

noSpam proxy

IDEE

ZIELE

LÖSUNG

VORTEILE

VORAUSSETZUNGEN



DATENBLATT

www.nospamproxy.de

© Net at Work Netzwerksysteme GmbH
Am Hoppenhof 32, D-33104 Paderborn
Tel. +49 5251 304-600, Fax -650

info@netatwork.de
www.netatwork.de

IDEE

ZIELE

LÖSUNG

VORTEILE

VORAUSSETZUNGEN



DATENBLATT

DIE IDEE

Der Anlass **NoSpamProxy** zu entwickeln, ist der gestiegene Schutzbedarf von Unternehmen mit eigenem Mail-Server. SPAM ist ein globales Problem, das täglich größer wird.

Im Unterschied zu herkömmlicher SPAM-Software erkennt **NoSpamProxy** die unerwünschten Werbemails bereits während des Übertragungsversuches an den Mail-Server.

Die Abwehr unerwünschter Werbemails funktioniert vereinfacht ausgedrückt nach einem „Umkehr-Prinzip“. Abgelehnte und blockierte Mails verschwinden nicht einfach, sondern führen zu einer Unzustellbarkeitsmeldung (NDR), die vom Absendersystem generiert wird. Manuelle Nachbearbeitungszeit für Quarantäne-Mails entfällt.

NoSpamProxy perfektioniert dieses Verfahren durch ein Filtersystem, das über ein fein granuliertes Regelwerk einstellbar ist. Zahlreiche Parameter ermöglichen die präzise Anpassung an individuelle Erfordernisse und Systembedingungen.

ZIELE FÜR NOSPAMPROXY

NoSpamProxy ist das Ergebnis einer ausführlichen Analyse und des gestiegenen Schutzbedarfs unserer Kunden. Als Systemingenieure und Exchange Consultants haben wir klare Vorstellungen davon, wie ein Spam-Filter aufgebaut sein muss.

- Analyse der Mails während dem Empfang per SMTP
- Einsatz vor oder auf dem SMTP-Server
- Keine Software auf dem Client
- Keine Änderung oder Eingriff am Mail-Server
- Kein SMTP-Relay mit Queueing etc.
- Offene Schnittstellen zur Erweiterung der Filter
- Plattform: Windows und .NET

IDEE

ZIELE

LÖSUNG

VORTEILE

VORAUSSETZUNGEN



DATENBLATT

DIE LÖSUNG

Im Unterschied zu herkömmlicher SPAM-Software erkennt **NoSpamProxy** die unerwünschten Werbemails bereits während der Übertragung an den Mail-Server. Im Falle einer SPAM-Klassifizierung wird die Verbindung mit einem Fehler unterbrochen.

Die Übertragung einer Nachricht teilt sich in fünf logisch trennbare Abschnitte auf:

▪ Verbindungsaufbau

Die Gegenstelle baut eine Verbindung (z.B.: über das Protokoll TCP/IP) zum Empfängersystem auf und meldet sich an. Der Empfänger kennt bisher nur die „Adresse“ des Absenders (z.B. IP-Adresse).

▪ Austausch der Adressinformation (ENVELOPE)

Der Absender übermittelt die Zustellenden für die Nachricht (z. B. Absender, Empfänger). Es sind weitere Funktionen möglich wie z.B. Autorisierung, Abfrage der maximalen Nachrichtengröße.

▪ Übertragung der Nachrichtenkopfzeilen (HEADER)

Der Anfang der Nachricht wird übertragen. Bestandteil sind hier z.B. der Betreff und die Zustelloptionen (Lesequittung, Zustellquittung etc.).

▪ Übertragung des Nachrichtenkörpers (BODY)

Nach den Kopfzeilen wird die eigentliche Nachricht übertragen. Diese besteht in der Regel aus der Nachricht selbst und den Anlagen.

▪ Verbindungsabbau

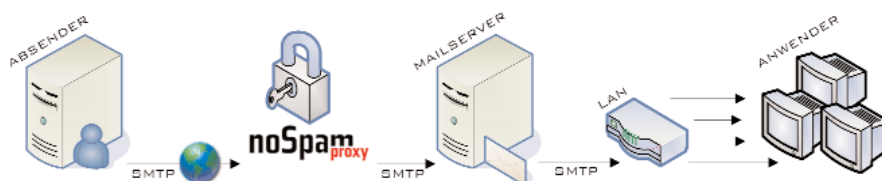
Nach der Bestätigung des Empfängers über die erfolgreiche Übertragung wird die Verbindung vom Absender wieder abgebaut.

Erst nach dem letzten Schritt liegt die Nachricht vollständig auf dem Zielsystem vor und gilt als "zugestellt". Erst dann können die meisten Lösungen die Nachricht untersuchen und behandeln. Dies ist aber zu spät!

NoSpamProxy arbeitet nach einem sehr einfachen aber wirkungsvollem Prinzip. **NoSpamProxy** wird vor den ersten SMTP-Server des Unternehmens geschaltet und nimmt alle eingehenden SMTP-Verbindungen an.

NoSpamProxy baut seinerseits die Verbindung zum internen Mailserver auf, um die Daten weiter zu leiten.

NoSpamProxy buffert nur so viel der Mail, wie für die eigene Verarbeitung erforderlich ist.



Dabei wird die Mail dekodiert und den Filtern zur Bewertung zur Verfügung gestellt. Wird eine Nachricht als SPAM klassifiziert, dann unterbricht **NoSpamProxy** die SMTP-Verbindung. Der interne Mail-Server verwirft die angefangene Nachricht, der externe Server sendet dem Absender eine Unzustellbarkeitsquittung (NDR) zu.

