Neuerungen in Postfix 2.8

Ralf Hildebrandt

Charité Universitätsmedizin Berlin

sage@guug – Berlin, 3. März

- “Botnets now produce 95% of spam”
  `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,
- 92.7 % for IT Services,

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,
- 92.7 % for IT Services,
- 92.6 % for the Chemical & Pharmaceutical sector,

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,
- 92.7 % for IT Services,
- 92.6 % for the Chemical & Pharmaceutical sector,
- 91.7 % for Public Sector and

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,
- 92.7 % for IT Services,
- 92.6 % for the Chemical & Pharmaceutical sector,
- 91.7 % for Public Sector and
- 91.2 % for Finance.

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,
- 92.7 % for IT Services,
- 92.6 % for the Chemical & Pharmaceutical sector,
- 91.7 % for Public Sector and
- 91.2 % for Finance.

Effiziente Behandlung von Clients aus Botnetzen wäre sinnvoll!

Spezifische Gegenmaßnahmen

- DNSBLs

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)
- Erkennung von “Earlytalkern”

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)
- Erkennung von “Earlytalkern”
  - Gibt es noch gar nicht!

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)
- Erkennung von “Earlytalkern”
  - Gibt es noch gar nicht!
- Erkennung von anderem “abnormen” Verhalten

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)
- Erkennung von “Earlytalkern”
  - Gibt es noch gar nicht!
- Erkennung von anderem “abnormen” Verhalten
  - Gibt es noch gar nicht!

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)
- Erkennung von “Earlytalkern”
  - Gibt es noch gar nicht!
- Erkennung von anderem “abnormen” Verhalten
  - Gibt es noch gar nicht!

Aktuelle Entwicklung in Postfix

Postscreen ist der Codename für einen neuen Daemon der vor Postfixs `smtpd` sitzt und Verbindungen ausfiltert.

Aktuelle Entwicklung in Postfix

service “smtpd” has reached its process limit “100”: new smtpd clients may experience noticeable delays to avoid this condition, increase the process count in master.cf or reduce the service time per client

Aktuelle Entwicklung in Postfix II

Ziele:

- Zombies von Postfixs `smtpd` fernhalten
- Erhöhung der Skalierbarkeit. . .

Aktuelle Entwicklung in Postfix II

Ziele:

- Zombies von Postfixs `smtpd` fernhalten
- Erhöhung der Skalierbarkeit. . .
  indem zeitintensive Operationen wie DNSBL Abfragen und SMTP Protokollcheck aus dem `smtpd` ausgelagert werden

Aktuelle Entwicklung in Postfix II

Ziele:

- Zombies von Postfixs `smtpd` fernhalten
- Erhöhung der Skalierbarkeit. . .
  indem zeitintensive Operationen wie DNSBL Abfragen und SMTP Protokollcheck aus dem `smtpd` ausgelagert werden

Angriff der Zombiehorden

Angriff der Zombiehorden II

- Der Kernel queued Verbindungen
- Postfix arbeitet “nur” 100 Verbindungen (genauer `default_process_limit`) simultan ab

Angriff der Zombiehorden II

- Der Kernel queued Verbindungen
- Postfix arbeitet “nur” 100 Verbindungen (genauer `default_process_limit`) simultan ab

-> Serverüberlastung

Angriff der Zombiehorden II

- Der Kernel queued Verbindungen
- Postfix arbeitet “nur” 100 Verbindungen (genauer `default_process_limit`) simultan ab

-> Serverüberlastung

Symptome einer Serverüberlastung

- Clients erfahren eine extreme Verzögerung bevor Postfix antwortet
  - Clients geben auf bevor Postfix antwortet
- Postfix loggt viele “`lost connection`” Einträge
- Postfix ab Version 2.3 loggen “`all server ports busy`”-Warnungen

postscreen - master.cf

Aus

```
smtp      inet  n       -       -       -       -       smtpd
```

wird

```
smtp      inet  n       -       -       -       1       postscreen
smtpd     pass  -       -       -       -       -       smtpd
```

Man beachte das Process Limit von 1 – `postscreen` ist wirklich nur ein einzelner Daemon.

postscreen - master.cf

Aus

```
smtp      inet  n       -       -       -       -       smtpd
```

wird

```
smtp      inet  n       -       -       -       1       postscreen
smtpd     pass  -       -       -       -       -       smtpd
```

Man beachte das Process Limit von 1 – `postscreen` ist wirklich nur ein einzelner Daemon.

