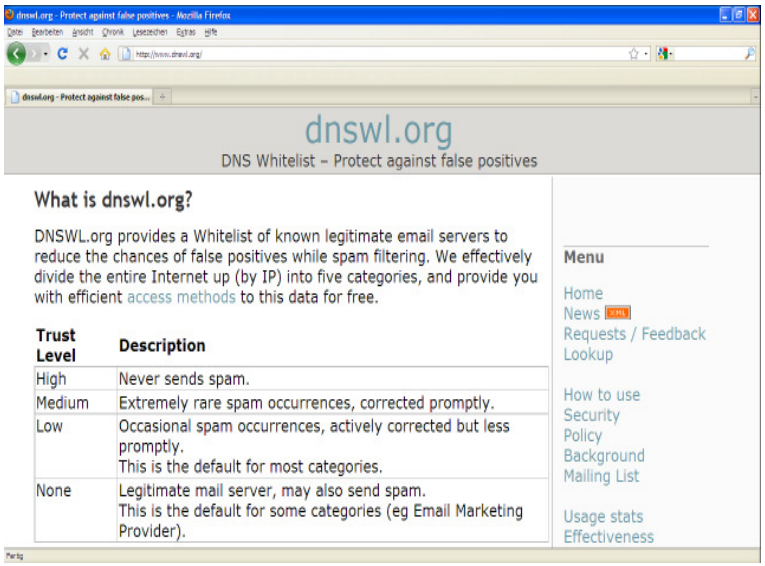
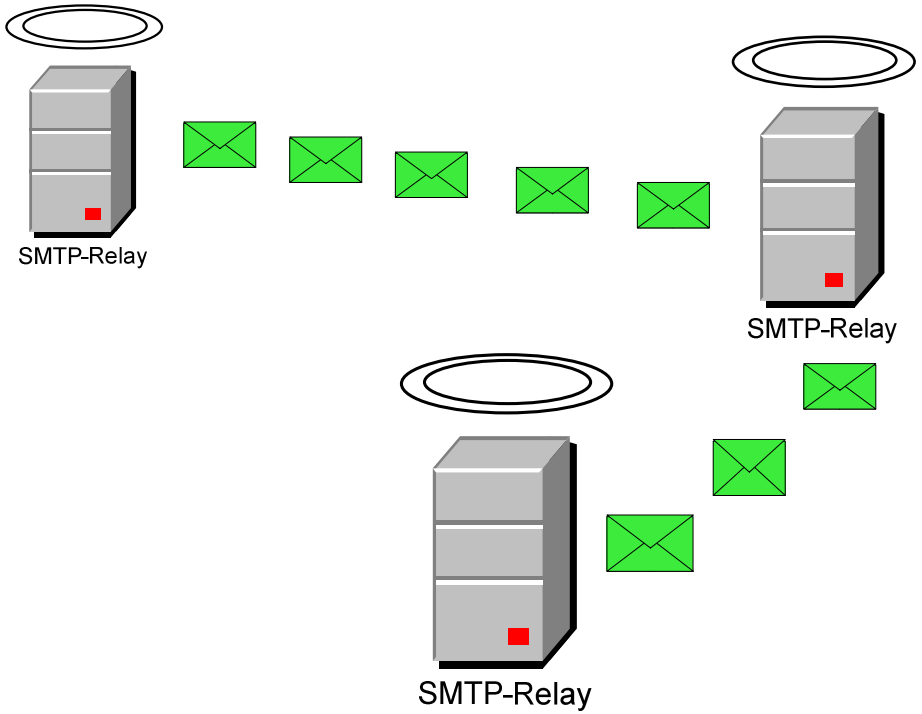




Matthias Leisi

Martin Blapp

d n s w l . o r g

protect against false email positives

About us

Matthias Leisi,
Dnswl.org project founder,
Head Datacenter/Network Swisscom
matthias@leisi.net

Martin Blapp,
Just one of the dnswl.org co-admins
Dnswl.swinog founder
UNIX Consultant
mbr@freebsd.org

What is dnswl.org ?

- A DNS based whitelist of official mail relays
- Sorted by „Trust Level“ and „Category“
- Made to protect your server against false positive mails
- The list should include your mailrelay too

d n s w l . o r g

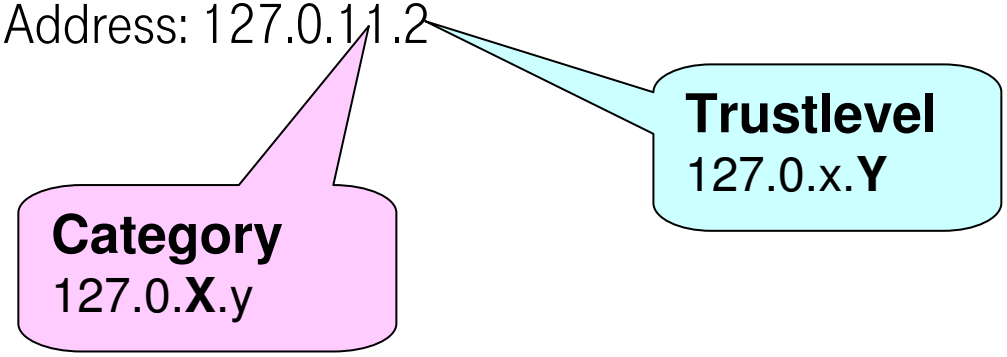
Why another (white)list ?

