gibt an den Clientmodul die Ergebnisse zurück.

Wenn es notwendig ist, dass der E-Mail-Absender der SPF-Richtlinie entspricht, übergibt Filterungsprozess eine Anfrage an den SPF-Hilfsprogramm (ap-spf), welches alle nötigen Anfragen an den DNS-Server erledigt und denn die Ergebnisse an den Filterungsprozess übergibt.

Die E-Mail-Analyse und Anwenden der Richtlinien, die in den Filterungsrichtlinien definiert sind, wird nur beim Vorhandensein des gültigen Lizenzschlüssels durchgeführt.

Alle Überprüfungen, die Lizenzierung betreffen, werden von dem Lizenz-Modul (*kas-license*) auf Anfrage von dem Filterungsprozess durchgeführt.

Nach dem die E-Mail-Bearbeitung beendet ist, wartet Filterungsprozess auf neue Anfrage. Filterungsprozess wird beendet nach dem maximale Anzahl der E-Mails bearbeitet wurde (gewöhnlich sind es 300) oder sich über eine lange Zeit in Wartezustand befindet.

Skript für automatische Updates (*sfupdates*) wird nach Zeitplan gestartet (mit Hilfe des Dienstes **cron**), gewährleistet das Downloaden der letzten Version der Inhaltsfilterung-Datenbanken von den Update-Server und Installation der Datenbanken zur Weiterverwendung von dem Filterungsserver.

Verwaltungszentrale bietet ein Webinterface, mit Hilfe dessen stellt der Systemadministrator das Produkt und Spam-Filterungsrichtlinien ein.

Überwachungssystem führt die Kontrolle über Zustand der Komponente des Kaspersky Anti-Spam aus und warnt den Administrator, wenn Störungen bei der Arbeit des Filterungsservers oder andere Komponente des Produktes auftreten.

Das Bearbeiten des E-Mailverkehrs wird vom Kaspersky Anti-Spam 3.0 nach folgendem Algorithmus durchgeführt:

1. Clientmodul des Produktes wird in den Mailserver integriert.
2. Mailserver übergibt die Nachrichten an den Clientmodul zur anschließenden Überprüfung durch den Filterungsserver.
3. Filterungsserver überprüft E-Mails nach Spamanzeichen und, abhängig von dem Ergebnis, modifiziert die Nachrichten entsprechend den vordefinierten Richtlinien.

4. Bearbeitete E-Mails werden von dem Clientmodul an den Mailserver zurückgegeben, damit die E-Mails an den Empfänger zugestellt werden.

2.2. Erkennungstechnologie

Kaspersky Anti-Spam bietet ein mächtiges Werkzeug für Spamerkennung in der E-Mailflut. In diesem Abschnitt wird kurz über Spamerkennung-Technologien erzählt, die im Produkt benutzt wurden.

2.2.1. Analyse der formellen Anzeichen

Diese Methode benutzt einen Regelsatz, welcher auf der Untersuchung von bestimmten Kopfzeilen (Header) der E-Mail und dem Vergleich dieser Zeilen mit den Header, welche für Spam typisch sind, basiert. Außer Analyse der Kopfzeilen, wird beim Untersuchen auch E-Mail-Struktur, E-Mail-Größe, angehängte Dateien und andere Ähnlichkeiten berücksichtigt.

Die Methode gewährleistet auch die Analyse der Daten, die der Absender während der SMTP-Sitzung übermittelt. Insbesondere werden folgende Informationen analysiert:

- IP-Adresse des Servers, von dem E-Mail empfangen wurde und seine Zugehörigkeit zu der "weiße" oder "schwarze" Listen der Absender;
- IP-Adressen der Zwischenserver, die zum Weiterleiten der Nachrichten benutzt werden. Die Adressen werden dem Header Received *entnommen*;
- E-Mail-Adressen des Absenders und Empfängers, die in den Befehlen der SMTP-Sitzung übergeben werden;
- Dazugehören der E-Mail-Adressen des Absenders und Empfängers zu der "weißen" oder "schwarzen" Listen der E-Mail-Adressen;
- Übereinstimmung der bei SMTP-Sitzung übermittelten Adressen und E-Mail-Adressen, welche im Header angegeben sind, wie auch eine Reihe anderen Prüfungen.

2.2.2. Inhaltsfilterung

Inhaltsfilterung wird von Kaspersky Anti-Spam zur Analyse der Inhalte von Nachrichten benutzt. Dabei, unter Benutzung der Technologie des künstlichen Intellektes, wird E-Mail-Inhalt (Header *Subject* eingeschlossen) analysiert wie auch die Einlagdateien der folgenden Typen:

- Text: plain text (ASCII, nicht multibyte);
- HTML (2.0, 3.0, 3.2, 4.0, XHTML 1.0);

- Microsoft Word (Version 6.0, 95/97/2000/XP);
- RTF.



Aufgabe der Spamfilterung besteht darin, die Anzahl der unerwünschten Korrespondenz in den Postfächern der Benutzer zu verringern. Hundertprozentiges Auffinden des Spams kann nicht garantiert werden, denn zu strenge Kriterien unvermeidlich zum Ausfiltern der nützlichen Korrespondenz führen wird.

Zum Auffinden der Spam-Nachrichten werden drei Methodengruppen benutzt:

- **Vergleichen des Textes mit den Symantischen Muster** unterschiedlicher Kategorien (auf Basis der Suche in dem E-mail-Körper der Schlüsselbegriffe (Wörter und Wortgruppen) und darauf folgenden stochastischen Analyse). Diese Methode gewährleistet heuristische Suche der spezifischen Sätze und Redewendungen in dem Text.
- **Ungenaues Vergleichen der analysierten E-Mail mit einem Satz der Muster-E-Mail** durch Vergleichen der Signaturen. Diese Methode erlaubt modifizierte Spam-Nachrichten zu identifizieren.
- Analyse der grafischen Einlagen.

Alle Daten, die Kaspersky Anti-Spam für Inhaltsfilterung benutzt, – *Rubrikator* (Hierarchische Liste der Kategorien), Muster-E-Mail, charakteristische Begriffe u.s.w. – sind in den Inhaltsfilterung-Datenbanken gespeichert.



Analisten-Gruppe von Kaspersky Lab führt ständige Untersuchungen durch, um die Inhaltsfilterung-Datenbanken zu erweitern und zu verbessern, deswegen wird es empfohlen die Datenbanken ständig zu erneuern (s. Pkt. 4.4 auf S. 56).

Sie können die Muster der Spam-E-Mail an Kaspersky Lab senden, die von Kaspersky Anti-Spam nicht erkannt wurden, wie auch Muster der E-Mail, die Fälschlicherweise als Spam identifiziert wurden. Ihre Daten werden uns dabei helfen, die Inhaltsfilterung-Datenbanken zu verbessern und schnell auf neue Arten des Spams zu reagieren. Details dazu sehe Anhang B auf S. 126.

2.2.3. Überprüfen mit Hilfe der externe Dienste

Außer Text- und Headeranalyse erlaubt Kaspersky Anti-Spam folgende Untersuchungen mit Hilfe der externe Netzwerkservices durchzuführen:

- Überprüfung des Vorhandenseins von IP-Adresse des E-Mail-Absenders in dem DNS (reverse DNS lookup);

- Überprüfung des Vorhandenseins der IP-Adresse des E-Mail-Absenders in einem oder mehreren DNSBL (DNS-based black hole list);
- Überprüfung des E-Mail-Absenders nach Übereinstimmung dessen Adressese mit der SPF-Richtlinie (Sender Police Framework) für die Domäne, aus der die E-Mail stammt;
- Überprüfung der Links, die in der E-Mail enthalten sind, auf Vorhandensein in der Spam-Datenbank mit Hilfe des Dienstes SURBL (Spam URL Realtime Blocklists – www.surbl.org).
- Erkennung der E-Mails mit der UDS-Technologie (Urgent Detection System).

Alle der oben genannten Überprüfungen, außer UDS-Überprüfungen, basieren auf Benutzung des DNS-Protokolls, und, im Regelfall, brauchen keine Extra-Einstellungen des Netzwerks.

2.2.4. Urgent Detection System Technologie

Technologie **Urgent Detection System** ist eine originelle Technologie für Auffinden des Spams, die von Kaspersky Lab erarbeitet und unterstützt wird. Funktionsweise der Technologie ist folgende:

1. Aus der analysierten E-Mail wird ein Satz der Eigenschaften ausgesondert, mit Hilfe deren die Identifikation der Nachricht ausgeführt wird. In dem Satz kann die Information aus dem Header, Textfragmente und andere Informationen über die zu bearbeitende E-Mail eingeschlossen sein.
2. Unter Benutzung der Eigenschaften erstellt der Fiterungsserver eine kompakte UDS-Anfrage und verschickt diese an einen der UDS-Server des Kaspersky Lab.



Da an externe Server keine Daten verschickt werden, die den Empfänger erkennen oder den Nachrichten-Text wiederherstellen lassen, ist das Benutzen der Methode in keiner Weise für die Sicherheit oder Vertraulichkeit Ihre Daten gefährlich.

3. Auf dem UDS-Server wird eine Überprüfung der Anfrage in der Datenbank der bekannten Spam-Versandlisten durchgeführt. In dem Fall, wenn die Anfrage einer der bekannten Versandlisten entspricht, wird an den Filterungsserver eine Nachricht darüber verschickt, dass die Nachricht höchstwahrscheinlich zum Spam gehört. Diese Information wird beim Vergeben des E-Mail-Status berücksichtigt.



Die UDS-Technologie erlaubt die bekannten Spam-Versandlisten auszufiltern, ohne dass die Inhaltsfilterung-Datenbanken erneuert sind.

Die Zusammenarbeit des Filterungsserver mit den UDS-Servern des Kaspersky Lab wird über UDP-Protokoll organisiert, für die Verbindung wird Port 7060 benutzt. Damit UDS-Server angesprochen werden kann, muss Filterungsserver ausgehende Verbindungen über den Port aufbauen können.

Information über zugängliche UDS-Server ist in den Inhaltsfilterung-Datenbanken enthalten. Auswahl des konkreten UDS-Server, mit Hilfe dessen die Analyse der E-Mails durchgeführt wird, erfolgt automatisch auf Basis der Analyse der Antwortzeit der zugänglichen UDS-Server.

2.3. Erkennungsergebnisse und E-Mail-Handhabung

Als Analyseergebnis wird an E-Mail ein Status vergeben:

- **Spam** – E-Mail wurde mit einer hohen Wahrscheinlichkeit als Spam erkannt.
- **Probable Spam** – E-Mail enthält einige Anzeichen vom Spam, kann aber nicht eindeutig als Spam identifiziert werden.
- **Formal** – E-Mail ist eine formale Nachricht, z. B., eine Benachrichtigung des E-Mail-Servers über das Zustellen der E-Mail, über die Unmöglichkeit der Zustellung oder darüber, dass die E-Mail mit einem Virus infiziert ist. Zur Kategorie zählen auch die Nachrichten, die automatisch durch die Client-Programme erstellt werden. Diese E-Mails werden nicht zur Spam-E-Mails gezählt.
- **Trusted** – E-Mail wurde von einer vertrauten Quelle bekommen, z.B. von den internen Servern. Eine Liste der vertrauten Quellen („weiße“ Liste der Absender) wird von dem Administrator erstellt. Status **Trusted** wird auch an E-Mails vergeben, für diese in der Gruppenrichtlinie das Überprüfen der E-Mails auf Spam-Vorhandensein ausgeschaltet ist.
- **Blacklisted** – E-Mail kommt von der E-Mail-Adresse, welche in die „schwarze“ Liste eingetragen ist. „Schwarze“ Liste wird von dem Administrator erstellt.
- **Not detected** – E-Mail wurde nicht als Spam erkannt.

Jeder E-Mail kann nur ein Status von den aufgezählten vergeben werden. Status, der einer E-Mail nach dem Überprüfen vergeben wurde, wird in den Extra-

Header **X-Spamtest-Status-Extended** eingetragen. Details zu den Kopfzeilen, die als Ergebnis der Filterung zur E-Mail hinzugefügt werden, s. Pkt. A.5 auf S. 120.

Nach der Erkennung kann an E-Mail eine der folgenden Aktionen vorgenommen werden:

- E-Mail annehmen;
- E-Mail oder eine Kopie davon an eine andere Adresse weiterleiten;
- Eine Markierung in das Betreff-Feld einfügen;
- Ein Extra-Header zur E-Mail hinzufügen;
- E-Mail löschen;
- Annahme der E-Mail verweigern.

Der Systemadministrator kann bestimmen, welche von den aufgezählten Aktionen auf die E-Mail mit dem bestimmten Status angewendet werden.



Hauptpriorität für Systemadministrator beim Einstellen des Produktes soll das Erhalten von nützlichen Korrespondenz sein, denn das Verlorengang einer E-Mail kann dem Endbenutzer mehr Schaden hinzufügen, als mehrere Dutzende nicht Spam-Nachrichten. Damit nützliche Korrespondenz nicht verloren geht, empfehlen wir die E-Mails, welche nach der Inhaltsanalyse als Spam oder Spamverdacht gekennzeichnet wurden, nur sanft zu behandeln, z. B., in dem Feld Betreff eine Markierung **[!! SPAM]** eintragen.

2.4. Inhaltfilterung-Datenbanken

Das Erkennen der E-Mails, welche Spam enthalten, wird auf Grund der Daten durchgeführt, die aus den ständig updatenden Datenbanken der Inhaltfilterung entnommen werden. Inhaltfilterung-Datenbanken enthalten Regelsätze, Begriffe und Signaturen der E-Mails, diese werden während der Filterung benutzt.

Inhaltfilterung-Datenbanken werden von den Updateservern des Kaspersky Lab mit Hilfe des Update-Moduls herunter geladen. Dabei werden, zum verringern des Umfangs zu ladenden Dateien, von dem Update-Server nur neue Daten herunter geladen.

Da neu Spam-Muster jeden Tag erscheinen, ist es notwendig, dass die Inhaltfilterung-Datenbanken ständig aktuell sind. Es wird empfohlen die Datenbanken alle zwanzig Minuten upzudaten.



Vergessen Sie nicht die Inhaltsfilterung-Datenbanken gleich nach dem Installieren des Produktes zu erneuern!

2.5. Filterungsrichtlinien

Filterungsrichtlinien werden von Kaspersky Anti-Spam zur Festlegung der Methoden der Spamerkennung, an den E-Mails ausführende Aktionen, wie auch zum bestimmen der „weißen“ und „schwarzen“ Listen benutzt.

Das Produkt benutzt ein zweistufiges System der Filterungsrichtlinien, welches aus allgemeinen Filterungsrichtlinie und Gruppen-Filterungsrichtlinie besteht. Allgemeine Filterungsrichtlinie enthält gemeinsame Einstellungen für alle Gruppen: Erkennungsmethoden für E-Mails, „weiße“ und „schwarze“ Listen der Absender. Gruppenrichtlinien, Außer oben genannten Einstellungen, bestimmen Aktionen, die an E-Mails vorgenommen werden.

Bevor der Administrator zum Einstellen der Gruppenrichtlinien übergeht, müssen Gruppen erstellt werden, welche aus eine Liste der Empfängeradressen bestehen.

Das Anwenden der Richtlinien wird nach folgenden Regeln durchgeführt: allgemeine Filterungsrichtlinie bestimmt standardmäßige Einstellungen für alle Gruppen, während die Gruppenrichtlinien diese Einstellungen entweder erben, oder auf neue bestimmen. So, z. B., kann für eine Benutzergruppe, die eine stärkere Filterung der E-Mails verlangt, die Methoden der Spamerkennung und die Aktionen verschärft werden.

Einstellungen der Erkennungsparameter sind sehr eng mit den Eigenschaften der Inhaltsfilterung-Datenbanken verbunden, und können erweitert und verändert werden den neuen Arten des Spams und Richtlinien der Spamerkennung entsprechend. Entsprechend neuen Inhaltsfilterung-Datenbanken werden dem Interface der Verwaltungszentrale neue Einstellungen zum steuern von Kaspersky Anti-Spam hinzugefügt.

2.6. Verwaltungszentrale

Verwaltungszentrale (*Control center*) ist ein Web-Interface, welches dem Administrator erlaubt die Arbeit von Kaspersky Anti-Spam zu kontrollieren und Einstellungen vorzunehmen.

Verwaltungszentrale gewährleistet das Ausführen folgenden Aufgaben:

- Überprüfen des jetzigen Zustand des Produktes und seine Komponente;
- Installieren von Lizenzschlüssel und Verwalten der Liste der geschützten Domänen;

- Statistik der bearbeiteten E-Mails ansehen und exportieren;
- Verwalten von Gruppenrichtlinien und allgemeinen Richtlinien der Spamfilterung;
- Filterungsserver und Produktkomponente verwalten.

2.7. Monitoring

Um den Zustand des Filterungsservers zu überwachen, ist in den Kaspersky Anti-Spam ein Überwachung-Modul eingebaut.

Die Information über Systemzustand ist in dem Abschnitt **Monitoring** der Verwaltungszentrale enthalten.

The screenshot displays the 'Monitoring - General Status' window. On the left, a sidebar menu includes 'Monitoring', 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main area is titled 'Monitoring' and contains two data sections. The first section, 'System Information', lists: Host Name: mail.test.local, System: FreeBSD 5.4-RELEASE-p7 i386, and Load Average: 0.13. The second section, 'Kaspersky Anti-Spam', lists: Product: Kaspersky Anti-Spam Enterprise Edition, Version: 3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45, Anti-Spam Engine: Errors..., Updates: OK, and License: Errors... The bottom of the window shows the copyright notice: Copyright © 2002-2006 Kaspersky Lab. All rights reserved.

Abbildung 2. Abschnitt **Monitoring** der Verwaltungszentrale

Dieser Abschnitt enthält Parameter, die von dem Überwachungssystem kontrolliert werden, wie auch Meldungen der Module, die zur Analyse des jetzigen Zustandes der Komponente von Kaspersky Anti-Spam benutzt werden können.

Während der Arbeit erstellt das Überwachungssystem Meldungen und Berichte. Monitoringskript wird periodisch gestartet und, wenn Fehler in Arbeit des Systems auftreten, versendet eine Nachricht mit den Fehlerdaten an den Systemadministrator. Nachricht wird einmalig in Moment der Problemmerkung verschickt, das garantiert schnelle Benachrichtigung über die Situation, welche das Eingreifen des Administrators verlangt.

Später, wenn der Fehler nicht behoben wurde, wird das Monitoring-System täglich einen Bericht über alle gefundene und nicht behobene Fehler versenden.

Die E-Mail-Adresse, an welche das System die Nachricht versenden wird, wird mit Hilfe der Verwaltungszentrale definiert.

KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-SPAM

Dieser Abschnitt enthält Informationen über das Installieren des Produktes, Integration der Clientmodule in den Mailserver, wie auch über das Einstellen des Zuganges zu dem Hauptwerkzeug der Systemverwaltung - Verwaltungszentrale.

3.1. Vorbereitung der Installation

Bevor Sie mit der Installation von Kaspersky Anti-Spam anfangen:

- Vergewissern Sie sich, dass das System den Systemanforderungen von Kaspersky Anti-Spam (s. Pkt. 1.3 auf S. 9) entspricht;
- Vergewissern Sie sich, dass Sie im Besitz eines Lizenzschüssels für Kaspersky Anti-Spam 3.0 sind;
- Vergewissern Sie sich, dass die Programme *bzip2*, *perl*, *which* installiert sind;
- Vergewissern Sie sich, dass Ihr Mailserver korrekt funktioniert;
- Machen Sie eine Sicherheitskopie der Konfigurationsdateien des Mailservers;
- Logen Sie sich als Benutzer **root** ein.



Es wird empfohlen die Installation zur Zeit der niedrigsten Auslastung des Mailservers durchzuführen.

Die Installation von Kaspersky Anti-Spam wird in fünf Etappen durchgeführt:

1. Installation des Kaspersky Anti-Spam Distributives.
2. Lizenzschlüssel-Installation.
3. Integration der Clientmodule in den Mailserver.
4. Einstellung des HTTP-Servers um Zugang zu dem Verwaltungsserver zu gewährleisten.
5. Update-Einstellungen der Inhaltsfilterung-Datenbanken und Einstellungen von Benutzung des UDS-Dienstes.

In den folgenden Abschnitten werden alle Etappen detailliert beschrieben.

3.2. Installation von Kaspersky Anti-Spam

Distributiv von Kaspersky Anti-Spam 3.0 wird in mehreren Versionen vertrieben:

- rpm-Paket für die meisten Versionen des Betriebssystems Linux (RedHat, SuSe, Mandrake, Fedora u.s.w.);
- deb- Paket für Debian-Distributiv;
- tgz- Paket für Betriebssystem FreeBSD 4.10;
- tbz-Paket für Betriebssystem FreeBSD 5.4;

Benutzung eines oder anderen Pakets ist von dem installierten Betriebssystem abhängig.

Um die Installation von Kaspersky Anti-Spam aus einem rpm-Paket zu starten, geben Sie in der Befehlszeile ein:

```
# rpm -i kas-3-<Distributiv-Version>.i386.rpm
```

Um die Installation von Kaspersky Anti-Spam aus einem deb-Paket zu starten, geben Sie in der Befehlszeile ein:

```
# dpkg -i kas-3-<Distributiv-Version>.i386.deb
```

Um die Installation von Kaspersky Anti-Spam aus einem tgz-Paket zu starten, geben Sie in der Befehlszeile ein:

```
# pkg_add kas-3-<Distributiv-Version>.tgz
```

Um die Installation von Kaspersky Anti-Spam aus einem tbz-Paket zu starten, geben Sie in der Befehlszeile ein:

```
# pkg_add kas-3-<Distributiv-Version>.tbz
```

Während der Installation werden folgende Aktionen unternommen:

- Benutzer und Gruppe **mailfit3** anlegen, mit dessen Rechte Kaspersky Anti-Spam gestartet wird;
- Installation alle Programme in den Ordner */usr/local/ap-mailfilter3*;
- Erstellung und Installation des Skriptes, welches das automatische Starten des Master-Prozesses der Filterung (*ap-process-server*), SPF-Hifsprogramms (*ap-spf*), Lizenzmoduls (*kas-license*) und HTTP-Servers (*kas-thttpd*) beim Starten des Betriebssystems gewährleistet;
- Das Starten von allen nötigen Dienste;

- Erstellen des cron-Tasks für Benutzer **mailft3**, um automatisches Starten der Updates der Inhaltsfilterung-Datenbanken zu gewährleisten, wie auch Skripte für Überwachung der Arbeit des Filterungs-Dienstes.

Nach der Installation des Filterungsservers, installieren Sie den Lizenzschlüssel und führen Sie die Integration von Kaspersky Anti-Spam in den Mailserver durch.

3.3. Zugangseinstellungen für die Verwaltungszentrale.

Nach der Installation wird der Dienst *kas-thttpd* gestartet, welcher den lokalen Zugang zu der Verwaltungszentrale gewährleistet. Standardmäßig werden folgende Einstellungen der Verwaltungszentrale benutzt:

- Adresse **http://127.0.0.1:3080/**.
- Benutzername: **admin**
- Passwort: **admin**



Sie sollen unbedingt nach der Installation von Kaspersky Anti-Spam den Benutzernamen und Passwort für den Zugang zur Verwaltungszentrale ändern. Das Benutzen der Standardwerte bedroht die Sicherheit Ihres Systems.

Es wird auch empfohlen den Port für die Verbindung mit der Verwaltungszentrale zu ändern.

Benutzername und Passwort werden in dem Ordner der cgi-Skripte der Verwaltungszentrale gespeichert */usr/local/ap-mailfilter3/control/www/*, in der Datei *.htpasswd*.

Das Erstellen eines neuen Benutzer oder das Ändern eines bestehenden Passworts wird mit dem Werkzeug *kas-htpasswd* durchgeführt, das zum Lieferumfang von Kaspersky Anti-Spam gehört. Beim Starten des Werkzeugs müssen Sie den Pfad zu der Datei angeben, die Passwörter enthält, wie auch den Namen des zu erstellenden Benutzers, oder des Benutzers, dessen Passwort geändert werden soll:

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd  
/usr/local/ap-mailfilter3/control/www/.htpasswd  
<Benutzername>
```

Nach der Eingabe des Befehls wird Ihnen angeboten das Passwort für den ausgewählten Benutzer einzugeben.

Um eine neu Passwortdatei für den ausgewählten Benutzer zu erstellen benutzen Sie die Befehlszeilenoption `-c`:

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd -c
/usr/local/ap-mailfilter3/control/www/.htpasswd
<Benutzername>
```

Passwortänderung tritt in Kraft sofort nach Modifikation der Datei `.htpasswd`.



Zugangsdaten für die Verwaltungszentrale werden in der Datei `.htpasswd` verschlüsselt gespeichert.

Interface und Portnummer für die Verbindung mit der Verwaltungszentrale werden in der `/usr/local/ap-mailfilter3/etc/kas-thttpd.conf` vorgegeben, mit Hilfe der Parameter **host** und **port** entsprechend. Z. B., Werte:

```
host=0.0.0.0
port=3080
```

bestimmen, dass die Verwaltungszentrale Verbindung über den Port 3080 an allen Netzwerkkarten des Servers erwartet. Standardmäßig ist Zugang zu der Verwaltungszentrale nur von dem Server möglich, auf dem Kaspersky Anti-Spam installiert ist (dem Parameter **host** ist Wert **127.0.0.1** vergeben).

Nach Änderung des Ports starten Sie die Verwaltungszentrale-Konfiguration neu. Unter Linux-Distributiv führen Sie den Befehl aus:

```
# /etc/init.d/kas3-control-center restart
```

- Für FreeBSD-Distributiv führen Sie den Befehl aus:

```
/usr/local/etc/rc.d/kas3-control-center.sh
restart
```

3.4. Lizenzschlüssel installieren

Ein Lizenzschlüssel wird entsprechend der erworbenen Lizenz mit dem Distributiv des Kaspersky Anti-Spam geliefert.



Wenn Sie aus irgendeinem Grund keinen Schlüssel haben, wenden Sie sich an den Support von Kaspersky Lab (Abschnitt **Dienste/Technischer Support** auf unser Internet-Seite).



Um neuen Lizenzschlüssel mit Hilfe des Verwaltungszentrales zu installieren:

1. Mit Hilfe von Web-Browsers verbinden Sie sich mit dem Verwaltungszentrale, in dem Sie in der Adressenzeile

- http://localhost:3080/** eingeben. Als Benutzername geben Sie **admin** ein, als Passwort – **admin**.
2. Gehen Sie auf die Seite der Lizenzschlüssel-Verwaltung License → License Keys.
 3. In dem Feld **Install a New License Key** dieses Abschnitts, geben Sie den Pfad zu der Lizenzschlüssel-Datei ein, oder benutzen Sie die Schaltfläsche **Choose** zum Auswählen der Datei.
 4. Klicken Sie auf die Schaltfläsche **Apply**.



Um einen neuen Lizenzschlüssel lokal mit Hilfe der Befehlszeile zu installieren, führen Sie folgenden Befehl aus:

```
# /usr/local/ap-mailfilter3/bin/install-key <key>
```

wobei <key> - Pfad zu der Datei ist, welche den Schlüssel enthält.

Wenn ein Lizenzschlüssel nicht installiert oder nicht gültig ist, wird Kaspersky Anti-Spam die Filterung der E-Mails nicht ausführen. Arbeitsfähigkeit des Servers wird dabei nicht beeinträchtigt, E-Mail-Verkehr wird ohne Filterung durchgelassen.

Es muß berücksichtigt werden, dass E-Mail-Filterung nur für die Benutzer der geschützten Domänen durchgeführt wird.



Vergessen Sie nicht vor Benutzung von Kaspersky Anti-Spam die Liste der geschützten Domänen auszuführen. Details s. Pkt. 4.3.4 auf S. 48

3.5. Kaspersky Anti-Spam in den Mailserver integrieren

Integration des Kaspersky Anti-Spam in den Mailserver besteht aus der Installation des Clientmoduls und dem Eintragen der Änderungen in die Konfigurationsdateien.

Diese Aktionen werden automatisch, mit Hilfe des Universal-Skriptes durchgeführt, oder, wenn die Skript-Integration nicht möglich ist (z.B. wenn keine standard Mailserverkonfiguration benutzt wird), mit Hilfe der Einstellungs-Skripte desjenigen Mailservers.

Eine ausführliche Information über Integrationsmöglichkeiten der Clientmodule für jeden der unterstützten Mailserver, und über die Änderungen in den Konfigurationsdateien, finden Sie im Anhang A.2 auf S. 89.



Um Kaspersky Anti-Spam in den Mailserver zu integrieren, der bei Ihnen installiert ist, starten Sie den Universalskript:

```
# /usr/local/ap-mailfilter3/bin/MTA-config.pl
```

Vorgegebener Skript erkennt den Typ des Mailservers und trägt die Änderungen in die Konfigurationsdateien ein.

Wenn aber Ihrer Mailserver nicht standardmäßig installiert oder konfiguriert ist, wird Skript *MTA-config.pl* die Konfigurationsdateien nicht finden können. In dem Fall benutzen Sie ein Skript zur Einstellung des konkreten Mailservers:

- Für die Integration von Kaspersky Anti-Spam in den Mailserver Sendmail führen Sie unter Benutzer **root** folgendes Befehl aus:

```
# /usr/local/ap-mailfilter3/bin/config-sendmail.pl <path>
```

wo **path** – Pfad zu der Sendmail-Konfigurationsdatei ist.

- Für die Integration von Kaspersky Anti-Spam in den Mailserver Postfix führen Sie unter Benutzer **root** folgendes Befehl aus:

```
# /usr/local/ap-mailfilter3/bin/config-postfix.pl <path>
```

wo **path** – Pfad zu der Konfigurationsdatei Postfix *master.cf* ist.

- Für die Integration von Kaspersky Anti-Spam in den Mailserver Exim führen Sie unter Benutzer **root** folgendes Befehl aus:

```
# /usr/local/ap-mailfilter3/bin/config-exim.pl <path>
```

wo **path** – Pfad zu der Konfigurationsdatei Exim ist.



Für Debian-Distributiv gibt es eine Reihe der Besonderheiten bei der Integration Kaspersky Anti-Spam in den Mailserver Exim. Für eine korrekte Integration benutzen Sie den Skript */usr/local/ap-mailfilter3/bin/config-exim-debian.pl*. Details s. Pkt. A.2.4.2 auf S. 98.

- Für die Integration von Kaspersky Anti-Spam in den Mailserver Qmail führen Sie unter Benutzer **root** folgendes Befehl aus:

```
# /usr/local/ap-mailfilter3/bin/config-qmail.pl <path>
```

wo **path** – Pfad zu dem Ordner Qmail ist.



Eine korrekte Integration in den Qmail Mailserver mit Hilfe des Skriptes *config-qmail.pl* ist nur dann möglich, wenn Qmail das Benutzerkonto **qmail** und die Gruppe **qmail** benutzt (beide werden standardmäßig benutzt).

Integration von Kaspersky Anti-Spam in den Mailserver Exim mit Hilfe des Clientmoduls *kas-exim*, wie auch mit dem Mailserver *CommuniGate Pro* wird von dem Administrator per Hand gemacht.

Information über Besonderheiten jedes von den Clientmoduls und Integrationsmöglichkeiten sind näher in dem Punkt A.2 auf S. 89 beschreiben.

