

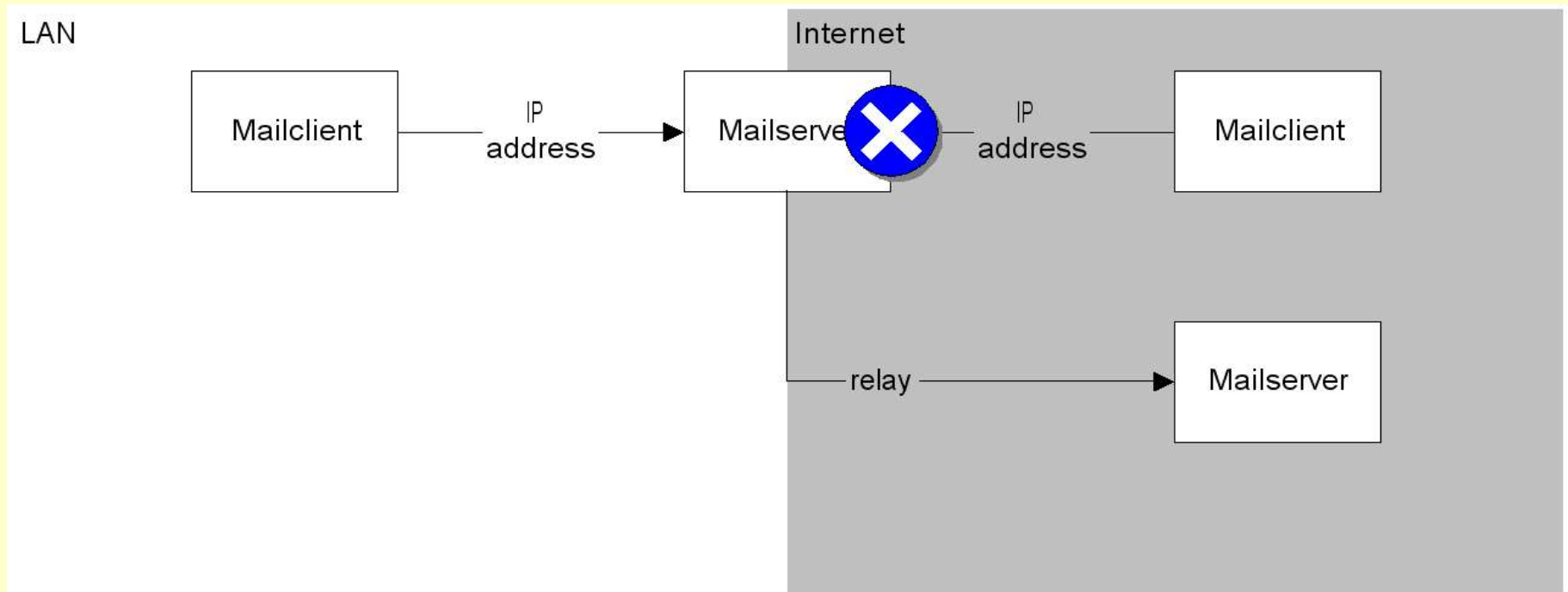
# Postfix and alternative, non-IP based relay concepts

## SMTP Authentication and Certificate Based Relaying with Postfix

# Index

1. Status Quo
2. Existing Solutions
3. Problems of existing solutions
4. Implementation Goals
5. Software Prerequisites
6. SMTP Authentication
7. SMTP Authentication: Steps
8. Configuring Cyrus SASL
9. Configuring Postfix
10. Certificate Based Relaying
11. Certificate Based Relaying: Steps
12. Creating Certificates in OpenSSL
13. Configuring TLS in Postfix server
14. Configuring TLS in Postfix client
15. Further Readings
16. about: speaker

# Status Quo



Mobile users need simple and secure access to their domains resources; IP-based identification to permit relaying is insufficient for dynamic IP-adresses.

# Existing Solutions

- Port-Forwarding with SSH
- Virtual Private Networks
- SMTP-after-POP
- SMTP Authentication
- Certificate Based Relaying

# Problems of existing solutions

- Port-Forwarding with SSH
  - Requires client side interaction  
“Users want to focus on the computing, not the computer.”
  - Too complicated for regular users
- SMTP-after-POP/IMAP
  - Does not solve the problem where it arises
  - Binds the MTA to an MDA
  - Introduces just another point of failure

