

Vorgehensweise bei der Einrichtung des SPAM-MAIL-BLOCKER für SMTP Zustellung auf Ihrem dedizierten Mailserver

1. Domain-Namen

Um Ihre Domain in unser System einzubinden, benötigen wir den kompletten primären Domainnamen, z.B. easywan.net. Falls Sie weitere Domainnamen filtern wollen, z.B. easywan.info oder easywan.de, benötigen wir auch diese.

2. E-Mail-Adressen

Zusätzlich benötigen wir alle gültigen E-Mail Adressen, z.B. m.peither@easywan.net. Falls Sie Alias Adressen einsetzen, z.B. matthias.peither@easywan.net, benötigen wir auch diese, um sie in unserem System einzubinden. Die Lizenzgebühren berechnen sich nur aus den gültigen E-Mail-Adressen.

Jede gültige E-Mail Adresse erhält, falls E-Mails im Filter erkannt werden, eine automatisch generierte E-Mail, das SPAM's erkannt wurden. Diese können dann mittels einer Web Oberfläche verifiziert und qualifiziert werden.

3. IP Adresse des Mailservers

Anhand Ihrer festen IP Adresse Ihres Mailservers erstellen wir einen separaten DNS Eintrag bei SPAM-MAIL-BLOCKER.de (z.B. mail-easywan-net.spam-mail-blocker.de) und erlauben Ihrem Server über unseren Relay Server E-Mails zu versenden.

4. Ihre Mailserverkonfiguration - Eingang

Unser System ergänzt die E-Mail Adresse um einen Zusatz, sodass bei Fehlkonfigurationen kein sog. Loop entsteht. (z.B m.peither@easywan.net in m.peither@**intern**.easywan.net). Der Filter verändert oder ergänzt keinerlei Informationen in Ihrer E-Mail, diese wird Ihrem System genauso zugestellt, wie wir diese auch erhalten haben.

Auf Ihrem Mailserver wird eine Regel erstellt, die alle ankommenden E-Mails (jetzt mit dem Zusatz **intern** hinter dem @) erstens empfangen werden dürfen und zweitens den jeweiligen internen Postfächern zuordnet.

5. Ihre Mailserverkonfiguration - Ausgang

In Ihrem Mailserver wird zusätzlich definiert, dass alle ausgehenden E-Mails über unseren Relay Server verschickt werden. Dies dient der Verbesserung des Filters, da das System auf diese Weise bereits Ihre Kommunikationspartner kennt und diese automatisch als vertrauenswürdig einstuft.

6. Systemtest - DNS Änderung

Nach dem erfolgreichen Systemtest können Sie Ihren Provider über die IP-Adress-Änderung im DNS informieren.

Alle E-Mails gehen somit auf die SPAM-MAIL-BLOCKER-Server, durch den sie dann der Filterung unterzogen und anschließend an Ihren Mailserver zugestellt werden, welcher sie dann entsprechend weiterverteilt.

7. Mailempfangsrichtlinie

Abschließend tragen Sie die IP-Adresse unseres Servers in Ihrem Mailserver oder Ihrer Firewall ein, damit Sie zukünftig nur noch E-Mails empfangen, die von unserem System an Sie verschickt werden. Hiermit schließen Sie aus, dass Ihr Mailserver weiterhin E-Mails - und damit auch SPAM Mails - aus anderen Quellen erhält.

Für Fragen zur Konfiguration Ihres Mailservers stehen wir Ihnen gerne zur Verfügung.