Mehr über Aufhebung der Integration und Wiederherstellung der ursprünglichen Einstellungen des Mailservers s. Kappitel 5 auf S. 82.

3.6. Einstellungen von Updates der Inhalt-Datenbanken und Benutzung des UDS-Dienstes

Standardmäßig sind nach der Installation von Kaspersky Anti-Spam die Updates der Inhalt-Datenbanken und die Benutzung des UDS-Dienstes abgeschaltet. Um die Updates und Benutzung UDS-Dienstes zu erlauben, starten Sie den Skript *enable-updates.sh*:

```
# /usr/local/ap-mailfilter3/bin/enable-updates.sh
Restarting as mailflt3
Enabling UDS...
uds-rtts finished successfully
Enabling automatic updates...
Install crontab for user mailflt3 - ok
=====
=====
You can adjust automatic updates settings via
control center.
=====
=====
Automatic updates and UDS are now enabled.
```

Sie können auch das Interface der Verwaltungszentrale benutzen, um die Updates der Inhaltsfilterung-Datenbanken einzuschalten (s. Pkt. 4.4 auf S. 56) und das Benutzen des UDS-Dienstes zu (s. Pkt. 4.44.5.4 auf S. 64).

KAPITEL 4. VERWALTUNG VON SPAMFILTERUNGSSERVER

Mittels Kaspersky Anti-Spam können Sie den E-Mailverkehr-Schutz gegen Spam organisieren. Schutzsystem wird auf dem Ausführen der Aufgaben aufgebaut, in welchen die Hauptfunktionen des Programms enthalten sind. Aufgaben, die von Kaspersky Anti-Spam realisiert werden, können in drei Gruppen aufgeteilt werden:

- Schutz des E-Mail-Verkehrs gegen Spam.
- Update der Inhaltsfilterung-Datenbanken, die zur Spamerkennung benutzt werden.
- Überwachung der Arbeit des Filterungsservers.

Jede Gruppe enthält kleinere Aufgaben. In diesem Kapitel werden wir einige davon behandeln. Administrator kann die Aufgaben den Bedürfnissen der Firma entsprechend kombinieren und verkomplizieren.

In dieser Dokumentation sind Einstellungen und das Starten der Aufgaben lokal aus der Befehlszeile beschrieben, wie auch Verwaltung des Produktes mit Hilfe der Verwaltungszentrale.

4.1. Starten und Verwalten der Komponente von Kaspersky Anti-Spam

Das Starten der Komponente des Filterungs-Servers, zu den der Hauptfilterungsprozess (*ap-process-server*), Lizenzierungsmodul (*kas-license*) und SPF-Hilfsprogramm (*ap-spf*) gehören, wird beim Starten des Betriebssystems mit Hilfe des Skripts durchgeführt, dessen Name und Lage für Linux und FreeBSD unterschiedlich ist. In dem Betriebssystem Linux wird Skript *kas3* benutzt, der in dem Verzeichnis */etc/init.d* liegt, in FreeBSD – *kas3.sh*, der in dem Verzeichnis */usr/local/etc/rc.d* abgelegt ist.

Obengenannte Skripte können mit den folgenden Befehlszeilenoptionen von Administrator zum Starten, Beenden und Neustarten der Komponenten des Filterungsservers benutzt werden:

start – Hauptkomponente des Filterungsservers starten;

stop – Arbeit der Hauptkomponente des Filterungsservers beenden;

restart – Hauptkomponente des Filterungsservers neustarten; diese Aktion ist dem aufeinander folgendem Ausführen der Aktionen **stop** und **start** gleich.

Das Starten des kas-thttpd-Dienstes, welcher den Zugang zu der Verwaltungszentrale von Kaspersky Anti-Spam frei gibt, wird unter Benutzung des Skriptes kas3-control-center (unter Linux) und Skripts kas3-control-center.sh (unter FreeBSD) ausgeführt.

Um das Starten, Beenden oder Neustarten des Dienstes kas-thttpd auszuführen, benutzen Sie den Skript mit den Befehlszeilenoptionen, die oben für den Skript kas3 beschrieben sind.

4.2. Verwaltungszentrale von Kaspersky Anti-Spam

Hauptwerkzeug für die Steuerung von Kaspersky Anti-Spam ist **Verwaltungszentrale**. Die Verwaltungszentrale ist eine Web-Anwendung, die es erlaubt, Einstellungen am Filterungsserver von einem entfernten Computer aus vorzunehmen. Dieser Abschnitt enthält eine detaillierte Beschreibung aller Elemente des Anwendung-Interfaces.

In dem oberen Teil des Fensters ist eine Reihe der Registerkarten vorhanden, welche den Zugang zu folgenden Funktionalitäten der Verwaltungszentrale anbieten:

- **Monitoring** – eine Registerkarte, die Informationen über Zustand der Komponente des Filterungsservers enthält; diese Information kann zum Erkennen der Fehler benutzt werden.
- **Statistics** – eine Registerkarte, die statistische Protokolle enthält, welche eine Anzahlanalyse der bearbeiteten E-Mails erlaubt.
- **Policies** – eine Registerkarte, die zum Einstellen von Richtlinien der Spamfilterung benutzt wird.

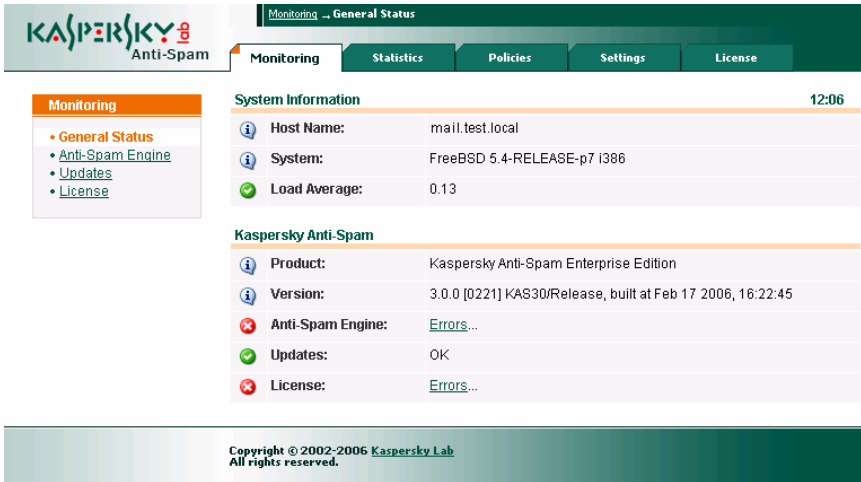


Abbildung 3. Verwaltungszentrale Kaspersky Anti-Spam

- **Settings** – eine Registerkarte, die Einstellungen des Spam-Filterungsservers, der Verwaltungszentrale und Update-Systems der Inhaltsfilterung-Datenbanken enthält.
- **License** – eine Registerkarte, die zum Verwalten der Lizenzen von Kaspersky Anti-Spam und Registrieren der Benutzer, die Produkt verwalten dürfen, benutzt wird.

In dem linken Teil des Fensters ist eine Auswahl, welche eine Liste von Seiten der ausgewählten Registerkarte enthält. Inhalt der Auswahl kann sich ändern, abhängig von der gewählten Registerkarte.

Außer aufgezählten Navigationsschaltfläschen ist in dem oberen Teil des Fensters eine Adressenzeile angebracht, die den Pfad zu der aktuellen Seite in der Hierarchie der Abschnitte der Verwaltungszentrale anzeigt.

Weiter werden die Aufgaben beschrieben, welche mit der Verwaltung des Filterungsserver und seiner Komponente zusammen hängen.

4.3. Verwaltung von Filterungsrichtlinien

Hauptfunktion von Kaspersky Anti-Spam ist das Erkennen und Filtern der unerwünschten Nachrichten. Verwaltungssystem bietet Ihnen ein mächtiges Werkzeug zum Einstellen des Spam-Erkennungsprozesses und der darauf folgenden Bearbeitung der E-Mails.

Einstellungen der Filterungsrichtlinien sind in dem Abschnitt **Policies** der Verwaltungszentrale enthalten.

Auswahl des Abschnittes Policies enthält folgende Unterabschnitte:

- **Common** – Einstellungen der allgemeinen Filterungsrichtlinie. Abschnitt enthält:
 - **Default Rules** – Verwaltung der Spamerkennung-Richtlinien.
 - **Black List** – Verwaltung einer "schwarzen" Liste der Absenderadressen, von den keine E-Mails angenommen werden.
 - **White List** – Verwaltung der "weißen" Liste der Absenderadressen, E-Mails von den in der Liste stehenden Absender werden nicht nach Spam untersucht.
 - **DNS Black Lists** – Verwaltung der Liste von benutzten DNSBL-Diensten.
- **Groups** – Benutzergruppen-Einstellungen, Erkennungsrichtlinien, welche auf bestimmten Gruppen angewendet werden, und Aktionen, welche an E-Mails vorgenommen werden:
 - **Group list** – Benutzergruppen-Verwaltung: hier können Sie Gruppen erstellen, löschen und Gruppeneigenschaften ändern.

Parametereinstellungen der Gruppenrichtlinien werden in dem Gruppenrichtlinien-Editor geändert. Gruppenrichtlinien-Editor wird in dem Fenster Group list **gestartet**.

Link Rebuild All Policies, der in der Auswahl **Build** platziert ist, wird zur erzwungenen Kompilierung der Filterungsrichtlinien benutzt (zum Einlesen und Anwenden der Konfigurationseinstellungen). Erzwungene Kompilierung kann, z.B., benutzt werden, wenn Einstellungen der Filterungsrichtlinien erneut eingelesen werden sollen, wenn sie früher falsch gelesen wurden.

4.3.1. Allgemeine Filterungsrichtlinie

Einstellungen der Filterungsrichtlinie, welche für alle Gruppen gleich ist, sind in dem Abschnitt **Default Rules** (s. Abb. 4) untergebracht. Um zu diesem Abschnitt zu gelangen, benutzen Sie den Link Default Rules, der in der Auswahl **Common** des Abschnitts **Policies** platziert ist.

The screenshot shows the 'Default Rules' configuration page in the Kaspersky Anti-Spam interface. The page has a green header with the Kaspersky Lab logo and navigation tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Policies' tab is active, showing a 'Common' section on the left with links to 'Default Rules', 'Black List', 'White List', 'DNS Black Lists', and 'Protected Domains'. The main content area lists five default rule categories, each with a description and the number of rules:

Rule Category	Description	Rules
1. General	General settings: may affect rules in other sections	5
2. DNS & SPF Checks	All checks in this section will be skipped if the corresponding settings on the 'General' page are 'Disabled'	3
3. Headers Checks		6
4. Eastern Encodings		4
5. Obscene Content	Use of "[-Obscene-]" mark	1

At the bottom of the page, there is a copyright notice: "Copyright © 2002-2006 Kaspersky Lab. All rights reserved."

Abbildung 4. Einstellungen der allgemeinen Filterungsrichtlinie

Einstellungen der Spam-Erkennungsrichtlinien sind in Gruppierungen nach dem Prinzip der Funktionsähnlichkeit aufgeteilt. Die Hauptseite zeigt eine Liste der Gruppierungen.



Die Kombinationen der Einstellungen und Funktionalitäten werden von den Inhaltsfilterung-Datenbanken bestimmt. Nach dem Update der Datenbanken können Kombinationen der Einstellungen und Funktionalitäten sich ändern.

Außer Gruppennamen der Abschnitte enthält die Liste folgende Informationen:

- Eine Kurze Abschnittbeschreibung;
- Gesamte Anzahl der Richtlinien im Abschnitt;
- Anzahl der Richtlinien, die modifiziert wurden, verglichen mit den ursprünglichen Einstellungen der Inhaltsfilterung-Datenbanken.

Rechts von den Beschreibungen der Abschnitte ist eine Schaltfläche platziert, die den Editor der Regeln des Abschnittes aufruft: . Für die Abschnitte, für welche die Regeln geändert wurden, wird diese Schaltfläche orange gekennzeichnet. Beim Klick auf die Schaltfläche wird die Redaktor-Seite geöffnet. Das Aufrufen der Redaktor-Seite kann auch durch den Klick auf den Namen des Abschnitts durchgeführt werden. Zum Widerrufen der Änderungen benutzen Sie die Schaltfläche .

4.3.1.1. Abschnitt *General*

Das Aufrufen der Regel-Einstellungen des Abschnitts **General** wird durch den Klick auf den Namen des Abschnitts in der Regelliste der allgemeinen Filterungsrichtlinie ausgeführt (s. Abb. 5).

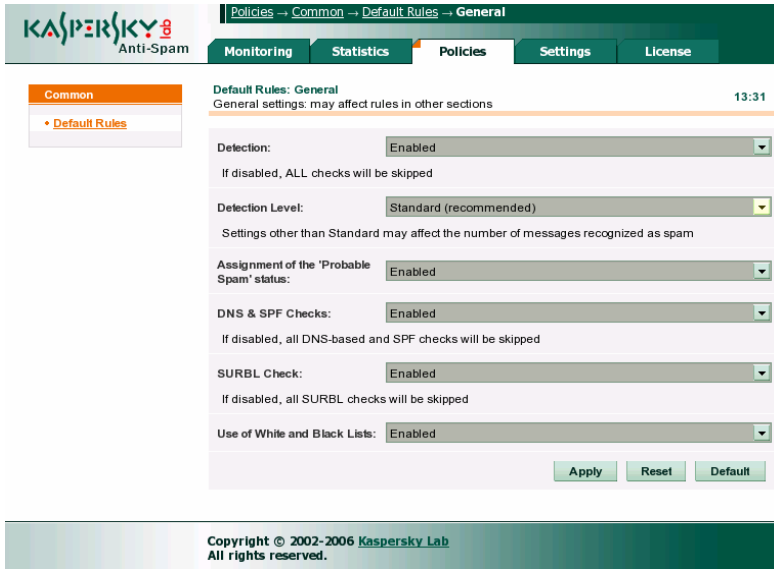


Abbildung 5. Regelabschnitt **General** der allgemeinen Filterungsrichtlinie

Abschnitt **General** erlaubt Ihnen folgende Parameter einzustellen:

- **Detection** – bestimmt, ob die Spam-Erkennung an E-Mails ausgeführt wird. Wenn die Erkennung ausgeschaltet ist, werden alle E-Mails den Status **Trusted** bekommen (Details s. Pkt. 2.3 auf S. 21).



Es wird nicht empfohlen die Erkennung auf der Ebene der allgemeinen Richtlinien abzuschalten. Diese Möglichkeit kann nützlich sein während der Testphase des Produktes, wie in den Situationen, wenn Spamfilterung nur für einige Benutzergruppen eingeschaltet werden soll.

- **Detection Level** – bestimmt Schärfestufe bei der Spamerkennung. Das Entscheiden, ob E-Mail Spam ist oder nicht, passiert auf Grund der Merkmale, die vom Filterungsmodul erkannt werden. Diese Einstellung bestimmt, wie der Filterungsmodul diese Merkmale bewertet beim Vergeben des Status an die Nachricht. Filterungsrichtlinie hat vier Schärfestufen: **Minimum**, **Standard**, **High**, **Maximum**. Um je höher die

Schärfestufe der Erkennung, um so wenige Anzahl der Merkmale führt zur Erkennung der E-Mail als Spam. Auf den Ebenen mit niedriger Schärfe-Stufe wird gleicher Satz der Merkmale nur dazu führen, dass E-Mail als verdächtige (Status Probable Spam), oder gar nicht als Spam anerkannt wird.



Es wird empfohlen die Schärfe-Stufe **Standard** zu benutzen.

Eine höhere Schärfe-Stufe der Filterung kann in dem Fall benutzt werden, wenn Kaspersky Anti-Spam die Spam-Nachrichten nicht erkennt, oder diese als verdächtige erkennt (Status **Probable Spam**). Aber in diesem Fall wird die Wahrscheinlichkeit des fälschlichen Funktionierens erhöht, wenn eine normale E-Mail als Spam anerkannt wird.

Eine niedrigere Schärfe-Stufe führt zu einer kleineren Wahrscheinlichkeit des fälschlichen Funktionierens, dabei erhöht sich die Wahrscheinlichkeit, dass Spam den Filter umgehen kann.



Außer Schärfe-Stufe werden die Filterungsergebnisse auch von den Erkennungsmethoden beeinträchtigt. Bei dem fälschlichen Funktionieren sollen Sie die Methoden überprüfen, die bei der Spamerkennung benutzt werden.

- **Assignment of the 'Probable Spam' status** – Ein- oder Ausschalten der Status-Vergabe **Probable Spam**. Wenn der Parameter den Wert **Disable** bekommt, dann wird Kaspersky Anti-Spam den Status **Probable Spam** nicht an E-Mails vergeben.
- **DNS & SPF Checks** – Überprüfung der Absender-Information über DNS und mit Hilfe der Dienste, die auf Basis von DNS, DNSBL, SPF u.s.w. aufgebaut sind.



Überprüfungen über DNS und Dienste auf Basis von DNS können zu wesentlichen Verzögerungen der E-Mail-Bearbeitung führen. Schalten Sie die Methode ab, wenn ihre Benutzung zu wesentlichen Verringerung der Leistungsfähigkeit des Filters führt.

Der Parameter bestimmt die Benutzung der DNS-Dienste durch den Filterungsserver, Ein / Ausschalten der Dienste wird in dem Abschnitt **DNS & SPF Checks** (s. Pkt. 4.3.1.2 auf S. 40) ausgeführt.

Details zu den Einstellungen der DNSBL-Dienste s. Pkt. 4.3.3 auf S. 46.


- **SURBL Check** – Benutzung der SURBL-Dienste.

- **Use of White and Black Lists** – Benutzung der "weisen" und "schwarzen" Listen der IP-Adressen und E-Mail-Adressen. Details über Benutzung der "weisen" und "schwarzen" Listen s. Pkt. 4.3.2 auf S. 44.

Schltfläsche **Apply** dient zu Speicherung der Einstellungen. Nach dem die Schltfläsche angeklickt wurde, werden Speicherung der Einstellungen, Kompilierung der Filterungsrichtlinien und Neustarten des Filterungsmodulcs durchgeführt. Dadurch werden die Änderungen sofort wirksam.

Schltfläsche **Reset** setzt die Werte der Parameter zurück (es werden alle nicht gespeicherte Änderungen aufgehoben).

Schltfläsche **Default** setzt die Einstellungen für die Inhaltsfilterung-Datenbanken auf standardmäßige zurück. Um die Einstellungen auf die Standardmäßige

zurück zu setzen können Sie auch die Schltfläche  benutzen, die gegen über von den Namen des Abschnittes in der Liste der Regeln der allgemeinen Filterungsrichtlinien platziert ist.

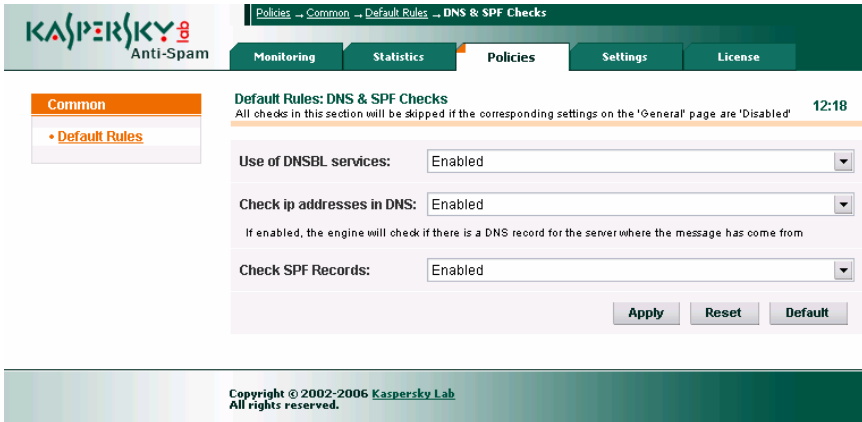
Um zu der Liste der Regeln von allgemeiner Filterungsrichtlinie zurück zu kehren, klicken Sie auf die Schltfläche **Apply** (dabei werden die Änderungen gespeichert) oder benutzen Sie den Link [Default Rules](#) der Aufstellung **Common** (dabei werden die Änderungen nicht gespeichert).

4.3.1.2. Abschnitt *DNS & SPF Checks*

Abchnitt **DNS & SPF Checks** (s. Abb. 6) enthält Einstellungen, welche die externe Dienste bestimmen, die für Spamerkenkung benutzt werden.

Die Parameter, welche in diesem Abschnitt platziert sind, erlauben Ihnen die Benutzung folgender Methoden Ein- und Ausschalten:

- **Use of DNSBL services** – Überprüfung der IP-Adresse des Absenders über die DNSBL-Dienste. Eine Liste der Dienste kann auf der Seite **Policies** → **Common** → **DNS Black Lists** erstellt werden. Details s. Pkt. 4.3.3 auf S. 46.
- **Check ip addresses in DNS** – Überprüfung der IP-Adresse des Absenders über DNS (reverse DNS lookup).
- **Check SPF Records** – Überprüfung der IP-Adresse des Absenders mit Hilfe der SPF-Technologie.



Policies → Common → Default Rules → DNS & SPF Checks

Monitoring Statistics Policies Settings License

Common

- [Default Rules](#)

Default Rules: DNS & SPF Checks 12:18

All checks in this section will be skipped if the corresponding settings on the 'General' page are 'Disabled'

Use of DNSBL services: Enabled

Check ip addresses in DNS: Enabled

If enabled, the engine will check if there is a DNS record for the server where the message has come from

Check SPF Records: Enabled

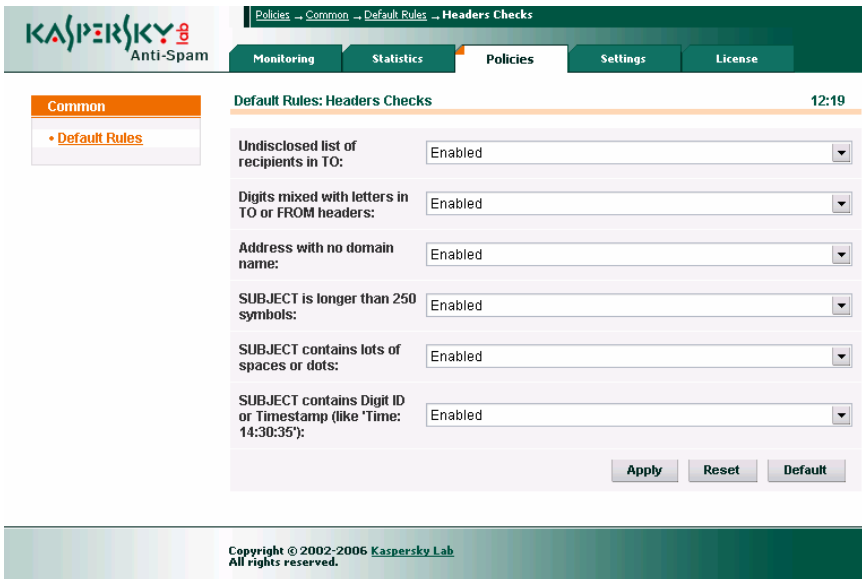
Apply Reset Default

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

Abbildung 6. Abschnitt **DNS & SPF Checks**.

4.3.1.3. Abschnitt *Headers Checks*

Abchnitt **Headers Checks** (s. Abb. 7) erlaubt Ihnen die Parameter der Regeln einzustellen, nach welche die Inhaltsanalyse der E-Mail-Header durchgeführt wird.



Policies → Common → Default Rules → Headers Checks

Monitoring Statistics Policies Settings License

Common

- [Default Rules](#)

Default Rules: Headers Checks 12:19

Undisclosed list of recipients in TO: Enabled

Digits mixed with letters in TO or FROM headers: Enabled

Address with no domain name: Enabled

SUBJECT is longer than 250 symbols: Enabled

SUBJECT contains lots of spaces or dots: Enabled

SUBJECT contains Digit ID or Timestamp (like 'Time: 14:30:35'): Enabled

Apply Reset Default

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

Abbildung 7. Abschnitt **Headers Checks** der allgemeinen Filterungsrichtlinie

Dieser Abschnitt enthält keine komplette Auflistung der Regeln, welche von Kaspersky Anti-Spam bei der Analyse der E-Mail-Titelzeilen benutzt werden, sondern eine Auflistung der Regeln, Anwendung dessen zur Ausfilterung von nützlichen E-Mails, welche Spam-Merkamale enthalten, führen kann. Zu solchen Merkmale gehören:

- **Undisclosed list of recipients in TO** – Vorhandensein der versteckten Empfängerlisten in dem Feld *TO*.
- **Digits mixed with letters in TO or FROM headers** (Vorhandensein der Zahlen in Absender- oder Empfänger-Adresse). Anwendungen, welche zum Spam-Versand benutzt werden, benutzen des Öfteren als Absender- oder Empfängeradressen automatisch generierte Adressen, die eine Gruppe von Zahlen enthalten. Wenn Benutzer Ihres Mailservers keine Adressen mit Zahlen benutzen, ist es ratsam diese Regel einzuschalten.
- **Address with no domain name** (fehlende Domäneninformation in der Adresse). Beim Versenden der Spamnachrichten werden oft unvollständige Adressen benutzt (ohne Angabe der Mail-Domäne), E-Mail Client-Programme dagegen geben eine volle E-Mail-Adresse an, z. B. user@domain.com. Es wird empfohlen diese Regel für solche Benutzer abzuschalten, die E-Mail-Versand mit unvollständigen Adressen zulassen.
- **SUBJECT is longer than 250 symbols** (Langer Text in Feld "Betreff"). Anwendungen, welche zum Spam-Versand benutzt werden, tragen des Öfteren in das Feld "Betreff"(Subject) lange zufällige Zeichen- oder Wörter-Reihenfolgen (mehr, als 250 Zeichen), um Filter zu umgehen. Schalten Sie diese Regel aus, wenn in Ihrem System Versand solchen Nachrichten erlaubt ist.
- **SUBJECT contains lots of white space or dots** (Text in Feld "Betreff" enthält viele Leerzeichen und Punkte). Anwendungen, welche zum Spamversand benutzt werden, tragen in das Feld "Betreff" viele Leerzeichen und Punkte ein, um Filter zu umgehen. Schalten Sie diese Regel aus, wenn in Ihrem System Versand von solchen Nachrichten erlaubt ist.
- **SUBJECT contains DIGIT ID or Timestamp (like 'Time: 14:30:35')** (Text im Feld "Betreff" enthält Zeitmuster oder Digitale ID). Die Methode, bei welcher in das Feld "Betreff" Zeitmuster oder Digitale ID eingetragen werden, wird auch von den Spamversand-Programmen benutzt, um Spam-Filter zu umgehen.

Ein Dropdown-Menü rechts von den aufgezählten Regeln erlaubt Ihnen die Benutzung der Regel Ein- (Wert **Enabled**) oder Auszuschalten (Wert **Disabled**).



Endgültige Entscheidung, welcher Status der Nachricht vergeben wird, wird auf Grund viele Merkmale gefällt. Deswegen bedeutet das Ein- oder Ausschalten einer Regel oder Regel-Gruppe noch nicht, dass die zu bearbeiteten E-Mails als Spam erkannt werden oder, im Gegenteil, vom Filterungsserver durch gelassen werden. Das Einstellen der Regel erlaubt es, die Fehlerquote beim Erkennen des Spams zu verkleinern.

Aufgezehlte Regeln können nicht nur für alle Benutzer in der allgemeinen Filterungsrichtlinie, sondern auch für einzelne Gruppen eingeschaltet werden, mit Hilfe der Gruppenrichtlinie.

4.3.1.4. Abschnitt *Eastern Encodings*

Im Abschnitt **Eastern Encodings** (s. Abb. 8) können Sie die Sprachen und Kodierungen der Nachrichten angeben, welche den Benutzern Ihres E-Mail-Systems zugeschickt werden dürfen und nicht zum Spam gehören.

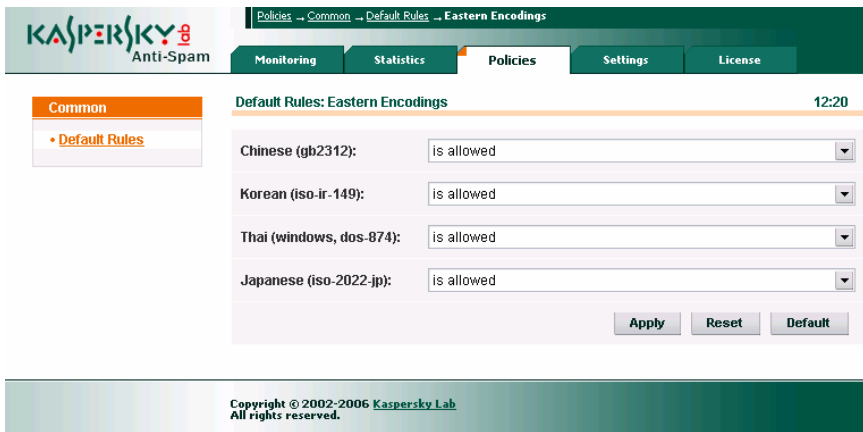


Abbildung 8. Abschnitt **Eastern Encodings** der allgemeinen Filterungsrichtlinie.

In der laufenden Produkt-Version wird Gruppe der asiatischen Sprachen kontrolliert: Chinesische, Koreanische, Taiwanesische und Japanische.

Wenn die Benutzer Ihres E-Mail-Systems einer der aufgezählten Sprachen benutzt, wählen Sie für diese Sprache den Punkt **is allowed** aus dem **Dropdown-Menü**. Wenn keine der Sprachen von den Benutzern Ihres E-Mail-Systems benutzt wird, wählen Sie den Wert **is treated as suspicious aus**.

4.3.1.5. Abschnitt *Obscene Content*

Abschnitt **Obscene Content** (s. Abb. 9) erlaubt Ihnen zu bestimmen, ob die Nachrichten mit obszönen Ausdrücken markiert werden sollen. Kaspersky Anti-Spam erkennt Obszönitäten aus Russischer und Englischer Sprachen.



Abbildung 9. Abschnitt **Obscene Content** der allgemeinen Filterungsrichtlinie.

Wenn Parameter **Message with obscene words and phrases** den Wert **mark in Subject** bekommt, werden alle E-Mails mit obszönen Ausdrücken mit Kennzeichnung **[--Obscene--]** in dem Betreff-Feld gekennzeichnet.

4.3.2. Verwaltung der "weißen" und "schwarzen" Listen

"Weiße" Absenderliste (**White List**) wird benutzt um eindeutig die Adressen anzugeben, von welchen kommende E-Mails nicht nach Spam untersucht werden. In diese Liste können IP-Adressen der internen Mailserver oder Versandlisten eingetragen werden. E-Mails von Absender aus der "weißen" Liste werden Status Trusted **bekommen**.

"Schwarze" Absenderliste (**Black List**) hat eine gegenteilige Bedeutung. In diese Liste trägt der Filterungsserver-Administrator die Absender-Adressen, welche zum Versenden der Spam-E-Mails benutzt werden. Nachrichten, dessen Absender in der "schwarzen" Liste sind, bekommen den Status Blacklisted.

Verwaltung der Listen ist identisch. In diesem Abschnitt werden Beispiele der Einstellungen der "weißen" Liste betrachtet (s. Abb. 10).

