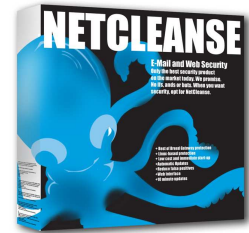


# NetCleanse-Konfiguration – Checkliste

NetCleanse bietet Ihnen umfassende Möglichkeiten und Optionen, um Ihr Netzwerk effizient am Gateway gegen SPAM und Viren zu schützen. Damit Sie eben diese Optionen auch in Ihrem Netzwerk optimal nutzen können, möchten wir Ihnen in der folgenden Checkliste einige Konfigurationseinstellungen aufzeigen, mit denen Sie unter anderem die SPAM-Erkennung in Ihrem Netzwerk blitzschnell optimieren.



Wir empfehlen Ihnen, diese kurze Checkliste vor Inbetriebnahme Ihrer NetCleanse-Installation kurz durchzugehen und die Einstellungen ggf. entsprechend anzupassen.

## Configuration -> General

Menüpunkt	Angepasst
„SPAM Identification Threshold“ unter „SPAM Settings“ auf den Wert 4 gesetzt?	
„Insert X-SPAM Result Headers on SPAM“ unter „SPAM Settings“ aktiviert?	
„Insert X-SPAM Result Headers on HAM“ unter „SPAM Settings“ aktiviert?	
„Block SPAM Messages“ unter „SPAM Settings“ aktiviert?	
„Use SPAM Identification Threshold“ unter „SPAM Settings -> Block SPAM Messages“ aktiviert?	
„Enable Archive Reports“ unter „Archive Reports“ aktiviert?	
Unter „Archive Reports -> Release Address“ die IP des NetCleanse-Servers hinterlegt? *	

\* = Sollen E-Mails auch von außerhalb des Netzwerkes freigegeben werden können, so tragen Sie den Domain-Namen ein.

## Configuration -> SPAM

Menüpunkt	Angepasst
„Greylisting“ unter „SMTP-Level Anti-SPAM“ mit bestehenden Einstellungen aktiviert? *	
Bei POP3-Nutzung: „Score Averaging“ unter „Heuristics“ deaktiviert?	
„SURBL Boost“ unter „Heuristics -> Enable Network Tests“ aktiviert? (Multiplication Factor = 5)	
„RBL Boost“ unter „Heuristics -> Enable Network Tests“ mit bestehenden Einstellungen aktiviert?	
„Advanced Textual Classifier“ inkl. „Unattended Teaching“ aktiviert?	

\* = Kann nicht im Zusammenhang mit POP3-Konten genutzt werden!

**Configuration -> Virus & Attachment Filters**

Menüpunkt	Angepasst
„Archive Infected Messages“ unter „Actions for Infected Messages“ aktiviert? *	
„Archive Messages with Filtered Attachments“ unter „Actions for Filtered Attachements“ aktiviert? *	
„Replace Infected Attachments“ unter „Actions for Infected Messages“ aktiviert?	

\* = Durch Aktivierung der beiden Funktion werden aufgrund von Virenbefall oder verbotener Dateianhänge geblockte Nachrichten in Quarantäne gelegt und können so ggf. durch den Admin nachträglich freigegeben werden.

**Configuration -> Archive Reports**

Menüpunkt	Angepasst
„Copy to HAM Corpus“ unter „Actions for released Messages“ aktiviert?	
„Purge Messages older than“ unter „Archive Management -> Enable Archive Purging“ auf 20 gesetzt? *	

\* = Beachten Sie bitte, dass bei höheren Werten die Nachrichten länger von NetCleanse in der Quarantäne gespeichert werden und das daher evtl. ein höheres Speichervolumen der Festplatte erforderlich sein kann.

**Configuration -> SMTP**

Menüpunkt	Angepasst
„Validate Recipients via SMTP“ unter „Connection“ aktiviert?*	
„Undeliverable Age“ unter „Undeliverables auf 72 gesetzt? **	

\* = Kann nicht im Zusammenhang mit POP3-Konten genutzt werden!

\*\* = Durch die Einstellung speichert NetCleanse Ihre E-Mails für 72 Stunden, wenn diese nicht direkt zustellbar sind. Somit gehen keine E-Mails verloren, wenn Ihr interner E-Mail-Server zum Beispiel an einem Freitag-Abend abstürzt. Im Gegenzug versucht NetCleanse aber auch für 72 Stunden ausgehende Nachrichten zuzustellen. Somit bekommen Sie die Meldung, dass eine ausgehende Nachricht evtl. nicht zugestellt werden konnte, auch mit 72 Stunden Verzögerung!