# Implementation Goals

- Low dependencies
- Secure
- Set and forget

# Software Prerequisites

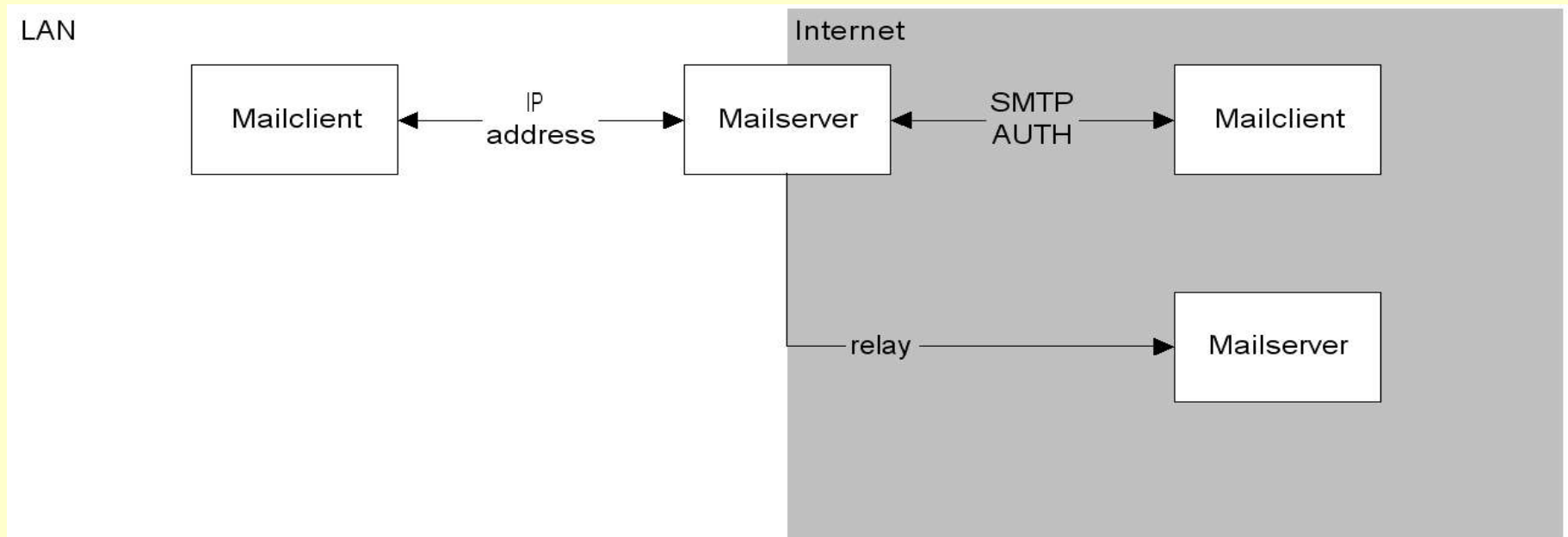
- **Server**

- Cyrus SASL > 2.1.17 (from CVS) for SMTP Authentication
- OpenSSL > 0.9.7c for Certificate Based Relaying
- Postfix with SASL2 and TLS enabled

- **Client**

- SMTP AUTH capability
- Client side TLS

# SMTP Authentication



SMTP Authentication identifies the mail client using the credentials it submits; an authenticated client may relay messages.

# SMTP Authentication: Steps

You have to configure how Postfix interacts with Cyrus SASL **and** how Postfix interacts with clients.

- Postfix interaction with Cyrus SASL
  - Choose a password verification service
  - Choose mechanisms to offer
  - Configure password verification service
  - Test authentication with Cyrus SASL tools
- Postfix interaction with mail clients
  - Enable SMTP AUTH
  - Set security settings
  - Test SMTP AUTH

# Configuring Cyrus SASL

Cyrus SASL configuration settings for Postfix are stored in `/usr/lib/sasl2/smtpd.conf`.

```
pwcheck_method: saslauthd
mech_list: plain login cram-md5 digest-md5
log_level: 7
```