Zugang zu der Bearbeitungsmaske der "weißen" Liste wird über den Menüpunkt **Policies** → **Common** → **White List** (für die "schwarze" Liste – **Policies** → **Common** → **Black List**).

Eine Liste der Vertrauten Adressen wird in IP-Adressen-Liste und E-Mail-Adressen-Liste unterteilt. Für die Adresseneingabe dient ein Textfeld in der Mitte der Seite. Der Schalter e-mails | ip addresses wird zum Auswählen der Eintragungstypen der "weißen" Liste benutzt.

Schaltfläche **Apply** dient zu Speicherung der eingetragenen Änderungen. Damit nicht gespeicherte Änderungen verworfen werden, benutzen Sie die Schaltfläche **Reset**.



Speichern Sie die Änderungen, bevor Sie den Schalter **e-mails | ip addresses** benutzen. Beim Umschalten gehen alle nichtgespeicherte Änderungen verloren.

Abbildung 10. Einstellungsseite der "weißen" Liste

Um die E-Mail-Adressen einzugeben werden folgende Schreibweisen benutzt:

- *user@domain* – eine bestimmte Adresse;
- *@domain* – alle Adressen aus der Domäne **domain**.

In den E-Mail-Adressen können auch spezielle Sonderzeichen benutzt werden:

- * (Stern) – eine Zeichenzeile willkürlicher Länge;
- ? (Fragezeichen) – ein willkürlicher Zeichen.

Z. B., Eintrag *user*@mycompany.com* zeigt auf alle Adressen, die mit dem Wort *user* anfangen und aus der E-Mail-Domäne *mycompany.com* kommen.

Zum Eintragen der IP-Adressen wird CIDR-Schreibweise benutzt, die folgenden Varianten zulässt:

- *aaa.bbb.ccc.ddd* – bestimmte IP-Adresse, z. B., 192.168.0.17;
- *aaa.bbb.ccc.ddd/mm* – Subnetz-Adresse mit vorgegebener Nummer und Maske, z. B. 192.168.0.0/16.

Adressen in der Liste können durch Lehrzeichen, Zeilenvorschub, Semikolon und Punkt getrennt werden.

4.3.3. Verwaltung von Listen der benutzten DNSBL-Diensten

Um auf die Seite der Verwaltung von Listen der DNSBL-Dienste zu gelangen, benutzen Sie den Link [DNS Black Lists](#) im Menü **Common** des Abschnittes **Policies** (s. Abb. 11).

Liste der Einstellungen der benutzten DNSBL-Dienste gehört zur allgemeinen Filterungsrichtlinie. Später können Sie für jede Benutzergruppe angeben, ob die Ergebnisse der Untersuchung mit Hilfe der DNSBL-Dienste für diese Gruppe benutzt werden sollen. Die Liste der Dienste ist für alle Benutzergruppen gleich.

In der Mitte der Seite ist eine Liste der benutzten Dienste platziert. Für jeden DNSBL-Dienst wird seine Adresse angegeben, über welche die Anfragen an den Dienst geschickt werden, wie auch Popularität des Dienstes.

Dienst-Popularität bestimmt die Vertrauensstufe des Administrators an den Dienst. Bei der Überprüfung der IP-Adresse in den DNSBL verschickt Kaspersky Anti-Spam Anfragen an alle Dienste aus der Liste. Nach dem die Ergebnisse vorliegen, werden die Popularitäten der Dienste summiert, welche angegebenen IP-Adressen erkannt haben als die Adresse, von der Massenversand stattfindet.

The screenshot shows the 'DNS Black Lists' management page in the Kaspersky Anti-Spam interface. The page title is 'Policies → Common → DNS Black Lists'. The main content area displays a table of DNSBL services with the following data:

	Hostname	Rate	
1	combined-hib.dnsiplists.completewhois.com	70	✗
2	bl.spamcop.net	30	✗
3	list.dsbl.org	50	✗
4	dnsbl.njabl.org	50	✗
5	relays.ordb.org	70	✗
6	xbl-sbl.spamhaus.org	50	✗
+			

At the bottom of the table, there are 'Apply' and 'Reset' buttons. The page footer contains the copyright information: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Abbildung 11. Seite der Verwaltung von DNSBL-Listen

Wenn die Summe der Popularitäten DNSBL-Dienste höher ist, als 100, wird der Absender als einer aus der "schwarzen" Liste behandelt und die Nachricht

bekommt Status **blackisted**, unabhängig von den Ergebnissen der Anderen Methoden. Bei bestimmter Schärfestufe können auch die Situationen analysierte werden, wann die Summe der Dienstpopularitäten, welche den Absender in "schwarzer" Liste haben, weniger als 100 ist. In diesem Fall wird die Information von den DNSBL-Diensten nur als zusätzlicher Merkmal benutzt und die Nachricht erhält den Spamstatus nur denn, wenn die Spammerkmale auch mit Hilfe anderen Methoden festgestellt wurden.

Es sind folgende Aktionen an der Liste der DNSBL-Dienste möglich:

- Einen Dienst hinzufügen.
- Dienst-Popularität ändern.
- Dienst entfernen.

Sehen wir jede Aktion detailliert an:

- Um einen neuen Dienst zu Liste zuzufügen:
 1. Dienst-Adresse in der unteren freien Zeile mit dem Zeichen **+** angeben;
 2. Dienst-Popularität angeben;
 3. Ergebnisse speichern, in dem Sie auf die Schaltfläche **Apply** klicken.
- Um Popularität eines existierenden **DNSBL-Dienst zu ändern**:
 1. neuen Popularitätswert in der Tabelle **Rate** des Dienstes angeben;
 2. Ergebnisse speichern, in dem Sie auf die Schaltfläche **Apply** klicken.
- Um einen Dienst aus der Liste zu Löschen:

Auf die Schaltfläche  klicken, die rechts von der Adressenzeile des Dienstes platziert ist.



Auswahl zu benutzenden DNSBL sollte mit Vorsicht getroffen werden. Bei den unterschiedlichen Diensten unterscheiden sich die Richtlinien der Listenerstellung. Lesen Sie die Richtlinien der Dienste sorgfältig, bevor Sie Listen des Dienstes zur E-Mail-Filterung benutzen.

4.3.4. Verwaltung von Liste der geschützten Domänen

Liste der geschützten Domänen enthält Domännennamen, an den Spamfilterung ausgeübt wird. Für die Listenverwaltung dient die Seite, die an der Adresse **Policies** → **Common** → **Protected Domains** platziert ist (s. Abb. 12).

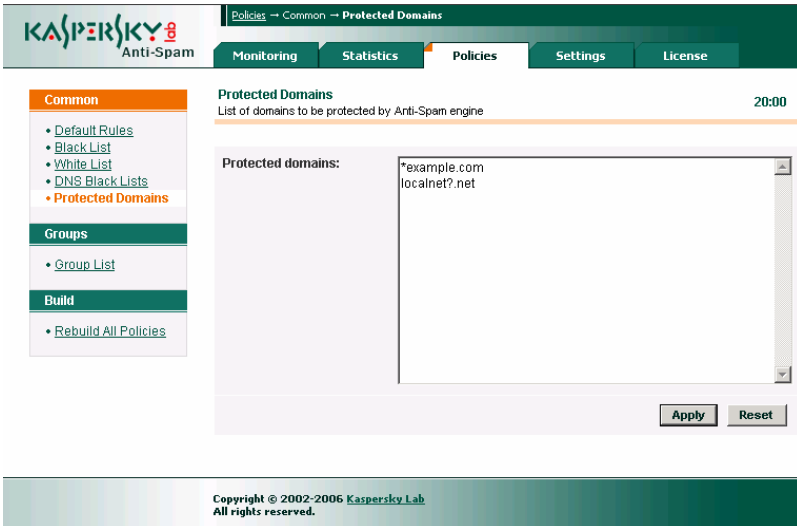


Abbildung 12. Liste der geschützten Domänen

Beim Angeben von Adressen geschützten Domänen dürfen Sonderzeichen benutzt werden: * – beliebige Anzahl von Zeichen, ? – ein beliebiges Zeichen. Z. B.; um Domäne **example.com** und Ihre Subdomänen in die Liste der geschützten aufzunehmen, ist es ausreichend einen Eintrag zu machen:

*example.com

Um den Produkt auf Filterung aller E-Mails einzustellen, können Sie entweder die Liste leer lassen, oder fügen Sie folgende Zeile hinzu:

*

Nach dem Bearbeiten der Liste klicken Sie auf die Schaltfläche **Apply** um die Änderungen zu bestätigen, und auf **Reset** um die Änderungen zu verwerfen.



Für die Domänen, die in Liste der geschützten aufgenommen sind, wird Kontrolle der Lizenz-Begrenzung durchgeführt (z. B., Umfangkontrolle des E-Mail-Verkehrs, wenn Lizenz-Schema mit Begrenzung nach diesem Parameter benutzt wird).

Änderungen in die Liste können auch lokal eingetragen werden, unter Benutzung der Befehlszeile. Domänenliste wird in Form einer Textdatei *protected_domains*, in dem Verzeichnis */usr/local/ap-mailfilter3/conf* abgelegt.

Nach dem die Datei bearbeitet ist, führen Sie folgenden Befehl als Benutzer **root** aus:

```
# /usr/local/ap-mailfilter3/bin/kas-restart -f
```



An alle E-Mails, die an Benutzer nicht geschützten Domänen weitergeleitet werden, wird ein folgender Header eingefügt:
X-SpamTest-Info: Not protected
Details über spezielle Header s. Pkt. A.5 auf S. 120.

4.3.5. Gruppenverwaltung

Filterungsserver-Administrator kann unterschiedliche Spamerkennung-Einstellungen für verschiedene Benutzer vorgeben. Dafür dienen die Gruppen-Filterungsrichtlinien.

Bevor Sie zu den Einstellungen der Regeln von Gruppen-Richtlinien übergehen, muss eine Liste von E-Mail-Adressen definiert werden, für welche Gruppen-Richtlinie wirksam sein soll.

Außer von dem Administrator erstellten Gruppen, benutzt das Produkt eine Gruppe namens **All**, die bei der Installation standardmäßig erstellt wird. Diese Gruppe bestimmt die E-Mail-Bearbeitungsregel, welche nicht unter Wirkung anderer Gruppen fallen. Gruppe **All ist eine Systemgruppe** und kann nicht gelöscht werden.

Um zu den Gruppeneinstellungen zu gelangen ist Menüpunkt **Groups** vorgesehen, welchen Sie an der linken Seite des Fensters im Abschnitt **Policies** finden.

Link [Group List](#) öffnet eine Seite, diese enthält eine Auflistung aller Gruppen (s. Abb. 13).

The screenshot shows the 'Policies → Group List' page in the Kaspersky Anti-Spam interface. The left sidebar contains a 'Groups' section with a 'Group List' link. The main content area shows a table of recipient groups:

Group List		13:44
List of recipient groups		
1.	Accounting Accounting department employees	
2.	▲ Managers Company managers	
3.	▲ Sales Sales department employees	
4.	All All recipients not included in any other group	

At the bottom of the main area, a green checkmark icon is followed by the text: 'Settings have been saved and applied successfully'.

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

Abbildung 13. Auflistung von Kaspersky Anti-Spam benutzten Gruppen

Es sind folgende Aktionen an den Gruppen möglich:

- Gruppeneigenschaften ändern.
- Eine neue Gruppe erstellen.
- Eine Gruppe Löschen.
- Gruppenanordnung ändern.

Weiter werden jede der aufgezählten Aufgaben detailliert behandelt:



Um Gruppeneigenschaften-Editor zu öffnen, gehen Sie wie folgt vor:

klicken Sie rechts von dem Namen der Gruppe, deren Eigenschaften Sie bearbeiten wollen, auf die Schaltfläche .


- Gruppeneigenschaften-Editor erlaubt Ihnen zu bearbeiten:
- Allgemeine Gruppenparameter, wie z. B., Gruppenname, Anmerkungen, wie auch die Liste der E-Mail-Adressen, an welche die Regeln der Gruppe angewendet werden.
- Spamerkennung-Regeln;
- Aktionen, die an den E-Mails unternommen werden;
- "schwarze" und "weiße" Absenderlisten.



Name und die E-Mail-Adressen von der Gruppe **All** sind fürs Bearbeiten unzugänglich, denn diese Gruppe bestimmt Bearbeitungsregeln aller Nachrichten, Absender und Empfänger deren in keine von Administrator erstellten Gruppen eingeschlossen sind.



Um eine neu Gruppe zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf Schaltfläche , welche sich über die Gruppenliste befindet.
2. In dem darauf folgenden Fenster (s. Abb. 14) wählen Sie Gruppennamen aus, tragen Sie die Anmerkungen (wenn nötig ist) und die E-Mail-Adressen ein.


Das Feld **Group Id** enthält Gruppen-Bezeichner, diese Gruppen-Bezeichner wird beim erstellen der Gruppe vergeben. Dieser Parameter kann nicht geändert werden.

Text aus dem Feld **Comments** wird in der Gruppenliste unter dem Namen der erstellten Gruppe angezeigt.

Für E-Mail-Einträge wird die gleiche Schreibweise benutzt, wie für Adressen in der "schwarzen" und "weißen" Absenderlisten (s. Pkt. 4.3.2 auf S. 44).




Um eine Gruppe zu löschen,

Klicken Sie auf die Schaltfläche , welche sich rechts von dem Namen der Gruppe befindet.



Um Anzeigereihenfolge der Gruppen zu ändern,,

Klicken Sie auf die Schaltfläche , welche sich links von dem Namen der Gruppe befindet. Dabei wird die Gruppe in der Liste nach oben verschoben.

Bei E-Mail-Bearbeitung durchsucht der Filterungsmodul die Gruppen in der vorgegebenen Reihenfolge (vom Anfang zu Ende). Dabei wird E-Mail nach Regel der Gruppe bearbeitet, in welcher Liste die Empfängeradresse als erstes gefunden wird. Wenn Empfänger in keiner der Gruppen gefunden wird, wird E-Mail nach Regeln der Gruppe **All** behandelt.

The screenshot displays the Kaspersky Anti-Spam 3.0 interface. At the top, there is a navigation bar with 'Policies -- Group Policy -- General'. Below this, there are tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The main content area is titled 'General Settings - Group: Sales' with a timestamp of 12:41. On the left, a sidebar shows 'Groups' with a 'Group List' link and 'Group Policy' with links for 'General', 'Actions', 'Rules', 'Black List', and 'White List'. The 'General' section is selected. The main area contains the following fields:

- Group Name:** Sales
- Group Id:** 1
- Description:** Sales employees
- E-mail addresses of group members:**
 - alice@sales.local
 - bob@sales.local
 - jack@sales.local
 - john@sales.local
 - mike@sales.local
 - ann@sales.local
 - bob@sales.local

At the bottom right of the main area, there are 'Apply' and 'Reset' buttons. At the very bottom of the interface, a footer contains the text: 'Copyright © 2002-2006 Kaspersky Lab All rights reserved.'

Abbildung 14. Erstellung einer neuen Gruppe

4.3.6. Verwaltung von Gruppen-Filterungsrichtlinien

Für jede Gruppe, auch für Gruppe **All**, können eigene Erkennungseinstellungen vorgegeben werden, wie auch eigene "schwarze" und "weiße" Absenderlisten. So hat der Administrator eine Möglichkeit unterschiedliche Regeln für verschiedene Benutzergruppen zu definieren.

Standardmäßig erben alle Gruppen die Erkennungsregeln von der allgemeinen Filterungsrichtlinie, jedoch kann der Administrator die Erkennungsregeln für Gruppen umdefinieren.

Zu den Einstellungen von Erkennungsregeln der Gruppen-Filterungsrichtlinie können Sie über Link Rules im Menü **Group Policy** des Richtlinieneditors gelangen. Die Regeln-Struktur ist mit der Struktur von allgemeinen Filterungsrichtlinie identisch .

Der einzige Unterschied besteht darin, dass die Liste möglichen Richtlinien-Werte einen Parameter by default **enthält**. Das bedeutet, dass dieser Parameter die Einstellungen von der allgemeinen Filterungsrichtlinie erbt.

Auf Abbildung 15 ist Fenster **Rules** der Gruppen-Filterungsrichtlinie gezeigt.

Wie aus der Abbildung zu sehen ist, erbt die Gruppe alle Einstellungen von allgemeinen Filterungsrichtlinie (Wert by default) mit Ausnahme von Parameter DNS & SPF Checks. Das Benutzen dieser Methode ist ausgeschaltet.

Um "schwarze" und "weiße" Absenderlisten zu definieren sind Links [White List](#) und [Black List](#) bestimmt, welche sich im Menü **Group Policy** befinden. Listeneinstellungen für Gruppen sind den Einstellungen von allgemeinen Filterungsrichtlinie identisch.

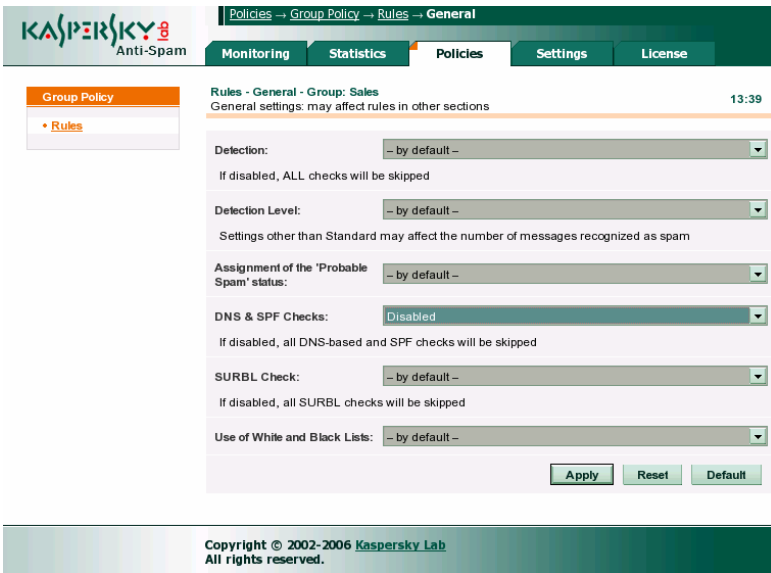


Abbildung 15. Seite **Rules** der Gruppen-Filterungsrichtlinie

4.3.7. Aktionen an den E-Mails

Gruppenrichtlinie enthält auch eine Reihe von Weiterleitungs- und Modifikationsaktionen, die an den von Filterungsmodul erkannten E-Mails vorgenommen werden. Benutzen Sie den Link [Actions](#), welcher sich in dem Menü Group Policy des Richtlinieneditors befindet, um die Aktionen einzustellen.

Aktionen werden von dem Status bestimmt, welcher während der Überprüfung durch Filterungsmodul vergeben wird. Die Seite Actions (s. Abb. 16) enthält ein Muster, welches Ihnen erlaubt die Aktionen für jeden Status zu definieren.

Eine dropdown-Liste, welche sich unter Statusbeschreibung befindet, dient zur Bestimmung von Aktionen.

Administrator kann folgende Aktionen definieren:

- **Accept this message** – Mailserver nimmt E-Mail an und stellt dem Empfänger zu.
- **Send a copy of this message to other recipient(s)** – Mailserver nimmt E-Mail an, stellt dem Empfänger zu und verschickt eine Kopie an die Adresse, welche in dem Feld **Send message to** eingetragen ist.
- **Redirect this message to other recipient(s)** – Mailserver nimmt E-Mail an und leitet an die Adresse weiter, die im Feld **Send message to** eingetragen ist. An den E-Mail-Empfänger wird die Nachricht nicht zugestellt. Diese Option kann zum Versenden von Spam-Nachrichten an das Spamspeicherung-Postfach benutzt werden.
- **Reject this message** – Mailserver lehnt die Nachricht ab und schickt an den Absender eine Benachrichtigung über Unmöglichkeit der Zustellung. Wenn Zustellung für alle Empfänger abgelehnt wird, versendet Mailserver Benachrichtigung Ablehnung der Zustellung direkt während der SMTP-Sitzung (reject message). Wenn die Zustellung für mindestens einen Benutzer erlaubt sein sollte, wird dem Absender eine Benachrichtigung über Unmöglichkeit der Zustellung an die einzelnen Empfänger verschickt (bounce message). Text der Benachrichtigung können Sie unter **Settings** → **Reject Messages** einstellen (Details s. Pkt. 4.5.4 auf S. 64).
- **Delete this message** – Mailserver erhält E-Mail und löscht sie, ohne dem Empfänger zu zustellen. Dabei erhält der Absender keine Benachrichtigung über Unmöglichkeit der Zustellung.

KASPERSKY
Anti-Spam

Policies → Group Policy → **Actions**

Monitoring | **Statistics** | Policies | Settings | License

Groups

- Group List
- Group Policy**
- General
- **Actions**
- Rules
- Black List
- White List

Actions - Group: Sales 12:45

Actions to be performed on incoming messages

If a message is recognized as 'Spam':

Accept this message:

Prepend to the Subject:

Set X-SpamTest-Header:

If a message is recognized as 'Probable Spam':
Messages suspected of being spam

Accept this message:

Prepend to the Subject:

Set X-SpamTest-Header:

If a message is recognized as 'Blacklisted':
Messages from senders or relays included in common or group black lists

Accept this message:

Prepend to the Subject:

Set X-SpamTest-Header:

If a message is recognized as 'Formal':
Automatic replies or notifications

Accept this message:

Prepend to the Subject:

Set X-SpamTest-Header:

If a message is recognized as 'Trusted':
Messages from trusted senders or relays (included in common or group white lists)

Prepend to the Subject:

Set X-SpamTest-Header:

If a message is recognized as 'Not Detected':
Other messages

Prepend to the Subject:

Set X-SpamTest-Header:

Abbildung 16. Seite **Actions** der Gruppenrichtlinie

Nachrichten, welche Status Not detected (E-Mail wurde nicht als Spam erkannt) oder Status Trusted (Nachricht kommt aus vertrauter Quelle oder für Empfänger wurde in Gruppenrichtlinien Spamuntersuchung der E-Mails ausgeschaltet), werden immer an den Empfänger zugestellt.



Trotzdem, dass Produkt ständig weiterentwickelt wird, um die Qualität der Spamerkennung zu steigern und Fehlfunktionen beim Filtern zu mindern, können die Fehlfunktionen, wenn normale E-Mails als Spam erkannt werden, nicht vollständig ausschließen. In diesem Zusammenhang empfehlen wir das Löschen der E-Mails mit Vorsicht zu benutzen.

Außer Weiterleitung kann Administrator Aktionen für Nachrichten-Modifizierung definieren. Dieses ist wie für die Visualisierung der Erkennung-Ergebnisse, so auch für die Filterung der Nachrichten in den E-Mail-Clientprogrammen bequem.

Kaspersky Anti-Spam bietet Ihnen folgende Möglichkeiten der Modifizierung:

- Eine Markierung in Feld „Betreff“ eintragen (am Anfang der Zeile). Für Texteingabe der Markierung dient Feld Prepend to the Subject.
- Einen zusätzlichen Header *X-Spamtest-Header* hinzufügen, welche vom Administrator vorgegebenen Text enthält. Diese Headermarkierung kann zur automatischen E-Mail-Bearbeitung von den Client-Programmen benutzt werden. Um ein Text für die Headermarkierung einzugeben, benutzen Sie das Feld **Set X-Spamtest-Header**. Mehr über Headermarkierungen, die bei Filterung zur E-Mail hinzugefügt werden s. Pkt. A.5 auf S. 120.

4.4. Inhaltsfilterung-Datenbanken updaten

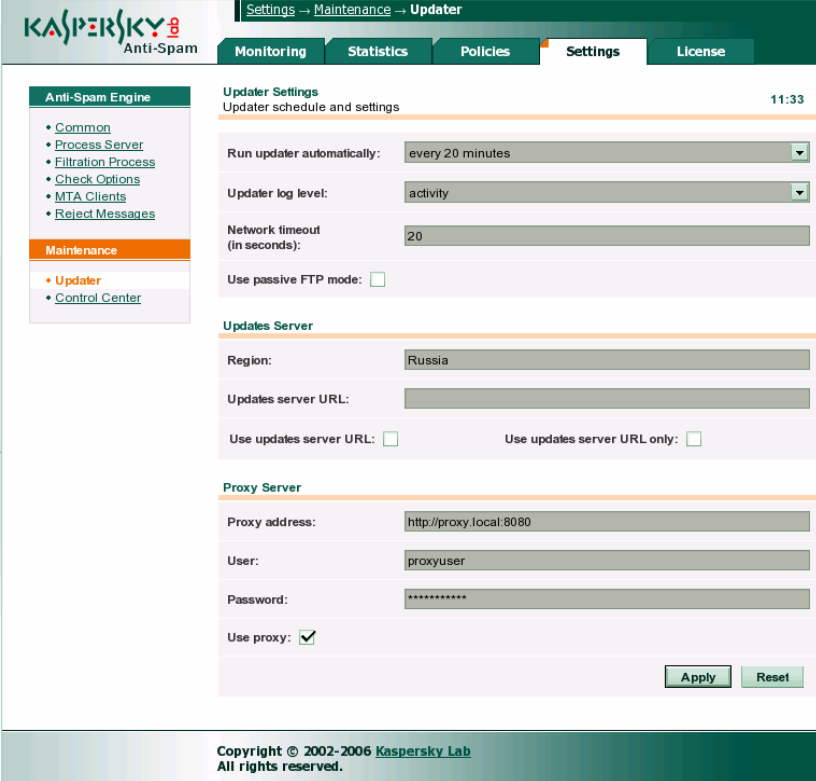
Update von Inhaltsfilterung-Datenbanken, welche zur Inhaltsanalyse von E-Mails benutzt werden, führt eine Anwendungskomponente aus – *sfpdates*.

Als Quelle für die Updates der Inhaltsfilterung-Datenbanken kann Kaspersky-Lab-Updateserver im Internet oder ein Netzwerkordner dienen.

Updatestart wird entweder per Hand aus Befehlszeile mit Hilfe eines Skripts oder automatisch nach Zeitplan mit Hilfe des Dienstes cron gestartet.

4.4.1. Update-Parameter einstellen

Um die Update-Parameter einzustellen, benutzen Sie die Seite **Settings** → **Maintenance** → **Updater** in der Verwaltungszentrale (s. Abb. 17).



Settings → Maintenance → Updater

KASPERSKY Anti-Spam

Monitoring Statistics Policies Settings License

Anti-Spam Engine

- Common
- Process Server
- Filtration Process
- Check Options
- MTA Clients
- Reject Messages

Maintenance

- Updater
- Control Center

Updater Settings 11:33

Updater schedule and settings

Run updater automatically: every 20 minutes

Updater log level: activity

Network timeout (in seconds): 20

Use passive FTP mode:

Updates Server

Region: Russia

Updates server URL:

Use updates server URL: Use updates server URL only:

Proxy Server

Proxy address: http://proxy.local:8080

User: proxyuser

Password: *****

Use proxy:

Apply Reset

Copyright © 2002-2006 Kaspersky Lab All rights reserved.

Abbildung 17. Updatemodul von Kaspersky Anti-Spam einstellen

Sektion **Updater Settings** enthält allgemeine Update-Parameter:

- **Run updater automatically** – Zeitspanne zwischen Downloadvorgängen. Zeitspanne kann von 20 Minuten bis 3 Stunden betragen.



Es wird empfohlen eine kurze Zeitspanne anzugeben. Schnellere Updates der Inhaltsfilterung-Datenbanken bietet eine schnelle Reaktion auf neue Versandlisten. Empfohlene Zeitspanne ist: 20 Minuten.

Parameter-Wert bestimmt Zeitspanne, in welcher der cron-Task für Produkt-Update gestartet wird. Beim Bedarf kann cron-Task- Einstellung per Hand gemacht werden.

- **Updater log level** – Stufe der Updateprotokoll-Genauigkeit. Es sind folgende Genauigkeitsstufen vorhanden:

- **fatal** – Es werden kritische Fehler in das Protokoll eingetragen;
 - **error** – Es werden Informationen über alle Fehler in das Protokoll eingetragen (kritische und nicht kritische).
 - **warning** – Es werden Warnungen und Fehler in das Protokoll eingetragen;
 - **info** – Außer Warnungen und Fehlermeldungen werden in das Protokoll Informative Meldungen eingetragen (Information über das Starten des Update-Moduls, Updateergebnisse und s.w.);
 - **activity** – In das Protokoll wird Information eingetragen, die Stufe **info** entspricht, wie auch erweiterte Informationen über Update-Verlauf (Verbindung mit dem Update-Server, Kopiervorgang der Dateien u.s.w.);
 - **debug** – In das Protokoll wird Information eingetragen, die Stufe **activity** entspricht, wie auch Information für die Fehlersuche.
- **Network timeout** – Timeout (in Sekunden) für die Netzwerk-Verbindungen beim Updaten der Inhaltsfilterung-Datenbanken. Empfohlener Wert: **30**.
 - **Use passive FTP mode** – dieser Parameter zeigt, dass bei Verbindung über FTP-Protokol passive Modus benutzt werden soll (empfohlen).

Sektion **Updates Server** enthält Serverparameter des Update-Servers:

- **Region** – Region-Name. Wird vom Produkt zur Auswahl des nächsten Update-Servers benutzt.
- **Updates server URL** – Adresse des Update-Servers. Dieser Parameter wird in Verbindung mit den Parametern Use updates server URL und Use updates server URL only **benutzt**. Standardmäßig ist die Server-Liste der Update-Server in der Datei updcfg.xml *definiert*, die Datei ist in dem Produkt-Distributiv enthalten. Beim Updaten wählt Kaspersky Anti-Spam automatisch einen Server aus dieser Liste. Mit Hilfe der Einstellung **Use updates server URL können Sie angeben, dass für Updates Server benutzt werden soll, welcher im Parameter Updates server URL definiert ist**. Wenn Option Use updates server URL only **benutzt wird**, dann wird Kaspersky Anti-Spam nur den angegebenen Server zum updaten der Inhaltfilterungs-Datenbanken, dabei wird nicht versucht andere Server zu benutzen.

Als Update-Quellen lässt dieser folgende Parameter zu:

- HTTP-Server. *Schreibweise:* http://<Serveradresse>
- FTP-Server. *Schreibweise:* ftp://<Serveradresse>

- Lokaler Verzeichnis . *Schreibweise* /<Verzeichnispfad>/

Benutzen eines lokalen Verzeichnisses als Update-Quelle erlaubt das Updaten mehrere Server in einem großen Netzwerk zu organisieren.

Sektion **Proxy Server** enthält Zugangseinstellungen für Proxy-Server:

- **Proxy address** – Adresse des Proxy-Servers, welcher für Internet-Zugang benutzt wird. *Schreibweise*: `http://url:port`, wo `url` und `port` Adresse und Port für die Verbindung mit dem Proxy-Server sind. Wenn die Adresse nicht angegeben ist, wird dieser Wert der Variablen `http_proxy` entnommen.
- **User** – Benutzername für Zugang zum Proxy-Server.
- **Password** – Benutzerpasswort für Zugang zum Proxy-Server.
- **Use proxy** – dieser Parameter zeigt, dass ein HTTP-Proxy-Server zum updaten der Inhaltsfilterung-Datenbanken benutzt werden muss.

