lokales DNS-Black- und Whitelisting mit rbldnsd

Manchmal ist es nötig, bestimmte IP-Netze, die zwar viel Spam verschicken, aber dennoch nirgends gelistet werden, manuell auf eine eigene Blacklist zu setzen. Dann gibts da auch IP-Netze, z.B. von Orange in Frankreich, die den zahlenden Kunden zur Verfügung gestellt werden, über die dann aber auch soviel Müll verschickt wird, dass diese regelmäßig (zurecht) auf irgendwelchen Listen landen.

Hier will ich nun kurz zeigen, wie man sich für diese zwecke einen eigenen DNS-Blacklisting bzw. DNS-Whitelisting Server aufsetzt.

Installation

Ich habs unter Fedora 4 getestet, neuere Versionen weichen möglicherweise ab:

```
yum -y install rbldnsd
```

Konfiguration

Die Konfiguration ist sehr einfach gehalten. Über die Datei /etc/sysconfig/rbldnsdd werden nur einige Parameter gesetzt. Ich habe hier ein Setup mit nur einer Zone für eine DNS-Whitelist, zu Dokumentationszwecken habe ich trotzdem mal die komplette Datei mit Kommentaren eingefügt:

```
# /etc/default/rbldnsd
# This file should set one variable, RBLDNSD, to be a multiline
# list of all instances of rbldnsd to start.  Every line in that
# list consist of a key (basename for a pid file), and rbldnsd
# command line, e.g.:
#
RBLDNSD="dnswl -r /var/lib/rbldnsd/dnswl -q -b 127.0.0.1 dnswl.magenbrot.net:ip4set:dnswl.magenb
#
# or, using multiple lines and line continuations:
#
# RBLDNSD="dsbl -r/var/lib/rbldnsd/dsbl -q -b 127.2 \
#   list.dsbl.org:ip4set:list \
#   multihop.dsbl.org:ip4set:multihop \
#   unconfirmed.dsbl.org:ip4set:unconfirmed \
#
# local -r/var/lib/rbldnsd/local -q -b 127.3 \
#   dialups.bl.example.com:ip4set:dialups \
#   spews.bl.example.com:ip4set:spews \
#   inputs.bl.example.com:ip4set:inputs \
#   bl.example.com:ip4set:dialups \
#   bl.example.com:ip4set:spews \
#   bl.example.com:ip4set:inputs \
#
#  "
#
# This is the recommended way to keep entries readable and
# easily editable.
#
# the first word, key, will be used to form pid file name, like
# /var/run/rbldnsd-dsbl.pid, /var/run/rbldnsd-local.pid etc.
# So, all keys should be unique.  This is done in order to support
# several instances of rbldnsd, if that'll be required.  In a
```

```
# simple case, when only one instance is needed, key may be
# specified as a single dash, -, and in this case pid file
# will be /var/run/rbldnsd.pid :
#
# RBLDNSD="- -r/var/lib/rbldnsd -q -b127.2 \
#   zone list...\
# "
#
# See rbldnsd(8) for descriptions of options.
#
```

wichtig ist hier nur die eine Zeile, deren Format ich hier kurz erkläre:

```
RBLDNSD="dnswl -r /var/lib/rbldnsd/dnswl -q -b 127.0.0.1 dnswl.magenbrot.net:ip4set:dnswl.magenb
         key der zone fuers pidfile      |  |            |
               chroot-verzeichnis        |  |            |
                                         |zuerst in den hintergrund wechseln, dann die zonen lad
                                            |nur auf dieser Adresse lauschen
                                                         |Zonenname:Typ:Filename
```

Zonefile erzeugen

jetzt muss noch das Zonefile erstellt werden. Für das obige Beispiel lautet der Dateiname etwa /var/lib/rbldnsd/dnswl/dnswl.magenbrot.net. Das Dateiformat sieht dann so aus:

```
80.12.242.128/28        orange in france is allowed
```

Dies legt liefert jetzt für das komplette Netz 80.12.242.128/28 ein Ergebnis (A- und TXT-Record, reverse).

