Konfiguracja serwera poczty elektronicznej

Postfix a spam

dr inż. Maciej Miłostan
Zespół bezpieczeństwa PCSS

Agenda

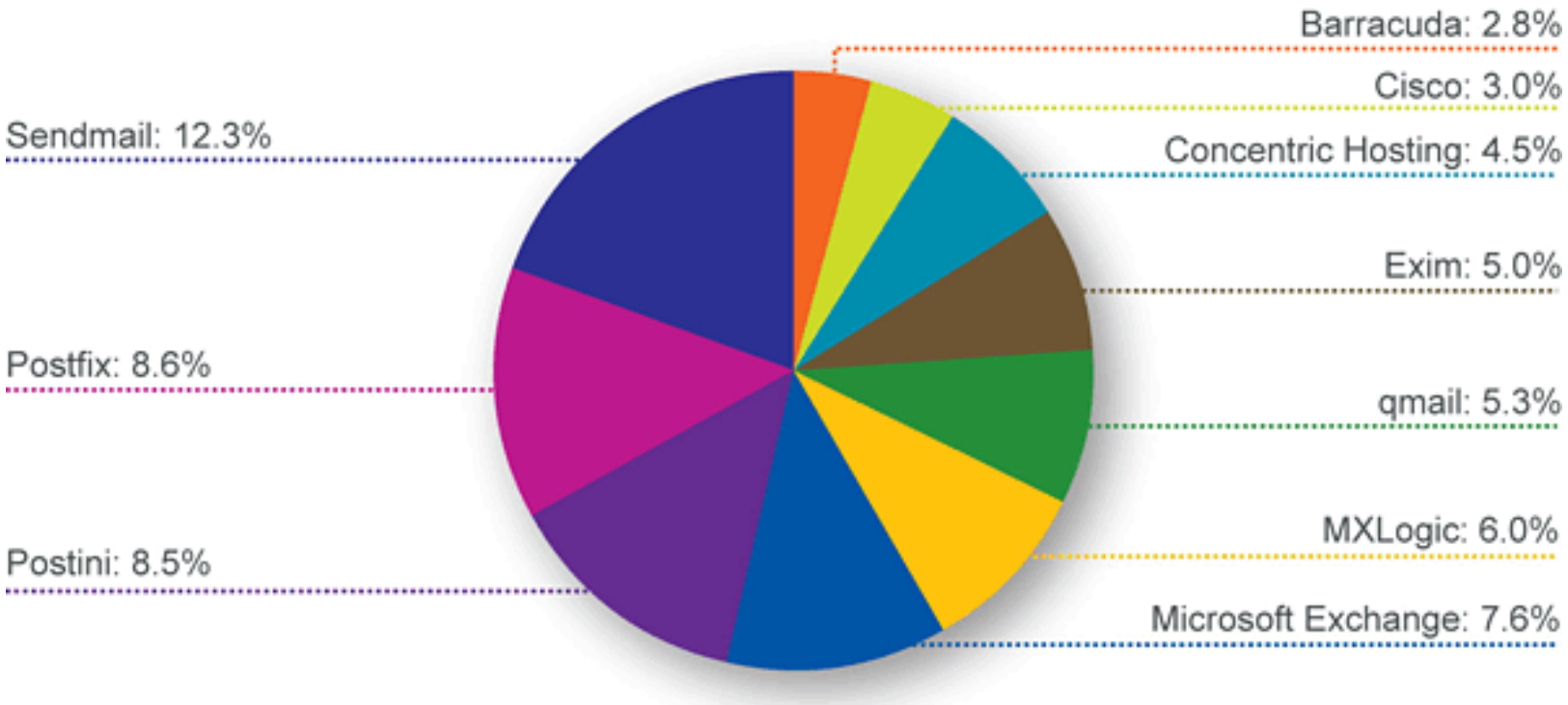
- Co to jest Postfix?
- Podstawowa konfiguracja
- Autoryzacja, TLS itp.
- Opcje antyspamowe
- Integracja zewnętrznych filtrów
- Podsumowanie

Postfix

- MTA (Mail Transfer Agent)
- IBM Research
- Secure Mailer open source release (grudzień 1998)
- Lekki, bezpieczny
- Alternatywa dla sendmail-a
- Szybki, łatwy w użytkowaniu i bezpieczny

