PRISTOPI K REŠEVANJU NEŽELENE ELEKTRONSKE POŠTE

Jernej Porenta, jernej.porenta@arnes.si
SINOG, 2015-04-01

naročena sporočila

posredovana sporočila

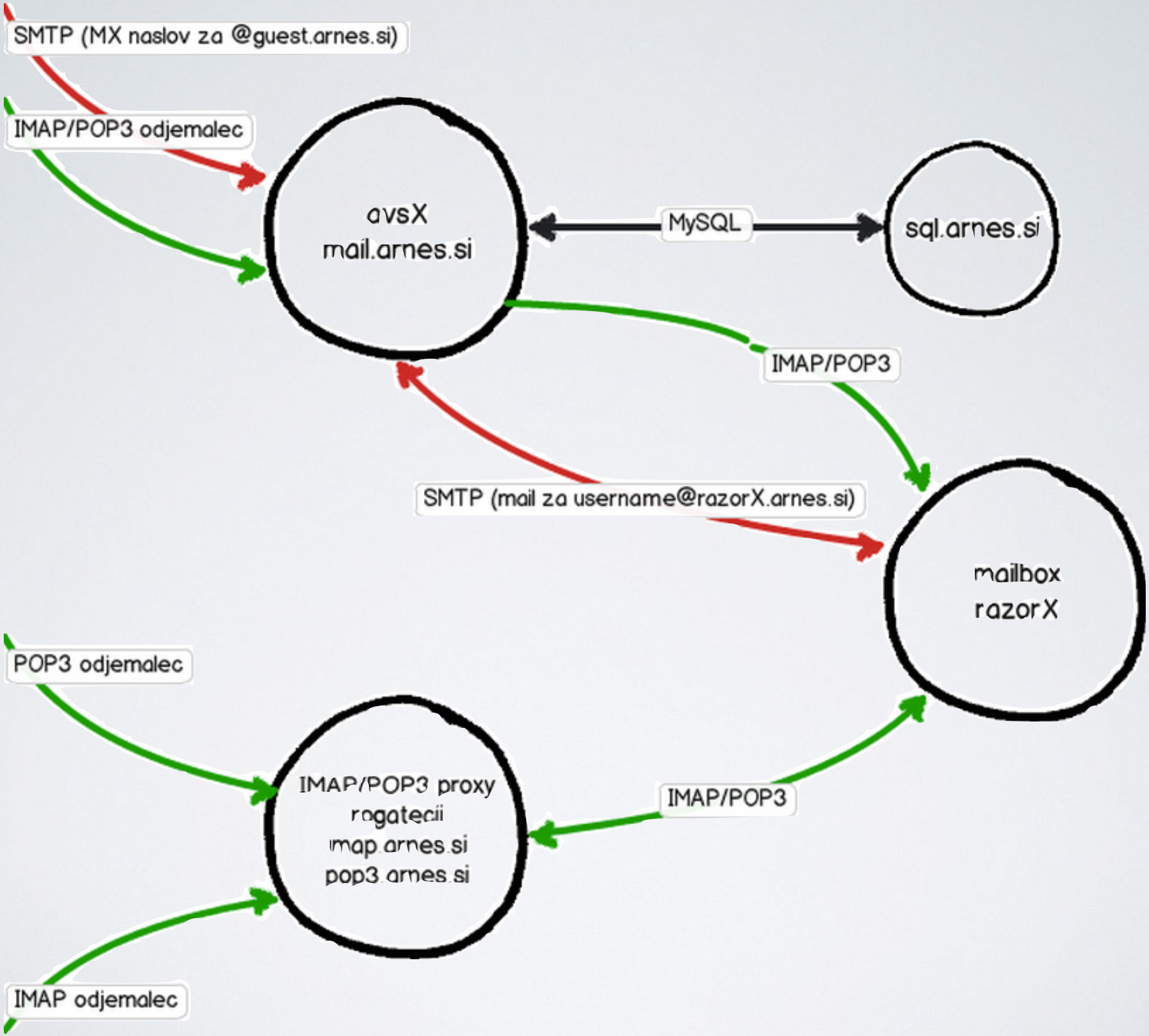
samodejna sporočila

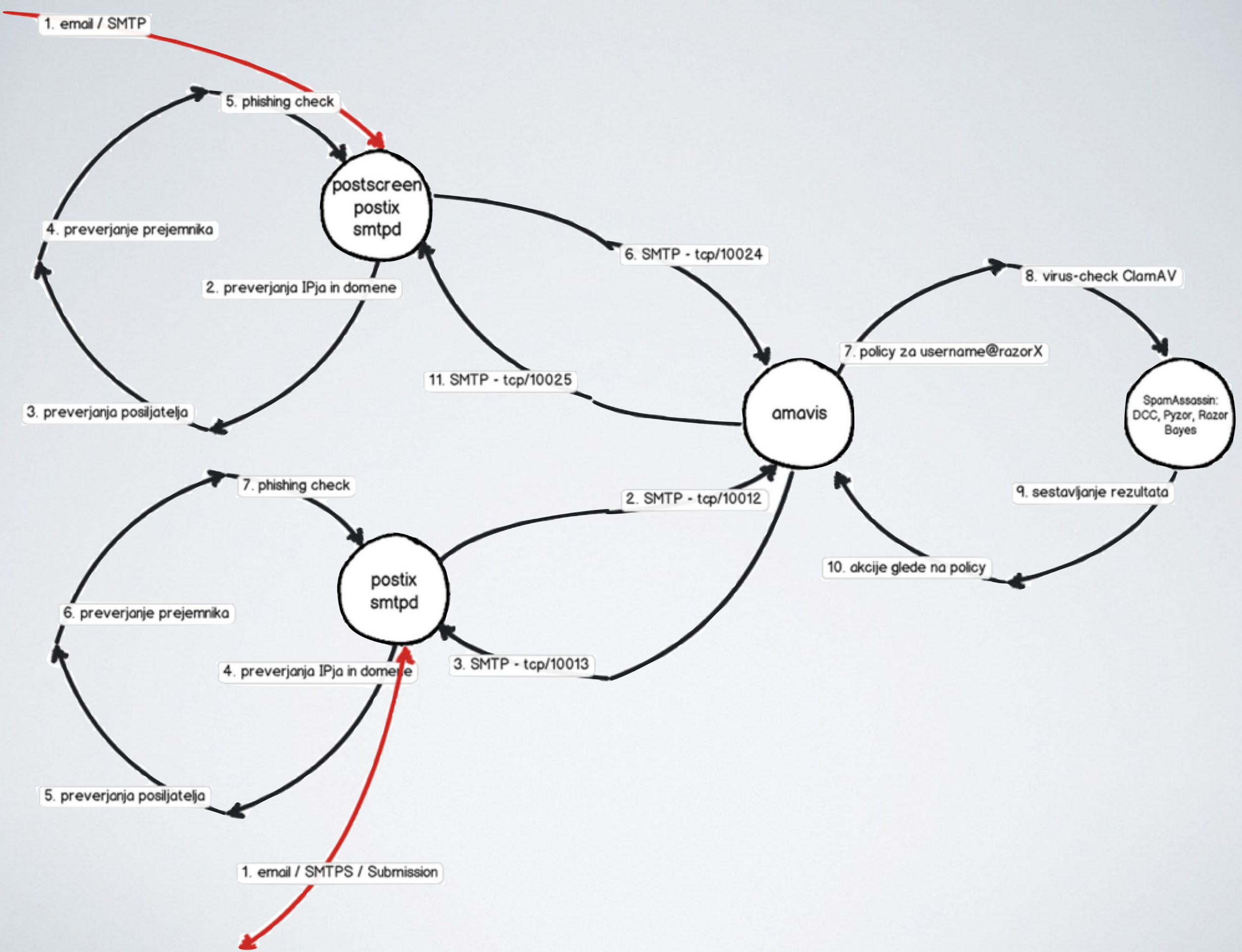
obvestila o napakah

niso spam

2010	2011	2012	2013
89%	75%	69%	66%

2014


SMTP (MX naslov za @guest.arnes.si)
IMAP/POP3 odjemalec
avsX
mail.arnes.si
MySQL
sql.arnes.si
IMAP/POP3
SMTP (mail za username@razorX.arnes.si)
mailbox
razorX
POP3 odjemalec
IMAP/POP3 proxy
ragatecii
imap.arnes.si
pop3.arnes.si
IMAP/POP3
IMAP odjemalec


1. email / SMTP
5. phishing check
postscreen
postix
smtpd
4. preverjanje prejemnika
2. preverjanja IPja in domene
3. preverjanja posiljatelja
6. SMTP - tcp/10024
11. SMTP - tcp/10025
amavis
7. policy za username@razorX
8. virus-check ClamAV
SpamAssassin:
DCC, Pyzor, Razor
Bayes
9. sestavljanje rezultata
10. akcije glede na policy
2. SMTP - tcp/10012
7. phishing check
postix
smtpd
6. preverjanje prejemnika