Deep protocol checks

- Bedingt durch die Art der Tests läuft ein Client ersteinmal tief in die Protokollanalyse der postscreen daemon hinein.
- Es gibt dann keine Methode, um diesen Status an den smtpd abzugeben.

Deep protocol checks

- Bedingt durch die Art der Tests läuft ein Client ersteinmal tief in die Protokollanalyse der postscreen daemon hinein.
- Es gibt dann keine Methode, um diesen Status an den smtpd abzugeben.
- Daher TEMPFAIL und führen einer Datenbank von “guten” Clients.

Deep protocol checks

- Bedingt durch die Art der Tests läuft ein Client ersteinmal tief in die Protokollanalyse der postscreen daemon hinein.
- Es gibt dann keine Methode, um diesen Status an den smtpd abzugeben.
- Daher TEMPFAIL und führen einer Datenbank von “guten” Clients.

Deep protocol checks

- Bedingt durch die Art der Tests läuft ein Client ersteinmal tief in die Protokollanalyse der postscreen daemon hinein.
- Es gibt dann keine Methode, um diesen Status an den smtpd abzugeben.
- Daher TEMPFAIL und führen einer Datenbank von “guten” Clients.

postscreen - `main.cf`

```
postscreen_dnsbl_sites =
  zen.spamhaus.org*2, bl.spamcop.net
  b.barracudacentral.org, swl.spamhaus.org*-2
postscreen_dnsbl_threshold = 2
postscreen_access_list = permit_mynetworks
  cidr:/etc/postfix/postscreen_access.cidr

postscreen_bare_newline_enable = yes
postscreen_pipelining_enable = yes
postscreen_non_smtp_command_enable = yes

postscreen_greet_action = enforce
postscreen_dnsbl_action = enforce
postscreen_bare_newline_action = drop
postscreen_hangup_action = drop
```

```
Feb 21 13:45:33 mail postfix/postscreen[8534]: \
PASS OLD [195.140.185.23]:44965
```

Hier wurde ein “guter” Client im Cache gefunden

```
Feb 21 13:45:33 mail postfix/postscreen[8534]: \
PASS OLD [195.140.185.23]:44965
```

Hier wurde ein “guter” Client im Cache gefunden

postscreen - das Log

```
postscreen[8534]: CONNECT from [117.196.140.106]:11464
postscreen[8534]: PREGREET 22 after 0.4 from [117.196.140.106]:11464: HELO home-0cdf3c9fc3\r\
postscreen[8534]: DNSBL rank 1 for [117.196.140.106]:11464
postscreen[8534]: NOQUEUE: reject: RCPT from [117.196.140.106]:11464: 550 5.7.1 Service unava
```

Hier wurde ein “schlechter” Client in genau einer der `postscreen_dnsbl_sites` gefunden.

postscreen - das Log

```
postscreen[8534]: CONNECT from [117.196.140.106]:11464
postscreen[8534]: PREGREET 22 after 0.4 from [117.196.140.106]:11464: HELO home-0cdf3c9fc3\r\n
postscreen[8534]: DNSBL rank 1 for [117.196.140.106]:11464
postscreen[8534]: NOQUEUE: reject: RCPT from [117.196.140.106]:11464: 550 5.7.1 Service unava
```

Hier wurde ein “schlechter” Client in genau einer der `postscreen_dnsbl_sites` gefunden.

Die in `postscreen` eingebaute SMTP-Engine konnte envelope sender, recipient und HELO bestimmen!

postscreen - das Log

```
postscreen[8534]: CONNECT from [117.196.140.106]:11464
postscreen[8534]: PREGREET 22 after 0.4 from [117.196.140.106]:11464: HELO home-0cdf3c9fc3\r\
postscreen[8534]: DNSBL rank 1 for [117.196.140.106]:11464
postscreen[8534]: NOQUEUE: reject: RCPT from [117.196.140.106]:11464: 550 5.7.1 Service unava
```

Hier wurde ein “schlechter” Client in genau einer der `postscreen_dnsbl_sites` gefunden.
Die in `postscreen` eingebaute SMTP-Engine konnte envelope sender, recipient und HELO bestimmen!