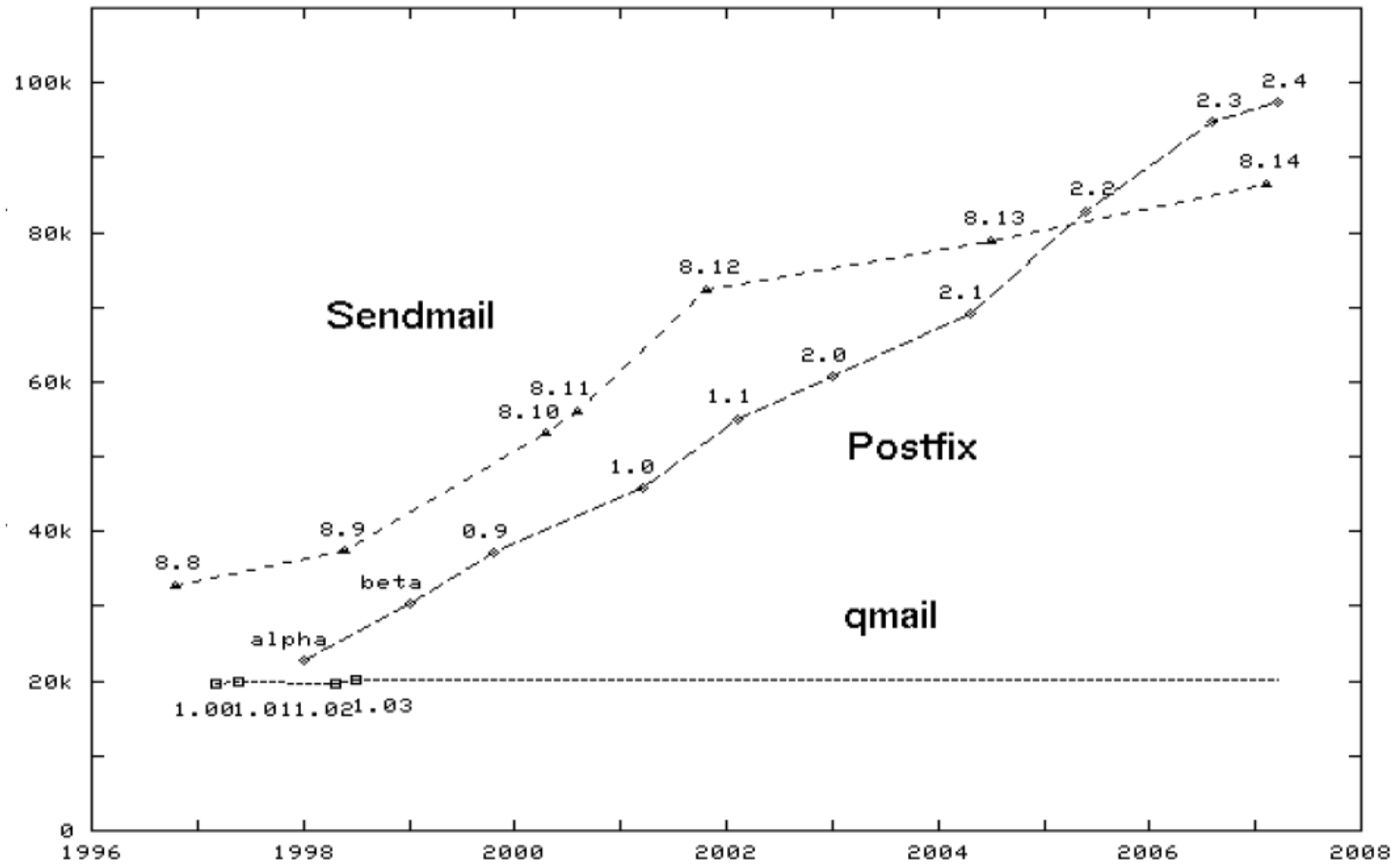
Wietse Zweitze Venema

Udział w rynku



Na podstawie opracowania Ken-a Simpson-a i Stas-a Bekman-a, O'Reilly SysAdmin, Styczeń 2007.
http://www.oreillynet.com/pub/a/sysadmin/2007/01/05/fingerprinting-mail-servers.html