4. preverjanja IPja in domene
3. SMTP - tcp/10013
5. preverjanja posiljatelja
1. email / SMTPS / Submission

SMTP SERVER

- Postfix 2.11
  - postscreen

```
Mar 31 02:21:29 avs1 postfix/postscreen[10347]: PREGREET 22
after 0.25 from [153.122.53.218]:55939: HELO www.tolstli.com\r\n
```

  - RBL:
    - zen.spamhaus.org
    - swl.spamhaus.org
    - Invaluement
- Anti-phishing reply list - http://aper.sf.net

POLICY SERVER

- postfwd2 - 1.3.5
  - hapolicy
- preverjanje v END-OF-DATA fazi prejema
- quota/rate-limiting
  - per user (sasl username)
  - per IP
  - različne nastavitve ponoči in podnevi, čez vikend in ob delavnikih

POLICY SERVER

```
# rate limit to 250 recipients during weekends
id=RATE_WEBMAIL_WEEKEND
        &&WEBMAIL
        days=Sat-Sun
        action=rcpt(sender/250/3600/450 4.7.1 sorry, max
250 recipients per hour)

# rate authenticated senders to 500 recipients per hour
id=RATE_SASL_AUTHENTICATED_HOUR
        !!&&SASL_IZJEME
        sasl_username=~/^(\S+)$/
        action=rcpt(sasl_username/1000/3600/450 4.7.1