- Concentrate efforts in different countries
  (Our Swinog whitelist has almost only swiss entries)
- Non profit, no business idea like Senderbase etc.
- A free project, everybody can add to it
- Everybody can use it

How does it work ?

```
> nslookup 108.2.2.141.list.dnswl.org
Server: 127.0.0.1
Address: 127.0.0.1#53
Non-authoritative answer:

Name: 108.2.2.141.list.dnswl.org
Address: 127.0.11.2
```



Categories, 127.0.X.y

2 - Financial services
3 - Email Service Providers
4 - Organisations (both, profit and non-profit)
5 - Service/network providers
6 - Personal/private servers
7 - Travel/leisure industry
8 - Public sector/governments
9 - Media and Tech companies
10 - some special cases
11 - Education, academic
12 - Healthcare
13 - Manufacturing/Industrial
14 - Retail/Wholesale/Services
15 - Email Marketing Providers

Trust level, 127.0.x.Y

0 = none - only avoid outright blocking

1 = low - reduce chance of false positives

2 = medium - make sure to avoid false positives but allow override for clear cases

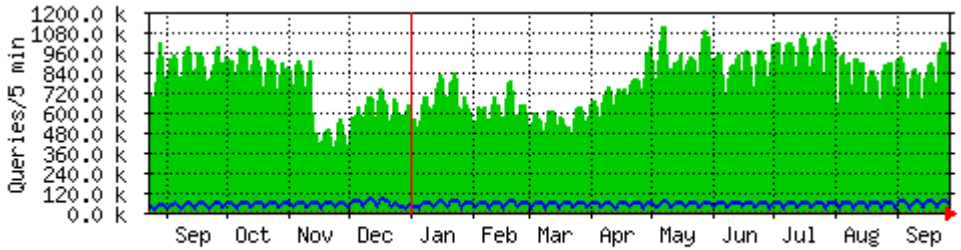
3 = high - avoid override

Whitelist vs. Blacklists

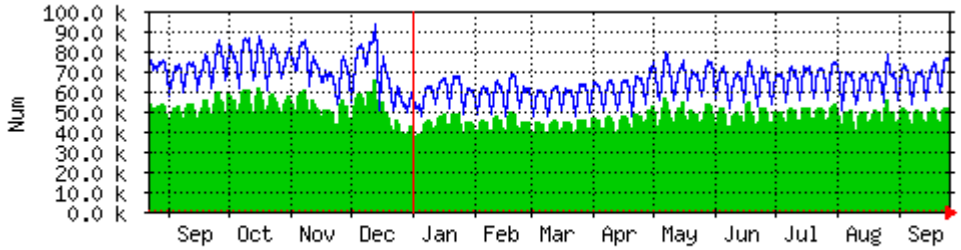
- Whitelist != Blacklist
- It a good thing to be listed
- Only a few millons of listed IP-adresses
- Too many whitelists means more untrusted sources
- Whitelists are more consistent than blacklists
- Blacklist vendors need a reliable whitelist

Monitoring of three DNS-mirrors:

- Number of requests: Yearly Graph (1 Day Average)



- Connecting Hosts: Yearly Graph (1 Day Average)