bare newline detection

- bare newline detection

  Real spambots don't make this mistake anymore, but poorly-written software still does.

```
Feb 21 10:26:12 mail postfix/postscreen[27228]: BARE NEWLINE from [79.193.32.98]:62058
```

Böse Falle

Abfragen mit `echoping` scheitern bei Postfix-2.8.x mit aktiviertem postscreen:

```
Jan 26 15:38:01 mail postfix/postscreen[9288]:
   CONNECT from [46.182.18.28]:43024
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   PREGREET 6 after 5 from [46.182.18.28]:43024: QUIT\r\n
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   DISCONNECT [46.182.18.28]:43024
```

Böse Falle

Abfragen mit `echoping` scheitern bei Postfix-2.8.x mit aktiviertem postscreen:

```
Jan 26 15:38:01 mail postfix/postscreen[9288]:
   CONNECT from [46.182.18.28]:43024
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   PREGREET 6 after 5 from [46.182.18.28]:43024: QUIT\r\n
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   DISCONNECT [46.182.18.28]:43024
```

Man muss dann einfach whitelisten:

Böse Falle

Abfragen mit `echoping` scheitern bei Postfix-2.8.x mit aktiviertem postscreen:

```
Jan 26 15:38:01 mail postfix/postscreen[9288]:
   CONNECT from [46.182.18.28]:43024
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   PREGREET 6 after 5 from [46.182.18.28]:43024: QUIT\r\n
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   DISCONNECT [46.182.18.28]:43024
```

Man muss dann einfach whitelisten:

```
postscreen_access_list =
   permit_mynetworks
   cidr:/etc/postfix/postscreen_access.cidr
```

Böse Falle

Abfragen mit `echoping` scheitern bei Postfix-2.8.x mit aktiviertem postscreen:

```
Jan 26 15:38:01 mail postfix/postscreen[9288]:
   CONNECT from [46.182.18.28]:43024
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   PREGREET 6 after 5 from [46.182.18.28]:43024: QUIT\r\n
Jan 26 15:38:05 mail postfix/postscreen[9288]:
   DISCONNECT [46.182.18.28]:43024
```

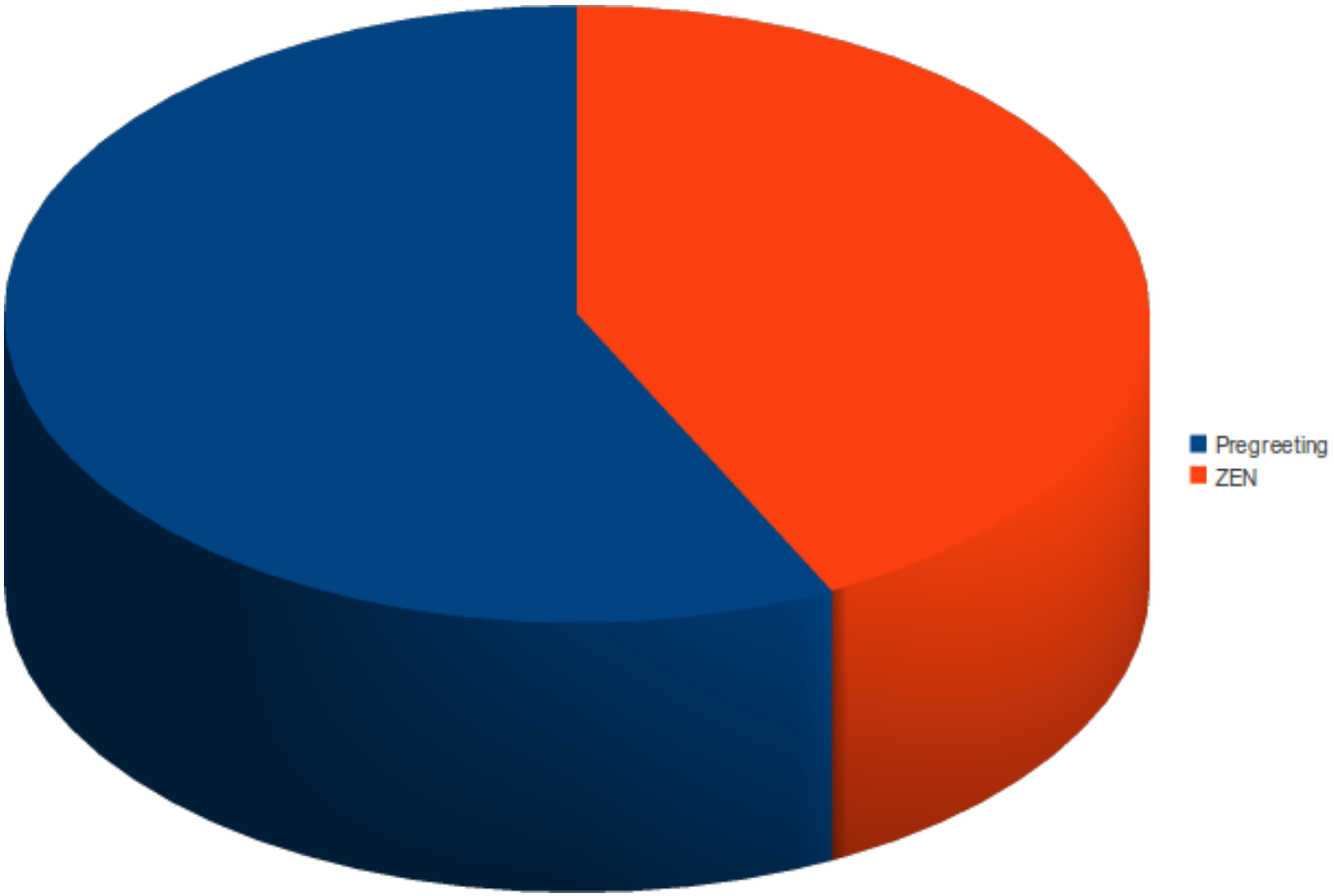
Man muss dann einfach whitelisten:

```
postscreen_access_list =
   permit_mynetworks
   cidr:/etc/postfix/postscreen_access.cidr
```