4.4.2. Update starten

Sie können das Updaten der Inhaltsfilterung-Datenbanken auf zwei Wegen starten:

- Automatisch nach Zeitplan;
- Per Hand aus Befehlszeile.

Es wird empfohlen automatische Updates einzustellen, dieses erlaubt Ihnen die Inhaltsfilterung-Datenbanken im aktuellen Zustand zu halten und gewährleistet effiziente Spamfilterung.



Um Update per Hand zu starten, geben Sie in der Befehlszeile ein:

```
# /usr/local/ap-mailfilter3/bin/sfupdates
[schlüssel]
```

wo `[schlüssel]` – ein Skript-Startparameter ist. Eine volle Parameterliste des Skriptes `sfupdates` s. Pkt. A.4.8 auf S. 119.

Wenn Sie keinen Schlüssel zum Starten des Skriptes benutzen, werden neue Inhaltsfilterung-Datenbanken von dem Server kopiert, wird eine Vollständigkeitsuntersuchung durchgeführt, die Datenbanken werden installiert und Filterungsmodul wird neu gestartet.

Standardmäßig wird bei Produktinstallation Dienstprogramm `cron` zum automatischen Start des Updateskriptes für Benutzer **mailfit3** mit 20-minütigen

Zeitabständen konfiguriert. Wenn es notwendig ist den Start-Task des Update-Skripts per Hand einzustellen, gehen Sie wie folgt vor:

1. Starten Sie den Task-Editor des Prozesses **cron** für den Benutzer **mailflt3**

```
# crontab -u mailflt3 -e
```

2. in die Task-Datei fügen Sie, z. B., ein:

```
*/20 * * * * /usr/local/ap-  
mailfilter3/bin/sfupdates -q
```



Bevor Sie automatisches Staten der Updates wählen, vergewissern Sie sich, dass Benutzer **mailflt3** in den Verzeichnissen */usr/local/ap-mailfilter3/cfdata* und */usr/local/ap-mailfilter3/conf* Schreibrechte hat.

4.5. Einstellungen von Spamfilterung-Server

Im Abschnitt **Settings** befinden sich die Einstellungen des Spamfilterung-Servers. Zu den Seiten gelangen Sie über Links, welche sich im Menü **Anti-Spam Engine** befinden:

- Common – allgemeine Einstellungen des Spamfilterung-Servers.
- Process Server – Einstellungen des Master-Prozesses *ap-process-server*.
- Filtration Process – Funktionsparameter der Filterungsprozesse *ap-mailfilter*.
- Check Options – Spamerkennung-Parameter.
- MTA Clients – Parameter der Clientmodule.
- Reject Messages – Texte der Nachrichten, welche beim Ablehnen der E-Mail-Annahme an den Absender verschickt werden.

Die Parameter können auch per Hand in der Konfiguratsdatei *filter.conf* bearbeitet werden. Eine Detaillierte Beschreibung der Konfigurationsdatei *filter.conf* s. Pkt. A.3.1 auf S. 107.

4.5.1. Allgemeine Filterungsserver-Parameter

Allgemeine Filterungsserver-Parameter befinden sich auf der Seite **Settings** → **Anti-Spam Engine** → **Common** (s. Abb. 18), dazu gehören:

- **Syslog facility** – Systemprotokoll-Kategorie, in welche Kaspersky Anti-Spam-Einträge geschrieben werden. Standardmäßig werden die Einträge in die Kategorie **mail** geschrieben, bei Bedarf kann der Administrator die Einträge in folgende Kategorien schreiben lassen: **mail**, **user**, **local0** – **local7**.



Nach dem Parameter **Syslog facility** geändert wurde, stellen Sie das Hilfsprogramm **syslog** ein, um das Schreiben in die Kategorie zu gewährleisten. Diese Einstellungen werden per Hand in der Konfigurationsdatei `/etc/syslog.conf` vorgenommen. Details dazu s. [manual pages für syslogd und syslog.conf](#).

Systemprotokolle werden von dem Monitoring-System benutzt um die Informationen über Arbeit des Filterungsservers und seine Komponente anzuzeigen. Um den Pfad des Verzeichnis zu definieren werden Parameter-Werte aus der Konfigurationsdatei `/etc/syslog.conf` benutzt.

- **Verbose level** – Stufe der Protokollgenauigkeit der Information, welche in Module-Protokoll des Kaspersky Anti-Spam geschrieben wird. Als Wert für den Parameter kann benutzt werden: **minimum**, **low**, **normal**, **high**, **debug**, **more debug**. Bei Wertvergabe sollen Sie beachten, dass die Einstellungen der Konfigurationsdatei `/etc/syslog.conf` abhängig von der Kategorie die Protokollgenauigkeit-Stufe beeinträchtigen können (**syslog facility**). Z. B., in FreeBSD Standardmäßiger Wert für Kategorie **mail** ist **mail.info**; auch wenn dem Parameter **Verbose level** Wert **more debug** **vergeben ist, wird die** Protokollgenauigkeit-Stufe durch standardmäßig en Wert gesenkt.



Stufe der Protokollgenauigkeit **more debug** führt zu höherer Server-Belastung und kann so zum Senken der Leistungsfähigkeit führen. Bitte, benutzen Sie diese Stufe nur während Fehlsuche.



Abbildung 18. Allgemeine Einstellungen des Filterungsservers

Nachdem die allgemeine Parameter geändert sind, klicken Sie auf die Schaltfläche **Apply** und starten den Server neu, in dem Sie folgenden Befehl ausführen:

```
# /etc/init.d/kas3 restart
```

unter Linux-Betriebssystem;

```
# /usr/local/etc/rc.d/kas3.sh restart
```

unter FreeBSD-Betriebssystem.

4.5.2. Parameter des Master-Filterungsprozesses

Seite **Settings** → **Anti-Spam Engine** → **Process Server** enthält folgende Parameter des Master-Filterungsprozesses (s. Abb. 19):

- **Max. number of filtration processes** – Maximale Anzahl der Filterungsprozesse, welche gleichzeitig gestartet werden. Standardmäßiger Wert: **10**.
- **Number of filtration processes at server start-up** – Anzahl der Filterungsprozesse, welche beim Start des Filterungsserver gestartet werden. Standardmäßiger Wert ist **0**; das heißt, dass die Filterungsprozesse nur nach Einkommen der Nachrichten gestartet werden.
- **Number of spare filtration processes** – Maximale Anzahl der gestarteten Filterungsprozesse, welche in Anfrage-Wartezustand sind.

Wenn die Anzahl der Prozesse vorgegebener Begrenzung übersteigt, wird Zwangsbeenden der nicht benutzten Prozesse ausgeführt. Standardmäßiger Wert: **0**.

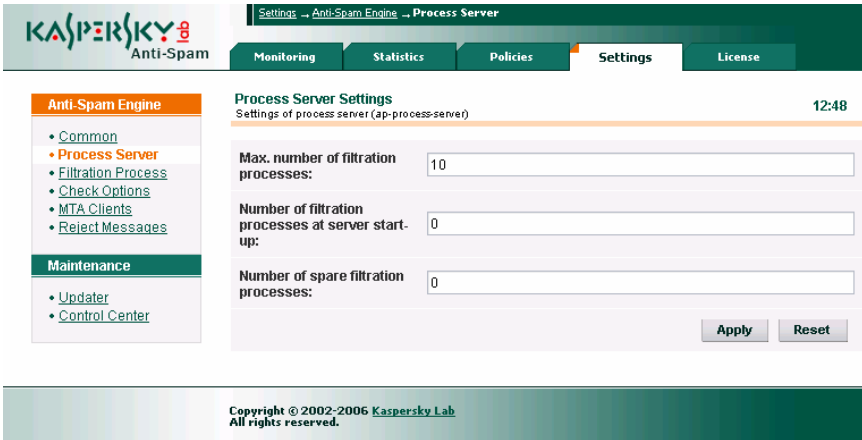


Abbildung 19. Параметры работы мастер-процесса фильтрации

Nach dem die Parameter des Master-Filterungsprozesses geändert sind, klicken Sie auf die Schaltfläche **Apply** und starten den Server neu, in dem Sie folgenden Befehl ausführen:

```
# /etc/init.d/kas3 restart
```

unter Linux-Betriebssystem;

```
# /usr/local/etc/rc.d/kas3.sh restart
```

unter FreeBSD-Betriebssystem.

4.5.3. Parameter der Filterungsprozesse

Seite Settings → Anti-Spam Engine → Filtration Process (s. Abb. 20) **enthält** folgende Parameter der Filterungsprozesse *ap-mailfilter*:

- **Max. number of mail messages to be processed** – Maximale Anzahl der Nachrichten, die vom Filterungsprozess bearbeitet werden. Nach dem die vorgegebene Anzahl der Nachrichten bearbeitet wurde, wird Filterungsprozess beendet, und es wird ein neuer Filterungsprozess gestartet. Abhängig von der Serverauslastung kann dieser Parameter geändert werden. Empfohlener Wert: **300**.
- **Max. number of mail messages randomization** – dieser Wert wird von Kaspersky Anti-Spam zum Bestimmen der maximalen Anzahl der Nachrichten, welche von dem Filterungsprozess bearbeitet werden

können. Für jeden Filterungsprozess diese Anzahl wird zufällig aus dem Bereich ausgewählt, dessen niedrigste Grenze von der Zahl **Max. number of mail messages to be processed**, und höchste aus der Summe der Zahlen **Max. number of mail messages to be processed** und **Max. number of mail messages randomization** errechnet wird. Daher, wenn die Werte entsprechend **300** und **30** sind, dann jeder der Filterungsprozesse wird von 300 bis 330 Nachrichten bearbeiten. Diese Einstellung erlaubt der Situation zu entgehen, dass mehrere Filterungsprozesse in den Spitzenzeiten der Auslastung beendet und gestartet werden.

- **Max. idle time (in seconds)** – maximaler Zeitraum (in Sekunden), während dessen ein Filterungsprozess im Wartezustand sein kann. Wenn in dem Zeitraum Filterungsprozess keine Aufgabe bekommt, dann wird seine Arbeit beendet. Standardmäßiger Wert: **300**.
- **Exit delay (in seconds)** – maximale Verzögerungszeit (in Sekunden) beim Beenden des Filterungsprozesses. Standardmäßig ist dem Parameter der Wert **0** vergeben, das heißt, dass nach dem Befehl den Prozess zu beenden, wird Filterungsprozesses sofort nach Bearbeitung der Nachricht beendet wird.

The screenshot displays the 'Filtration Process Settings' page in the Kaspersky Anti-Spam 3.0 interface. The page title is 'Filtration Process Settings' with a timestamp of 12:48. Below the title, it specifies 'Single/individual filtration process settings (ap-mailfilter)'. The settings are as follows:

Parameter	Value
Max. number of mail messages to be processed:	300
Max. number of mail messages randomization:	30
Max. idle time (in seconds):	300
Exit delay (in seconds):	0

At the bottom right, there are 'Apply' and 'Reset' buttons. The footer of the interface reads: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Abbildung 20. Parameter der Filterungsprozesse

4.5.4. Spamerkennungsparameter

Die Seite Settings → Anti-Spam Engine → Check Options (s. Abb. 21) enthält folgende Parameter der Filterungsprozesse *ap-mailfilter*.

- **Number of 'Received' headers to be parsed while retrieving ip address (for use in DNSBL checks)** – dieser Parameter gibt an, dass die

Zwischenserver mit Hilfe DNSBL-Dienstes überprüft werden sollen. Es ist üblich, dass beim Überprüfen der Absender-IP-Adresse nur die IP-Adresse des Absendeservers überprüft wird. Wenn aber die Nachricht einen oder mehrere Zwischenserver passiert, wird die Absendeserver-IP-Adresse versteckt. Um die Adressen-Überprüfung nicht nur Absendeserver-IP-Adresse, sondern auch der Zwischenserver einzuleiten, setzen Sie mit Hilfe dieses Parameters die Anzahl zu überprüfenden Zwischenserver. Die Analyse wird mit Hilfe des Headers Received *durchgeführt*. Wert **0** bedeutet, dass die Analyse des Headers Received nicht durchgeführt wird.



Ein höherer Wert des Parameters zeigt dem Filterungsserver, dass eine größere Anzahl der Zwischenserver überprüft werden soll. Einerseits erhöht es die Wahrscheinlichkeit, dass Spam erkannt wird, andererseits erhöht es die Auslastung des Filterungsservers und kann zu Fehlfunktionen des Filters führen.

- **Overall timeout of all DNS requests (in seconds)** – Wartezeit (in Sekunden) auf Antwort von einem DNS-Server bei den auf DNS basierten Überprüfungen. Standardmäßiger Wert: **10**.
- **Check MS Word and RTF files** – dieser Parameter schaltet die Untersuchung der Texteinlagen, z. B., Word Document (doc) und RTF, ein und aus.

The screenshot shows the 'Settings → Anti-Spam Engine → Check Options' page. The left sidebar contains a navigation menu with categories like 'Anti-Spam Engine' (containing Common, Process Server, Filtration Process, Check Options, MTA Clients, and Reject Messages) and 'Maintenance' (containing Updater and Control Center). The main content area is titled 'Check Options' and 'Settings of different check options' with a timestamp of 13:41. It features several settings:

- Number of 'Received' headers to be parsed while retrieving ip address (for use in DNSBL checks):** 12
- Overall timeout of all DNS requests (in seconds):** 10
- Check MS Word and RTF files:**
- UDS enabled:**
- Timeout for receiving response from UDS server (in seconds):** 10

At the bottom right of the settings area are 'Apply' and 'Reset' buttons. The footer of the interface contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Abbildung 21. Spamerkennung Parameter

- **UDS enabled** – dieser Parameter schaltet den Überprüfungsmodus mit Hilfe UDS-Dienstes ein und aus. Diese Überprüfungsmethode erlaubt schnell Versandlisten zu Blockieren, ohne auf Update der Inhaltsfilterung-Datenbanken zu warten. Es wird empfohlen die Überprüfungen über UDS nur dann auszuschalten, wenn die Methode erheblich die Auslastung des Servers steigert oder wenn es keine Möglichkeiten gibt die Zusammenarbeit mit den UDS-Server von Kaspersky Lab zu gewährleisten.

Mehr über UDS-Dienst s. Pkt. 2.2.4 auf S. 20.

- **Timeout for receiving response from UDS server (in seconds)** – Timeout für Verbindungsaufbau zwischen Filterungsserver und UDS-Server. Wenn während der Zeitspanne Filterungsserver keine Antwort von dem UDS-Server bekommt, wird versucht eine Verbindung mit dem nächsten UDS-Server von Kaspersky Lab aufzubauen.

4.5.5. Einstellungen von Clientmodulen

Die Seite Settings → Anti-Spam Engine → MTA Clients (s. Abb. 22), enthält Einstellungen für Clientmodule, welche für die Zusammenarbeit des Mailserver und Filterungsserver verantwortlich ist:

- **Filtering size limit (KB)** – maximale Grösse der Nachrichten, die vom Filterungsserver bearbeitet werden (in KB). Wenn Grösse der Nachricht den definierten Wert übersteigt, wird keine Überprüfung durchgeführt. Standardmäßiger Wert: **500**.
- **On filtering error** – damit wird die Reaktion des Clientmodules bei Fehler während des Zusammenwirkens mit dem Filterungsserver definiert. Dem Parameter können folgende Werte vergeben werden:
 - **accept message** – wenn ein Fehler auftritt, wird die Nachricht dem Empfänger übergeben, ohne Bearbeitung durch Filterungsserver;
 - **reject message** – Zustellung der Nachricht, bei Bearbeitung welcher ein Fehler auftritt, wird nicht ausgeführt;
 - **generate temporary error** – Zustellung der Nachricht wird nicht ausgeführt, dem Absender wird eine Meldung über temporären Mailserver-Fehler verschickt. Normalerweise, versucht Absender-Server die Nachricht noch ein Mal zu verschicken.
- **Default domain** – Mail-Domänen Name, welche standardmäßig in die E-Mail-Adresse eingesetzt wird, wenn keine Domäne angegeben wurde. Z.

B., wenn als standardmäßige Domäne mycompany.com *angegeben ist*, wird die Adresse someuser als someuser@mycompany.com *interpretiert*.

- **Connection timeout (in seconds)** – Timeout (in Sekunden) für die Verbindung zwischen dem Clientmodul und Filterungsserver. Standardmäßiger Wert: **40**.
- **Data exchange timeout (in seconds)** – Timeout (in Sekunden) für die Ausführung der Lese- und Schreiboperationen zwischen dem Clientmodul und Filterungsserver. Standardmäßiger Wert: **30**.



Wenn Fehler regelmässig auftreten, wenden Sie sich an den technischen Support des Kaspersky Lab. Kontaktinformationen finden .

The screenshot shows the Kaspersky Anti-Spam web interface. The top navigation bar includes 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Settings' tab is active, displaying 'MTA Clients Settings' with a timestamp of 12:50. The settings are for 'Common settings of MTA clients' and include the following fields:

- Filtering size limit (KB): 500
- On filtering error: accept message
- Default domain: localhost
- Connection timeout (in seconds): 40
- Data exchange timeout (in seconds): 30

Buttons for 'Apply' and 'Reset' are located at the bottom right of the settings area. A sidebar on the left contains navigation links for 'Anti-Spam Engine' (Common, Process Server, Filtration Process, Check Options, MTA Clients, Reject Messages) and 'Maintenance' (Updater, Control Center). The footer contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Abbildung 22. Einstellungen der Clientmodule

4.5.6. Benachrichtigung über E-Mailablehnung

Wenn als Aktion an E-Mail beim bestimmten Status **Reject this message** angegeben ist, wird Filterungsserver diese Nachrichten nicht an den ursprünglichen Empfänger weiter leiten. Dabei wird an den Absender eine Meldung über Unmöglichkeit der Zustellung gesendet.

Filterungsserver benutzt zwei Arten von Meldungen. Die Benutzung einer oder anderen Art wird von Produkteinstellungen und Erkennungsergebnissen bestimmt.

Die erste Meldungsart – **Reject message**. Diese Meldung wird an den Absender direkt während die SMTP-Sitzung zusammen der Fehlercode verschickt, welche meldet, dass die Nachricht nicht zugestellt wurde. Folgender Beispiel der SMTP-Sitzung enthält den Meldungstext **Reject message**:

```
Server: 220 mail.mycompany.com ESMTP
Client: HELO spamhost.whatever.com
Server: 250 mail.mycompany.com
Client: MAIL FROM: <spamer@whatever.com>
Server: 250 Ok
Client: RCPT TO: <someuser@mycompany.com>
Server: 250 Ok
Client: DATA
Server: 354 End data with <CR><LF>.<CR><LF>
Client: >>>
Client: >>> Meldungstext...
Client: >>>
Client: .
Server: 550 The message is rejected by spam
filtering engine.
Client: QUIT
Server: 221 Bye...
```

Filterungsserver benutzt Meldungen **Reject message** nur denn, wenn nach der Überprüfung das Weiterleiten der E-Mail an alle Empfänger verboten ist.

Wenn E-Mail an mehrere Empfänger adressiert ist und für mindestens einen von Benutzer Empfang der E-Mail nach Filterungsrichtlinien erlaubt ist, wird während der SMTP-Sitzung der Server melden, dass E-Mail angenommen wurde. Danach wird an den Absender die Meldung **Bounce message** verschickt, zusammen mit den Empfängerinformationen, an welche die E-Mail nicht zugestellt wurde.

Zur Modifikation der Meldungstexte dient die Seite der Verwaltungszentrale **Settings** → **Anti-Spam Engine** → **Reject Messages** (s. Abb. 23).

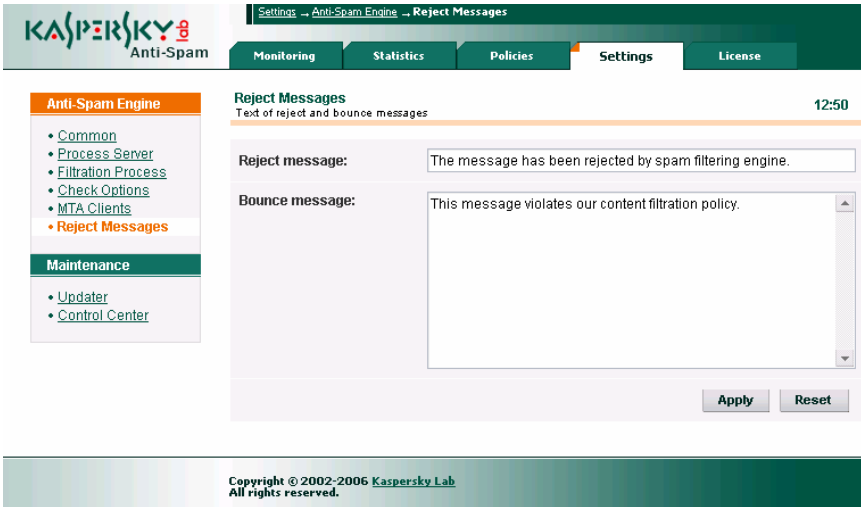


Abbildung 23. Benachrichtigung über E-Mailablehnung

4.6. Einstellungen der Verwaltungszentrale

Die Seite **Settings** → **Maintenance** → **Control Center** (s. Abb. 24), enthält Parameter, Benutzung dessen erlaubt Ihnen:

- Eine Adresse angeben, an welche die Meldungen des Monitoring-Systems verschickt werden, wie auch Meldungen über Fehler, welche während der Skriptausführung mit Hilfe des Dienstes cron passieren (Parameter **Send alerts to**);
- Monitoring des HTTP-Servers `kas-thttpd` ein- und ausschalten (Parameter **Monitoring of kas-thttpd daemon**);
- Monitoring des Clientmoduls `kas-milter`, welcher zur Zusammenwirkung mit dem Mailserver `Sendmail` benutzt wird, ein- und ausschalten (Parameter **Monitoring of kas-milter daemon**).

Meldungen, welche während des Monitoringsprozesses der Module `kas-thttpd` und `kas-milter` erstellt werden, werden auf der Seite **Monitoring** → **Anti-Spam Engine** angezeigt (s. Pkt. 4.8.1.1 auf S. 75).

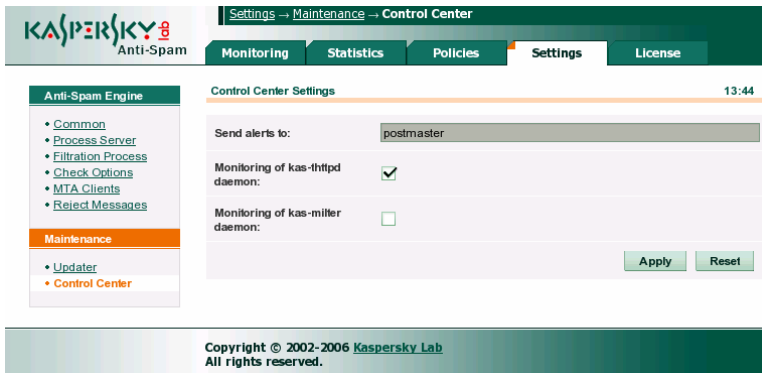


Abbildung 24. Einstellungen der Verwaltungszentrale

4.7. Verwaltung von Lizenzschlüsseln

Das Benutzen von Kaspersky Anti-Spam hängt von dem Vorhandensein eines *Lizenzschlüssels*. Der Lizenzschlüssel gehört zum Lieferumfang des Produktes und gibt Ihnen das Recht zur Nutzung der Anwendung von dem Tag an, an dem die Lizenz erworben und installiert wurde.



Ohne einen Lizenzschlüssel funktioniert Kaspersky Anti-Spam NICHT! Alle E-Mails werden ohne Filterung durch gelassen.

Lizenzschlüssel enthält alle mit der Lizenz verbundene Informationen, dazu zählen: Typ der Lizenz, Ende der Gültigkeitsdauer der Lizenz, Händlerinformationen, usw.

Während der Gültigkeitsdauer der Lizenz bekommen Sie neben dem Recht zur Nutzung der Anwendung folgende Möglichkeiten:

- Technische Unterstützung (rund um die Uhr);
- Update der Inhaltsfilterung-Datenbanken alle zwanzig Minuten.

Bei Ablauf der Gültigkeitsdauer der Lizenz behält die Anwendung ihre Funktionalitäten bei, außer Update der Inhaltsfilterung-Datenbanken. Sie können denn weiterhin die Filterung ausführen, werden aber dabei die Datenbanken, welche zur Auslaufzeit des Lizenzschlüssels aktuell waren. Daher wird Kaspersky Anti-Spam nicht mehr effektiv neue Arten vom Spam bekämpfen.

Aus diesem Grund ist es sehr wichtig, rechtzeitig die Lizenz auf Nutzung von Kaspersky Anti-Spam zu verlängern. Es ist auch möglich ein

Ersatzlizenzschlüssel zu installieren, welcher nach Ablauf des aktuellen Lizenzschlüssels vom Produkt benutzt wird.

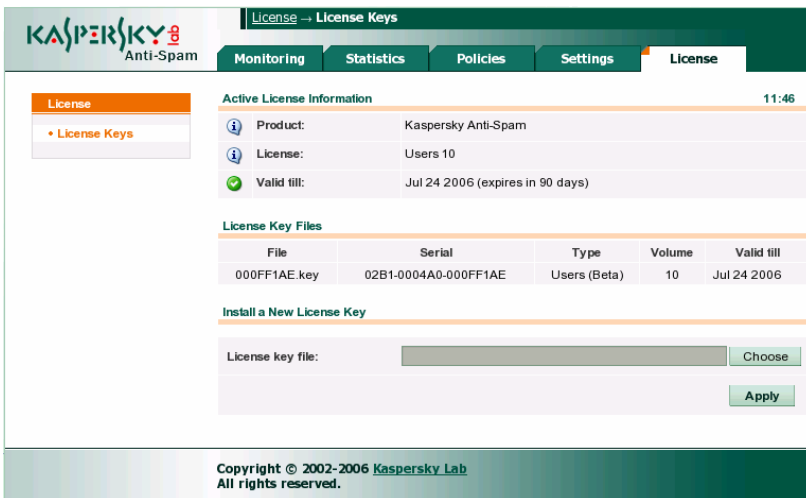
Alle Aktionen, die mit Verwaltung der Lizenzschlüssel verbunden sind, können mit Hilfe der Verwaltungszentrale durchgeführt werden.

4.7.1. Informationen über den Lizenzschlüssel ansehen

Um die Lizenzinformationen anzusehen und zu Verwalten dient eine Seite in der Verwaltungszentrale: **License** → **License Keys** (s. Abb. 25).

In dem oberen Teil der Seite befindet sich Abschnitt **Active License Information**, dieser enthält folgende Informationen:

- Produktname;
- Lizenz-Typ;
- Ablaufzeit der Lizenz;



The screenshot shows the 'License Keys' page in the Kaspersky Anti-Spam administration interface. The page is divided into several sections:

- Active License Information** (11:46):
 - Product: Kaspersky Anti-Spam
 - License: Users 10
 - Valid till: Jul 24 2006 (expires in 90 days)
- License Key Files**:

File	Serial	Type	Volume	Valid till
000FF1AE.key	02B1-0004A0-000FF1AE	Users (Beta)	10	Jul 24 2006
- Install a New License Key**:

License key file:

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

Abbildung 25. Информация о лицензии Kaspersky Anti-Spam

Information in den letzten zwei Zeilen erlaubt dem Systemadministrator die Einhaltung der Lizenzbedingungen einzuhalten (Ablaufzeit, vorgegebene Begrenzungen).

Abhängig von dem momentanen Zustand kann das Piktogramm folgendermaßen aussehen:

- ✔ – Lizenzbedingungen sind erfüllt;
- ! – das Produkt funktioniert unter Grenzbedingungen der Lizenz oder Gültigkeit der Lizenz läuft in zwei Wochen aus;
- ✘ – Der Zeitraum der Lizenzgültigkeit ist abgelaufen oder Grenzwerte wurden überschritten (z. B., Umfang des E-Mail-Vehrkers).

In den letzten zwei Fällen ist ein Erleuterungstext zu sehen.

Unter dem Erleuterungstext befindet sich eine Auflistung der Installierten Lizenzschlüssel von Kaspersky Anti-Spam, zu jedem der Schlüssel ist eine kurze Information zu sehen.

4.7.2. Neuen Lizenzschlüssel installieren

Um einen neuen Lizenzschlüssel zu installieren, kann der Systemadministrator entweder die Verwaltungszentrale benutzen, oder die Installation lokal aus der Befehlszeile ausführen.



Um einen neuen Lizenzschlüssel mit Hilfe der Verwaltungszentrale zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Seite der Lizenzschlüssel-Verwaltung License → License Keys.
2. In dem Feld, welcher sich in dem unteren Teil der Seite befindet, im Abschnitt **Install a New License Key**, geben Sie den Pfad zu der Lizenzschlüssel-Datei an oder benutzen Sie die Schaltfläche „Durchsuchen“ rechts von dem Feld um die Lizenzschlüssel-Datei auszuwählen.
3. Klicken Sie auf die Schaltfläche **Apply**.



Um einen neuen Lizenzschlüssel lokal mit Hilfe der Befehlszeile zu installieren, führen Sie folgenden Befehl aus:

```
# /usr/local/ap-mailfilter3/bin/install-key <key>
```

wo **key** – Pfad zur Lizenzschlüssel-Datei ist.

Wenn Sie einen neuen Lizenzschlüssel vor der Ablaufzeit des alten installieren wollen, dann können Sie den Lizenzschlüssel als ein Reserve-Lizenzschlüssel hinzufügen. Reserve-Lizenzschlüssel nimmt seine Funktion auf, wenn der aktuelle Lizenzschlüssel seine Gültigkeit verliert. Gültigkeitsdauer des Lizenzschlüssels wird von dem Moment der Aktivierung gezählt. Es kann nur ein Reserve-Lizenzschlüssel installiert werden.

4.7.3. Lizenzschlüssel entfernen

Um den aktuellen Lizenzschlüssel und den Reserve-Lizenzschlüssel zu entfernen, geben Sie in der Befehlszeile ein:

```
# /usr/local/ap-mailfilter3/bin/remove-key -a
```

Um den Reserve-Lizenzschlüssel zu entfernen, geben Sie in der Befehlszeile ein:

```
# /usr/local/ap-mailfilter3/bin/remove-key -r
```



Lizenzschlüssel können nicht mit Hilfe der Verwaltungszentrale entfernt werden.

4.8. Monitoring des Filterungsservers

Kaspersky Anti-Spam enthält ein Monitoring-System einzelne Produktkomponente. Monitoring-System erlaubt Ihnen die Arbeit des Produktes zu kontrollieren, wie auch den Administrator mit Hilfe des Verwaltungszentrale-Interface über Systemfehler zu informieren.

4.8.1. Allgemeine Informationen über Produktzustand

Die Seite, welche sich unter Adresse **Monitoring** → **General Status** befindet, zeigt dem Administrator kurz gefasste Informationen über Kaspersky Anti-Spam und den Zustand seine Hauptkomponente (s. Abb. 26).




Für jede der kontrollierten Komponente kann die Seite, außer Zustandinformation, auch Informationen über Ereignisse enthalten, welche mit der Komponente verbunden sind.