d n s w l . o r g

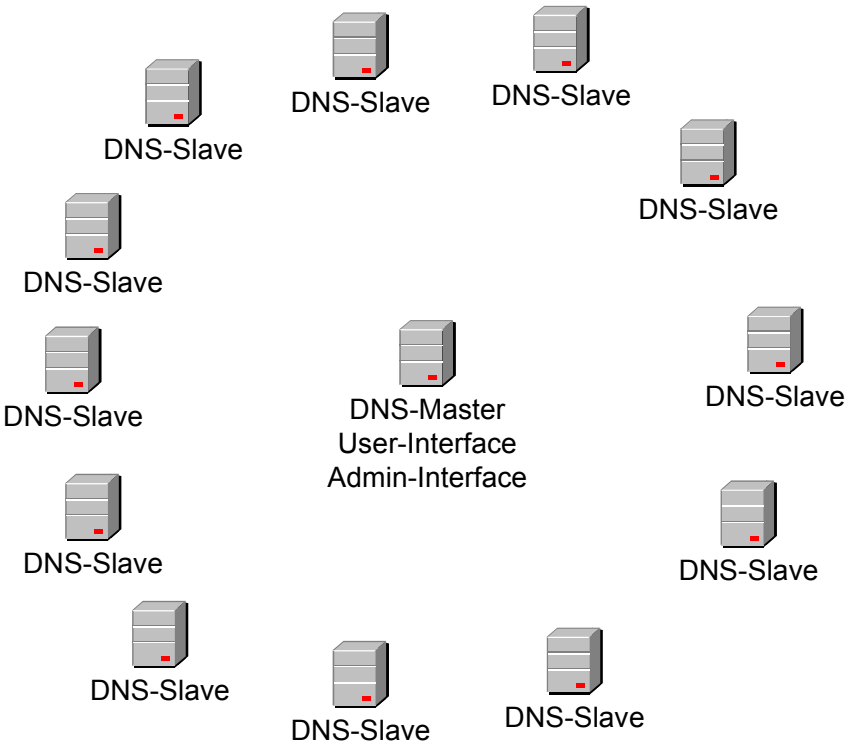
What we need

- More admins, especially in Asia (China, Japan)
  (Just ask us)
- Your help, tell us if a relay is missing
- Some sponsoring for the master infrastructure
- Optional: some sponsoring for part time job

Sponsoring: DNS-Master infrastructure

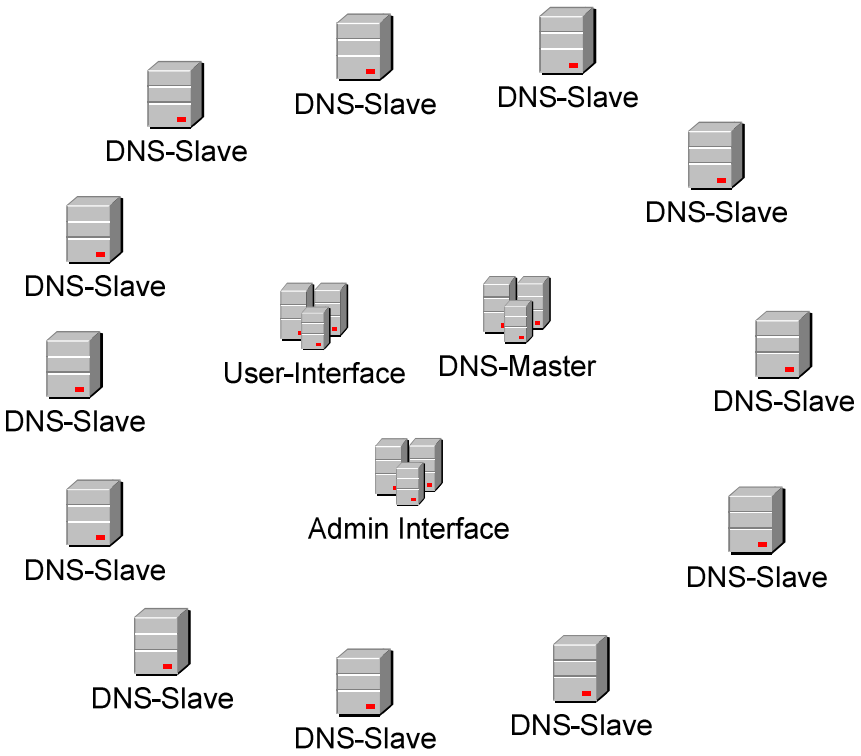
- Already have 10 sponsored DNS-Mirrors
- The main whitelist server (DNS master)
  is not sponsered, it runs on cheap hardware
- The project has no financial resources at all
  Sponsoring is needed to keep it alive
- No master HA-solution or site redundancy available
- We need 2-3 (virtual) servers, to make the
  project more safe against attacks

Current infrastructure



dnswl.org

Optimal infrastructure



dnswl.org

Sponsoring: Part time job

- Part time (2-3%) job, 1-2 hours / week
- Deal with listing/delisting requests
- Provide some basic help (for swinog members)
- Handle daily business stuff

Sponsoring ideas

- Logo placement on the dnswl.org webpage,
  Your logo on dnswl.org
- Create a dnswl logo, invite solution vendors to
  include the dnswl logo on their site / in their product
- We could call it Swinog‘s DNSWL.org
  Let‘s make swinog well known in the world

Future ?

- A new (independent) project leader
- More languages supported on the webpage
- All parts of the website translated to german
- Redundancy of master DNS- and webinterface servers
- Sponsoring ?

Any questions ?

For sponsoring please write to:

mbr@freebsd.org

matthias@leisi.net

d n s w l . o r g