Weitere Entwicklungen

- Greylisting
  nach Implementierung der SMTP-Engine nur eine kleine Erweiterung des Cache

Analysen vom 1.9.2010 bis 7.9.2010:



Analysen vom 1.9.2010 bis 7.9.2010 II:

- 605.391 Abweisungen durch postscreen (100%)
- 347.100 durch Pregreeting detection (ca. 57,3%)

Analysen vom 1.9.2010 bis 7.9.2010 II:

- 605.391 Abweisungen durch postscreen (100%)
- 347.100 durch Pregreeting detection (ca. 57,3%)
- 258.291 durch DNSBL (`zen.spamhaus.org`) (ca. 42,7%)

Analysen vom 1.9.2010 bis 7.9.2010 II:

- 605.391 Abweisungen durch postscreen (100%)
- 347.100 durch Pregreeting detection (ca. 57,3%)
- 258.291 durch DNSBL (`zen.spamhaus.org`) (ca. 42,7%)

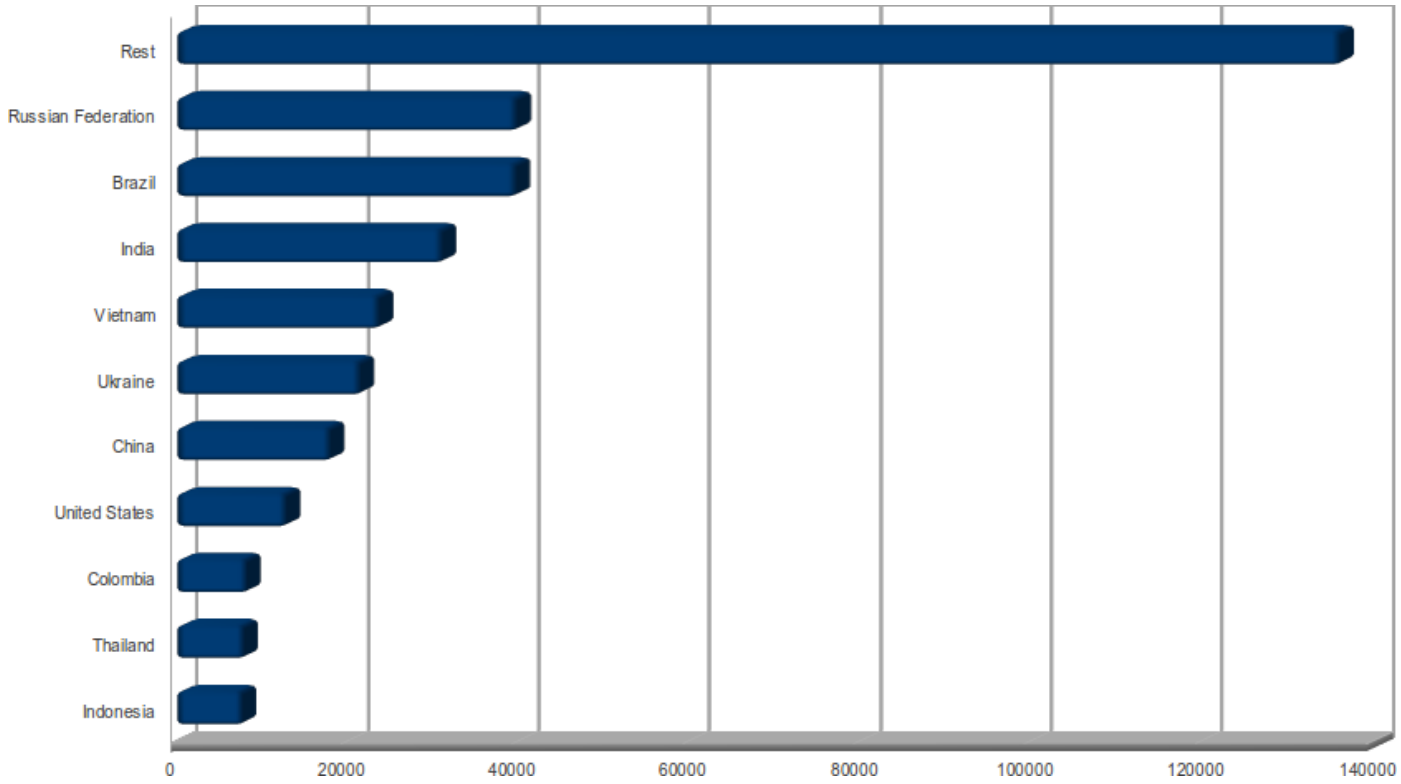
Das zeigt m.E. das Potential der SMTP-Engine in postscreen – denn diese Werte stammen aus der Zeit wo nur Pregreeting erkannt werden konnte!

Analysen vom 1.9.2010 bis 7.9.2010 II:

- 605.391 Abweisungen durch postscreen (100%)
- 347.100 durch Pregreeting detection (ca. 57,3%)
- 258.291 durch DNSBL (`zen.spamhaus.org`) (ca. 42,7%)

Das zeigt m.E. das Potential der SMTP-Engine in postscreen – denn diese Werte stammen aus der Zeit wo nur Pregreeting erkannt werden konnte!

