

# Ihr Schutz vor unerwünschter Post - PPP Mailfilter

Leistungsbeschreibung und Preise  
Stand 01.02.2006, Seite 1 von 4



## PPP Mailfilter

Die Zusendung unerwünschter E-Mail in Form von Werbemails und virenverseuchten Mails hat in den vergangenen Jahren stark zugenommen. PPP bietet infolge dessen mehrere Möglichkeiten, diese Flut unerwünschter E-Mails einzugrenzen. Es bestehen z.Z. folgende Möglichkeiten:

- Definition, welche Mailadressen Mails empfangen dürfen (Mailadreßfilter)
- Besondere Kennzeichnung durch Scannen des Inhaltes nach bestimmten Merkmalen auf Spam oder Viren (Spam- und Virenskan)
- Grundsätzliche Ablehnung von E-Mails im ersten Zustellversuch (Greylisting)

## PPP Mailadreßfilter

PPP bietet im Extranet unter dem Menüpunkt „Konfigurationsänderungen“ die Möglichkeit, gültige Mailadreßfilter zu definieren:

1. Es können Mails grundsätzlich angenommen und Ausnahmen dazu definiert werden. Dies eignet sich, um einzelne mißbrauchte Adressen zu sperren.
2. Es können Mails grundsätzlich abgelehnt und Ausnahmen dazu definiert werden. In diesem Falle müssen Sie alle E-Mail-Adressen, die erreichbar sein sollen, in der Datenbank als Ausnahme definieren, da nur diese adressierte Mails empfangen können.

Die Liste kann über ein Webinterface im Extranet von Ihnen erstellt und verwaltet werden. Im oberen Abschnitt des Interfaces können Sie dabei ein Grundverhalten einstellen: Entweder werden alle Mails angenommen oder abgelehnt. Außerdem kann das Filtern der Domain komplett deaktiviert werden. Dabei bleibt eine bestehende Liste erhalten, wird aber nicht beachtet. Das bedeutet: Alle Mails für die Domain werden angenommen. Im unteren Abschnitt können Sie in einer Liste Ausnahmen zum Grundverhalten (annehmen/ablehnen) definieren oder auch wieder löschen.

Die Aktualisierung der Konfiguration des Filters erfolgt in 15-minütigen Abständen.

Voraussetzung ist, daß die PPP-Mailserver als höchste MX-Hosts für Ihre Kundendomain im DNS eingetragen sind. Die Server nehmen Mails für diese Domain an und leiten diese an Ihren Mailserver weiter. Bei der Annahme der Mails wird eine Datenbank mit erlaubten und/oder verbotenen Empfänger-Mailadressen befragt. Ist der Empfänger einer Mail nicht als erlaubter Empfänger definiert, wird die Mail abgewiesen. Der Absender-Host bekommt die Meldung „Mailbox disabled for this recipient“ zurück. Es entsteht kein Mailvolumen für nicht definierte Empfängeradressen.

## Beispiel 1:

Mails für die Domain „kundendomain.de“ werden weitergeleitet, außer für die Accounts badaddress1 und badaddress2

Mails für alle in der Domain:

- annehmen     ablehnen     Filter inaktiv



außer für diese Accounts:

badaddress1@kundendomain.de

badaddress2@kundendomain.de

Beispiel 2:

Unter Domain „kundendomain.de“ werden nur Mails für die Accounts mitarbeiter1 und mitarbeiter2 angenommen, alle anderen Mails werden abgewiesen.

Mails für alle in der Domain:

annehmen     ablehnen     Filter inaktiv

außer für diese Accounts:

mitarbeiter1@kundendomain.de

mitarbeiter2@kundendomain.de

Die Nutzung des Mailadrefilters über das Webinterface ist kostenlos. Für umfangreichere Listen, welche automatisiert gepflegt werden sollen, bieten wir die Möglichkeit, die Liste bei uns in einem bestimmten Format einzureichen und automatisiert zu verarbeiten. Bei Bedarf sprechen Sie uns bzgl. Kosten und Realisierung dieser Lösung gerne an.

