1. Motivation
2. SMTP Grundlagen
3. Fallbeispiele
4. Einrichtung
5. Funktionsweise
6. Pro/Contra
7. Alternativen

Motivation

Zero Tolerance vs. Ideologie vs. Realität

„Denial Rampart Stage“ lässt sich schwer in einer diplomatischen Finanz-Welt vermitteln.

Dennoch existieren Regeln und Spielräume.

Spam/Fraud wird möglich durch

Soziale Defizite

Bürokratie, Faulheit, Verantwortungsweitergabe, Ignoranz, Desinteresse, Lern- und Fortbildungsrenitenz

Technische Defizite

SMTP-Design-Fokus lag bei Fehlertoleranz statt Sender und Daten-Authentizität (und das ist ganz in Ordnung)

SPF bietet keine Abhilfe, Benutzung falscher Sender Informationen weiterhin möglich, Forwarder müssen SRS implementieren.

Domainkeys bieten Authentizität, verhindern aber keine Benutzung falscher Senderinformationen oder Phishing oder Bandbreitenverbrauch im Generellen

Policyd-weight bietet dazu auch keine 100%-Lösung

Entscheidungshoheit

Blacklisten sind anfällig für:

- Überlistung von Automatismen
  Spamcop: Aufspüren und Ausnutzen derer Spamtraps
- Politische Entscheidungen
  Spamhaus: nic.at
- Menschliche Fehlentscheidungen

Postfix-Restrictions konnten schwer abwägend eingesetzt werden, die Anforderungen an die Flexibilität überstieg das Einfachkeitsprinzip

Logischer Schritt: Policy-Schnittstelle

Damit wurde eine sinnvolle und flexible Pre-Qeue-Entscheidungsfindung ermöglicht.

SMTP Grundlagen

Resultieren nicht nur aus RFCs sondern auch aus technischen o. sozialen Anforderungen

Adress- und Namensauflösung: IP->Hostname->IP

HELO Argument: tatsächlicher, im Internet erlaubter, vollständiger (absoluter) Name

IP/Hostname sowie HELO oder Sender-Domain sollten in einer für Menschen nachvollziehbaren Beziehung stehen, bei Forwardern zumindest IP/Hostname und HELO.

postmaster@helo-fqdn sollte erreichbar sein, da kürzester Pfad zur Verantwortlichkeit

Fallbeispiele

Kaputtes DNS:

```
weighted check:  NOT_IN_SBL_XBL_SPAMHAUS=-1.5 NOT_IN_SPAMCOP=-1.5
NOT_IN_BL_NJABL=-1.5 CL_IP_NE_HELO=1.5
(check from: .cruxforums. - helo: .cs.fit. - helo-domain: .fit.)
FROM_NOT_FAILED_HELO(DOMAIN)=3 RESOLVED_IP_IS_NOT_HELO=1.5;
<client=unknown[190.192.224.26]> <helo=cs.fit.edu>
<from=nzwaterfall@cruxforums.com> <to=xxx@kuttendreier.de>; rate:
1.5
```

Ungesichertes Listing auf der Manitu/iX-BL:

```
weighted check:  NOT_IN_SBL_XBL_SPAMHAUS=-1.5 NOT_IN_SPAMCOP=-1.5
NOT_IN_BL_NJABL=-1.5 IN_IX_MANITU=4.35 CL_IP_EQ_HELO_IP=-2 (check
from: .computerwissen. - helo: .versand6.simplethings. - helo-
domain: .simplethings.)  FROM/MX_MATCHES_HELO(DOMAIN)=-2;
<client=versand6.computerwissen.de[85.25.150.176]>
<helo=versand6.simplethings.de> <from=bounce@computerwissen.de>
<to=xxx@kuttendreier.de>; rate: -4.15
```

SPAMCOP und NJABL-Listing:

```
weighted check:  NOT_IN_SBL_XBL_SPAMHAUS=-1.5 IN_SPAMCOP=3.75
IN_BL_NJABL=4.25; <client=unknown[203.162.18.26]>
<helo=mail.hmu.edu.vn> <from=petraschoenmakers@gmail.nl>
<to=xxx@kuttendreier.de>; rate: 6.5
```

SPAMCOP-Listing und unplausible SMTP Parameter

```
weighted check:  NOT_IN_SBL_XBL_SPAMHAUS=-1.5 IN_SPAMCOP=3.75
NOT_IN_BL_NJABL=-1.5 CL_IP_NE_HELO=5.25 (check from:
.ipodlanyards. - helo: .vcuijsoi. - helo-domain: .vcuijsoi.)
FROM_NOT_FAILED_HELO(DOMAIN)=6.75 RESOLVED_IP_IS_NOT_HELO=1.5;
<client=unknown[200.62.249.249]> <helo=vcuijsoi>
<from=calksii043@ipodlanyards.com> <to=xxx@ek-muc.de>; rate: 14.25
```

Viele Viren (zb Sobig/Sober) verwenden als HELO die Sender-Domain.