The screenshot displays the 'Monitoring - General Status' window of Kaspersky Anti-Spam. The interface includes a navigation menu with 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' section is active, showing a sidebar with links to 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area is divided into two sections: 'System Information' and 'Kaspersky Anti-Spam'. The 'System Information' section lists 'Host Name: mail.test.local', 'System: FreeBSD 5.4-RELEASE-p7 i386', and 'Load Average: 0.13'. The 'Kaspersky Anti-Spam' section lists 'Product: Kaspersky Anti-Spam Enterprise Edition', 'Version: 3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45', 'Anti-Spam Engine: Errors...', 'Updates: OK', and 'License: Errors...'. Each item is accompanied by a status icon: a blue 'i' for information, a green checkmark for OK, and a red 'x' for errors.

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

Abbildung 26. Allgemeine Informationen über Komponente von Kaspersky Anti-Spam

Ein zusätzliches Mittel der Zustanddarstellung sind die Piktogramme, welche sich neben den Namen der Parameter befinden. Ein Piktogramm zeigt den Zustand der Komponente an:

-  – Fehler: ein Fehler in der Arbeit oder die Grenzwerte des kontrollierten Parameters sind überschritten.
-  – Warnung: es sind unkritische Fehler bei der Arbeit der Komponente aufgetreten, welche die Arbeit des Produktes insgesamt nicht beeinträchtigen oder kontrollierter Parameter ist sehr nah an den Grenzwerten.
-  – Normaler Zustand: die Komponente funktioniert korrekt oder der kontrollierter Parameter enthält zulässige Werte.

Abschnitt **System Information** enthält folgende Informationen über den Server, auf dem Kaspersky Anti-Spam installiert ist:

- **Host Name** – Servername.
- **System** – Bezeichnung, Version und Architektur des Betriebssystems.
- **Load Average** – Zahlenparameter, welcher Serverauslastung widerspiegelt. Details über den Parameter s. manual pages für Werkzeuge *top* und *uptime*.

Abschnitt **Kaspersky Anti-Spam** bietet eine Zusammenstellung der Produkt-Informationen und Informationen über Zustand seine Hauptkomponente. Abschnitt enthält folgende Felder:

- **Product** – voller Produktname.
- **Version** – Version- und Build-Info des Filterungsmoduls.
- **Anti-Spam Engine** – Zustand des Filterungsserver.
- **Updates** – Zustand der Inhaltsfilterung-Datenbanken und Updatesystems.
- **License** – Zustand des Lizenzierungsmoduls.

4.8.1.1. Detaillierte Information über Filterungsserver-Kernel

Beim Klick auf den Link Anti-Spam Engine, der sich in dem Menü **Monitoring** befindet, gehen Sie zur Seite über, welche Detaillierte Information über Filterungsserver-Komponente enthält (s. Abb. 27).

The screenshot shows the Kaspersky Anti-Spam Monitoring interface. The main title is 'Monitoring - Anti-Spam Engine'. The navigation menu includes 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' tab is selected, showing a table of system components and their status. The table has columns for 'Component', 'Status', and 'Details'. The components listed are: Version (3.0.0 [0232] KAS30/Release, built at May 17 2006, 17:57:59), ap-process-server (OK, pid=70527), ap-mailfilter (OK, processes: 0), ap-spf (OK, processes: 17), kas-httplib (OK, pid=71493), and Monitoring & Statistics (OK). Below the table is a section for 'Last Anti-Spam Engine Events' with a 'View' dropdown set to 'Notifications, Warnings and Errors'. The events list shows two restarts: '05:22 13:50:48 kas-restart: kas-milter is restarted' and '05:22 12:50:42 kas-restart: No ap-mailfilter processes running'.

Component	Status	Details
Version:		3.0.0 [0232] KAS30/Release, built at May 17 2006, 17:57:59
ap-process-server:	OK	pid=70527
ap-mailfilter:	OK	processes: 0
ap-spf:	OK	processes: 17
kas-httplib:	OK	pid=71493
Monitoring & Statistics:	OK	

Last Anti-Spam Engine Events

View: Notifications, Warnings and Errors

05:22 13:50:48	kas-restart: kas-milter is restarted
05:22 12:50:42	kas-restart: No ap-mailfilter processes running

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

Abbildung 27. Monitoringseite des Kernels von dem Filterungservers

Abschnitt **Anti-Spam Engine** enthält folgende Felder:

- **Version** – Version- und Build-Info des Filterungsmoduls.

- **ap-process-server** – Zustand des Master-Filterungsprozesses. Wenn Prozess normal funktioniert, enthält die Zeile auch die Prozess-ID (**pid**).
- **ap-mailfilter** – Zustand der Filterungsprozesse. Wenn alle Funktionen in Ordnung sind, enthält die Zeile Informationen über Anzahl der aktuellen Prozesse.
- **ap-spf** – Zustand des SPF-Hintergrundprogramms. Wenn das Hintergrundprogramm normal funktioniert, wird in der Zeile Anzahl der ausgeführten Prozesse angezeigt.
- **kas-thttpd** – Zustand des HTTP-Servers, welcher von Verwaltungszentrale benutzt wird.
- **Monitoring & Statistics** – Informationen über Skripts, welche mit dem Monitoring und Statistikbearbeitung verbunden sind. Außerdem, wird das Vorhandensein der cron-Starttasks für diese Skripts überprüft, unter Benutzerkennung **mailfit3**. Details s. Pkt. A.6 auf S. 123.

Abschnitt **Last Anti-Spam Engine Events** enthält Meldungen der Komponente des Filterungsservers, welche in das Systemprotokoll eingetragen wurden (syslog). Die Meldungen sind absteigend nach Datum sortiert und mit Piktogrammen versehen, welche auf die Wichtigkeitsstufe der Meldung hinweisen. Mit Hilfe des dropdown Liste **View** hat der Administrator die Möglichkeit die Kategorie der anzuzeigenden Meldungen zu bestimmen. Die Dropdown Liste enthält folgende Werte:

- **All messages** – alle Meldungen anzeigen;
- **Notices, Warnings and Errors** – alle Meldungen, Außer Informationsmeldungen anzeigen;
- **Warnings and Errors** – nur kritische Fehler und Warnungen anzeigen;
- **Errors only** – nur kritische Fehler anzeigen.

4.8.1.2. Detaillierte Information über Updatemodul

Um zu der Seite mit den Informationen über Updatemodul und Inhaltsfilterung-Datenbanken zu gelangen, benutzen Sie den Link [Updates](#), welcher sich im Menü Monitoring **befindet** (s. Abb. 28).

Abschnitt **Anti-Spam Updates**, welcher sich in dem oberen Teil der Seite befindet, enthält folgende Felder:

- **Automatic Updates** – dieses Feld zeigt, ob die automatischen Updates der Inhaltsfilterung-Datenbanken eingeschaltet sind. Details über die

Einstellungen der Inhaltsfilterung-Datenbanken s. Pkt. 4.4.1 auf S. 56 und P. A.6 auf S. 123.

- **Anti-Spam Database Id** – Informationen über installierte Inhaltsfilterung-Datenbanken: Datum und Urzeit der Publikation, wie auch Informationen über letzte Updates.
- **Last Update** – Datum und Urzeit des letzten Updates von Inhaltsfilterung-Datenbanken. Das Monitoring-System zeigt Warnungen an, wenn die Inhaltsfilterung-Datenbanken über eine lange Zeit nicht upgedatet wurden.

The screenshot displays the 'Monitoring - Updates' interface. On the left, a navigation menu includes 'Monitoring', 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area is titled 'Monitoring: Updates' with a timestamp of 13:34. It lists three items: 'Automatic Updates: Enabled' with a green checkmark; 'Anti-Spam Database Id: Daily update 17.02.2006 (day060217) + Recent 21.02.06 12:44:00 (MSK)' with an information icon; and 'Last Update: 2006-02-21 13:13' with a green checkmark. Below this is the 'Last Updater Events' section, which has a 'View' dropdown menu set to 'Notifications, Warnings and Errors'. It contains a list of three events, each marked with a green checkmark: '02-21 13:33:02 sfupdates: Data are up to date (upd time = 21.02.06 12:44:00 (MSK))', '02-21 13:13:11 sfupdates: New data installed (upd time = 21.02.06 12:44:00 (MSK))', and '02-21 11:09:05 sfupdates: New data installed (upd time = 21.02.06 10:44:00 (MSK))'. The footer of the page contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab All rights reserved.'

Abbildung 28. Monitoringseite des Updatesmoduls

Abschnitt **Last Updater Events** enthält Protokoll der Meldungen des Produktupdatesystems, diese Meldungen sind in das Systemprotokoll (syslog) eingetragen. Die Meldungen sind absteigend nach Datum sortiert und mit Piktogrammen versehen, welche auf die Wichtigkeitsstufe der Meldung hinweisen. Mit Hilfe der dropdown Liste **View** hat der Administrator die Möglichkeit die Kategorie der anzuzeigenden Meldungen zu bestimmen. Die Werte des Dropdown-Menüs und dessen Bedeutung sind den Werten gleich, welche auf der Seite des Monitorings vom Filterungsserver aufgeführt sind (s. Pkt. 4.8.1.1 auf S. 75).

4.8.1.3. Detaillierte Information über Lizenzierungsmodul

Die Seite, welche unter Monitoring → License Information über Updatemodul zu finden ist, liefert dem Administrator die Informationen über benutzte Lizenz, wie auch die einen Protokoll der Meldungen des Lizenzierungsmoduls (s. Abb. 29).

Abschnitt **Monitoring** → **License**, welcher sich in dem oberen Teil der Seite befindet, enthält folgende Felder:

- **Product** – Bezeichnung des installierten Produktes.
- **License** – Lizenztyp und Informationen über Lizenzbegrenzungen.

The screenshot displays the 'Monitoring → License' page in the Kaspersky Anti-Spam administration console. The interface includes a navigation menu on the left with options like 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area is titled 'Monitoring: License' and shows the following details:

- Product:** Kaspersky Anti-Spam
- License:** Users 10
- Valid till:** Jul 24 2006 (expires in 90 days)
- License Daemon:** OK, pid=15994

Below this information is a section for 'Last License Daemon Events' with a 'View' dropdown menu set to 'Notifications, Warnings and Errors'. The event log shows four entries:

- 04-24 19:17:17 install-key: Key file /usr/local/ap-mailfilter3/conf/ik-license/000FF1AE.key has been installed.
- 04-24 19:16:53 remove-key: License key was successfully removed.
- 04-24 19:13:47 install-key: Key file /usr/local/ap-mailfilter3/conf/ik-license/black-0010617B.key has been installed.
- 04-24 19:13:30 remove-key: License key was successfully removed.

The footer of the page contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Abbildung 29. Страница мониторинга работы модуля лицензирования

- **Valid till** – Auslaufdatum der Lizenz. Das Monitoring-System warnt den Administrator einen Monat vor dem Auslaufen der Lizenz;
- **License Daemon** – Zustand des Lizenzierungsdienstes. Wenn der Dienst normal funktioniert, wird in dem Feld auch Process-ID (**pid**) angezeigt.

Abschnitt **Last License Daemon Events** enthält ein Meldungsprotokoll des Lizenzierungsdienstes, diese Meldungen sind in das Systemprotokoll (syslog) eingetragen. Die Meldungen sind absteigend nach Datum sortiert und mit Piktogrammen versehen, welche auf die Wichtigkeitsstufe der Meldung hinweisen. Mit Hilfe des dropdown Liste **View** hat der Administrator die

Möglichkeit die Kategorie der anzuzeigenden Meldungen zu bestimmen. Die Werte des Dropdown-Menü und dessen Bedeutung sind den Werten gleich, welche auf der Seite des Monitorings vom Filterungsserver aufgeführt sind (s. Pkt. 4.8.1.1 auf S. 75).

4.8.2. Meldungen und Berichte des Monitoringssystems

Außer Monitoring-Werkzeuge, welche Verwaltungszentrale Ihnen zur Verfügung stellt, enthält Kaspersky Anti-Spam ein Skript *sfmonitoring*, welcher eine ständige Kontrolle des Filterungsserver gewährleistet. Das Starten dieses Skriptes wird automatisch von dem Dienst *cron* durchgeführt. Nach dem Start führte *sfmonitoring* die Untersuchung des Filterungsserver-Zustandes und im Fall, dass Fehler in der Arbeit des Filterungservers auftreten, wird an den Administrator eine Meldung darüber verschickt.

Es gibt zwei Meldungsarten, welche an den Administrator von dem Monitoring-Skript verschickt werden:

- **Meldungen über neu entdeckte Fehler** – Meldungen über bei der Arbeit des Filterungservers entdeckte Fehler, diese Meldungen enthalten eine Beschreibung der Situation. Fehlermeldung wird einmalig verschickt. Wenn das Problem nicht behoben wird, wird die Fehlermeldung in den täglichen Bericht über bekannte Probleme aufgenommen.
- **Tägliche Berichte über bekannte Probleme** – eine Auflistung aller Fehler und Warnungen, welche zur Zeit der Berichterstellung bekannt sind. In den Bericht werden wie neue Fehler, so auch früher entdeckte, aber zur Zeit der Berichterstellung nicht behobene Fehler aufgenommen. Dieser Bericht wird ein Mal in 24 Stunden, um Mitternacht, erstellt (der Serverzeit entsprechend). Um den Versand des Berichtes zu erzwingen, führen Sie folgenden Befehl unter Benutzerkennung **root** aus:

```
# su -m mailflt3 -c '/usr/local/ap-  
ailfilter3/control/  
bin/sfmonitoring -m'
```

Um den Bericht auf der Konsole anzusehen:

```
# su -m mailflt3 -c '/usr/local/ap-  
ailfilter3/control/  
bin/sfmonitoring -p'
```



Wenn Kaspersky Anti-Spam auf dem Server mit dem RedHat-Distributiv installiert ist, denn benutzen Sie zum Starten von *sfmonitoring* folgendes Befehl:

```
su - -m mailflt3 -c '/usr/local/ap-
```

```
mailfilter3/control/bin/sfmonitorin  
g  
-<Parameter>'
```

Systemmeldungen werden an die Adresse verschickt, welche auf der Seite Settings → Maintenance → Control center angegeben ist (s. Pkt. 4.6 auf S. 69).

4.9. Statistik von Kaspersky Anti-Spam

Um die quantitative Analyse der Ergebnisse des Produktes durchzuführen, enthält die Verwaltungszentrale einen Modul, welcher für Ansammlung der quantitative Daten über verarbeiteten E-Mails und für die grafische Darstellung der Ergebnisse in dem Interface der Verwaltungszentrale verantwortlich ist.

Sammlung der statistische Daten und deren Verarbeitung führen spezielle Skripte durch, welche mit Hilfe des *cron*-Dienstprogramms gestartet werden (Details zu den Skripten s. Pkt. A.6 auf S. 123). Bearbeitungsergebnisse werden in Form einer Diagramm auf den Seiten des Abschnitts **Statistics** angezeigt (s. Abb. 30).

Jede der Seiten des Abschnitts **Statistics** enthält statistische Information für eine bestimmte Zeitperiode. Links zu den Seiten befinden sich im Menü **Period** in der Linken Seite des Abschnitts **Statistics**:

- Last Day – Statistik der bearbeiteten E-Mail für die letzte 24 Stunden;
- Last Week – Statistik der bearbeiteten E-Mail für die letzte Woche;
- Last Month – Statistik der bearbeiteten E-Mail für den letzten Monat;
- Last Year – Statistik der bearbeiteten E-Mail für das letzte Jahr.

In dem oberen Teil der Seite ist eine Tabelle platziert, welche Gesamtinformation über Anzahl und Grösse der bearbeiteten E-Mails unterschiedlicher Typen enthält.

Unter der Tabelle ist eine graphische Darstellung des Umfangs der erkannten Nachrichten unterschiedlicher Typen zu sehen, nach Zeit sortiert (der gewählten Periode entsprechend), wie auch ein rundes Diagramm, welches prozentuellen Umfangsverhältnis der Nachrichten unterschiedlicher Typen darstellt.

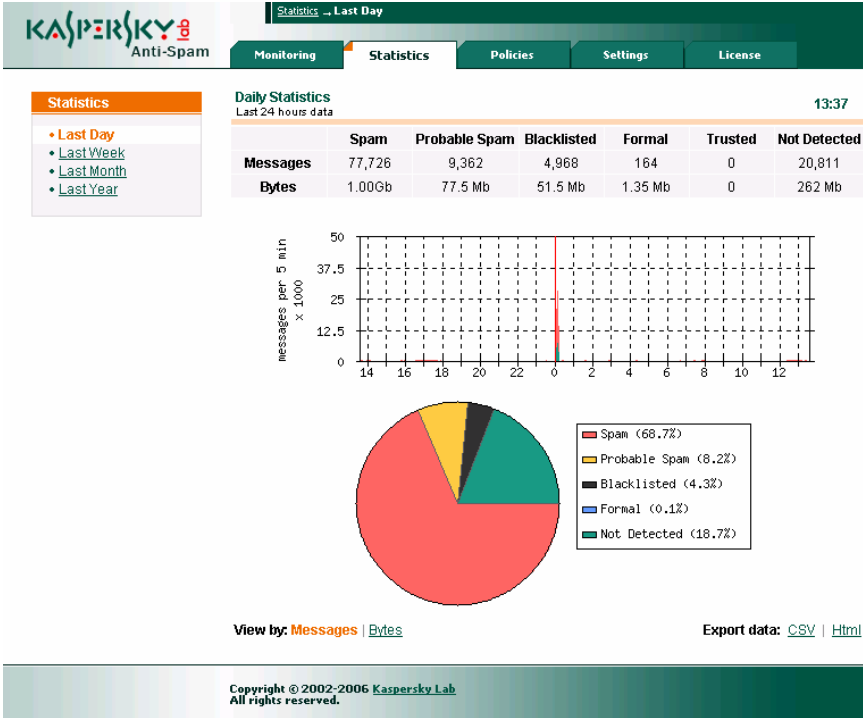


Abbildung 30. Statistik-Seite



Auf dem runden Diagramm wird Umfangsverhältnis der Nachrichten angezeigt. Nachrichten, welche nach Erkennung den gleichen Status bekommen haben, sind mit einem Segment bestimmter Farbe dargestellt. Für Übersichtlichkeit werden Segmente, dessen Größe nicht bedeutend ist, in einen einheitlichen Segment **Other** geschlossen.

Links [Messages](#) und [Bytes](#), welche sich in der linken unteren Ecke befinden, werden zur Auswahl der Einheiten bei der Darstellung der Statistik des bearbeiteten E-Mail-Verkehr - Nachrichten oder Bytes entsprechend.

Links [Export data](#) [CSV](#) | [Html](#), welche sich in der unteren rechten Ecke befinden, werden zum Exportieren der statistischen Daten im Format CSV (Comma Separated Values) oder in eine HTML-Tabelle benutzt.

KAPITEL 5. KASPERSKY ANTI-SPAM DEINSTALLIEREN

Um Kaspersky Anti-Spam deinstallieren zu können müssen Sie **root**-Rechte besitzen. Wenn Sie diese Rechte nicht besitzen, dann müssen Sie sich als Benutzer **root** einloggen.



Deinstallation-Prozess wird automatisch alle Kaspersky Anti-Spam-Dienste anhalten!

Beim Deinstallieren werden die Dienste von Kaspersky Anti-Spam angehalten, bei der Installation erstellte Verzeichnisse und Dateien werden gelöscht. Dennoch vom Administrator erstellte Verzeichnisse und Dateien (Konfigurationsdateien, Inhaltsfilterung-Datenbanken, Lizenzschlüsseldateien) bleiben erhalten. Es werden auch die Parameter von dem Mail-Server wiederhergestellt, die vor der Installation von Kaspersky Anti-Spam aktuell waren.



Wenn die Konfigurationsdatei des Mailservers nach der Installation von Kaspersky Anti-Spam verändert wurde, wird automatisches Wiederherstellen der vorherigen Einstellungen nicht ausgeführt und der Administrator wird die Änderungen, welche vom Produkt bei der Installation gemacht wurden, per Hand entfernen müssen.

Benutzerkennung **mailft3** und entsprechende Gruppe **mailft3** werden aus Sicherheitsgründen nicht entfernt. Diese Einträge können vom Administrator per Hand entfernt werden.

Die Deinstallation kann auf unterschiedlichen Wegen gestartet werden, abhängig von dem Paketmanager:

- Wenn Kaspersky Anti-Spam aus einem rpm-Paket installiert wurde, führen Sie zur Deinstallation in der Befehlszeile folgenden Befehl aus:

```
# rpm -e kas-3-<Version der Distribution>
```

- Wenn Kaspersky Anti-Spam aus einem deb-Paket installiert wurde, führen Sie zur Deinstallation in der Befehlszeile folgenden Befehl aus:

```
# dpkg -P kas-3
```

- Wenn Kaspersky Anti-Spam aus einem tgz- oder tbz-Paket installiert wurde, führen Sie zur Deinstallation in der Befehlszeile folgenden Befehl aus:

```
# pkg_delete kas-3-<Version der Distribution>
```



Da die Integration in den Mailserver Communicate Pro per Hand gemacht wird, sollen Sie vor der Deinstallation aus der Konfigurationsdatei von Communicate Pro die Einstellungen von Kaspersky Anti-Spam entfernen (s. Pkt. A.2.7 auf S. 104).

Wenn Sie die Einstellungen wiederherstellen wollen, welche der Mailserver vor der Installation von Kaspersky Anti-Spam hatte, ohne Produkt zu deinstallieren, benutzen Sie den Skript *MTA-unconfig.pl*, der sich in dem Verzeichnis */usr/local/ap-mailfilter3/bin* befindet. Dieses Skript wird die Parameter des Mailservers wiederherstellen, welche vor der Installation von Kaspersky Anti-Spam benutzt wurden.

Jedoch der oben genannter Skript nicht für die Wiederherstellung der Konfiguration des Mailservers benutzt werden, wenn:

- die Konfigurationsdatei des Mailservers nach der Installation von Kaspersky Anti-Spam geändert wurde;
- Mailserver Exim benutzt wird, und als Clientmodul – kas-exim;
- Mailserver Communicate Pro benutzt wird.

In den beschriebenen Situationen muß der Administrator die Änderungen per Hand aus der Konfigurationsdatei entfernen. Details zu den Änderungen, welche in der Konfiguration der Mailserver bei der Integration des Kaspersky Anti-Spam vorgenommen werden, sind in A.2 auf S. 89 beschrieben.

KAPITEL 6. HÄUFIGE FRAGEN

In diesem Kapitel beantworten wir ausführlich die von Benutzern häufig gestellten Fragen über Installation, Konfiguration und Funktion von Kaspersky Anti-Spam.



Frage: Wofür braucht das Produkt ist ein Lizenzschlüssel? Kann das Produkt ohne einen Lizenzschlüssel funktionieren?

Ohne Lizenzschlüssel funktioniert Kaspersky Anti-Spam nicht.

Wenn Sie sich zum Kauf des Produktes nicht entschlossen haben, können wir Ihnen einen Test-Schlüssel aushändigen (Trial), welcher im Laufe zwei Wochen oder einen Monat funktionieren wird. Danach wird dieser Schlüssel blockiert.



Frage: Was passiert, wenn die Lizenz zur Produktnutzung abläuft?

Bei Ablauf der Gültigkeitsdauer der Lizenz für die Nutzung von Kaspersky Anti-Spam setzt das Produkt seine Arbeit fort, aber die Verwendung neuer Inhaltsfilterung-Datenbanken ist nicht mehr möglich. Kaspersky Anti-Spam wird weiterhin die Filterung des E-Mail-Verkehrs durchführen, wird dabei jedoch die neuen Spam-Arten nicht erkennen können.

Sollte diese Situation eintreten, dann informieren Sie Ihren Systemadministrator oder wenden Sie sich zur Lizenzverlängerung an die Firma, bei der Kaspersky Anti-Virus erworben wurde, oder direkt an Kaspersky Lab Ltd.



Warum sind die regelmässigen Updates erforderlich?

Spam ist ein brennendes Problem für alle Internet-Benutzer, aber für Firmen stellt Spam eine Bedrohung des Geschäfts da. Nach Letzten Erkenntnissen Spamumfang beträgt momentan 75-80% vom dem gesamten Mail-Verkehr und es erscheinen immer neue Versandlisten. Um auf neue Versandlisten schnell zu und die Versandlisten zu blockieren, müssen die Inhaltsfilterung-Datenbanken ständig erneuert werden. Die Updates der Inhaltsfilterung-Datenbanken erscheinen alle 20 Minuten auf den Update-Server von Kaspersky Lab.



Frage: Die Anwendung funktioniert nicht. Was soll ich tun?

Wenn beim Benutze des Produktes Fehler auftreten, sehen Sie als erstes nach, ob das Problem in dieser Dokumentation oder auf Webseite von Kaspersky Lab im Abschnitt **Dienste/Wissensdatenbank** (<http://www.kaspersky.com/de/>) beschrieben ist.

Wenn Sie in der Dokumentation und auf der Webseite keine Lösung für das Problem gefunden haben, empfehlen wir Ihnen sich an das Technische Support von Kaspersky Lab zu wenden.

Bei dringenden Problemen rufen Sie uns an unter der Telefonnummer, welche im Abschnitt **Kontaktinformationen** angegeben ist. Benutzersupport wird 24-Stunden in Russischen, Englischen, Französischen und Deutschen Sprachen geleistet. Um Support zu erhalten, müssen Sie ein registrierter Benutzer sein und Ihre Registriernummer dem Support-Mitarbeiter durchgeben können (wenn sie das Produkt In-Box gekauft haben) oder Bestellnummer und registrierten Kundennamen, wenn Sie unsere Produkte über das Internet gekauft haben.

Außerdem können Sie eine Support-Anfrage an den Technischen Support von Kaspersky Lab stellen im Abschnitt **Dienste/Technischer Support/Support-Anfrage an den Technischen Support von Kaspersky Lab stellen**.

Beim Ausfüllen der Anfrage sollten Sie aufmerksam sein: geben Sie eine genaue Information an über das Produkt von Kaspersky Lab, die Registrierungsinformation und beschreiben Sie das Problem ausführlich. In den erforderlichen Feldern geben Sie an:

- Anfragetyp. Bitte wählen Sie einen passenden Typ für Ihre Anfrage aus.
- Den Namen des benutzten Produkts (z. B., **Kaspersky Anti-Spam 3.0**).
- Anfrage-Text. Bitte beschreiben Sie Ihre Anfrage.
- Registrierungsinformationen. Typ von Registrierungsinformation: Lizenzschlüssel, wenn sie das Produkt In-Box gekauft haben oder Bestellnummer und registrierten Kundennamen, wenn Sie unsere Produkte über das Internet gekauft haben. Abhängig von dem Registrierungstyp geben Sie Serien- oder Bestellnummer ein.

Informationen über Seriennummer von Kaspersky Anti-Spam können Sie der Seite **License** der Verwaltungszentrale entnehmen .

- E-Mail, über die Sie erreichbar sind.

In dem nächsten Fenster geben Sie die Kontaktinformationen, tragen Sie den Schützcode ein und klicken Sie auf die Schaltfläche **Anfrage absenden**. Unsere Support-Mitarbeiter werden das Problem sorgfältig untersuchen und mit Ihnen Kontakt aufnehmen.



Frage: Wie kann ich überprüfen, ob Kaspersky Anti-Spam die Spam-Filterung durchführt?

Um die Funktionsfähigkeit der Filterung zu überprüfen, können Sie ein Muster **GTUBE** (Generic Test for Unsolicited Bulk E-Mail) benutzen. Überprüfung der Spamfilterung mit Hilfe GTUBE ist der Funktionsüberprüfung des Antivirusprogramms mit Hilfe des Testvirus EICAR ähnlich.