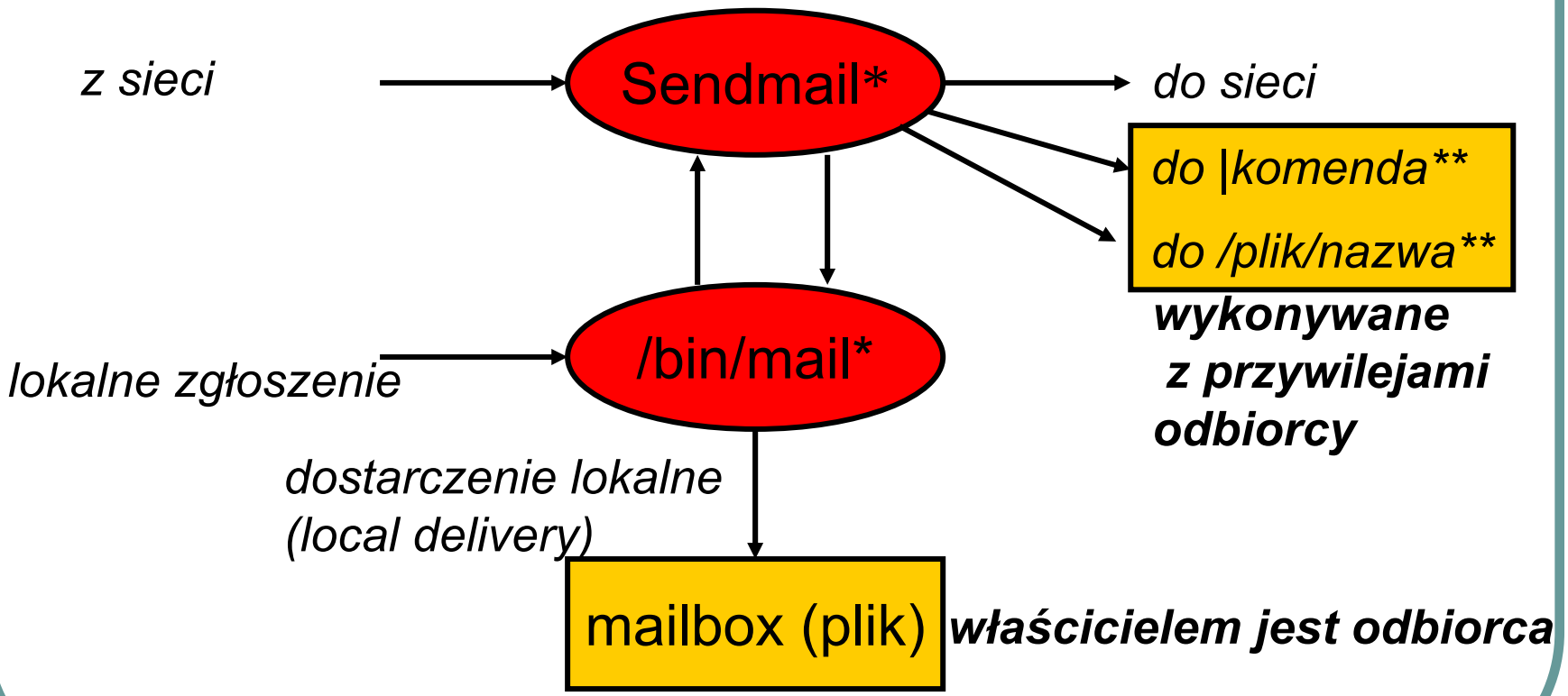
Wzrost rozmiarów MTA w czasie



Na podstawie: http://www.ceas.cc/2007/postfix-ceas-public.ppt

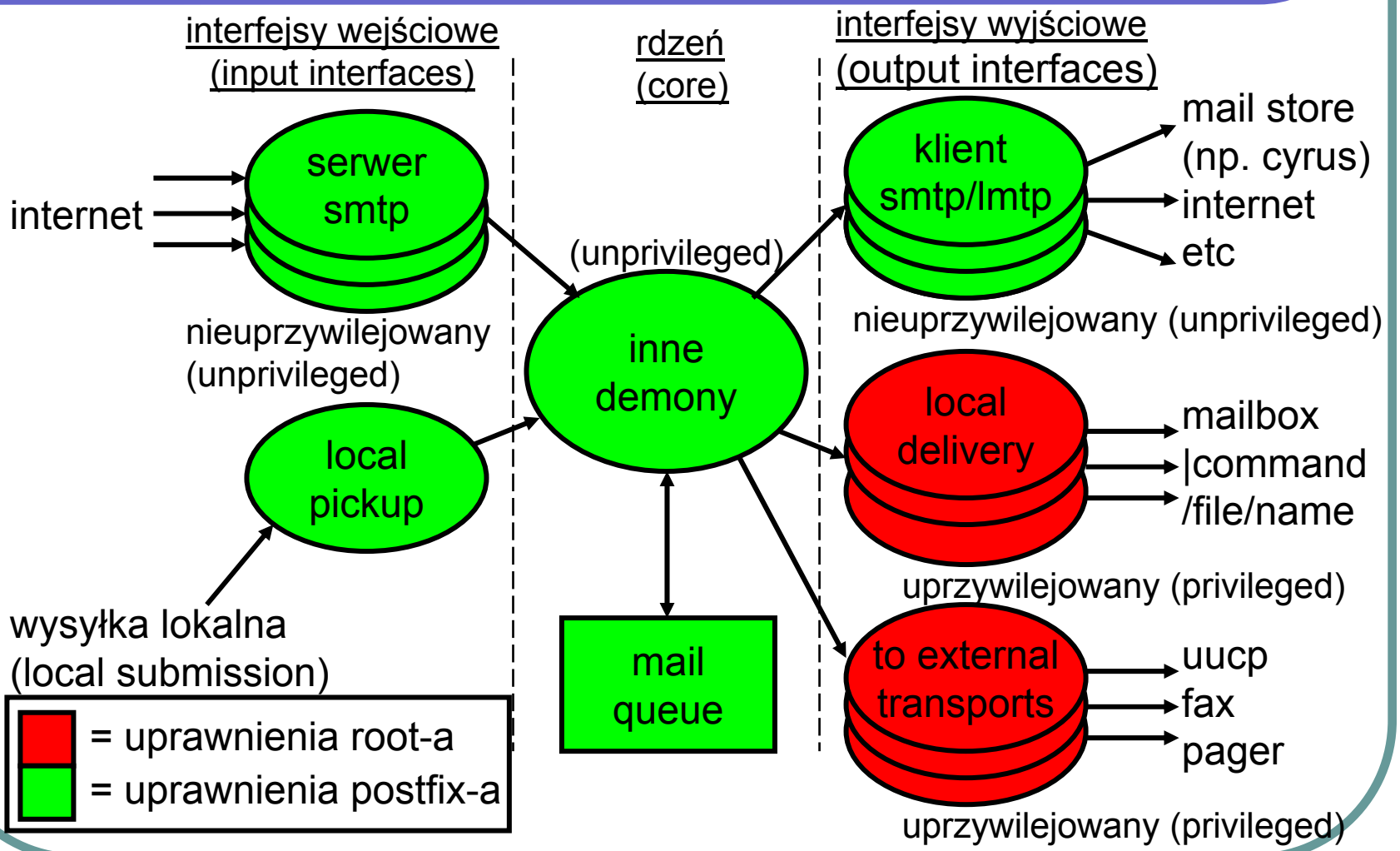
Architektura tradycyjnego systemu poczty z BSD UNIX

- impersonacja wymaga przywilejów, model monolityczny utrudnia kontrolę nad ew. zniszczeniami