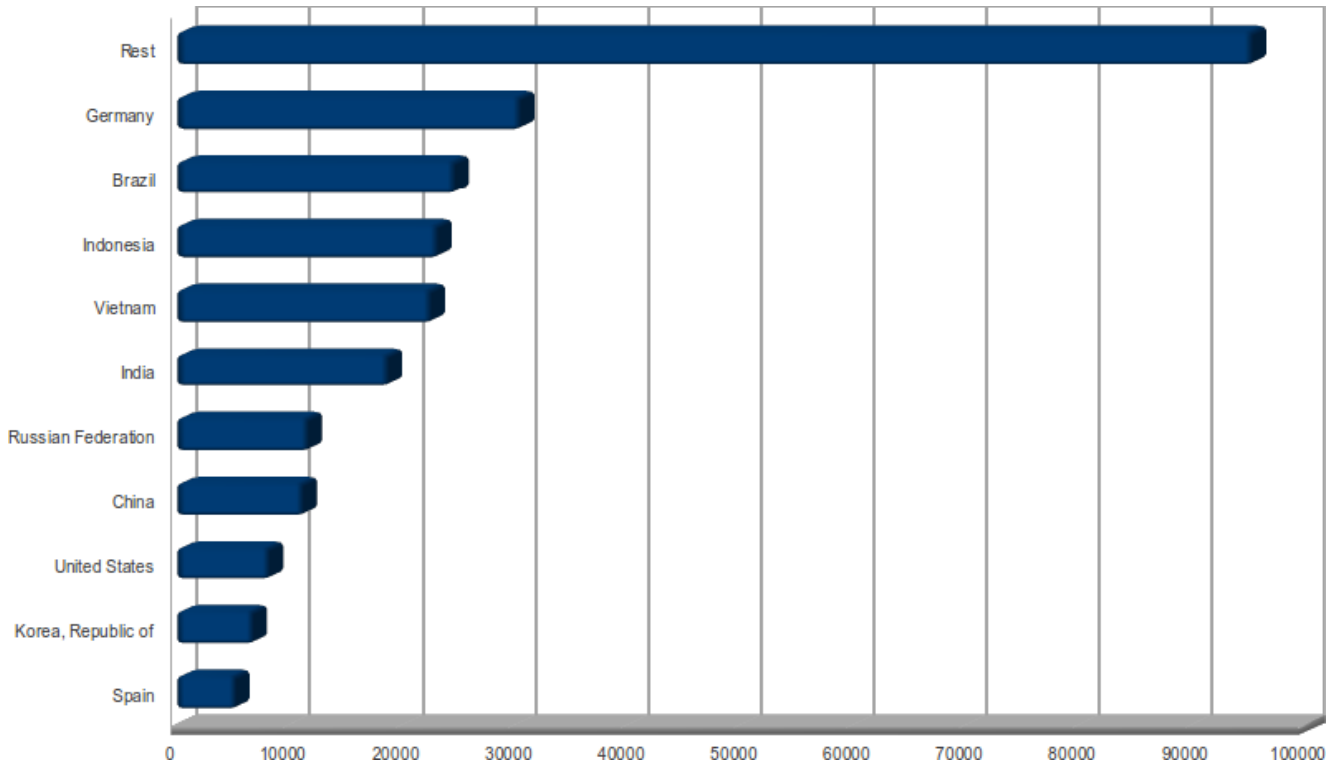
Pregreeter nach Ländern:



Pregreeter nach Ländern II:

- 39879 RU, Russian Federation (11,4%)
- 39799 BR, Brazil (11,4%)
- 31134 IN, India (8,9%)
- 23746 VN, Vietnam (6,8%)
- 21530 UA, Ukraine (6,2%)
- 18035 CN, China (5,1%)
- 12868 US, United States (3,7%)
- 8234 CO, Colombia
- 7898 TH, Thailand
- 7722 ID, Indonesia

DNSBL nach Ländern:



DNSBL nach Ländern II:

- 30505 DE, Germany (11,8%)
- 24689 BR, Brazil (9,5%)
- 23164 ID, Indonesia (8,9%)
- 22566 VN, Vietnam (8,7%)
- 18788 IN, India (7,2%)
- 11686 RU, Russian Federation (4,5%)
- 11233 CN, China (4,3%)
- 8229 US, United States (3,1%)
- 6794 KR, Korea, Republic of
- 5239 ES, Spain