IDEE

ZIELE

LÖSUNG

VORTEILE

VORAUSSETZUNGEN



DATENBLATT

DIE VORTEILE

Der Einsatz von **NoSpamProxy** eröffnet Unternehmen mit eigenem Mail-Server signifikante Vorteile zur Abwehr unerwünschter Nachrichten.

- **Transfervolumen wird eingespart**

Da ein hoher Prozentsatz von Nachrichten schon sehr früh erkannt wird, werden diese Nachrichten nicht empfangen.

- **Weniger CPU Belastung**

Je früher die Mail geblockt wird, desto weniger CPU Zyklen sind für die Zwischenspeicherung und Verwaltung erforderlich.

- **Arbeitszeiteinsparung**

Die manuelle Nachkontrolle klassifizierter Nachrichten in einer Quarantäne entfällt, da diese Nachrichten nicht empfangen werden. Werden irrtümlicherweise gute Nachrichten geblockt, dann landen diese nicht in der Quarantäne, sondern der Absender wird diese gar nicht erst los oder erhält von seinem Server eine Bestätigung.

- **Problem der „gelöschten“ Nachrichten**

Viele Produkte und Firmen löschen als SPAM klassifizierte Nachrichten nach einiger Zeit ohne weitere Kontrolle. Sollten jedoch irrtümlich wichtige Nachrichten so gelöscht werden, weil der Empfänger diese nicht vermisst und der Absender noch nicht nachgefragt hat, ist das Risiko beim Empfänger. Der Absender kann anhand von Protokollen die Zustellung der Nachrichten belegen.

- **Strafrechtliche Inhalte werden verhindert**

Sofern solche Nachrichten als SPAM erkannt werden, landen diese nicht im Mailserver und sind damit auch nicht empfangen.

- **Archivsysteme enthalten keine SPAM Nachrichten**

Denn diese werden schon vor dem Empfang abgelehnt. Eine Nachricht, die nie empfangen wurde, muss auch nicht archiviert werden.

- **Potentielle SPAM Sender werden abgeschreckt**

Durch die aktive Ablehnung der Nachrichten müssen Sender von einem Fehler ausgehen und die Adresse verliert für den SPAM-Sender an Wert.

IDEE

ZIELE

LÖSUNG

VORTEILE

VORAUSSETZUNGEN



DATENBLATT

Die Realisation als SMTP-Proxy hat aber noch weitere Vorteile für den Betrieb:

▪ **Frühzeitige Erkennung und Ablehnung**

Die meisten SPAM Nachrichten werden beim Connect, bei der Übertragung des SMTP Envelope oder anhand des Headers erkannt und blockiert. Anlagen oder große Nachrichten werden gar nicht erst angenommen. Der interne Mail-Server wird entlastet.

▪ **NDR-Fehler durch den Absenderserver**

Geblockte Nachrichten werden an den Absenderserver mit einem 4xx Fehler gemeldet. Damit ist klar, dass die Mail nicht angenommen wird und der Absender wird informiert. Besonders die "Unzustellbarkeitsquittungen" (NDR = Non Delivery Report) werden nicht von ihrem Mail-Server an die sicherlich falsche Adresse versendet.

▪ **Speziell das Ärgernis "offene Relays" werden auf den Absender verlagert**

Dort laufen die Mails in den Warteschlangen auf und helfen bei der Überzeugung, dass ein offenes Relay nicht mehr angemessen ist. Niemand kann ihnen verbieten, Nachrichten abzulehnen.

▪ **Verbergen des Mailservers**

Als Proxy kann **NoSpamProxy** auch die Antworten des SMTP-Servers manipulieren. So kann die Version des internen Mail-Servers im HELO-String angepasst und verborgen werden.

Alles in allem ist **NoSpamProxy** damit eine gelungene Lösung, um SPAMS frühzeitig aus dem Unternehmen fern zu halten. Durch die Modularität und offene Schnittstellen sind eigene Erweiterungen und Ergänzungen problemlos möglich.

IDEE

ZIELE

LÖSUNG

VORTEILE

VORAUSSETZUNGEN



DATENBLATT

DIE VORAUSSETZUNGEN

Voraussetzungen für den Einsatz von NoSpamProxy sind:

- **Windows 2000/2003 Server**
- **TCP/IP und SMTP für eingehende Nachrichten**
NoSpamProxy kann nur funktionieren, wenn die Nachrichten an ihr System über das Protokoll TCP/IP und SMTP direkt zugestellt werden. Wenn Sie ihre Nachrichten per POP3, UUCP etc. abholen, ist NoSpamProxy nicht das richtige Produkt für Sie.
- **Eigener vollwertiger Mailserver**
NoSpamProxy muss einen Mailserver kennen, an den er die eingehenden Verbindungen per SMTP weiterleiten kann.
- **100 MB freien Festplatten Speicher und 512 MB RAM**
Zusätzliche Filter und Module nicht mit eingerechnet.
- **Portumleitung oder Relaysystem**
NoSpamProxy muss statt ihres bisherigen Mailservers die Mails auf Port 25 annehmen. Wenn der Mail-Server und NoSpamProxy auf dem gleichen System installiert werden, muss der bisherige Port des Mail-Servers umgeleitet werden. Dies geht meist sehr einfach. Achtung, wenn der Mailserver intern selbst über SMTP-Daten austauscht (z.B. Exchange 2000/2003), hier helfen mehrere virtuelle SMTP-Server.