Erstellen Sie eine E-Mail, welche folgende Zeile enthalten wird (ohne Leerzeichen und Silbentrennungen):

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-
UBE-TEST-E-MAIL*C.34X
```

und schicken Sie ihn an die von Kaspersky Anti-Spam geschützte E-Mail. Nach der Erkennung wird der E-Mail Status **SPAM** vergeben und die Aktion vorgenommen, welche von der Filterungsrichtlinie definiert ist.



Frage: Bei hoher Auslastung des Kaspersky Anti-Spam führt der Server keine Filterung durch. Bearbeitete Nachrichten erhalten einen Header:

X-SpamTest-Info: Not processed

Höchstwahrscheinlich besteht das Problem daran, dass die Filterungsprozesse in der vorgegebenen Zeit es nicht schaffen, sich mit dem Lizenzierungsmodul (*kas-license*) zu verbinden, um die Lizenzbedingungen zu überprüfen.

Um das Problem zu beheben, erhöhen Sie den Wert Timeout für die Verbindung und Datenaustausch mit dem Modul *kas-license*, welcher die Parameter **FilterLicenseConnectTimeout** und **FilterLicenseDataTimeout** bestimmen. Wenn diese Aktion das Problem nicht löst, wenden Sie sich an den Technischen Support von Kaspersky Lab.



Frage: Kaspersky Anti-Spam führt die Spamfilterung nicht durch. Bearbeitete Nachrichten enthalten Brifkopf:

X-SpamTest-Info: No License

Problemursache ist, dass die Lizenz abgelaufen ist, oder kein Lizenzschlüssel installiert ist. Wergewissern Sie sich, dass der Schlüssel installiert ist oder Lizenz noch gültig ist.



Frage: Kaspersky Anti-Spam führt keine IP-Adressen-Untersuchung Version IPv6 durch, welche dem Header Received entnommen wurden.

Es ist keine Unterstützung der IP-Adressen Version IPv6 in das Produkt Kaspersky Anti-Virus 3.0 eingebaut.



Frage: Die Integration mit dem Mailserver Exim kann nicht mit Hilfe des Skripts MTA-config.pl ausgeführt werden. Es wird folgende Fehlermeldung auf der Konsole angezeigt:

```
Your Exim configuration file
/usr/local/etc/exim/configure already
contains kas-exim local_scan configuration
parameters. If your Exim hasn't been
integrated with kas-exim, remove all
local_scan parameters and try again.
```

Diese Meldung zeigt, dass die Integration schon per Hand durchgeführt wurde mit Hilfe des Moduls kas-exim. Beim Benutzen des Skripts *MTA-config.pl* wird versucht den Clientmodul kas-pipe zu installieren. Löschen Sie die Einstellungen für Zusammenarbeit mit dem Modul kas-exim (Details об использовании kas-exim s. Pkt. A.2.5 auf S. 100) aus der Konfigurationsdatei Exim und wiederholen Sie des Integrationsversuch.

ANHANG A.

ZUSÄTZLICHE INFORMATIONEN ÜBER KASPERSKY ANTI-SPAM

A.1. Anordnung der Dateien in den Verzeichnissen

Nach der Installation von Kaspersky Anti-Spam sind die Dateien folgendermassen verteilt:

/usr/local/ap-mailfilter3/ – Hauptverzeichnis von Kaspersky Anti-Spam, der enthält:

bin/ – Verzeichnis, in dem die ausführenden Dateien und Skripte des Kaspersky Anti-Spam abgelegt sind.

cfdata/ – Verzeichnis zum Speichern der Inhaltsfilterung-Datenbanken und Updates der Module von Kaspersky Anti-Spam.

conf/ – Verzeichnis zum Speichern der Konfigurationsdateien. Dieses Verzeichnis enthält folgende untergeordnete Verzeichnisse:

def/ – ein Verzeichnis, welches die für Kompilation nötigen Dateien enthält, eingeschlossen Quelldateien der Inhaltsfilterung-Datenbanken und die Dateien, welche Information über Filterungsrichtlinien beinhalten;

data/ – Verzeichnis zum Speichern der binären Konfigurationsdateien;

src/ – ein Verzeichnis, welches temporären Dateien der Filterungsregeln enthält. Die Daten werden zur Kompilierung der Regeln gebraucht.

tmp/ – temporärer Verzeichnis, in dem die Konfigurationsdaten zwischen gespeichert.

control/ – Verzeichnis, in dem die Dateien der Verwaltungszentrale abgelegt sind. Enthält folgende Unterverzeichnisse:

bin/ – Verzeichnis, in dem die ausführenden Dateien und Skripte der Verwaltungszentrale abgelegt sind;

lib/ – ein Verzeichnis, in dem die Bibliothek-Dateien gespeichert werden, welche von der Verwaltungszentrale benutzt werden;

stat/ – Dateien des Systems, welches die Protokolle und Statistik bearbeitet;

- tmp/* – Temporärer Verzeichnis der Verwaltungszentrale;
- www/* – cgi-Skripte und grafische Dateien, welche von der Verwaltungszentrale benutzt werden.
- etc/* – Konfigurationsdateien-Verzeichnis des Kaspersky Anti-Spam;
- lib/* – von dem Produkt benötigte Bibliotheken.
- log/* – Verzeichnis zum Speichern der Protokolldateien, welche für Statistikerstellung benutzt werden;
- run/* – рабочий каталог продукта. Этот каталог также служит для хранения pid-файлов запущенных процессов сервера фильтрации.
- src/* – каталог, содержащий исходные тексты модуля *kas-exim*.

A.2. Clientmodule der Mailserver

Zum Betsnd des Kaspersky Anti-Spam gehören folgende Clientmodule, welche für Integration des Produktes in den unterschiedlichen Mailserver benutzt werden:

- *kas-milter* – Clientmodul für den Mailserver Sendmail;
- *kas-pipe* – universeller Clientmodul; wird stamdartmässig für die Mailserver Postfix und Exim benutzt;
- *kas-exim* – Clientmodul für den Mailserver Exim (alternative Variante);
- *kas-qmail* – Clientmodul für den Mailserver Qmail;
- *kas-cgpro* – Clientmodul für den Mailserver Communigate Pro.

Integration in den Mailserver wird während der Installation von Kaspersky Anti-Spam durchgeführt mit Hilfe spezieller Konfigurationsskripte.

Dieser Anhang enthält Informationen über Arbeitsweise der Clientmodule, ihre Konfigurationsdateien und Besonderheiten der Einstellungen.

A.2.1. Zusammenarbeit des Clientmoduls mit dem Filterungsservers

Zusammenarbeit des Clientmoduls mit dem Filterungsservers funktioniert nach folgendem Algorithmus:

1. Clientmodul erhält die E-Mail von dem Mailserver und schickt eine Anfrage auf Verbindung mit dem Filterungsserver.

2. Masterprozess der Filterung wählt einen gestarteten Filterungsprozess oder startet einen neuen und stellt eine Verbindung zwischen dem Clientmodul und dem Filterungsprozess her.
3. Über diese Verbindung übergibt der Clientmodul die E-Mail zur Überprüfung und erhält von dem Filterungsprozess die Ergebnisse der Überprüfung.
4. Den Ergebnissen entsprechend nimmt Clientmodul Änderungen an der E-Mail vor und schickt die E-Mail an den Mailserver zurück.

Zusammenarbeit zwischen dem Clientmodul, dem Masterprozess und Filterungsprozess wird unter Benutzung eines internen Protokolls über einen Netzwerk- oder Lokalsocket realisiert.

Benutzung eines Netzwerksockets erlaubt Ihnen den Filterungsserver und den Mailserver mit dem integrierten Clientmodul auf unterschiedlichen Servern zu platzieren. Dabei kann Filterungsserver mehrere Mailserver bedienen, wenn zu bearbeitender E-Mail-Verkehr dieses erlaubt. Solche Konfiguration verlangt, dass die Parameter-Einstellungen der Zusammenarbeit von Kaspersky Anti-Spam und Mailserver per Hand eingestellt werden müssen.

A.2.2. Allgemeine Parameter der Clientmodule

Im Kaspersky Anti-Spam Version 3.0 werden die Einstellungen der Clientmodule in der gemeinsamen Konfigurationsdatei *filter.conf* gespeichert, welche sich im Verzeichnis */usr/local/ap-mailfilter3/etc/* befindet.

Folgende Einstellungen sind für alle Module gleich:

- **ClientConnectTo** – Socketadresse der Zusammenarbeit mit dem Filterungsserver. Die Schreibweise ist: **tcp:<host>:<port>**, wo **<host>** – IP-Adresse des Filterungsserver ist, und **<port>** – Verbindungsport ist, dass auf die Benutzung eines Netzwerksocket zeigt, die Schreibweise **unix:<Dateipfad>**, wo **<Dateipfad>** – Pfad zu der Socketdatei, das auf Benutzung eines lokalen Socket zeigt.
- **ClientConnectTimeout** – maximale Wartezeit (in Sekunden) bei der Herstellung der Verbindung.
- **ClientDataTimeout** – maximale Wartezeit (in Sekunden) bei dem Datenaustausch mit dem Filterungsserver.
- **ClientOnError** – Bearbeitung der aufgetretenen Fehler (keine Verbindung mit dem Filterungsserver, Timeout bei Datenaustausch ist abgelaufen u.s.w.). Mögliche Werte:

- **reject** – E-Mail-Empfang ablehnen, den Code 5xx zurückgeben während der SMTP-Sitzung;
 - **tempfail** – E-Mail-Empfang vorübergehend ablehnen, den Code 4xx zurückgeben während der SMTP-Sitzung (wird standardmäßig benutzt);
 - **accept** – E-Mail annehmen.



Wenn Sie Sendmail als Mailserver benutzen, wird Wert **accept** bedeuten, dass E-Mail, ohne weitere Bearbeitung von den anderen Militer-Filtern, welche nach Kaspersky Anti-Spam benutzt werden, angenommen wird.

- **ClientDefaultDomain** – имя почтового домена, подставляемое в адрес, в котором не указан почтовый домен. Ein Beispiel: wenn als Domänenname standardmäßig если в качестве домена по умолчанию указан домен `mycompany.com`, то адрес `someuser` будет интерпретирован как `someuser@mycompany.com`. Если данный параметр не задан, то подстановка имени домена не производится (по умолчанию параметр не задан).
- **ClientFilteringSizeLimit** – maximale Größe (in Kilobytes) der E-Mail, welche an den Filterungsserver übergeben wird. Größere E-Mails werden ohne Bearbeitung durch Filterungsserver durchgereicht. Standardwert: **500**.
- **ClientMessageStoreMem** – minimale E-Mail-Größe (in Kilobytes), bei der die Daten auf der Festplatte zwischengespeichert werden. Dieses erlaubt Ihnen den Umfang des benutzten Arbeitsspeichers zu kontrollieren. Wenn dem Parameter Wert **0** (Standardwert) vergeben ist, werden alle Daten in dem Arbeitsspeicher gehalten.
- **ClientTempDir** – Pfad zu dem Verzeichnis, in dem temporäre Daten gespeichert werden.

A.2.3. kas-milter – Clientmodul für den Mailserver Sendmail

Für die Integration in den Mailserver Sendmail benutzt Kaspersky Anti-Spam Clientmodul *kas-milter*. Zusammenarbeit des Clientmoduls mit dem Mailserver wird mittels Bibliothek *libmilter* realisiert.

Ein Diagramm der Zusammenarbeit der Module bei der Arbeit von Kaspersky Anti-Spam mit Sendmail ist auf der Abb. 31 gezeigt.

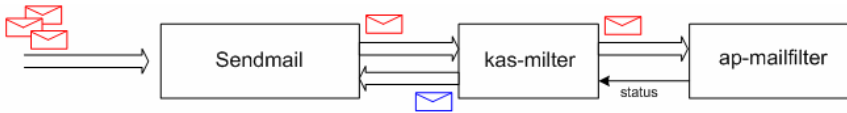


Abbildung 31. Zusammenarbeit von Kaspersky Anti-Spam mit dem Mailserver Sendmail

Parametereinstellungen der Zusammenarbeit des Clientmoduls und Mailservers können mit Hilfe der speziellen Skripte (s. Pkt. 3.5 auf S. 30), wie auch per Hand gemacht werden.

Parametereinstellungen werden per Hand in der Konfigurationsdatei *filter.conf* durchgeführt, diese Konfigurationsdatei befindet sich im Verzeichnis */usr/local/ap-mailfilter3/etc/*. Weiter sehen Sie ein Teil der Konfigurationsdatei, welcher die Clientmodul-Einstellungen enthält:

```
ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
SendMailAddress unix:/var/run/kas-milter.socket
ClientOnError accept
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
```

Außer den Parameter, welche in dem A.2.2 beschrieben werden, wird für den Modul *kas-milter* in der Konfigurationsdatei *filter.conf* Parameter **SendMailAddress** definiert, welcher den Socket für Zusammenarbeit mit Sendmail vorgibt.

Um Sendmail für die Zusammenarbeit mit *kas-milter* zu konfigurieren, fügen Sie folgende Zeilen in die Konfigurationsdatei *sendmail.cf*:

```
Xkasfilter,S=local:/var/run/kas-milter.socket,
T=C:10s,S:20s,R:30s
O InputMailFilters=kasfilter
```

Eine Detaillierte Beschreibung der Filtereinstellungen *sendmail.cf* ist in der Dokumentation von Sendmail vorhanden.



In der Regel wird Sendmail beim Starten vom Betriebssystem früher, als Kaspersky Anti-Spam gestartet, deswegen kann Sendmail den Socket für Zusammenarbeit nicht finden. In dem Fall wird in das Systemprotokoll folgendes eingetragen:

WARNING: Xkas: local socket name <Socketdatei> missing

Dies ist keine Störung, denn die Socketdatei wird von dem Clientmodul *kas-milter* erst nach dem Starten von Kaspersky Anti-Spam erstellt.

Das sind die Besonderheiten beim Benutzen des Clientmoduls `kas-milter` zusammen mit dem Mailserver `Sendmail`:

- `kas-milter` erstellt keine Kopien von E-Mails bei der Bearbeitung; wenn die E-Mail an mehrere Empfänger gesendet wurde, welche zu verschiedenen Gruppen mit unterschiedlichen Bearbeitungsregeln gehören, werden an die E-Mail Aktionen ausgeführt, welche in jeder der Gruppen definiert sind. Ein Beispiel:

die E-Mail ist an die Adressen `alice@mycompany.com` und `bob@mycompany.com` gerichtet. Diese Adressen gehören entsprechend zu den Gruppen **sales** und **managers**. Nach der Erkennung bekam E-Mail Status **Spam** für Gruppe **sales** und Status **Not detected** für Gruppe **managers**. Nach Regeln für die Gruppe **sales** wird in die E-Mail mit dem Status **Spam** in das Feld „Betreff“ eine Kennung **[!! SPAM]** hinzugefügt, und nach Regel der Gruppe **managers** für die E-Mail mit dem Status **Not Detected** ist Aktion **Accept this message** definiert. Als Ergebnis wird die E-Mail mit der Kennung **[!! SPAM]** in dem Feld „Betreff“ den beiden Empfängern zugelegt. Dabei enthält die E-Mail folgende Kopfzeilen:

X-Spamtest-Status-Extended: SPAM

X-Spamtest-Status-Extended: Not detected

X-Spamtest-Group-ID: 0000002

X-Spamtest-Group-ID: 0000001

Dies bedeutet, dass die E-Mail nach Regeln der Gruppen mit den Kennungen 1 und 2 (Kennungen, welche den Gruppen **sales** und **managers** gehören) bearbeitet wurde, und der E-Mail Status **SPAM** und **Not Detected** vergeben wurden. Detaillierte Beschreibung der Kopfzeilen s. Pkt. A.5 auf S. 120.

- Wenn die E-Mail an mehrere Empfänger gesendet wurde und dabei für einige von ihnen die Zustellung der E-Mail verboten ist (Aktion **reject message**), und für einige erlaubt ist (Aktion **accept message**), dann wird an den Absender die Meldung über Unmöglichkeit der Zustellung an einige Empfänger (bounce message) nicht gesendet;
- Da für `Sendmail` keine Möglichkeit gibt die Anzahl der Verbindungen über den Port 25 anzugeben, hängt die Anzahl der Filterungsprozesse `ap-mailfilter` direkt von der Anzahl der ankommenden Verbindungen ab. Dies kann zur zusätzlichen Serverbelastung führen.

A.2.4. *kas-pipe* – Clientmodul für die Mailserver Postfix, Exim

Modul *kas-pipe* ist ein universäler Clientmodul von Kaspersky Anti-Spam und kann zur Integration in den jeden von unterstützten Mailserver benutzt werden.

Bei der Standardinstallation wird *kas-pipe* für Integration in Postfix und Exim benutzt.

Modul *kas-pipe* nimmt E-Mails an, und übergibt diese nach der Filterung dem Mailserver, dabei benutzt der Modul Protokolle SMTP und LMTP.

Das Starten des Moduls *kas-pipe* wird von der externen Anwendung durchgeführt (z. B., durch den Mailserver). Zum Weiterleiten der E-Mails dient ein Netzwerk- oder Lokalsocket. Es wird auch das Starten der Anwendung mit Hilfe der Befehle *fork* und *exec* zugelassen.

Ein Diagramm der Zusammenarbeit zwischen Kaspersky Anti-Spam und dem Modul *kas-pipe* ist auf der Abb. 32 zu sehen.

Dieses Schema kann mit jedem Mailserver realisiert werden, welcher erlaubt seine Kopie mit anderen Einstellungen zu starten, die Zustellung über LMTP-Protokoll unterstützt, oder die Zustellung gesamten E-Mail-Verkehrs über SMTP an einen bestimmten Server unterstützt.

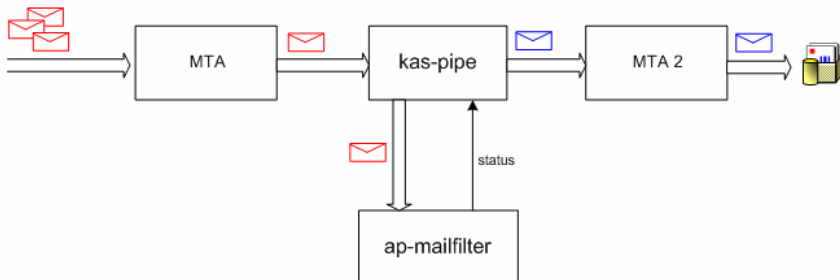


Abbildung 32. Benutzung des Moduls *kas-pipe*

Einstellungen der Parameter für die Zusammenarbeit des Clientmoduls und Mailservers kann wie mit Hilfe der Scripte (s. Pkt. 3.5 auf S. 30), so auch per Hand durchgeführt werden.

Händliche Einstellungen der Parameter werden in der Konfigurationsdatei *filter.conf* vorgenommen, welcher sich in dem Verzeichniss */usr/local/ap-mailfilter3/etc/* befindet. Weiter sehen Sie ein Teil der Konfigurationsdatei, welcher die Clientmodul-Einstellungen enthält:

```

ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
PipeInProtocol lmtp
PipeOutProtocol lmtp
  
```

```

PipeOutgoingAddr exec:/usr/sbin/sendmail -bs
PipeMultipleMessagesAllowed yes
ClientDefaultDomain localhost
ClientOnError accept
ClientFilteringSizeLimit 500

```

Außer Parameter, welche im Anhang A.2.2 beschrieben sind, enthalten die Moduleinstellungen des Moduls *kas-pipe* in der Konfigurationsdatei *filter.conf* folgende zusätzliche Parameter:

- **PipeInProtocol** – Protokoll, welcher für die Zustellung der E-Mails benutzt wird. Mögliche Werte: **smtp**, **lmp**.
- **PipeOutProtocol** – Protokoll, welcher für die Weiterleitung der bearbeiteten E-Mails benutzt wird. Mögliche Werte: **smtp**, **lmp**.
- **PipeHELOGreeting** – Domänenname, welche von dem Modul *kas-pipe* während der SMTP-Sitzung bei der Begrüßung benutzt wird. Standardwert: **kas30pipe.+ <Domänenname des Servers>**.
- **PipeOutgoingAddr** – Adresse des Sockets, welcher zur Weiterleitung der bearbeiteten E-Mails benutzt wird. Schreibweise: **tcp:<host>:<port>**, wo **<host>** – IP-Adresse des Filterungsserver ist, und **<port>** – Verbindungsport ist, zeigt auf Benutzung des Netzwerksockets, sie Schreibweise **unix:<Dateipfad>**, wo **<Dateipfad>** – Pfad zu der Socketdatei ist, das zeigt auf Benutzung eines lokalen Socket, die Schreibweise **exec:;<Pfad zu der ausführenden Datei des Produktes> -<Parameter>** zeigt auf das Programm, welches zur Übergabe der E-Mails gestartet wird.
- **PipeOutConnectTimeout=5...600** – Timeout für die Verbindung mit dem Socket oder mit dem Programm, welches zum Übergeben der bearbeiteten E-Mails benutzt wird (Wird durch Parameter **PipeOutgoingAddr** vorgegeben).
- **PipeOutDataTimeout=5...600** – Timeout für die Übergabe der Daten über den Socket oder das Programm, welches vom Parameter **PipeOutgoingAddr** bestimmt wird.
- **PipeMultipleMessagesAllowed** – einen Modus benutzen, bei dem Kopien der E-Mails erstellt werden, wenn Filterungsergebnisse für verschiedene Empfänger unterschiedlich sind. Mögliche Werte: **yes**, **no**.
- **PipeUseXForward** – Unterstützung des Befehls XForward, welche erlaubt die IP-Adresse des Servers zu bekommen, von dem E-Mail gekommen ist (nur bei Arbeit mit Postfix). Mögliche Werte: **yes**, **no**.

- **Pipe8BitHack** – Benutzung der Erweiterung 8BITMIME. Mögliche Werte: **yes**, **no**. Geben Sie den Wert **yes** ein, wenn Ihr Mailserver für die Unterstützung der Erweiterung 8BITMIME konfiguriert ist.
- **PipeBufferedIO** – Pufferung benutzen bei der Bearbeitung der E-Mails. Pufferung erlaubt die Bearbeitung der E-Mails zu beschleunigen, in dem zusätzlicher Arbeitsspeicher benutzt wird. Mögliche Werte: **yes**, **no**.

Besonderheiten bei Benutzung des Clientmoduls kas-pipe:

- Da die E-Mail dem Clientmodul kas-pipe über SMTP- oder LMTP-Protokoll übergeben wird, gibt es keine Möglichkeit (für alle Mailserver außer Postfix) die IP-Adresse des Absender-Servers fest zu stellen. Alle DNS-Überprüfungen können nur mit den IP-Adressen durchgeführt werden, welche sich in dem Brifkopf Received befinden. Beim Benutzen von Postfix geben Sie für den Parameter **PipeUseXForward** den Wert **yes** ein, damit Clientmodul kas-pipe die IP-Adresse des Absender-Servers bekommt.
- Так как kas-pipe интегрируется с почтовым сервером после очереди входящих сообщений, у клиентского модуля нет возможности выполнить действие **reject** в процессе SMTP-сессии. Если для сообщения задано действие **reject this message**, то отправителю будет отправлено уведомление о невозможности доставки письма адресату (bounce message);

A.2.4.1. Konfiguration von Postfix für die Arbeit mit *kas-pipe*

Dieser Abschnitt enthält ein Beispiel der Konfiguration von *kas-pipe* und Mailservers Postfix, in dem folgendes Arbeitsschema realisiert wird:

- *kas-pipe* arbeitet als Inhaltsfilter (*content_filter*);
- *kas-pipe* nimmt E-Mails über den Netzwerk-Socket *localhost:9026* und den Dienst *kas3scan* an, welcher per Hand in der Konfiguration von Postfix angegeben ist.
- *kas-pipe* übergibt E-Mails, welche von Kaspersky Anti-Spam bearbeitet wurden, über das SMTP-Protokoll auf den Socket *localhost:9025*.



Der Dienst *kas3scan* gibt eine Begrenzung der gleichzeitigen Verbindungen vor und benutzt die Option *smtp_send_xforward_command* zum Weitergeben an den Modul *kas-pipe* der IP-Adresse des Servers, von dem die E-Mail kam.



Um dieses Arbeitsschema zu realisieren, gehen Sie wie folgt vor:

1. In der Konfigurationsdatei *filter.conf* geben Sie folgende Parameterwerte ein:

```
ClientConnectTo tcp:127.0.0.1:2277
PipeMultipleMessagesAllowed Yes
PipeInProtocol smtp
PipeOutProtocol smtp
PipeOutgoingAddr tcp:127.0.0.1:9025
PipeUseXForward yes
```

2. Nehmen Sie Änderungen in der Konfigurationsdatei von Postfix (*master.cf*) vor:

```
smtp      inet  n       -       n       -       -       smtpd
### KASPERSKY ANTI-SPAM BEGIN ###
  -o content_filter=kas3scan:127.0.0.1:9026
### KASPERSKY ANTI-SPAM END ###

pickup   fifo  n       -       n       60     1       pickup
### KASPERSKY ANTI-SPAM BEGIN ###
  -o content_filter=kas3scan:127.0.0.1:9026
### KASPERSKY ANTI-SPAM END ###

### KASPERSKY ANTI-SPAM BEGIN ###
127.0.0.1:9026 inet  n       n       n       -       20      spawn
user=mailflt3 argv=/usr/local/ap-mailfilter3/bin/
kas-pipe
127.0.0.1:9025 inet  n       -       n       -       25      smtpd
-o smtpd_authorized_xforward_hosts=127.0.0.0/8
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
```

```

-o
smtpd_recipient_restrictions=permit_mynetworks,
reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=no
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000

kas3scan  unix  -  -  n  -  10  smtp
-o smtp_send_xforward_command=yes
### KASPERSKY ANTI-SPAM END ###

```



Für Postfix Version 2.1 und höher ist die Benutzung von *kas-pipe* als Proxy-Server möglich (*smtpd_proxy_filter*). Dies erlaubt die Aktion **reject** während der SMTP-Sitzung zu benutzen, was die E-Mail-Bearbeitung beschleunigen wird. Solche Einstellung wird nur für wenig Belastete Mailserver empfohlen. Um *kas-pipe* als Proxy-Server zu konfigurieren, ändern Sie zwei Zeilen in dem oben beschriebenen Beispiel auf folgende:

```

smtp  inet  n  -  n  -  -  smtpd
-o smtpd_proxy_filter=127.0.0.1:9026

```

A.2.4.2. Konfiguration von Exim für die Arbeit mit *kas-pipe*

Die Integration von *kas-pipe* in den Mailserver Exim wird durch das Hinzufügen in die Exim-Konfiguration eines neuen Router am Anfang der Routerliste, wie auch eines Transports zum Starten vom Modul *kas-pipe*. Dieser Router ist symbolisch, er reagiert nicht auf E-Mails, welche lokal über ESMTP-Protokoll verschickt wurden.

Die Überprüfung der E-Mails unter Benutzung des Clientmoduls *kas-pipe* mit Exim wird nach folgendem Schema durchgeführt:

1. Exim nimmt auf den Port 25 ankommende E-Mails an und verschiebt diese in die Warteschlange.
2. Exim sucht eine E-Mail aus der Warteschlange und durchsucht die Liste der Router um den passenden zur diese E-Mail auszuwählen. Da der Router welcher auf *kas-pipe* zeigt als erster in der Liste steht, werden alle Nachrichten mit dem entsprechenden Transport an den Client-Modul *kas-pipe* übergeben.

3. Nach der Überprüfung der Nachricht übergibt kas-pipe diese zurück, in dem er Befehl `exim -bs` ausführt. E-Mail wird erneut in die Warteschlange von Exim verschoben, jetzt wird aber der Router für den Modul kas-pipe nicht reagieren, da die E-Mail lokal verschickt wurde.
4. Exim stellt die E-Mail dem Empfänger zu.



Um dieses Schema zu realisieren, gehen Sie wie folgt vor:

1. In der Konfigurationsdatei `filter.conf` vergeben Sie an die Parameter folgende Werte:

```
PipeInProtocol lmtp
PipeOutProtocol smtp
PipeOutgoingAddr exec:/usr/local/sbin/exim -bs
```

2. Nehmen Sie folgende Änderungen in der Exim-Konfigurationsdatei vor:

- Im Abschnitt **ROUTERS** fügen Sie folgende Zeilen ein:

```
begin routers
# ROUTER ADDED BY KAS 3.0 INSTALLER
kas30router:
  driver = accept
  local_parts = passwd;$local_part : lsearch
  condition = "${if !eq {$received_protocol}
{local-esmtp}{yes}}"
  transport = kas30transport
```

- Im Abschnitt **TRANSPORTS** fügen Sie folgende Zeilen ein:

```
begin transports
# TRANSPORT ADDED BY KAS 3.0 INSTALLER
kas30transport:
  driver = lmtp
  batch_max = 100
  command = /usr/local/ap-mailfilter3/bin/kas-pipe
  return_path_add = false
```

Im Debian-Distributiv hat die Integration in Exim einige Besonderheiten. Dies hängt damit zusammen, dass die Konfiguration des Mailservers durch ein Skript `update-exim4.conf` aus einem Muster `/etc/exim4/exim4.conf.template` generiert wird, welcher sich in dem Verzeichnis `/etc/exim4/conf.d/` befindet. Das Benutzen einen oder mehreren Muster wird mit dem Parameter **use_split_files** der Konfigurationsdatei Exim `exim4-update.conf.conf` definiert. Die daraus

entstehende Konfiguration wird unter `/var/lib/exim4/config.autogenerated` gespeichert.

Die Integration von Kaspersky Anti-Spam in den Mailserver Exim unter Debian-Distributiv kann wie automatisch mit Hilfe des speziellen Skript (s. Pkt. 3.5 auf S. 30), so auch per Hand gemacht werden.



Um Exim für die Arbeit mit dem Clientmodul *kas-pipe* einzustellen, gehen Sie wie folgt vor:

- Wenn für die Einstellung der Exim-konfiguration das Muster *exim4.conf.template* benutzt wird, dann fügen Sie in die entsprechende Abschnitte **ROUTERS** und **TRANSPORTS** die obengenannte Zeilen ein.
 - Wenn für die Einstellung der Exim-konfiguration das Muster aus dem Verzeichnis `/etc/exim4/conf.d/` benutzt wird, denn
1. im Ordner `/etc/exim4/conf.d/router/` erstellen Sie Datei *099_exim4-config_kas30router* und fügen Sie in die Datei folgende Zeilen ein:

```
kas30router:
    driver = accept
    local_parts = passwd;$local_part : lsearch
    condition = "${if !eq {$received_protocol}
{local-esmtp}{yes}}"
```

transport = kas30transport

2. in dem Verzeichnis `/etc/exim4/conf.d/transport/` erstellen Sie Datei *30_exim4-config_kas30transport* und fügen Sie in die Datei folgende Zeilen ein:

```
kas30transport:
    driver = lmtp
    batch_max = 100
    command = /usr/local/ap-mailfilter3/bin/kas-pipe
    return_path_add = false
```

Danach starten Sie das Skript *update-exim4.conf*, um das System auf das Benutzen neuer Parameten einzustellen.

A.2.5. *kas-exim* – Clientmodule für den Mailserver Exim

Modul *kas-exim* ist für die Integration von Kaspersky Anti-Spam in den Mailserver Exim Version 4.xx unter Benutzung *localscan API* bestimmt.

Arbeit über `kas-exim` ist eine alternative Entscheidung. Bei der Standardinstallation wird die Integration in den Exim-Server mit Hilfe des Clientmoduls `kas-pipe` durchgeführt. Im Gegensatz zum Modul `kas-pipe`, verlangt `kas-exim` keine zweite Kopie des Mailserver für Weiterleitung der E-Mail.

Benutzung von `localscan API` verlangt eine neue Compilierung von Exim, deswegen wird Modul `kas-exim` als Quellcode (Programmiersprache C) und die Installation wird per Hand durchgeführt.



Um Mailserver Exim zu compilieren und den Modul `kas-exim` anzubinden, gehen zu wie folgt vor:

1. legen Sie die Datei `kas_exim.c`, welche im Verzeichnis `/usr/local/ap-mailfilter3/src/` sich befindet, in den Ordner `Local` des Stammverzeichnisses der Quelldateien von Exim.
2. fügen Sie folgende Änderungen in die Datei `Makefile` hinzu, welche sich im Ordner `Local` befindet:

```
CFLAGS= -I/usr/local/ap-mailfilter3/include
EXTRALIBS_EXIM=-L/usr/local/ap-mailfilter3/lib
-lspamtest
LOCAL_SCAN_SOURCE=Local/kas_exim.c
LOCAL_SCAN_HAS_OPTIONS=yes
```

3. führen Sie die Compilierung von Exim aus.



Alle Arbeitsparameter des Moduls `kas-exim` werden in der Konfigurationsdatei von Exim vorgegeben, nicht in der Datei `filter.conf`.

Unten sehen Sie einen Ausschnitt der Konfigurationsdatei von Exim, welcher die Einstellungen des Moduls `kas-exim` enthält:

```
begin local_scan
kas_connect_to = tcp:127.0.0.1:2277
kas_connect_timeout = 40
kas_data_timeout = 30
kas_default_domain = localhost
kas_filtering_size_limit = 500
kas_on_error=accept
kas_log_level=3
```

Dieser Ausschnitt enthält folgende Parameter:

- **kas_connect_to** – Socketadresse der Zusammenarbeit mit dem Filterungsserver. Schreibweise **tcp:<host>:<port>**, wo **<host>** – IP-Adresse des Filterungsserver, wo **<port>** – Verbindungsport ist, was auf Benutzung eines Netzwerksocket zeigt, Schreibweise **unix:<Dateipfad>**, wo **<Dateipfad>** – Pfad zu der Socketdatei ist, das auf Benutzung eines lokalen Socket zeigt.
- **kas_connect_timeout** – maximale Wartezeit (in Sekunden) bei der Herstellung der Verbindung mit dem Filterungsserver.
- **kas_data_timeout** – maximale Wartezeit (in Sekunden) bei Datenaustausch mit dem Filterungsserver.
- **kas_default_domain** – Name der Mail-Domäne, welche in die Adresse eingesetzt wird, wenn keine Domäne angegeben wurde.
- **kas_filtering_size_limit** – maximale Größe (in Kilobites) der E-Mail, welche an den Filterungsserver weitergeleitet werden kann. Größere E-Mails werden ohne Bearbeitung von Filterungsserver durchgereicht.
- **kas_on_error** – Bearbeitung der aufgetretenen Fehler (keine Verbindung mit dem Filterungsserver, Timeot bei Datenaustausch ist abgelaufen u.s.w.). Mögliche Werte:
 - **reject** – E-Mail-Empfang ablehnen, den Code 5xx zurückgeben während der SMTP-Sitzung;
 - **tempfail** – E-Mail-Empfang vorübergehend ablehnen, den Code 4xx zurückgeben während der SMTP-Sitzung (wird standardmäßig benutzt);
 - **accept** – E-Mail annehmen;
- **kas_log_level** – Protokollgenauigkeitsstufe beim Schreiben in die Protokolldatei. Das Schreiben wird im Testbetrieb von Exim durchgeführt.

Besonderheiten beim Benutzen des Moduls kas-exim zusammen mit dem Mailserver Exim:

- Modul kas-exim, wie auch Modul kas-milter, erstellt keine Kopien während der E-Mail-Bearbeitung; daraus folgt, dass wenn die E-Mail an mehrere Empfänger geschickt wurde, welche zu unterschiedlichen Gruppen mit verschiedenen Bearbeitungsregeln gehören, werden an der E-Mail Aktionen unternommen, welche für jede der Gruppen definiert sind.
- Wenn die E-Mail an mehrere Empfänger gesendet wurde und dabei für einige von ihnen die Zustellung der E-Mail verboten ist (Aktion **reject message**), und für einige erlaubt ist (Aktion **accept message**), denn wird

an den Absender die Meldung über Unmöglichkeit der Zustellung an einige Empfänger (bounce message) nicht gesendet.

A.2.6. kas-qmail – Clientmodul für den Mailserver Qmail

Clientmodul *kas-qmail* ist für die Integration von Kaspersky Anti-Spam in den Mailserver Qmail bestimmt. Wenn dieser Modul benutzt wird, wird E-Mail-Verkehr nach folgenden Algorithmus durchgeführt:

1. der Modul *qmail-queue* des Mailservers Qmail wird durch Clientmodul *kas-qmail* ersetzt, welcher die Übergabe der ankommenden E-Mails an den Filterungsserver realisiert.
2. Bearbeiteter E-Mail-Verkehr wird an den Modul *kas-qmail* zurückgegeben und dann an den Modul *qmail-queue* weitergeleitet.

Ein Diagramm der Zusammenarbeit von Kaspersky Anti-Spam und *kas-qmail* ist auf der Abb. 33 zu sehen.

Parametereinstellungen der Zusammenarbeit des Clientmoduls und Mailservers kann wie mit Hilfe der speziellen Skripte (s. Pkt. 3.5 auf S. 30), so auch per Hand durchgeführt werden.

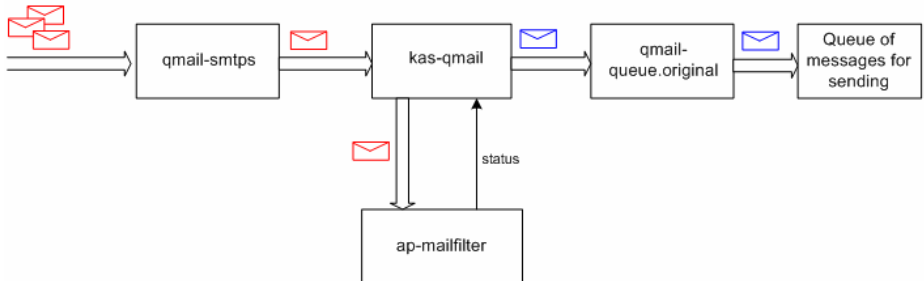


Abbildung 33. Zusammenarbeit von Kaspersky Anti-Spam mit dem Mailserver Qmail

Einstellungen für Clientmodul, welche per Hand gemacht werden, müssen durch Änderung der Konfigurationsdatei *filter.conf* durchgeführt, welche sich im Verzeichnis */usr/local/ap-mailfilter3/etc/* befindet.

Weiter sehen Sie einen Ausschnitt aus der Datei *filter.conf*, welcher die Einstellungen des Moduls *kas-qmail* enthält:

```

ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
QMailOriginalQueue /var/qmail/bin/qmail-queue.kas
  
```

```
ClientOnError accept
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
```

Außer Parameter, welche im Anhang A.2.2 beschrieben sind, enthält die Datei einen Parameter **QMailOriginalQueue**, welcher den Pfad zum ursprünglichen Modul *qmail-queue* vorgibt.



Um Qmail zur Arbeit mit dem Clientmodul *kas-qmail* einzustellen, gehen Sie wie folgt vor:

1. benennen Sie die ursprüngliche Datei des *qmail-queue* Moduls, in dem Sie folgenden Befehl ausführen:

```
# mv /var/qmail/bin/qmail-queue
/var/qmail/bin/qmail-queue.kas
```

2. Installieren Sie den Modul *kas-qmail* an Stelle von *qmail-queue*, dem Sie folgende Befehle ausführen:

```
# cp /usr/local/ap-mailfilter3/bin/kas-qmail
/var/qmail/bin/qmail-queue
# chown qmailq /var/qmail/bin/qmail-queue
# chgrp qmail /var/qmail/bin/qmail-queue
# chmod 04755 /var/qmail/bin/qmail-queue
```

A.2.7. kas-cgpro – Clientmodul für den Mailserver CommuniGate Pro

Clientmodul *kas-cgpro* ist für die Integration von Kaspersky Anti-Spam in den Mailserver CommuniGate Pro bestimmt. Wenn dieser Modul benutzt wird, wird E-Mail-Verkehr nach folgenden Algorithmus durchgeführt:

1. CommuniGate Pro übergibt den kompletten E-Mail-Verkehr an das Modul *kas-cgpro*.
2. Modul *kas-cgpro* bearbeitet die E-Mails, modifiziert sie (unter Anderem kennzeichnet die E-Mail mit einem speziellen Brifkopf) und verschiebt in den Verzeichnis *Submitted*, dabei wird an CommuniGate Pro DISCARD zurückgegeben.
3. Treiber *PIPE* übergibt die E-Mails aus dem Verzeichnis *Submitted* erneut an den Mailserver CommuniGate Pro, welcher; an seiner Stelle, die Nachricht an den Modul *kas-cgpro* übergibt.
4. Da der Modul *kas-cgpro* die E-Mail, welche schon die Filterung passiert haben (mit einem Brifkopf gekennzeichnet sind), nicht noch ein Mal

bearbeitet, wird an den Commuigate Pro ein „OK“ gesendet und die E-Mail wird an den Empfänger zugestellt.

Die Integration von Commuigate Pro kann nur per Hand durchgeführt werden. Parameter der Zusammenarbeit für den Clientmodul werden durch die Bearbeitung der Konfigurationsdatei *filter.conf* angegeben, und für Commuigate Pro mit Hilfe eines Web-Interfaces des Mailservers.

Weiter sehen Sie einen Ausschnitt aus der Datei *filter.conf*, welcher die Einstellungen des Clientmoduls enthält:

```
ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
CGProSubmittedFolder Submitted
CGProMaxThreadCount 50
CGProLoopHeader X-Proceed_240578_by_spamtest
CGProAllTransports No
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
```

Außer Parameter, welche im Anang A.2.2 beschrieben sind, werden beim Einstellen von kas-cgpro folgende zusätzliche Parameter benutzt:

- **CGProSubmittedFolder** – Verzeichnisname, in dem die bearbeiteten E-Mails abgelegt werden.
- **CGProMaxThreadCount** – maximale Anzahl der gleichzeitig bearbeitenden E-Mails.
- **CGProLoopHeader** – Brifkopf, welcher in die bearbeiteten E-Mails zugefügt wird.
- **CGProAllTransports** – erlaubt oder verbietet die Bearbeitung der E-Mails, welche von allen Transporten ankommen. Mögliche Werte: **yes** – werden alle E-Mails bearbeitet, **no** – werden nur die E-Mails von dem Transport SMTP bearbeitet (standardmäßiger Wert).



Um Commuigate Pro für die Zusammenarbeit mit dem Clientmodul kas-cgpro einzustellen, gehen Sie in dem Web-Interface des Mailservers wie folgt vor:

1. Im Menü **Settings**→**General**→**Helpers** fügen Sie neuen *content-filter* mit den folgenden Parameter hinzu:

```
Use Filter: kas-cgpro
Log: Problems
```

```
Path: /usr/local/ap-mailfilter3/bin/kas-cgpro
Time-Out: 5 minutes
Auto-Restart: 15 seconds
```

2. Im Menü **Settings**→**Rules** (**Settings**→**Queue**→**Rules** für die Version Communicate Pro höher, als 5.0) erstellen Sie eine neue Regel, nach welche die Untersuchung aller Nachrichten, deren Größe 500 KB nicht übersteigt, ausgeführt wird :

```
Data: Message Size
Operation: less than
Parameter: 500000
Action: external filter
Parameters: kas-cgpro
```

Besonderheiten beim Benutzen des Clientmoduls kas-cgpro zusammen mit Communicate Pro:

- Clientmodul kas-cgpro besitzt keine Möglichkeit die E-Mail während der SMTP-Sitzung abzulehnen, für welche die Aktion **reject this message** definiert wurde. Anstatt dessen verschickt Communicate Pro an den Absender eine Meldung über Unmöglichkeit der Zustellung der E-Mail (bounce message).
- Meldungstext für bounce message wird von dem Mailserver bestimmt, und nicht von dem Parameterwert **Bounce message**, welcher mit Hilfe des Interfaces der Verwaltungszentrale vergeben wird (s. Pkt. 4.5.4 auf S. 64).
- Versand der Meldungen des Monitoring-Systems, wie auch Fehlermeldungen beim Ausführen der Skripte wird von Filterungsserver unter Benutzerkennung **mailflt3** ausgeführt. Da Communicate Pro keine System-Benutzerkennungen in eigene Datenbank hinzufügt, erstellen Sie in der Benutzerdatenbank von Communicate Pro die Benutzerkennung **mailflt3**.
- Wenn in Communicate Pro die Option **Drop Root** benutzt wird, wird Mailserver auf das Benutzen der **nobody**-Rechte umgeschaltet. Diese Umschaltung wird nicht für den Modul kas-cgpro ausgeführt, das führt zum Verlust der Zusammenarbeit zwischen dem Mailserver und Slientmodul. Um die Zusammenarbeit wieder rher zu stellen, gehen Sie wie folgt vor:
 1. Im Menü Communicate Pro **Settings**→**General**→**Helpers** schalten Sie die Benutzung des Filters kas-cgpro aus, in dem Sie die Option **Use Filter** deaktivieren. Um die Konfiguration zu erneuern, klicken Sie auf die Schaltfläsche **Update**.

2. Fügen Sie den Filter `kas-cgpro` erneut hinzu. Die Parameter sind oben in der Beschreibung von `Communigate Pro` und `Clientmodul kas-cgpro` zu finden.

A.3. Konfigurationsdateien von Kaspersky Anti-Spam

Dieser Abschnitt enthält eine Beschreibung der Konfigurationsdateien von Kaspersky Anti-Spam, welche die Einstellungen für die Arbeit der Hauptkomponente des Filterungsserver enthalten.

A.3.1. Haupt-Konfigurationsdatei *filter.conf*

Konfigurationsdatei `/usr/local/ap-mailfilter3/etc/filter.conf` enthält Einstellungen der Arbeitsparameter aller Komponente von Kaspersky Anti-Spam außer Update-Moduls.

Allgemeine Einstellungen:

RootPath – Pfad zum Verzeichnis der Installation von Kaspersky Anti-Spam. Standardmäßiger Wert: `/usr/local/ap-mailfilter3`.

LogFacility=mail|user|local0|local1|local2|local3|local4|local5|local6|local7 – die Kategorie, entsprechend welcher die Einträge in das Systemprotokoll ausgeführt werden (syslog facility). Standardmäßiger Wert: `mail`.

LogLevel=0|1|2|3|4|5 – Stufe der Protokollgenauigkeit der Einträge in das Systemprotokoll (syslog). Standardmäßiger Wert: `2`.

User – Benutzer, mit Rechten dessen die Filterungsserver-Prozesse gestartet werden. Als Wert kann wie Benutzername, so auch die `uid` benutzt werden.

Group – Gruppe, mit Rechten deren die Filterungsserver-Prozesse gestartet werden. Als Wert kann wie Name der Gruppe, so auch die `uid` benutzt werden.

Filterungsserver-Einstellungen

ServerListen – Socket für die Zusammenarbeit zwischen dem Filterungsserver und Clientmodul, welcher in den Mailserver integriert ist. Schreibweise `tcp:<host>:<port>`, wo `<host>` – IP-Adresse (oder Name) des Filterungsservers, `<port>` – Verbindungsport, zeigt auf Benutzung eines Netzwerksockets, Schreibweise `unix:<Dateipfad>`,

wo **<Dateipfad>** – Pfad zu der Socket-Datei, was auf Benutzung eines lokalen Sockets zeigt. Um den Filterungsserver für die Verbindung mit beliebigen Interface einzustellen, stellen Sie den Parameter **<host>** auf den Wert 0.0.0.0 ein .



Lokaler Socket, welcher für Zusammenarbeit von den Mailserver und Filterungsserver erstellt wird, erlaubt jedem der im System authentifizierten Benutzer in den Socket zu schreiben.

FilterPath – Pfad zur ausführenden Datei des Filterungsprozess *ap-mailfilter*.

ServerMaxFilters=1...200 – maximale Anzahl der gleichzeitig arbeitende Filterungsprozesse *ap-mailfilter*. Standardmäßiger Wert: **10**.

ServerStartFilters – Anzahl der Filterungsprozesse *ap-mailfilter*, welche beim Starten des Moduls mitgestartet werden. Standardmäßiger Wert: **0**. Wert **ServerStartFilters** soll den Parameterwert von **ServerMaxFilters** nicht übersteigen.

ServerSpareFilters – minimale Anzahl der Filterungsprozesse welche sich im Wartezustand befinden (keine E-Mails bearbeiten). Wenn die Anzahl der Prozesse den Grenzwert übersteigt, werden nicht benutzte Prozesse zwangsleufig beendet. Standardmäßiger Wert: **0**. Wert **ServerSpareFilters** soll den Parameterwert von **ServerMaxFilters** nicht übersteigen.

Einstellungen der Filterungsprozesse

FilterMaxMessages=10...1000 – maximale Anzahl der Nachrichten, welche von dem Filterungsprozess bearbeitet werden kann. Nach dem die angegebene Anzahl bearbeitet wurde, wird Filterungsprozess beendet. Standardmäßiger Wert: **300**.



Maximale Anzahl der Nachrichten, welche vom Filterungsprozess bearbeitet werden können, ist zufällig und wird vom Programm ausgewählt aus dem Bereich **[FilterMaxMessages; FilterMaxMessages + (FilterRandMessages–1)]**. Die Einstellung erlaubt dem galeichzeitigen Starten einer großen Anzahl der Filterungsprozesse zu entgehen während großen Serverauslastung.

FilterRandMessages=0...50 – Wert, welcher für die Bestimmung der maximalen Anzahl der Nachrichten benutzt wird, welche von dem Filterungsprozess bearbeitet werden können.

FilterMaxIdle=30...3600 – maximaler Zeitraum (in Sekunden), während dem der Filterungsprozess sich im Wartezustand befinden kann. Wenn während der Zeit Filterungsprozess keine Nachrichten zur Bearbeitung bekommen hat, wird der Filterungsprozess beendet. Standardmäßiger Wert: **300**.

- FilterDelayedExit=0...30** – maximale Verzögerungszeit (in Sekunden) vor dem Beenden des Filterungsprozess nach dem der Filterungsprozess den Befehl zum Beenden bekommt. Wenn der Wert nicht Null ist, wird Filterungsprozess seine Arbeit in einem Zeitraum beenden, welcher eine zufällige Zahl aus dem Bereich ist [0; (FilterDelayedExit-1)]. Standardmäßiger Wert: **0**.
- FilterDataTimeout=10...100** – Timeout (in Sekunden) des Datenempfangs für Filterungsprozess von dem Clientmodul. Wenn Filterungsprozess während der angegebenen Zeit keine Daten bekommt, wird die E-Mail-Bearbeitung abgebrochen. Standardmäßiger Wert: **30**.
- FilterLicenseConnectTimeout=1..10** – Timeout (in Sekunden) für die Verbindung zwischen dem Filterungsprozess und Lizenzierungsmodul (*kas-license*) um übereinstimmung zwischen Anfrage und LizenzBedingungen zu überprüfen. Standardmäßiger Wert: **2**.
- FilterLicenseDataTimeout=1..10** – Timeout (in Sekunden) der Schreibe- und Leseoperationen für den Soker der Zusammenarbeit zwischen dem Filterungsprozess und Lizenzierungsmodul. Standardmäßiger Wert: **1**.
- FilterSPFDataTimeout=1..10** – Timeout (in Sekunden) der Schreibe- und Leseoperationen für den Soker der Zusammenarbeit zwischen dem Filterungsprozess und SPF-Hifsprogramm. Standardmäßiger Wert: **1**.
- FilterDNSTimeout=1...60** – Timeout (in Sekunden) für alle mögliche Überprüfungen mit Hilfe von DNS. Standardmäßiger Wert: **10**.
- FilterLicenseConnectTo** – Pfad zu der Socketdatei der Zusammenarbeit mit dem Lizenzierungsmodul. Standardmäßiger Wert: **/usr/local/ap-mailfilter3/run/kas-license.socket**.
- FilterSPFConnectTo** – Pfad zu der Socketdatei der Zusammenarbeit mit dem SPF-Hifsprogramm. Standardmäßiger Wert: **/usr/local/ap-mailfilter3/run/ap-spf.socket**.
- FilterReceivedHeadersLimit=0...100** – Anzahl der Brifkopfe Received, welche über die IP-Adressen-Listen und DNSBL-Dienste analysiert werden. Standardmäßiger Wert: **2**.
- FilterParseMSOffice=yes|no** – Parameter, welcher bestimmt, ob die Textanalyse der Einlagen im Format Word Document (doc) und RTF durchgeführt wird. Standardmäßiger Wert: **no**.
- FilterStatLogFile** – Pfad zur Datei, welche zur Speicherung der Statistik über bearbeitete Nachrichten dient.
- FilterUserLogFile** – Pfad zur Datei, welche zur Speicherung der benutzerdefinierten Statistik dient.
- FilterUDSCfgFile** – Pfad zur Datei, welche die Konfiguration des UDS-Dienstes enthält.

FilterUDSEnabled=yes|no – Parameter, welcher die Überprüfung der E-Mails mit Hilfe UDS-Dienstes ein- und ausschaltet.

FilterUDSTimeout=1...60 – Timeout für die Verbindung zwischen Filterungsserver und UDS-Server. Wenn während diesem Zeitraum Filterungsserver keine Antwort von dem UDS-Server bekommt, wird ein Versuch unternommen mit einem anderen UDS-Server von Kaspersky Lab zu verbinden.

Einstellungen des Lizenzierungsmodul

LicenseListen – Pfad zur Socketdatei, welche vom Lizenzierungsmodul für Zusammenarbeit mit den Filterungsprozessen benutzt wird. Standardmäßiger Wert: **/usr/local/ap-mailfilter3/run/kas-license.socket**.

LicenseKeysPath – Pfad zum Verzeichnis, in dem die Lizenzschlüssel gespeichert werden. Standardmäßiger Wert: **/usr/local/ap-mailfilter3/conf/lk-license/**.

LicenseMaxConnections=10...300 – maximale erlaubte Anzahl der gleichzeitigen Verbindungen mit dem Lizenzierungsmodul. Standardmäßiger Wert: **200**.

LicenseIdleTimeout=1...100 – maximale Zeit (in Sekunden) für die Verbindung des Lizenzierungsmoduls mit dem Filterungsprozess, welcher keine Daten sendet. Nach Ablauf der Zeit wird die Verbindung unterbrochen, wenn keine Anfragen gekommen sind. Standardmäßiger Wert: **30**.

LicenseDataTimeout=1..100 – Timeout (in Sekunden) der Schreibe- und Leseoperationen für den Socket der Zusammenarbeit mit den Filterungsprozessen. Standardmäßiger Wert: **1**.

Einstellungen des SPF-Hifsprogramms

SPFDListen – Pfad zu der Socketdatei, welche von dem SPF-Hifsprogramm für die Zusammenarbeit mit den Filterungsprozessen benutzt wird. Standardmäßiger Wert: **/usr/local/ap-mailfilter3/run/ap-spf.socket**.

SPFDPoolSize=1...50 – Anzahl der gleichzeitig gestarteten Tochter-Prozesse des SPF-Hifsprogramms. Standardmäßiger Wert: **5**.

SPFDMaxRequestsPerChild=50...10000 – maximale Anzahl der Anfragen, welche von dem Tochter-Prozess des SPF-Hifsprogramms bearbeitet werden. Nach dem Tochter-Prozess die vorgegebene Anzahl der Anfragen bearbeitet, wird seine Arbeit beendet und SPF-Hifsprogramm startet ein neues Prozess. Standardmäßiger Wert: **1000**.

SPFDMaxQueueSize=10...1000 – maximale Anzahl der Anfragen, welche in die Bearbeitungswarteschlange gestellt werden können. Standardmäßiger Wert **200**.

SPFDCleanupInterval=30...3600 – Zeitspanne (in Sekunden) für die Cacheleerung des SPF-Hilfsprogramms. Standardmäßiger Wert **600**.

Allgemeine Einstellungen der Clientmodule

ClientConnectTo – Socketadresse für die Zusammenarbeit des Clientmoduls mit dem Filterungsmodul. Schreibweise **tcp:<host>:<port>**, wo **<host>** – IP-Adresse des Filterungsserver, wo **<port>** – Verbindungsport ist, zeigt, dass ein Netzwerksocket benutzt wird, und die Schreibweise **unix:<Dateipfad>**, wo **<Dateipfad>** – Pfad zu Socketdatei ist, das zeigt, dass ein lokaler Socket benutzt wird.

ClientConnectTimeout=10...100 – Timeout (in Sekunden) für die Herstellung einer Verbindung zwischen Clientmodul und Filterungsprozess. Standardmäßiger Wert **40**.

ClientDataTimeout=10...100 – Timeout (in Sekunden) für den Datenaustausch zwischen Clientmodul und Filterungsmodul.

ClientOnError – Bearbeitung der aufgetretenen Fehler (keine Verbindung mit dem Filterungsserver, Timeot bei Datenaustausch ist abgelaufen u.s.w.). Mögliche Werte:

- **reject** – E-Mail-Empfang ablehnen, den Code 5xx zurückgeben während der SMTP-Sitzung;
- **tempfail** – E-Mail-Empfang vorübergehend ablehnen, den Code 4xx zurückgeben während der SMTP-Sitzung (wird standardmäßig benutzt);
- **accept** – E-Mail annehmen.

ClientDefaultDomain – Mail-Domäne-Name, welche in die E-Mail-Adresse eingefügt wird, wenn die Mail-Domäne nicht angegeben wurde. Ein Beispiel: wenn als Domänenname standardmäßig *mycompany.com* angegeben ist, dann wird die Adresse *someuser* als *someuser@mycompany.com* interpretiert. Wenn Dieser Parameter nicht angegeben ist, wird Domänenname nicht gesetzt. Standardmäßig ist Parameter nicht definiert.

ClientFilteringSizeLimit=0...10000 – – maximale Größe (in Kilobytes) der E-Mail, welche an den Filterungsmodul übergeben wird. Größere E-Mails werden ohne Bearbeitung durch Filterungsserver durchgereicht. Standardwert: **500**.

ClientMessageStoreMem – minimale E-Mail-Größe (in Kilobytes), bei der die Daten auf der Festplatte zwischengespeichert werden. Dieses erlaubt Ihnen den Umfang des benutzten Arbeitsspeichers zu

kontrollieren. Wenn dem Parameter Wert **0** (Standardwert) vergeben ist, werden alle Daten in dem Arbeitsspeicher gehalten.

ClientTempDir – Verzeichnis, in dem die temporären Dateien gespeichert werden.

Einstellungen der Verwaltungszentrale

ControlCenterSendAlertsTo – Adresse, an welche Meldungen des Monitoring-Systems verschickt werden, wie auch Fehlermeldungen der Skripte, mit Hilfe cron-Dienstes.

ControlCenterLang=en – Sprache des Interfaces der Verwaltungszentrale.

MonitoringHttpd=yes|no – dieser Parameter definiert, ob Monitoring des HTTP-Servers *kas-thttpd* ausgeführt wird.

MonitoringKasMilter=yes|no – dieser Parameter definiert, ob Monitoring des Clientmoduls *kas-milter* ausgeführt wird, welcher zur Gewährleistung der Zusammenarbeit mit dem Mailserver Sendmail benutzt wird.



Beschreibung der speziellen Einstellungen für einzelne Clientmodule s. Pkt. A.2 auf S. 89.

A.3.2. Konfigurationsdatei *kas-thttpd.conf*

Konfigurationsdatei *kas-thttpd.conf*, die sich in dem Verzeichnis */usr/local/ap-mailfilter3/etc/* befindet, enthält Parameter des HTTP-Servers, welcher das Web-Interface des Hauptwerkzeuges von Kaspersky Anti-Spam bietet – Verwaltungszentrale.

Diese Datei enthält folgende Parameter:

user – Benutzername, mit Rechten dessen die Skripte der Verwaltungszentrale ausgeführt werden. Es wird nicht empfohlen den Wert **mailflt3** zu ändern, das kann zu unkorrekten Arbeit des Systems führen.

host – IP-Adresse der Netzwerkkarte, an der Web-Server auf die Verbindungen mit der Verwaltungszentrale erwartet. Wert **0.0.0.0** bedeutet, dass der Server die Anfragen an allen Netzwerkkarten des Servers erwartet.

port – Portnummer für die Verbindungen mit der Verwaltungszentrale.

pidfile – Name der pid-Datei des HTTP-Servers. Standardmäßiger Wert: */usr/local/ap-mailfilter3/run/kas-thttpd.pid*

logfile – Name der Protokoll-Datei des HTTP-Servers. Standardmäßiger Wert: */usr/local/ap-mailfilter3/log/kas-thttpd.log*

dir – Pfad zum Verzeichnis, in dem die cgi-Skripte der Verwaltungszentrale gespeichert sind. Standardmäßiger Wert: **/usr/local/ap-mailfilter3/control/www**.

cgipat – ein Muster für Namen der cgi-Skripte. Soll einen Wert ****.cgi** haben.

A.4. Dienstprogramme von Kaspersky Anti-Spam

Dieser Abschnitt enthält Beschreibungen der Werkzeuge von Kaspersky Anti-Spam, dessen Bestimmung und die Befehlszeilenoptionen, welche jeder der Komponente benutzt. Um die Werkzeuge zu starten, müssen Sie als Benutzer **root** eingeloggt sein.

A.4.1. kas-htpasswd

Dienstprogramm *kas-htpasswd* wird zur Verwaltung der Passwortdateien für die Verwaltungszentrale benutzt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd [-c]
<passwort_datei> <Benutzername> [-h]
```

Befehlszeilenoptionen:

- **passwort_datei** – Pfad zur Datei, welche die Passwörter beinhaltet. Standardmäßig wird die Datei *.htpasswd* benutzt. Dienstprogramm kann entweder einen neuen Benutzer hinzufügen, oder Passwort eines existierenden Benutzer ändern;
- **benutzername** – Benutzername des Benutzer, für welchen das Passwort geändert wird;
- **-c** – neue Passwortdateie erstellen; wenn dieser Parameter nicht angegeben ist, muß Parameter **passwort_datei** auf eine existierende Datei zeigen;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.

A.4.2. kas-show-license

Dienstprogramm *kas-show-license* wird zum Ansehen der Informationen über Installierte Lizenzdateien in der Befehlszeile benutzt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/kas-show-license
[-k <schlüsseldatei>] [-c <konfigurationsdatei>]
```

Befehlszeilenooptionen:

- k** <**schlüsseldatei**> – die Informationen über Lizenzschlüssel mit dem Namen **schlüsseldatei** anzeigen;
- c** <**konfigurationsdatei**> – Pfad zur Konfigurationsdatei *filter.conf* neue definieren. Wenn die Konfigurationsdatei *filter.conf* nicht im standardmäßigen Verzeichnis abgelegt ist, geben Sie als Parameter **konfigurationsdatei** den kompletten Pfad zur Datei *filter.conf*.



Wenn keine Parameter beim Starten des Werkzeugs angegeben werden, wird auf der Konsole die Information über alle installierte Lizenzschlüssel angezeigt.

A.4.3. install-key

Dienstprogramm *install-key* wird zur Installation der Lizenzschlüssel von Kaspersky Anti-Spam benutzt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/install-key -i [-
q] [-d]
[-v] [-l] [-V <protokollgenauigkeit>]
[-L <Protokollgenauigkeit>] [-c
<konfigurationsdatei>]
[-k <skript_kas-conf>] [-h]
```

Befehlszeilenooptionen:

- –**i** – keine Information über Lizenz nach der Installation auf der Konsole anzeigen;
- –**q** – nur Fehlermeldungen auf der Konsole anzeigen;
- –**d** – Detaillierte Informationen über Installationsvorgang des Lizenzschlüssels auf der Konsole anzeigen;
- –**v** – eine höhere, im Vergleich mit standardmäßigen, Detaillierung der Meldungen benutzen, welche auf der Konsole angezeigt werden;
- –**V** <**protokollgenauigkeit**> – angegebene Stufe der Protokollgenauigkeit für die Konsole benutzen, mögliche Werte: **1...10**;
- –**l** – eine höhere Detaillierung der Meldungen beim Eintragen in Systemprotokoll benutzen, als standardmäßig definiert ist;

- **-L <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Meldungen benutzen, welche in Systemprotokoll geschrieben werden; mögliche Werte: **1...10**;
- **-c <konfigurationsdatei>** – den Pfad zur Konfigurationsdatei *filter.conf* neue definieren; wenn die Datei *filter.conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **konfigurationsdatei** den vollständigen Pfad zur Datei *filter.conf*;
- **-k <skript_kas-conf>** – den Pfad zum Skript *kas-conf*, welches das Einlesen der Kaspersky Anti-Spam Konfiguration ausführt, neue definieren; wenn *kas-conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **skript_kas-conf** den vollständigen Pfad zur Datei *kas-conf*;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.