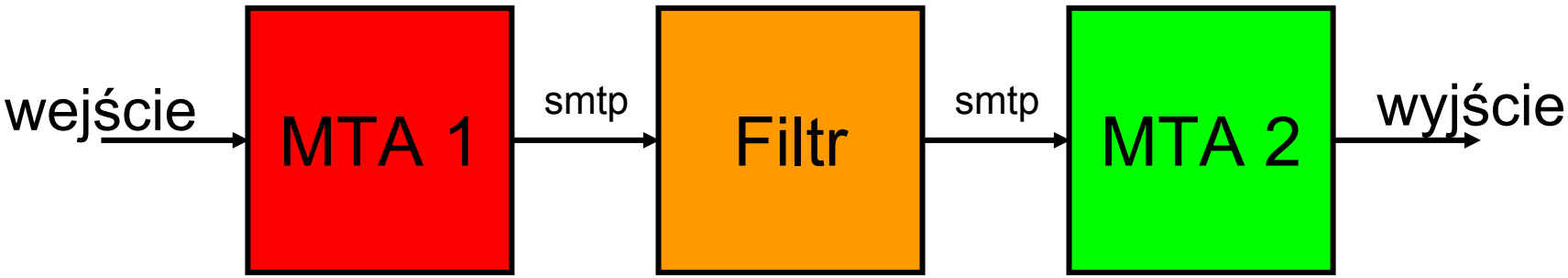


* używa przywilejów root-a (root privileges)
** w plikach .forward użytkowników i bazie aliasów systemowych

Architektura Postfix-a (~~client server~~ service oriented)

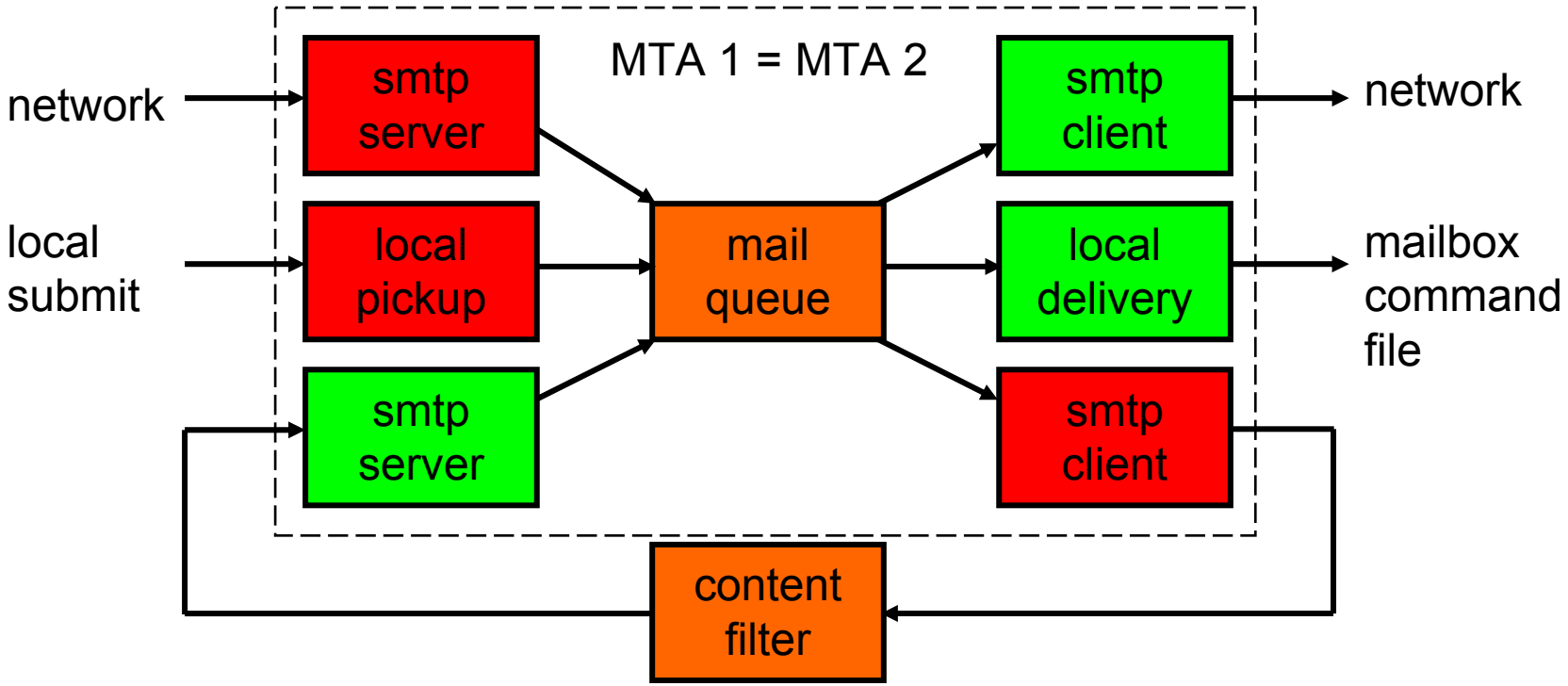


Inspekcja zawartości poprzez SMTP (post queue)