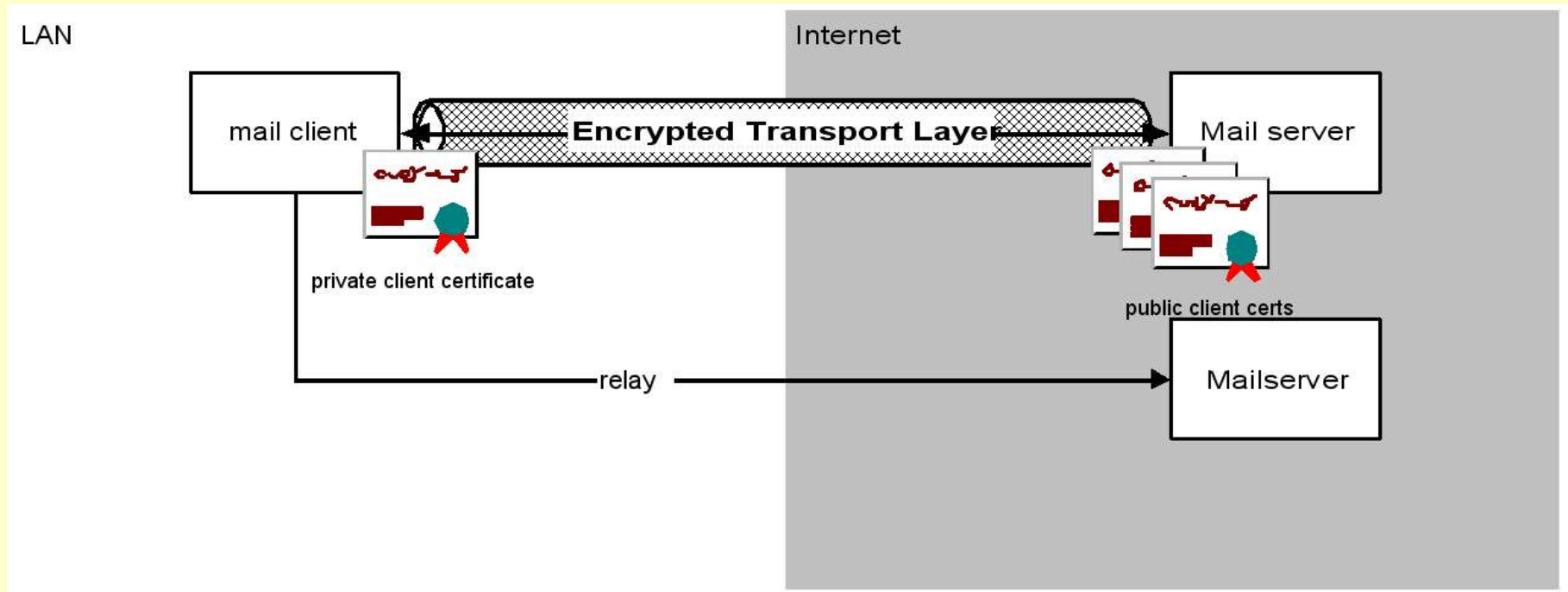
Use `server` and `client` from Cyrus SASL to test authentication before you enable SMTP AUTH in Postfix.

# Configuring Postfix

SMTP AUTH settings for Postfix are configured in `/etc/postfix/main.cf`:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain =
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
    permit_sasl_authenticated,
    permit_mynetworks,
    reject_unauth_destination,
    ...
```

# Certificate Based Relaying



Certificate Based Relaying uses the clients certificate to identify clients that may relay.

# Certificate Based Relaying: Steps

- **OpenSSL**
  - Create server cert
  - Create client cert
  - Sign certs
- **Postfix Server**
  - Enable TLS for smtpd daemon
  - Add clients cert fingerprint to lookup map
  - Ask for client certificates
- **Postfix Client**
  - Add server's CA cert to CA store
  - Enable TLS for smtp daemon

# Creating Certificates in OpenSSL

- Create CA cert

```
# ./CA.pl -newca
```

- Create cert

```
# openssl req -new -nodes -keyout \  
postfix_private_key.pem -out \  
postfix_private_key.pem -days 365
```

- Sign cert

```
# openssl ca -policy policy_anything -out \  
postfix_public_cert.pem -infile \  
postfix_private_key.pem
```

# Configuring TLS in Postfix server

```
# cd /etc/postfix/certs  
# chmod 600 postfix_private_key.pem
```

```
smtpd_use_tls = yes  
smtp_tls_loglevel = 2  
smtpd_tls_CApath = /etc/postfix/certs  
smtpd_tls_cert_file = /etc/postfix/certs/postfix_public_cert.pem  
smtpd_tls_key_file = /etc/postfix/certs/postfix_private_key.pem  
smtpd_tls_received_header = yes  
tls_random_source = dev:/dev/urandom  
  
smtpd_tls_ask_ccert = yes
```

# Configuring TLS in Postfix client

```
# cd /etc/postfix/certs  
# chmod 600 postfix_private_key.pem
```

```
smtp_use_tls = yes  
smtp_tls_CApath = /etc/postfix/certs  
smtp_tls_loglevel = 2  
smtp_tls_note_starttls_offer = yes  
smtp_tls_cert_file = /etc/postfix/certs/postfix_public_cert.pem  
smtp_tls_key_file = /etc/postfix/certs/postfix_private_key.pem
```

# Further Readings

## Online

- Postfix  
<http://www.postfix.org>
- Postfix TLS patch  
[http://www.aet.TU-Cottbus.DE/personen/jaenicke/postfix\\_tls/](http://www.aet.TU-Cottbus.DE/personen/jaenicke/postfix_tls/)
- Cyrus SASL  
<http://asg.web.cmu.edu/cyrus/download/sasl/>
- Postfix SMTP AUTH (and TLS) HOWTO  
<http://postfix.state-of-mind.de/patrick.koetter/smtpauth/>

## Offline

The Book of Postfix, Best practice guide to Postfix - alternative to Sendmail  
Ralf Hildebrandt and Patrick Koetter, No Starch Press, June 2004  
<http://www.postfix-book.com>

# about: speaker

Patrick Ben Koetter

WebSite: [www.state-of-mind.de](http://www.state-of-mind.de)

E-Mail: [p@state-of-mind.de](mailto:p@state-of-mind.de)