rbldnsd testen

Das oben verwendete Netz gehört der Firma Orange in Frankreich. Es beheimatet deren SMTP-Server für Kundenmails. Bei einem RBL-Check werden die konfigurierten RBL-Listenserver mit der Reverse-Adresse befragt. Testen kann man das z.B. so:

```
# dig 141.242.12.80.dnswl.magenbrot.net @localhost

; <<>> DiG 9.3.1 <<>> 141.242.12.80.dnswl.magenbrot.net @localhost
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59106
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;141.242.12.80.dnswl.magenbrot.net.        IN A

;; ANSWER SECTION:
141.242.12.80.dnswl.magenbrot.net. 2100 IN A 127.0.0.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jul  6 14:37:24 2009
;; MSG SIZE  rcvd: 72
```

Der TXT-Record dazu wird so abgefragt:

```
# dig 141.242.12.80.dnswl.magenbrot.net @localhost TXT
```

```
; <<>> DiG 9.3.1 <<>> 141.242.12.80.dnswl.magenbrot.net @localhost TXT
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23300
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;141.242.12.80.dnswl.magenbrot.net.        IN TXT

;; ANSWER SECTION:
141.242.12.80.dnswl.magenbrot.net. 2100 IN TXT "orange in france is allowed"

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jul  6 14:43:10 2009
;; MSG SIZE  rcvd: 96
```

Konfiguration des MTA

Postfix

FIXME Achtung, das hier ist noch ungetestet, keine Ahnung ob das so funktioniert!

Blacklist

```
smtpd_client_restrictions = ..., check_client_access dns:maps_rbl, ...

maps_rbl_base = localhost
maps_rbl_lookup = reverse-quad:A
maps_rbl_result = notfound:ignore, 127.0.0.2:ignore, *:deny, ...
```

Whitelist

```
smtpd_client_restrictions = ..., check_client_access dns:maps_rwl, ...

maps_rwl_base = localhost
maps_rwl_lookup = reverse-quad:A
maps_rwl_result = notfound:ignore, 127.0.0.2:ignore, *:ok, ...
```

Sendmail

Blacklist

in /etc/mail/sendmail.mc folgende Zeilen eintragen:

```
FEATURE(`dnsbl',`ix.dnsbl.manitu.net',`"554 Rejected " $&{client_addr} " found in ix.dnsbl.manit
FEATURE(`dnsbl',`sbl-xbl.spamhaus.org',`"554 Rejected " $&{client_addr} " found in sbl-xbl.spamh
```

Whitelist

Für Sendmail muss der folgende m4-Hack in /usr/share/sendmail-cf/feature/dnswl.m4 abgelegt werden:

```
# based IP address white list local
divert(8)
R$*                     $: $&{client_addr}
R::ffff:$-.$-.$-.$-     $: <?> $(host $4.$3.$2.$1._ARG_. $: NotFound $)
```

```
R$-.$-.$-.$-            $: <?> $(host $4.$3.$2.$1._ARG_. $: NotFound $)
R<?>NotFound            $: OKSOFAR
R<?>$+                  $@ <OK>
divert(-1)
```

Jetzt wird folgende Zeile VOR der Konfiguration der DNS-Blacklists eingefügt:

```
dnl whitelist
FEATURE(`dnswl',`localhost')dnl
dnl blacklists
FEATURE(`dnsbl',`ix.dnsbl.manitu.net',`"554 Rejected " $&{client_addr} " found in ix.dnsbl.manit
FEATURE(`dnsbl',`sbl-xbl.spamhaus.org',`"554 Rejected " $&{client_addr} " found in sbl-xbl.spamh
```

Konfiguration von Spamassassin

für Spamassassin wird die local.cf (meist in /etc/mail/spamassassin) mit folgenden Zeilen ergänzt, der Score-Parameter ist nach belieben einzustellen. Soll die DNS-Liste als Blacklist dienen, so ist ein positiver Wert einzutragen, soll die Liste als Whitelist dienen muss ein negativer Wert eingetragen werden.

```
header DNSWL    eval:check_rbl('localDNSWL', 'localhost')
describe DNSWL  local DNS-Whitelisting
score DNSWL     -100
```

Revision #1
Created 2021-04-30 13:02:50 UTC by magenbrot
Updated 2021-04-30 13:03:39 UTC by magenbrot