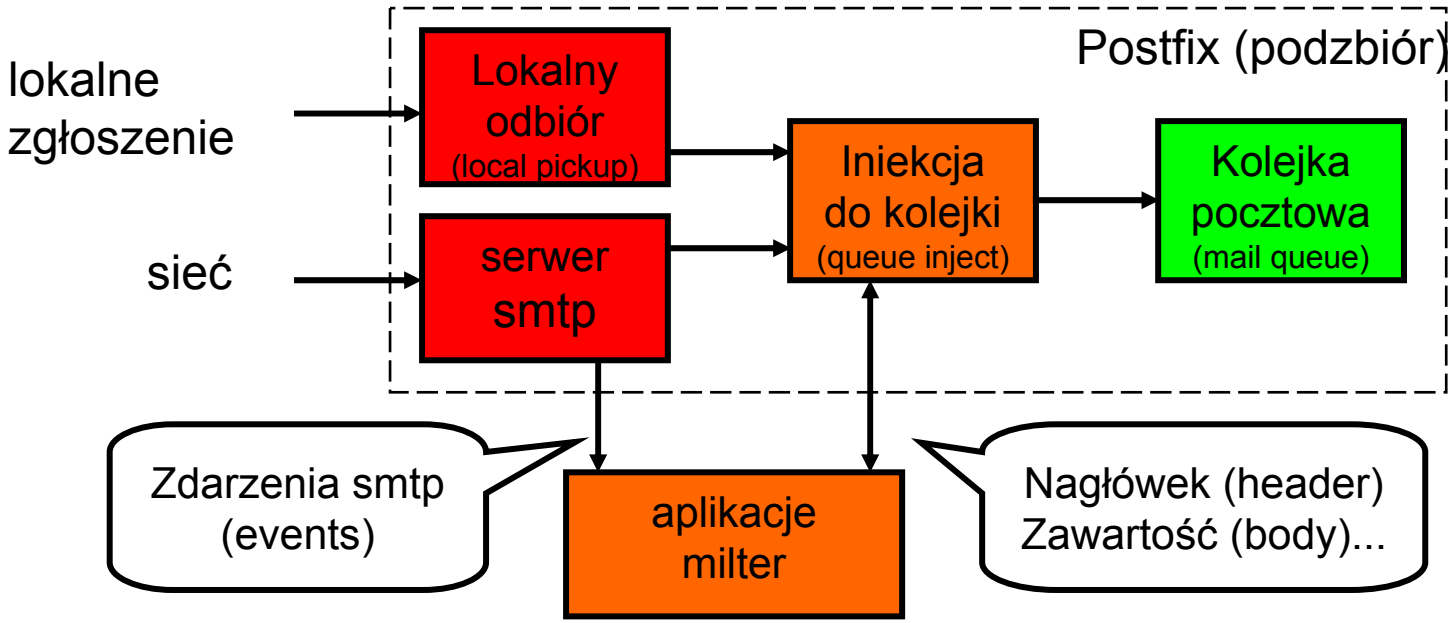
- Czerwony = brudny, zielony = czysty.
- To nie może być takie proste, prawda?
- Użycie dwóch MTA to marnotrawstwo!

Inspekcja zawartości poprzez SMTP (post queue)



- Złożenie dwóch MTA w jeden system powoduje zaoszczędzenie zasobów, ale zwiększa złożoność

Milter a Postfix



- Czerwony = brudny, zielony = czysty
- Twórca Postfixa został uhonorowany nagrodą Sendmaila za dodanie tej funkcjonalności