sorry, max 1000 recipients per hour for $$sasl_username)
```

AMAVISD-NEW

Hvala Mark!

AMAVISD-NEW

- Verzija 2.9.1
- SpamAssassin 3.4 - SVN
- MySQL
  - nastavitve glede označevanja virusov, spama, datotek, …
  - karantena zavrnjenih in izbrisanih emailov - 7 dni
- Redis:
  - Bayes, penpals, IP reputation
  - logging

AMAVISD-NEW

- DKIM
  - podpisovanje Arnesovih domen (@guest.arnes.si, @arnes.si, @cert.si, …)
- Dodatki:
  - DCC - dcc1.arnes.si, Pyzor, Razor
  - ClamAV (+ SaneSecurity signatures + Si.Postmaster rules)
  - CRM114
  - p0f - passive OS fingerprinting

MAILBOX SERVER

- Dovecot - v. 2.2.16
- Linux CentOS7
- LDAP backend
- MDBOX
- CLucene IMAP search index
- Configuration management: Puppet

ANALITIKA

- postfix-logreport
- amavis-logreport
- logstash
- elasticsearch
- splunk
- kibana
- grafana

BCP

- Nadzor svojih uporabnikov:
  - GeoIP > 3
  - quota
  - FBL velikih ponudnikov
- Podpisovanje:
  - DKIM, SPF(forward?), DMARC
  - Pregledovanje odhajajoče pošte