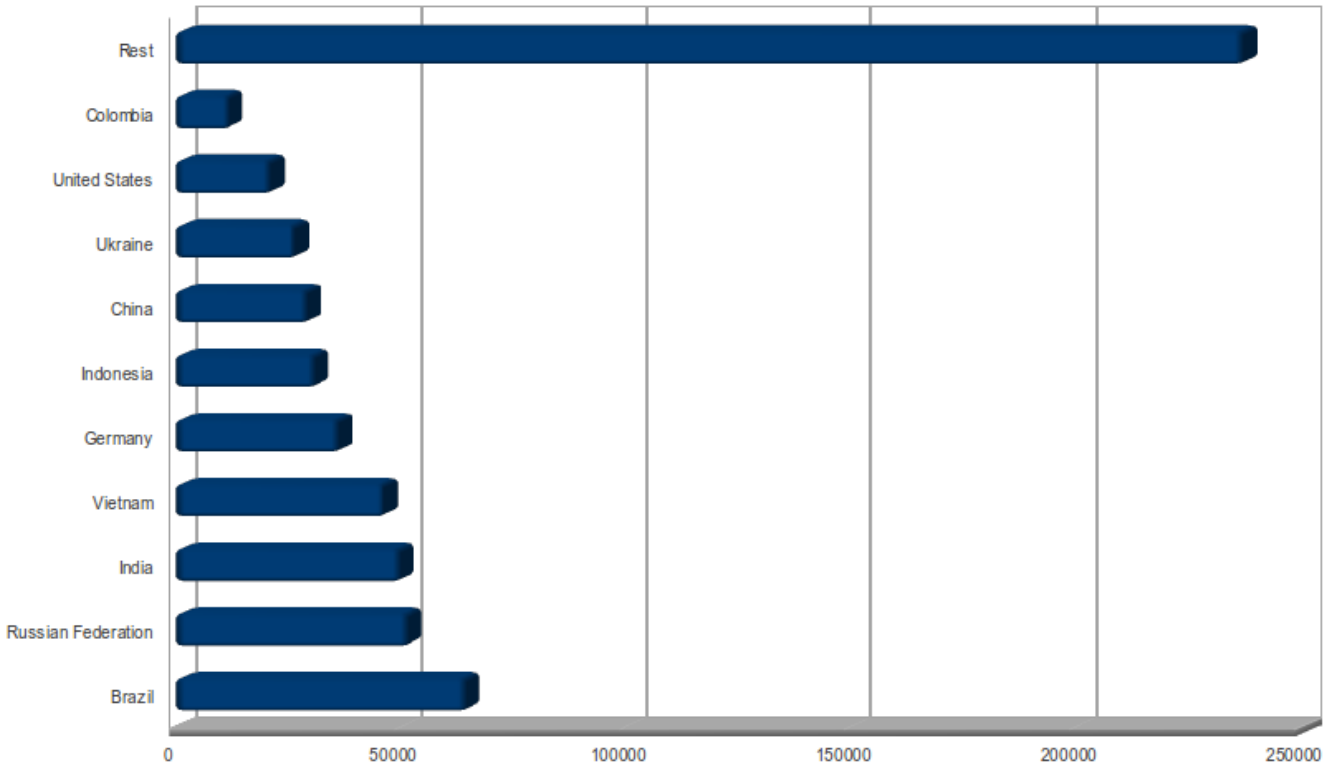
Pregreeter nach Städten:

- 4735 TW, Taipei
- 5258 PE, Lima
- 5786 VN, N/A
- 5945 TH, Bangkok
- 6487 RU, Moscow
- 6645 BR, N/A
- 6842 BR, Sao Paulo
- 6921 CN, Changchun (1,9%)
- 10297 VN, Hanoi (2,9%)
- 11106 UA, Kiev (3,1%)

DNSBL nach Städten:

- 2865 UA, Kiev
- 3047 VN, Ho Chi Minh City
- 3556 RU, Moscow
- 3573 BR, N/A
- 4765 KR, Seoul (1.8%)
- 5786 DE, N/A
- 5862 VN, N/A
- 6424 ID, Jakarta (2.4%)
- 9444 VN, Hanoi (3.6%)
- 18116 DE, Nürnberg (7.0%)

Gesamt nach Ländern:



Gesamt nach Ländern II:

- 11736 CO, Colombia
- 21097 US, United States
- 26590 UA, Ukraine
- 29268 CN, China
- 30886 ID, Indonesia (5,1%)
- 36237 DE, Germany (5,9%)
- 46312 VN, Vietnam (7,6%)
- 49922 IN, India (8,2%)
- 51565 RU, Russian Federation (8,5%)
- 64488 BR, Brazil (10,6%)

Gesamt nach Städten:

- 8102 TH, Bangkok
- 8136 CN, Changchun
- 8953 ID, Jakarta
- 9297 BR, Sao Paulo
- 10043 RU, Moscow
- 10218 BR, N/A
- 11648 VN, N/A
- 13971 UA, Kiev
- 18118 DE, Nürnberg
- 19741 VN, Hanoi

Neue DNSBL, DNSWL Syntax

Endlich sind DNS-basierte Whitelists möglich:

- `permit_dnswl_client`
  whitelists a client by IP address

Neue DNSBL, DNSWL Syntax

Endlich sind DNS-basierte Whitelists möglich:

- `permit_dnswl_client`
  whitelists a client by IP address
- `permit_rhswl_client`
  whitelists a client by its hostname.

Neue DNSBL, DNSWL Syntax

Endlich sind DNS-basierte Whitelists möglich:

- `permit_dnswl_client`
  whitelists a client by IP address
- `permit_rhswl_client`
  whitelists a client by its hostname.