→ Automatische Konfiguration für SMTP-Betrieb ist schwierig

Sobig uA nutzt folgende Schwachstelle aus:

→ soziale Anforderung an Postmaster: „Ich seh nicht ein, warum ich an meinem Server so eine Lapalie wie HELO → IP Auflösung richten soll, zeig mir erstmal die technische Anforderung dazu“

Diese Art Viren werden bei policyd-weight meist mit dem Score 1 oder 1.5 abglehnt. Spielraum für Toleranz: sehr niedrig. Deswegen höhere Verantwortlichkeit bei den Serverbetreibern.

Einrichtung

```
smtpd_restriction_classes =
 check_policyd_weight

check_policyd_weight =
 check_policy_service inet:127.0.0.1:12525

smtpd_recipient_restrictions =
    permit_mynetworks
    permit_sasl_authenticated
    reject_unauth_destination
    check_client_access hash:/path/to/polw_whitelist
    check_recipient_access hash:/path/to/polw_users
```

File polw_whitelist:

```
1.2.3.4   permit_auth_destination
yahoo.com permit_auth_destination
```

File polw_users:

```
kunde1.tld       check_policyd_weight
user@kunde2.tld check_policyd_weight
```

Sinnvolle Einstellungen

Ort: /etc/policyd-weight.conf

Oder `-f /path/policyd-weight.conf`

1. `$REJECTLEVEL = 4;  # default: 1 (WERT)`

   REJECTLEVEL-Werte größer 4 sind für den Anfang empfohlen.
   Die Entwicklung legt aber stets den Wert 1 zugrunde.

2. `$dnsbl_checks_only = 1; # default: 0 (BOOL)`

   Damit wird nur gegen DNSBLs geprüft, weitere Prüfungen entfallen.

Funktionsweise

1. **Master Prozess**
   Überwacht/limitiert die Prüfprozesse.

2. **Cache Prozess**
   Wird beim Start des Master erstellt oder, falls nicht vorhanden, von einem Prüfprozess.
   Er speichert die Entscheidung: IP, Score, ggf. Senderdomain und Timestamps.
   Das „warum“ muss im Maillog gesucht werden.

3. **Prüfprozesse (Child)**
   Kommunizieren direkt mit dem `smtpd(8)`
   Fragen den Cache ab
   Erledigen DNS/RBL/Scoring Aufgaben

Scoring

1. SPAM Cache? HAM-Cache? Wie lange? Wie oft?
   Je nach Ergebnis: sofort ablehnen; sofort annehmen;
   RBL prüfen; komplett prüfen.

2. RBL Prüfung, sequentiell zur Resourcenschonung

3. Sender sowie HELO-Domain werden geprüft (MX/A),
   ob sie zur IP bzw den 24er oder 16er Subnets der
   Client-IP gehören. Ausserdem ob verbotene Werte in
   den RRs stehen (127/8, 192.168/16, 10/8, 172.16/12)

4. Prüfung ob der HELO Parameter eine IP-Notierung
   enthält (1.2.3.4 oder [1.2.3.4]) – Wertung als Spam-Indiz.

5. Prüfung ob die HELO-Domain oder der Client-Hostname
   DNS-mässig mit dem Absender in Verbindung stehen
   (gleiche Domain-Namen, MXe in gleicher Domain)

6. evtl. Prüfung ob IP zum HELO-Parameter passt

7. Prüfung ob Client dynamischer Natur ist: IP auf DialUp-Listen, Hostname oder HELO erscheinen als dynamsich: dsl, ppp, dialup und Ähnliches im Hostname

8. Nobody/Anonymous check. In den seltensten Fällen eine existente Adresse, Bounces gehen wohin? Schlechte bis garkeine Konfiguration.

9. Sender-Domain multi-parted Check: besteht die Senderdomain Aus mehreren Labels (sub-domains)

10. Random Sender Check: localpart des Senders besteht aus zu vielen Buchstaben ohne Vokalen

11. RHSBL Checks: ist die Sender-Domain in SURBL, AHBL oder rfc-ignorant.org

Pro / Contra

Pro:

Einsparungen von Bandbreite sowie After-Queue-Resourcen (CPU, Speicher, Storage)

Rechtssicher, da keine Annahme des Mail-Body, die E-Mail gelangt somit nicht in den Verwaltungsbereich des Empfängers

Ein echter Absender erfährt sofort von Problemen. Der MTA muss keine Bounces an evtl gefälschte Absender schicken.

Simpel zu installieren

Mehr Kontrolle über die DNS-Blacklisten

Kaum Wartung

Contra:

Anpassung des Scorings kaum nachvollziehbar, Auswirkungen auf unterschiedliche SMTP/DNS-Konstellationen können kaum im Vorfeld erkannt werden. Default-Scoring basiert auf langjährigen Kompromissen und Erkenntnissen.

Alternativen

- Postfwd - www.postfwd.org
  Sinnvoll für Administratoren die ein Regelwerk selber entwickeln wollen
- Perl, Python und http://www.postfix.org/SMTPD_POLICY_README.html