#### PPP Spam- und Virenschan

Der Inhalt der E-Mail wird vor Zustellung auf bestimmte Parameter überprüft. Wird die E-Mail nach einem heuristischen Verfahren als Spam oder als virenbehaftet erkannt, erfolgt die Kennzeichnung in der Betreffzeile mit XXX\*\*\*\*\*XXX und ist so übersichtlich aus dem regulären Mailverkehr filterbar. Auf Wunsch können geschäftskritische E-Mailadressen, bei denen eine Kennzeichnung nicht gewünscht ist, von dem Verfahren ausgenommen werden.

PPP Spamschan untersucht eingehende Mails daraufhin, ob sie massenhaft versandte Werbe- oder ähnliche Mails darstellen, kennzeichnet sie und erleichtert somit die Aussortierung der empfangenen Spam-E-Mails.

Alle eingehenden Mails werden bei Nutzung unseres Spamschans durch ein dynamisches und komplexes Filterprogramm bewertet. Wird eine bestimmte Anzahl an spamverdächtigen Kriterien erreicht, so ergänzt der Spamschan das Subject der untersuchten Mail zu einer definierten Syntax (XXXSPAMXXX + Subject). Auf Ihrem lokalen Mailclient bzw. Mailserver sollten Sie eine automatische Weiterbearbeitung solcher Mails einrichten, z.B. Verschiebung in einen separaten Ordner.

Die Spamkriterien, z.B. ob die Mail einen HTML-Teil enthält, die Form des Subjects, ob darin oder im Mailtext Reizwörter enthalten sind und ob der absendende Mailserver gültige Konfigurationen besitzt, werden von uns ständig angepaßt und erweitert. Eine volumenabhängige Preisgestaltung mit günstiger monatlicher Pauschale sichert eine faire Abrechnung nach Verbrauch:

PPP Spamschan	Einrichtung	Monatlich
Spamschan	30,00 €	15,00 €
zzgl. Datenvolumen mit einem Volumenfaktor von 1,7 auf die aktuellen Volumenpreise		





Die Scans können nur Domain-und/oder Hostweise durchgeführt werden. Der Spamscan kann für SMTP-Weiterleitungen oder über PPP genutzte virtuelle Mailserver erfolgen.

Beim Spam-Scan kommt es vor, daß auch solche E-Mails als Spam deklariert werden, die keine sind. Um dieses weitgehend zu verhindern, bieten wir Ihnen die Möglichkeit, Whitelist-Einträge zum Spamscan vornehmen zu lassen: Durch Eintrag der E-Mail-Adresse des Absenders und des Empfängers in eine Filterliste werden diese E-Mails von der Prüfung auf Spam ausgenommen und als gültige Adressen klassifiziert. Dadurch ist gesichert, daß die E-Mails nicht im Spamordner landen. Sprechen Sie uns an, wenn Sie Whitelist-Einträge dieser Art einrichten möchten. Die Einrichtung wird nach Aufwand abgerechnet.

PPP Virensan schützt Sie vor virenverseuchten Mails und verhindert langwierige und kostenintensive Reparaturmaßnahmen befallener Systeme. Alle eingehenden Mails werden gründlich auf Virenbefall gescant und bei Übereinstimmung mit aktuell bekannten Virenmustern bei uns in Quarantäne gelegt. Sie erhalten lediglich eine ungefährliche E-Mail des Virensans über den Fund eines infizierenden Virus oder Wurms mit dem Subject der untersuchten Mail und einer definierten Syntax (XXXVIRUSXXX + Subject).

PPP Virensan benutzt durchdachte Technologie, die laufend mit den aktuell bekannten Informationen auf den neuesten Stand gebracht wird und erreicht so einen hohen Erkennungsgrad. Der Extranetbereich der Webpräsenz informiert Sie aktuell über die neuesten Vireninformationen und Virenstatistiken des PPP Virensan. Ein nutzungsorientiertes Abrechnungsmodell garantiert faire Preise passend zum Mailaufkommen. Der Scan von E-Mails auf Viren kann für Mailweiterleitungen, Mailboxen und virtuelle Mailserver beauftragt werden.