A.4.4. remove-key

Dienstprogramm `remove-key` ist zum Löschen der Lizenzschlüssel von Kaspersky Anti-Spam bestimmt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/remove-key [-a|-r] [-q] [-d] [-v] [-l] [-V <protokollgenauigkeit>] [-L <protokollgenauigkeit>] [-c <konfigurationsdatei>] [-k <skript_kas-conf>] [-h]
```

Befehlszeilenoptionen:

- **-a** – Alle installierte Lizenzschlüssel entfernen;
- **-r** – Reserve-Schlüssel entfernen;
- **-q** – nur Fehlermeldungen auf der Konsole anzeigen;
- **-d** – einen Detaillierten Bericht über Deinstallationsprozess des Lizenzschlüssels auf der Konsole anzeigen;
- **-v** – eine höhere, im Vergleich mit standardmäßigen, Detaillierung der Meldungen benutzen, welche auf der Konsole angezeigt werden;
- **-V <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Konsole benutzen; mögliche Werte: **1...10**;

- **-l** – eine höhere Detaillierung der Meldungen beim Eintragen in Systemprotokoll benutzen, als standardmäßig definiert ist;
- **-L <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Meldungen benutzen, welche in Systemprotokoll geschrieben werden; mögliche Werte: **1...10**;
- **-c <konfigurationsdatei>** – den Pfad zur Konfigurationsdatei *filter.conf* neue definieren; wenn die Datei *filter.conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **konfigurationsdatei** den vollständigen Pfad zur Datei *filter.conf*;
- **-k <skript_kas-conf>** – den Pfad zum Skript *kas-conf*, welches das Einlesen der Kaspersky Anti-Spam Konfiguration ausführt, neue definieren; wenn *kas-conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **skript_kas-conf** den vollständigen Pfad zur Datei *kas-conf*;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.

A.4.5. kas-restart

Dienstprogramm *kas-restart* wird zum Neustarten von Kaspersky Anti-Spam und seine einzelne Komponente benutzt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/kas-restart [-f]
[-p] [-s] [-m] [-w] [-W] [-q] [-d] [-v] [-l]
[-V <protokollgenauigkeit>] [-L
<protokollgenauigkeit>]
[-c <konfigurationsdatei>] [-k <skript_kas-conf>]
[-h]
```

Befehlszeilenoptionen:

- **-f** – Filterungsprozesse *ap-mailfilter* *neustarten*. Die Prozesse bearbeiten die E-Mails und werden beendet abhängig von den Einstellungen der Zeitverzögerung und Anzahl zu bearbeitenden E-Mails (Details s. Pkt. 0 auf S. 63);
- **-p** – Masterprozess der Filterung *ap-process-server* *neustarten*. Führt auch zum Neustart der Filterungsprozesse *ap-mailfilter*. Wenn diese Option benutzt wird, werden die Filterungsprozesse sofort nach der Bearbeitung der laufenden E-Mail neugestartet. Die Option wird benutzt, wenn Änderungen an den Startoptionen der Filterungsprozesse vorgenommen wurden;
- **-s** – Lizenzierungsmodul *neustarten* *kas-license*;

- **-m** – Modul *kas-milter* neustarten;
- **-w** – Web-Server *kas-tthttpd* neustarten;
- **-W** – Wechsel der log-Dateien des Web-Servers *kas-tthttpd* durchführen (neue Protokolldatei erstellen).
- **-q** – "leisen" Modus benutzen; auf der Konsole werden nur Fehlermeldungen und Warnungen angezeigt;
- **-d** – einen detaillierten Bericht über die Arbeit des Werkzeuges auf der Konsole anzeigen;
- **-v** – eine höhere, im Vergleich mit standardmäßigen, Detaillierung der Meldungen benutzen, welche auf der Konsole angezeigt werden;
- **-V <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Konsole benutzen; mögliche Werte: **1...10**;
- **-l** – eine höhere Detaillierung der Meldungen beim Eintragen in Systemprotokoll benutzen, als standardmäßig definiert ist;
- **-L <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Meldungen benutzen, welche in Systemprotokoll geschrieben werden; mögliche Werte: **1...10**;
- **-c <konfigurationsdatei>** – den Pfad zur Konfigurationsdatei *filter.conf* neue definieren; wenn die Datei *filter.conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **konfigurationsdatei** den vollständigen Pfad zur Datei *filter.conf*;
- **-k <skript_kas-conf>** – den Pfad zum Skript *kas-conf*, welches das Einlesen der Kaspersky Anti-Spam Konfiguration ausführt, neue definieren; wenn *kas-conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **skript_kas-conf** den vollständigen Pfad zur Datei *kas-conf*;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.



Das Starten des Werkzeuges ohne Optionen ist dem Starten mit der Option **-f** gleich.

A.4.6. mkprofiles

Dienstprogramm *mkprofiles* wird zum Bilden und Kompilieren der Filterungsrichtlinien von Kaspersky Anti-Spam benutzt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/mkprofiles
[-c <konfigurationsdatei>] [-l <berichtsdatei>] [-q] [-v] [-h]
```

wo

- **-c <konfigurationsdatei>** – den Pfad zur Konfigurationsdatei *filter.conf* neu definieren; wenn die Datei *filter.conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **konfigurationsdatei** den vollständigen Pfad zur Datei *filter.conf*,
- **-l <berichtsdatei>** – Prozessergebnisse in eine Datei speichern, welche mit dem Parameter **berichtsdatei** definiert ist;
- **-q** – "leisen" Modus benutzen; auf der Konsole werden nur Fehlermeldungen und Warnungen angezeigt;
- **-v** – alle Meldungen über Kompilationsprozess auf der Konsole anzeigen;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.

Wenn Werkzeug ohne Optionen gestartet wird, werden auf der Konsole Meldungen über Fehler und Warnungen, wie auch Informationen über erfolgreich abgeschlossene Operationen angezeigt.

A.4.7. sfmonitoring

Dienstprogramm *sfmonitoring* durchführt die Überprüfung des laufenden Zustands der Komponente von Kaspersky Anti-Spam und zeigt, wenn Fehler auftreten, Fehlerinformationen auf der Konsole.

Startbefehl:

```
su -m mailflt3 -c '/usr/local/ap-mailfilter3/control/bin/sfmonitoring [-p] [-m] [-q] [-h]'
```

Wenn Kaspersky Anti-Spam auf einem Server mit RedHat-Betriebssystem installiert ist, geben Sie zum Starten des Werkzeugs *sfmonitoring* *in der Befehlszeile folgendes ein*:

```
su - -m mailflt3 -c '/usr/local/ap-mailfilter3/control/bin/sfmonitoring [-p] [-m] [-q] [-h]'
```

Befehlszeilenoptionen:

- **-p** – Systemzustand überprüfen und die Informationen über Fehlfunktionen des Kaspersky Anti-Spam auf der Konsole anzeigen;

- **-m** – Systemzustand überprüfen und die Informationen über Fehlfunktionen des Systems per E-Mail versenden;
- **-q** – leisen" Modus benutzen; auf der Konsole werden nur Fehlermeldungen und Warnungen angezeigt;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.

Wenn Dienstprogramm ohne Optionen gestartet wird, wird Systemzustand überprüft, beim Auffinden von neuen Fehlfunktionen wird eine E-Mail mit Warnung über gefundene Fehler versendet.

A.4.8. sfupdates

Dienstprogramm sfupdates wird zum Downloaden der Updates für Inhaltsfilterungsdatenbanken und deren Installation für weitere Verwendung von Filterungsserver benutzt.

Startbefehl:

```
# /usr/local/ap-mailfilter3/bin/sfupdates
[-c <konfigurationsdatei>] [-f] [-k <skript_kas-
conf>] [-s] [-q] [-v] [-d] [-V
<protokollgenauigkeit>] [-l]
[-L <protokollgenauigkeit>] [-h]
```

Befehlszeilenoptionen:

- **-c <konfigurationsdatei>** – den Pfad zur Konfigurationsdatei *filter.conf* neu definieren; wenn die Datei *filter.conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **konfigurationsdatei** den vollständigen Pfad zur Datei *filter.conf*;
- **-f** – das Kompilieren der Konfiguration erzwingen. Wenn die Option nicht angegeben ist, wird die Konfiguration nur dann kompiliert, wenn Updates für Inhaltsfilterungsdatenbanken bekommen wurden;
- **-k <skript_kas-conf>** – den Pfad zum Skript *kas-conf*, welches das Einlesen der Kaspersky Anti-Spam Konfiguration ausführt, neu definieren; wenn *kas-conf* sich nicht im standardmäßigen Verzeichnis befindet, geben Sie als Parameterwert für **skript_kas-conf** den vollständigen Pfad zur Datei *kas-conf*;
- **-s** – Updatedownload übergehen;
- **-q** – nur Fehler auf der Konsole anzeigen. Dieser Modus wird zum Starten per *cron*-Dienst empfohlen;

- **-v** – eine höhere, im Vergleich mit standardmäßigen, Detaillierung der Meldungen benutzen, welche auf der Konsole angezeigt werden;
- **-d** – die höchste Stufe der Protokollgenauigkeit der Meldungen benutzen, welche auf der Konsole gezeigt werden;
- **-V <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Konsole benutzen; mögliche Werte: **1...10**;
- **-l** – eine höhere Detaillierung der Meldungen beim Eintragen in Systemprotokoll benutzen, als standardmäßig definiert ist;
- **-L <protokollgenauigkeit>** – angegebene Stufe der Protokollgenauigkeit für die Meldungen benutzen, welche in Systemprotokoll geschrieben werden; mögliche Werte;
- **-h** – Hilfe zum Werkzeug auf der Konsole anzeigen.

Wenn keine der Aufgezählten Optionen benutzt wurde, werden auf der Konsole Meldungen über Fehler und Warnungen, wie auch Informationen über erfolgreich abgeschlossene Operationen angezeigt.

A.5. Extra-Header des Filterungsmoduls

Bei der Bearbeitung der E-Mail fügt Kaspersky Anti-Spam folgende Header der E-Mail hinzu:

- **X-Spamtest-Version – Header, welcher** Informationen über Kaspersky Anti-Spam Version enthält.
- **X-Spamtest-Status und X-Spamtest-Status-Extended** – Header, welche den nach der Filterung erhaltenen E-Mail-Status enthalten. Header X-Spamtest-Status **wurde in früheren** Versionen des Produkts benutzt. Dieser Header enthält eine Reihe der Statuse, welche der Version von Kaspersky Anti-Spam 2.0 entsprechen, und wird für die Abwärtskompatibilität benutzt. **Mögliche werte** des Headers werden in der Tabelle aufgezählt.

Header	Wert	Beschreibung
X-Spamtest-Status	Trusted	Absender ist in der "weißen" Liste oder für diesen Benutzer ist Spamuntersuchung

		ausgeschaltet.
	SPAM	Nachricht wurde als Spam klassifiziert.
	Probable Spam	Nachricht wurde als möglicher Spam klassifiziert.
	Not detected	Nachricht wurde nicht als Spam oder möglicher Spam klassifiziert.
X-Spamtest-Status-Extended	trusted	Absender ist in der "weißen" Absender-Liste oder für diesen Absender ist in Gruppenrichtlinien die Untersuchung nach Spam ausgeschaltet.
	blacklisted	Absender ist in der "schwarzen" Absender-Liste.
	Spam	Nachricht wurde als Spam identifiziert.
	probable_spam	Nachricht wurde als möglicher Spam klassifiziert.
	formal	Nachricht wurde als formale Mailserverantwort klassifiziert.
	not_detected	Nachricht wurde nicht als Spam oder möglicher Spam klassifiziert.

- **X-Spamtest-Header** – Header, welcher den vom Administrator mit Hilfe der Verwaltungszentrale vorgegebenen Text enthält (s. Pkt. 4.3.7 auf S. 53);
- **X-Spamtest-Obscene** – Header, welcher in die E-Mail mit Obszönitäten eingefügt wird.

- **X-SpamTest-Formal** – Header, welcher in die E-Mail mit dem Status **Formal** eingefügt wird.
- **X-Spamtest-Rate** – Header, welcher die Bewertung enthält, die während der Filterung der E-Mail vergeben. Kaspersky Anti-Spam benutzt diesen Wert bei Statusvergabe für die E-Mail;
- **X-Spamtest-Group-ID** – Header, der den Gruppenidentifikator der Gruppe enthält, nach Regeln welcher die E-Mail bearbeitet wurde.
- **X-SpamTest-Categories** – Header, welcher den Namen der Kategorie enthält, die an E-Mail nach der Filterung vergeben wurde.
- **X-SpamTest-Info** – Header, welcher Info-Meldungen enthält.
- **X-Spamtest-Envelope-From** – Header, welcher die Absenderadresse aus dem SMTP-Paket enthält. Dieser Header wird zum Verfolgen der Reaktion von lokalen "schwarzen" und "weißen" Listen benutzt .
- **X-SpamTest-Method** – Header, welcher Bezeichnung der Methoden enthält, die bei der Statusvergabe benutzt wurden. Mögliche **werte** des Headers werden in der Tabelle aufgezählt.

Wert	Methode
white ip list	IP-Adressen der Absender werden über "weiße" Liste überprüft.
white E-Mail list	E-Mail-Adressen der Absender werden über "weiße" Liste überprüft.
black ip list	Überprüfung über die "schwarze" Liste der Absender IP-Adressen.
black E-Mail list	Überprüfung über die "schwarze" Absenderliste.
GSG	Analyse der grafischen Signaturen.
headers und headers plus	E-Mail-Kopf Analyse.
DNSBL	Überprüfung mit Hilfe DNSBL-Dienste.

UDS	Überprüfung mit Hilfe UDS- Dienste.
UDS BL	Überprüfung mit Hilfe des UDS-Dienstes. Ist eine kombinierte Überprüfung nach heuristischen Regeln und "schwarzen" Listen
SURBL	Überprüfung mit Hilfe des SURBL- Dienstes.
Content	Überprüfung des E-Mail-Inhalts.
probable	Methode "möglicher Spam".
detection disabled	Für Empfänger ist in den Gruppenrichtliniern die Überprüfung der E-Mails auf Spam ausgeschaltet.
Multiple	Bei der Statusvergabe wurden mehrere Methoden benutzt.
None	Keine der Methoden erlaubt es, die E-Mail zu klassifizieren. Solche Nachrichten erhalten den Status Not detected .

A.6. Einstellungen des *cron*-Dienstes

Für korrekte Arbeit von Kaspersky Anti-Spam muß das Starten von Skripte mit Hilfe des Dienstes cron unter Benutzerkennung **mailflt3** gewährleistet werden.

Um die Parameter der Skripte zu ändern benutzen Sie folgenden Befehl:

```
# crontab -u mailflt3 -e
```

In die Taskliste tragen Sie folgende Skripte ein:

- **Updateskript der Inhaltsfilterung-Datenbanken.**

Startbefehl: `/usr/local/ap-mailfilter3/bin/sfupdates -q`

Empfohlener Rhythmus: alle zwanzig Minuten.



Um der Überlastung der Updateserver ausweichen, geben Sie eine Verzögerung bezüglich Stundenanfang an, z. B.:

```
7,27,47 * * * * /usr/local/ap-mailfilter3/bin/sfupdates -q
```

- **Monitoringskript.**

Startbefehl:

```
/usr/local/ap-  
mailfilter3/control/bin/sfmonitoring -q
```

Empfohlene Rhythmus: alle fünf Minuten.

- **Skript der Protokollbearbeitung und Statistikerneuerung.**

Dieses Skript sammelt die Statistik über bearbeitete Nachrichten aus den Protokollen von Kaspersky Anti-Spam, und führt die Bearbeitung der Protokolle des Filterungsserver für die Darstellung in dem Interface von Verwaltungszentrale.

Startbefehl:

```
/usr/local/ap-mailfilter3/control/bin/dologs.sh -  
q
```

Empfohlener Rhythmus: jede Minute.

- **Skript zur erneuerung der statistischen Diagramme.**

Dieses Skript führt die Erstellung der statistischen Diagramme für bearbeitete Nachrichten durch, zur Darstellung im Abschnitt **Statistics** der Verwaltungszentrale.

Startbefehl:

```
/usr/local/ap-mailfilter3/control/bin/dograph.sh  
-q
```

Empfohlener Rhythmus: ein Mal in fünf Minuten.

- **Protokollrotierung-Skript.**

Um die Überfühlung der Festplatten zu umgehen und die Leistungsfähigkeit zu steigern, wird es empfohlen die Protokolldateien des Filterungsserver zu rotieren. Dieses Skript ist zur Rotation der interne Protokolle bestimmt, welche von der Verwaltungszentrale benutzt werden.

Startbefehl:

```
/usr/local/ap-  
mailfilter3/control/bin/logrotate.sh -q
```

Empfohlene Zeitspanne: zwei Mal am Tag. Bei steigender Belastung können die Protokolle öfter rotiert werden.

- **Skript für die Zeitberechnung des Zugangs zu den UDS-Servern.**

Skript *uds-rtts.sh* wird zur Zeitbestimmung für den Zugang zu den UDS-Servern von Kaspersky Lab. Die errechneten Daten werden zur Bestimmung des optimalen Servers für UDS-Anfrage benutzt.

Startbefehl:

```
/usr/local/ap-mailfilter3/bin/uds-rtts.sh -q
```

Empfohlener Rhythmus: alle 10-15 Minuten.

Außer Einstellungen der Skripte wird empfohlen folgendes zu tun:

- Pfad zum Verzeichnis angeben, in dem die Skripte ausgeführt werden, als Wert der Variablen *HOME*. Empfohlener Pfad: */usr/local/ap-mailfilter3/run*.
- Liste der Pfade zu den System-Dienstprogrammen angeben, unter Anderem zum Werkzeug *sendmail*², als Wert der Variablen *PATH*. Standardmäßiger Wert: */bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin*
- Adresse angeben, an welche die Meldungen über Skriptausführung mit Hilfe der Variablen *MAILTO* gesendet werden. Standardmäßiger Wert: *postmaster*.

Weter sehen Sie ein Beispiel der Datei *crontab*, welches die beschriebenen Einstellungen zeigt:

```
MAILTO=admin@mycompany.com
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin
:/usr/local/sbin
HOME=/usr/local/ap-mailfilter3/run
7,27,47 * * * * /usr/local/ap-
mailfilter3/bin/sfupdates -q
*/5 * * * * /usr/local/ap-
mailfilter3/control/bin/sfmonitoring -q
* * * * * /usr/local/ap-
mailfilter3/control/bin/dologs.sh -q
*/5 * * * * /usr/local/ap-
mailfilter3/control/bin/dograph.sh -q
0 */12 * * * /usr/local/ap-
mailfilter3/control/bin/logrotate.sh -q
4-59/11 * * * * /usr/local/ap-
mailfilter3/bin/uds-rtts.sh -q
```

² Wird vom Monitoringskript benutzt.

ANHANG B. WIE KANN SPAM AN DIE ANALYTIK-GRUPPE VERSCHICKT WERDEN

Kaspersky Lab ist allen Benutzern dankbar, welche neuen Spam-Muster an die Spam-Analytiker zu senden. Diese Muster helfen uns schnell auf neue Arten vom Spam zu reagieren und den Spam-Versand im Anfangsstadium zu bekämpfen.

Sie können auch die Muster an uns schicken, welche fälschlicher Weise als Spam erkannt wurden. Diese Nachrichten werden von unseren Linguisten sorgfältig untersucht, dies hilft uns die Qualität der Spamerkennung und die Anzahl der Fehlfunktionen zu verringern.

Wenn das Zusenden der Muster nach der unten angebrachten Vorschrift passiert, wird die Bearbeitung der Nachrichten automatisieren lassen und so die Reaktionszeit verringern.

E-Mailadresse für Spam:	spam@kaspersky.com
E-Mailadresse für fälschlicher Weise als Spam erkannte Nachrichten:	notspam@kaspersky.com



Die Spammuster sollen als eingefügte Dateie zugesand werden.

Unterschiedliche Programme haben verschiedene Mittel, welche es erlauben die E-Mail-Header bei der Weiterleitung zu erhalten. Wir werden die Handlungen für die am Meisten benutzten Programme beschreiben.

1. Um Spammuster aus dem Microsoft Office Outlook zu versenden, gehen Sie wie folgt vor:
 - Wenn sie nur eine E-Mail weiterleiten wollen, dann erstellen Sie eine neue Nachricht mit Hilfe der Schaltfläche **New** (Neue) oder des Befehls **New Mail Message** (Neue Nachricht) und ziehen Sie mit der Maus die Spam-Nachricht in die neue E-Mail;
 - Wenn Sie mehrere Nachrichten weiterleiten wollen, dann markieren Sie diese Nachrichten und klicken Sie auf die Schaltfläche **Forward** (Weiterleiten). E-Mail-Programm wird

diese Nachrichten automatisch als Einlagen in die neue E-Mail einfügen.

2. Um Spammuster aus dem Programm The Bat! zu versenden, gehen Sie wie folgt vor:
 - Wenn Sie die Nachricht per Hand weiterleiten wollen, markieren Sie eine oder mehrere E-Mails und benutzen Sie den Befehl **Weiterleiten (alternative Methode)** oder **Alternative Forward**. Dieser Befehl wird in dem Menü **Specials** ausgewählt.
 - Wenn Sie automatisches Weiterleiten einstellen wollen, erstellen Sie die Sortierregel in dem "Nachrichtensortierer" wie folgt:
 - Deaktivieren Sie Häkchen **Einlagen nicht weiter leiten**;
 - Setzen Sie Häkchen **Standard MIME benutzen**.
3. Um Spam aus dem Microsoft Outlook Express weiter zu leiten, markieren Sie eine oder mehrere E-Mails und führen Sie den Befehl **Message → Forward as Attachmen (Nachricht → Als Einlage weiterleiten)** aus.

ANHANG C. DAS UNTERNEHMEN

Kaspersky Lab wurde im Jahr 1997 gegründet. Heute ist Kaspersky Lab ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz.

Kaspersky Lab ist ein weltweites Unternehmen. Das Hauptquartier ist in Moskau und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China. In Frankreich wurde eine neue Niederlassung eröffnet – Europäisches Zentrum für Antivirus-Forschungen. Unser Partner-Netzwerk besteht aus über 500 Firmen in der ganzen Welt.

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, zehn von ihnen haben MBA-Diplom, sechzehn haben Doktorgrad; darunter sind auch Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board.

Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen. Dank unserer weitreichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien. Das Hauptprodukt, Kaspersky Anti-Virus[®], gewährleistet einen sicheren Schutz für alle Angriffsziele der Viren: Arbeitsstationen, Fileserver, E-Mailsysteme, Router, und PDA. Bequeme Mittel geben den Benutzern die Möglichkeit den Schutz maximal zu automatisieren. Viele Firmen benutzen in ihren Programmen den Kern vom Kaspersky Anti-Virus[®], z. B., solche, wie: Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

C.1. Weitere Produkte und Services von Kaspersky Lab

Kaspersky® OnLine Scanner

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Webbrowser ausgeführt und verwendet die Technologie Microsoft ActiveX®. Dadurch kann der Benutzer auf schnelle Weise herausfinden, ob sein Computer von einer Infektion durch schädliche Programme bedroht ist. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.;
- standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen;
- die Untersuchungsergebnisse in Berichten mit dem Format txt und html speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Webbrowser ausgeführt und verwendet die Technologie Microsoft ActiveX®. Im Rahmen der Untersuchung kann der Benutzer:

Archive und Mail-Datenbanken von der Untersuchung ausschließen;

standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen;

die Untersuchungsergebnisse in Berichten mit dem Format txt und html speichern.

Антивирус Касперского® 6.0

Kaspersky Anti-Virus 6.0 dient dem Schutz eines Personalcomputers vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antivirenuntersuchung, die folgende Optionen umfasst:

Antivirenuntersuchung des Mail-Datenstroms auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und

SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm, sowie Untersuchung und Desinfektion von Mail-Datenbanken;

Antivirenuntersuchung des Internet-Datenstroms, der per HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus;

Antivirenuntersuchung beliebiger einzelner Dateien, Ordner und Laufwerke. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystems Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

Kontrolle über Veränderungen im Dateisystem. Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.

Überwachung von Prozessen im Arbeitsspeicher. Kaspersky Anti-Virus 6.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn normale Prozesse auf unerlaubte Weise verändert werden.

Überwachung von Veränderungen in der Registrierung des Betriebssystemes durch die Kontrolle des Zustands der Systemregistrierung.

Sperren gefährlicher Makros des Typs Visual Basic for Applications in Microsoft Office Dokumenten.

Systemwiederherstellung nach schädlicher Einwirkung von Spyware: Die Wiederherstellung wird durch die Speicherung aller Veränderungen in der Registrierung und im Dateisystem des Computers und durch das vom Benutzer initiierte Rückgängigmachen der Veränderungen ermöglicht.

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Microsoft Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeicher, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

einen Virenschanner, der eine Überprüfung der Daten (sowohl im Speicher des PDA selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;

den Antivirus-Monitor, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung im Speicher des PDA und auf Speicherkarten.

Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz³ vor Viren für:

Computerarbeitsplätze unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation, Linux.

Dateiserver unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD und OpenBSD, Linux, Samba Servers.

Mailsysteme vom Typ Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail und Qmail.

Internet-Firewalls: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Kaspersky Anti-Virus® Business Optimal beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite ist eine integrierte Softwarelösung zum Datenschutz für Ihr gesamtes Firmennetzwerk ohne Einschränkungen hinsichtlich Größe und Struktur. Die enthaltenen Programmkomponenten schützen jeden Punkt ihres firmeninternen Netzes. Sie sind kompatibel mit den meisten heute verbreiteten Betriebssystemen und Anwendungen, über ein zentrales Verwaltungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

Kaspersky® Corporate Suite bietet Rundumschutz⁴ vor Viren für:

Computerarbeitsplätze unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation und Linux.

³ Je nach Lieferumfang

⁴ Je nach Lieferumfang

Dateiserver unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux und Samba Servers.

Mailsysteme vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.

Internet-Firewalls: Microsoft ISA Server 2004 Enterprise Edition.

Handheld-PCs, die unter Microsoft Windows CE und Palm OS arbeiten, sowie Smartphones, die unter Microsoft Windows Mobile 2003 for Smartphone und Microsoft Smartphone 2002 arbeiten.

Kaspersky® Corporate Suite beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux / Unix dient dem Antivirenschutz von E-Mails, die per SMTP-Protokoll weitergeleitet werden. Die Anwendung umfasst eine Reihe von zusätzlichen Filterinstrumenten für den Mailverkehr (Filterung nach Namen und MIME-Typen von Attachments) sowie eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu verringern und Hackerangriffe abzuwehren. Dazu zählen die Begrenzung der maximalen Mailgröße, der Anzahl von Adressaten usw. Die Unterstützung der Technologie DNS Black List schützt vor dem Empfang von Mails, die von Servern stammen, die auf diesen Listen stehen und als Verbreitungsquellen für Spam gelten.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security® for Microsoft Exchange bietet die Antivirenuntersuchung der eingehenden, ausgehenden und auf dem Server gespeicherten E-Mail-Nachrichten einschließlich der Nachrichten in gemeinsamen Ordnern. Außerdem führt er die Filterung unerwünschter Korrespondenz aus, wobei intelligente Technologien zur Spam-Erkennung in Verbindung mit den Technologien der Firma Microsoft verwendet werden. Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe der Mail, Kopfzeile) dient. Außerdem analysiert er den Inhalt der Mails und seiner Anhänge mit Hilfe von intelligenten Technologien, wie eindeutige grafische Signaturen zum Erkennen von Spam in grafischer Form. Der Untersuchung werden sowohl der Nachrichtenkörper als auch angehängte Dateien unterzogen.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway ist eine universelle Lösung für den komplexen Schutz der Benutzer von Mailsystemen. Die Anwendung wird zwischen dem Unternehmensnetzwerk und dem Internet installiert und führt die Untersuchung aller Elemente einer E-Mail auf Viren und andere schädliche Programme (Spyware, Adware usw.) durch. Außerdem erfolgt die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale. Die Lösung enthält ferner eine Reihe zusätzlicher Optionen für die Filterung des E-Mail-Stroms.

C.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH

Steinheilstraße 13

85053 Ingolstadt

Technischer Support	Tel.: +49 (0) 841 98 18 90 Fax: +49 (0) 841 98 18 918 E-Mail: support@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.de http://www.viruslist.de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG D. ANWENDUNGEN DER FERMDANBIETER

Während der Ausarbeitung von Kaspersky Anti-Spam 3.0 wurden folgende Anwendungen der Drittanbieter benutzt:

Bibliothek Berkeley DB 1.85 unter folgenden Bedingungen benutzt:

Copyright (c) 1990, 1993, 1994 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Margo Seltzer.

- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
- Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bibliothek libjpeg 6b wird unter folgenden Bedingungen benutzt:

LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

Bibliothek libungif wird unter folgenden Bedingungen benutzt:

The GIFLIB distribution is Copyright (c) 1997 Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy,

modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Bibliothek libevent wird unter folgenden Bedingungen benutzt:

Copyright (c) 2000-2004 Niels Provos <provos@citi.umich.edu>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Web-Server thttpd wird unter folgenden Bedingungen benutzt:

Copyright 1995,1998,1999,2000,2001 by Jef Poskanzer <jef@acme.com>.

All rights reserved.

1. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
2. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
3. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bibliothek libspf2 wird unter folgenden Bedingungen benutzt:

The code in the libspf-alt distribution is Copyright 2004 by Wayne Schliitt, all rights reserved. Copyright retained for the purpose of protecting free software redistribution.

This program is free software; you can redistribute it and/or modify it under the terms of either:

- a. the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1, or (at your option) any later version,

OR

- b. The two-clause BSD license.

Some code in the 'replace' subdirectory was obtained from other sources and have different, but compatible, licenses. These routines are used only when the native libraries for the OS do not contain these functions. You should review the licenses and copyright statements in these functions if you are using an OS that needs these functions.

The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bibliothek libpatricia wird unter folgenden Bedingungen benutzt:

Copyright (c) 1997, 1998, 1999

The Regents of the University of Michigan ("The Regents") and Merit Network, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of Michigan, Merit Network, Inc., and their contributors.

4. Neither the name of the University, Merit Network, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bibliothek pcre wird unter folgenden Bedingungen benutzt:

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bibliothek xdr wird unter folgenden Bedingungen benutzt:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

Bibliothek zlib wird unter folgenden Bedingungen benutzt:

zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.3, July 9th, 1998

Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <ftp://ds.internic.net/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](ftp://ds.internic.net/rfc/rfc1951.txt) (deflate format) and [rfc1952.txt](ftp://ds.internic.net/rfc/rfc1952.txt) (gzip format).

Bibliothek expat wird unter folgenden Bedingungen benutzt:

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

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Bibliothek STLport wird unter folgenden Bedingungen benutzt:

Copyright (c) 1994

Hewlett-Packard Company

Copyright (c) 1996-1999

Silicon Graphics Computer Systems, Inc.

Copyright (c) 1997

Moscow Center for SPARC Technology

Copyright (c) 1999, 2000, 2001, 2002

Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

Bibliothek libmilter unter folgenden Bedingungen benutzt:

The following license terms and conditions apply, unless a different license is obtained from Sendmail, Inc., 6425 Christie Ave, Fourth Floor, Emeryville, CA 94608, USA, or by electronic mail at license@sendmail.com.

License Terms:

Use, Modification and Redistribution (including distribution of any modified or derived work) in source and binary forms is permitted only if each of the following conditions is met:

1. Redistributions qualify as "freeware" or "Open Source Software" under one of the following terms:
 - a. Redistributions are made at no charge beyond the reasonable cost of materials and delivery.
 - b. Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means the complete compilable and linkable source code of sendmail including all modifications.
2. Redistributions of source code must retain the copyright notices as they appear in each source code file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.
3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided

with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

"Copyright (c) 1998-2004 Sendmail, Inc. All rights reserved."

4. Neither the name of Sendmail, Inc. nor the University of California nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission. The name "sendmail" is a trademark of Sendmail, Inc.
5. All redistributions must comply with the conditions imposed by the University of California on certain embedded code, whose copyright notice and conditions for redistribution are as follows:

Copyright (c) 1988, 1993 The Regents of the University of California. All rights reserved.

- a. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
- b. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 - I. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 - II. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 - III. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
6. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY SENDMAIL, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SENDMAIL, INC., THE REGENTS OF THE UNIVERSITY OF CALIFORNIA OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Bibliothek OpenSSL wird unter folgenden Bedingungen benutzt:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

=====

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Bibliothek FreeBSD wird unter folgenden Bedingungen benutzt:

Copyright (C) 1992-2005 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Programm mcpp wird unter folgenden Bedingungen benutzt:

Copyright (c) 1998, 2002-2004 Kiyoshi Matsui <kmatsui@t3.rim.or.jp>

All rights reserved.

Some parts of this code are derived from the public domain software DECUS cpp (1984,1985) written by Martin Minow.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.