Address patterns in `reject_rbl_client`:

Example

```
reject_rbl_client example.com=127.0.0.[2;4;6..8]
```

weist Clients ab, wenn das Lookup Resultat `127.0.0.2`, `127.0.0.40`, `127.0.0.6`, `127.0.0.7` oder `127.0.0.8` ist.
Beispiel:

Example

```
reject_rbl_client list.quorum.to=127.0.0.[2;4;5]
```

Address patterns in `reject_rbl_client`:

Example

```
reject_rbl_client example.com=127.0.0.[2;4;6..8]
```

weist Clients ab, wenn das Lookup Resultat `127.0.0.2`, `127.0.0.40`, `127.0.0.6`, `127.0.0.7` oder `127.0.0.8` ist. Beispiel:

Example

```
reject_rbl_client list.quorum.to=127.0.0.[2;4;5]
```

sqlite Unterstützung

(Lese)-Unterstützung für sqlite:

Example

```
alias_maps = sqlite:/etc/postfix/sqlite-aliases.cf
```

Example

```
# Path to database
dbpath = /some/path/to/sqlite_database

# See sqlite_table(5) for details.
query = SELECT forw_addr FROM mxaliases
   WHERE alias='%s' AND status='paid'
```

Namensauflösung

Der Postfix SMTP Client hängt nicht länger die lokale Domain an einen Hostnamen ohne "." an, wenn der DNS Name aufgelöst werden soll.

Mit `smtp_dns_resolver_options = res_defnames` kriegt man das alte Verhalten zurück.

Namensauflösung

Der Postfix SMTP Client hängt nicht länger die lokale Domain an einen Hostnamen ohne "." an, wenn der DNS Name aufgelöst werden soll.
Mit `smtp_dns_resolver_options = res_defnames` kriegt man das alte Verhalten zurück.

Verbessertes Logging

Bei einem `content_filter` Setup wird nun die QueueID vor dem Filter mitgeloggt:

```
postfix/smtpd[4074]: 6B4A9924782:
  client=localhost[127.0.0.1],
  orig_queue_id=951F692462F
  orig_client=hades.porcupine.org[168.100.189.10]
```

Verbessertes Logging

Bei einem `content_filter` Setup wird nun die QueueID vor dem Filter mitgeloggt:

```
postfix/smtpd[4074]: 6B4A9924782:
  client=localhost[127.0.0.1],
  orig_queue_id=951F692462F
  orig_client=hades.porcupine.org[168.100.189.10]
```

Leider nicht bei `smtp_proxy_filter`!

Verbessertes Logging

Bei einem `content_filter` Setup wird nun die QueueID vor dem Filter mitgeloggt:

```
postfix/smtpd[4074]: 6B4A9924782:
  client=localhost[127.0.0.1],
  orig_queue_id=951F692462F
  orig_client=hades.porcupine.org[168.100.189.10]
```

Leider nicht bei `smtp_proxy_filter`!

Reply Footer

Man kann nun an die REJECT-Meldungen des smtpd eine vordefinierte Zeichenkette anhängen:

```
smtpd_reject_footer = Contact postmaster@charite.de for technical
 assistance. Please provide the following information in your
 problem report: error message, time ($localtime),
 client ($client_address) and server ($server_name).
 We speak both English and German.
```

Reply Footer

Man kann nun an die REJECT-Meldungen des smtpd eine vordefinierte Zeichenkette anhängen:

```
smtpd_reject_footer = Contact postmaster@charite.de for technical
 assistance. Please provide the following information in your
 problem report: error message, time ($localtime),
 client ($client_address) and server ($server_name).
 We speak both English and German.
```

Gilt auch für postscreen (wegen `postscreen_reject_footer`).

Reply Footer

Man kann nun an die REJECT-Meldungen des smtpd eine vordefinierte Zeichenkette anhängen:

```
smtpd_reject_footer = Contact postmaster@charite.de for technical
 assistance. Please provide the following information in your
 problem report: error message, time ($localtime),
 client ($client_address) and server ($server_name).
 We speak both English and German.
```

Gilt auch für postscreen (wegen `postscreen_reject_footer`).

Kein `undisclosed-recipients` Header mehr

Postfix fügt keinen `To: undisclosed-recipients:;`-Header an, wenn keiner vorhanden ist.

Fragen?