PPP Virensan	Einrichtung	Monatlich
PPP Virensan	40,00 €	25,00 €
zzgl. Datenvolumen mit einem Volumenfaktor von 1,8 auf die aktuellen Volumenpreise		

PPP bietet bei Versendung über den Mailserver mailout.ppp.net die Möglichkeit, ausgehende E-Mail auf Viren zu scannen. Dies dient dem Schutz Ihrer Geschäftspartner vor versehentlich abgesandten virenbehafteten E-Mails. Dazu müssen Sie nur den SMTP-Port 26 als Ausgangsport einstellen. Der Datenverkehr wird in diesem Fall mit dem Faktor 1,8 abgerechnet

Wenn Sie die Produkte PPP Virensan und PPP Spamsan in Verbindung nutzen, bieten wir Ihnen vergünstigte Preise an:

PPP Viren- und Spamsan Bundle	Einrichtung	Monatlich
PPP Viren- und Spamsan im Bundle	55,00 €	35,00 €
zzgl. Datenvolumen mit einem Volumenfaktor von 2,0 auf die aktuellen Volumenpreise		



### PPP Greylisting

Dieses Verfahren lehnt zuzustellende E-Mails von externen Mailservern grundsätzlich im 1. Versuch mit der Nachricht ab, daß die Mail momentan nicht angenommen wird, aber die Zustellung später noch einmal versucht werden soll (Spammer versuchen i.d.R. nur einmal, Mails zuzustellen). Dies wird dem versendenden Server übermittelt, worauf dieser nach einer auf dem Server standardmäßig konfigurierten Zeitspanne erneut versucht, die Mail zuzustellen. Unser Server wertet einliefernden Mail-Host, Absenderadresse und Empfängeradresse aus. Wird die Mail innerhalb der nächsten 24 Stunden noch einmal zugestellt, erfolgt ein Eintrag in eine sog. Whitelist, welche den Mail-Host- als gültigen Versender für einen Zeitraum von 5 Tagen klassifiziert. Bei jeder weiteren Zustellung mit diesen Daten innerhalb dieser Zeit wird der Zeitraum verlängert, ansonsten wird der Eintrag wieder entfernt.

Die Vorteile dieses Verfahrens liegen auf der Hand: Verringerte Gefahr durch Viren, Würmer, Spambelastung und ein verringertes Datenvolumen. Es birgt allerdings auch zwei Nachteile: Die Maileinlieferung beim 2. Versuch von absendenden Servern kann verzögert oder u.U. gar nicht erfolgen. Standardmäßig sind Mailserver zwar so zu konfigurieren, daß ein zweiter Zustellungsversuch nach einer vom jeweiligen Administrator festgelegten Zeit erfolgen soll, jedoch ist dies nicht bei allen Servern standardkonform eingestellt. Zusätzlich sind die Zeiten für den zweiten Zustellungsversuch u.U. sehr hoch eingestellt, so daß die Mail mit einer relativ hohen zeitlichen Verzögerung zugestellt wird. Das Greylisting-Verfahren kann für einzelne Domains oder empfangende E-Mailadressen deaktiviert werden, so daß geschäftskritische Empfangsadressen von diesem Verfahren ausgenommen werden können. Die Kosten für Einrichtung und regelmäßige Pflege werden nach Aufwand berechnet.

Zu der technischen Realisierung der Anbindung kontaktieren Sie bitte einen unserer Service-Mitarbeiter. Die aktuellen Preise für den E-Mail-Traffic entnehmen Sie bitte dem Produktblatt PPP Lines. Weitere Informationen zur Einrichtung und Betreuung von Mailservern bietet Ihnen das Produktdatenblatt PPP Mail.