Pliki konfiguracyjne

/etc/postfix/master.cf

/etc/postfix/main.cf

- Dwa główne pliki konfiguracyjne

Filtracja a protokół SMTP

```
>telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.xxx.poznan.pl ESMTP Postfix on SuperServer
helo client.some.domain
250 mail.xxx.put.poznan.pl
mail from: mm@xxx.poznan.pl
250 2.1.0 Ok
rcpt to: mm@xxx.poznan.pl
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Test Postfix-a
To: Administrator <administrator@xxx.poznan.pl>
Witaj Administratorze,
Pozdrawiam.

.
250 2.0.0 Ok: queued as 10D5C5E
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

← smtpd_client_restrictions

← smtpd_helo_restrictions

← smtpd_sender_restrictions

← smtpd_recipient_restrictions

← smtpd_data_restrictions

← smtpd_end_of_data_restrictions

smtpd_etrn_restrictions

Konfiguracja domyślna

Nazwa listy ograniczeń	Status
smtpd_client_restrictions	Opcjonalna
smtpd_helo_restrictions	Opcjonalna
smtpd_sender_restrictions	Opcjonalna
smtpd_recipient_restrictions	**Wymagana**
smtpd_data_restrictions	Opcjonalna
smtpd_end_of_data_restrictions	Opcjonalna
smtpd_etrn_restrictions	Opcjonalna

smtpd_delay_reject = yes

Restrykcje względem klientów, nadawców i odbiorców

- Co możemy sprawdzać:
  - Poprawność składniową adresu e-mail
  - Rekordy w DNS:
    - MX
    - NS
    - A
    - TEXT (np. SPF)
  - Zgodność działania klienta z protokołem
  - Czy komendy są przesyłane po uzyskaniu odpowiedzi na poprzednie
  - Czy lokalny użytkownik jest zalogowany
  - Czy lokalny użytkownik może wysyłać z danego adresu e-mail
  - Z jakiego adresu IP zostało nawiązane połączenie, czy z zaufanego adresu itp. itd.

Konfiguracja domyślna i podstawowe parametry

- Nazwa domeny, nazwa hosta

/etc/postfix/main.cf:

myhostname = host.my.domain (nazwa hosta nie jest FQDN, rose (NFQDN) vs. rose.man.poznan.pl (FQDN))

mydomain = my.domain
(gdzie my.domain jest konkretną domeną, np. man.poznan.pl)

myhostname = host.virtual.domain (virtual interface)

myhostname = virtual.domain (virtual interface)

Konfiguracja domyślna i podstawowe parametry

- Poczta wychodząca (outbound mail)

  /etc/postfix/main.cf:

myorigin = $myhostname (domyślnie: wysyła e-mail jako "user@$myhostname")
myorigin = $mydomain (prawdopodobnie pożądana forma: "user@$mydomain")

Konfiguracja domyślna i podstawowe parametry

- Poczta przychodząca – obsługiwane adresy

/etc/postfix/main.cf:

mydestination = $myhostname localhost.$mydomain localhost (domyślnie)

mydestination = $myhostname localhost.$mydomain localhost $mydomain
(serwer dla całej domeny)

mydestination = $myhostname localhost.$mydomain localhost

www.$mydomain ftp.$mydomain
(host z wieloma rekordami A w DNS)
Uwaga: w celu uniknięcia pętli (mail delivery loops) trzeba wylistować wszystkie nazwy danej maszyny

Konfiguracja domyślna i podstawowe parametry

- Ograniczanie przesyłania z naszych adresów, czyli „what clients to relay mail from”

/etc/postfix/main.cf:

mynetworks_style = subnet
(default: authorize subnetworks)
mynetworks_style = host
(safe: authorize local machine only)
mynetworks = 127.0.0.0/8
(safe: authorize local machine only)
mynetworks = 127.0.0.0/8 168.100.189.2/32
(authorize local machine)

mynetworks_style jest ignorowane

Konfiguracja domyślna i podstawowe parametry

- Metoda doręczania – pośrednio czy bezpośrednio /etc/postfix/main.cf:

relayhost =
(default: direct delivery to Internet)
relayhost = $mydomain
(deliver via local mailhub)
relayhost = [mail.$mydomain]
(deliver via local mailhub)
relayhost = [mail.isp.tld]
(deliver via provider mailhub)

Nawiasy eliminują wyszukiwanie rekordu MX w DNS-ie

Konfiguracja domyślna i podstawowe parametry

- Postmaster

/etc/aliases:

```
postmaster: you
root: you
```

- O czym (domyślnie) informować:

/etc/postfix/main.cf:

```
notify_classes = resource, software
```

Konfiguracja domyślna i podstawowe parametry

- O czym informować (notify_classes)

1. bounce
2. 2bounce
3. delay
4. policy
5. protocol
6. resource
7. software

Konfiguracja domyślna i podstawowe parametry

- /etc/postfix/main.cf:

  inet_interfaces = all

  inet_interfaces = virtual.host.tld
  (virtual Postfix)
  inet_interfaces = $myhostname
  localhost...
  (non-virtual Postfix)

Dostarczanie do skrzynek

- **local_recipient_maps**

local_recipient_maps =
    proxy:unix:passwd.byname $alias_maps

Niezbędne przy dostarczaniu e-maili do użytkowników bez konta unix-owego

(odrzucanie maili do nieznanych użytkowników, domyślne ustawienie)

- **mailbox_transport** (default:empty)

mailbox_transport = lmtp:unix:/var/imap/socket/lmtp

(dostarczanie za pomocą protokołu LMTP np. do skrzynek cyrus imap-a nasłuchującego na lokalnym gniazdku (socket))

Przykładowa konfiguracja

/etc/postfix/main.cf

```
…
myhostname = cos.costam.poznan.pl
mydomain = costam.poznan.pl
inet_interfaces = all
notify_classes = resource, software
relayhost =
relay_domains = $mydestination
mydestination = $myhostname, localhost.$mydomain, $mydomain,
    mail.$mydomain
mynetworks = 150.254.x.x, 127.0.0.0/8
alias_database = hash:/etc/mail/aliases
alias_maps = hash:/etc/aliases
smtpd_recipient_restrictions = permit_mynetworks
    reject_unauth_destination
```

Problemy

- Pocztę na zewnątrz mogą wysyłać tylko użytkownicy sieci/hostów wyspecyfikowanych w *mynetworks*
- Spamerzy mogą podszywać się pod wewnętrznych użytkowników
- Wewnętrzni użytkownicy mogą fałszować adresy nadawców i wysyłać do dowolnych odbiorców

Rozwiązanie problemu

- Pocztę na zewnątrz mogą wysyłać tylko użytkownicy sieci/hostów wyspecyfikowanych w *mynetworks*
- Rozwiązanie:
  - wykorzystać

    ~~check_sender_access hash:/etc/postfix/access~~
  - użyć autoryzacji

    SMTP AUTH = permit_sasl_authenticated
    + SASL

Autoryzacja

- SASL

  /etc/postfix/main.cf:

```
smtpd_sasl_auth_enable = yes
smtpd_recipient_restrictions =
permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
(smtpd_sasl_authenticated_header = yes)
(broken_sasl_auth_clients = yes)
```

Autoryzacja

- Cyrus SASL version 2.1.x
  /etc/sasl2/smtpd.conf:

```
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN
```

- W celu użycia PAM (Pluggable Authentication Modules), uruchom saslauthd z opcją "-a pam".

Testowanie autoryzacji

```
>printf '\0username\0password'|mimencode
AHVzZXJuYW1lAHBhc3N3b3Jk
>telnet server.example.com 25
. . .
220 server.example.com ESMTP Postfix
EHLO client.example.com
250-server.example.com
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH DIGEST-MD5 PLAIN CRAM-MD5
250 8BITMIME
AUTH PLAIN AHVzZXJuYW1lAHBhc3N3b3Jk
235 Authentication successful
```

Problem z hasłem

- Hasło jest przesyłane „czystym tekstem”
- Rozwiązanie:
  - szyfrowanie transmisji, czyli TLS

Szyfrowanie

- TLS

/etc/postfix/main.cf

```
smtpd_use_tls = yes
smtpd_tls_auth_only = no
smtpd_tls_key_file = /etc/postfix/postfix.key
smtpd_tls_cert_file = /etc/postfix/postfix.crt
smtpd_tls_CAfile = /etc/postfix/CA.crt
smtpd_tls_loglevel = 2
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

Problemy

- Pocztę na zewnątrz mogą wysyłać tylko użytkownicy sieci/hostów wyspecyfikowanych w *mynetworks*
- Spamerzy mogą podszywać się pod wewnętrznych użytkowników
- Wewnętrzni użytkownicy mogą fałszować adresy nadawców (niekoniecznie lokalnych) i wysyłać do dowolnych odbiorców

Fałszowanie nagłówków

```
>telnet mail.xxx.poznan.pl
Trying mail.xxx.poznan.pl...
Connected to localhost.
Escape character is '^]'.
220 mail.xxx.poznan.pl ESMTP Postfix on SuperServer
helo client.some.domain
250 mail.xxx.poznan.pl
mail from: mm@xxx.poznan.pl
250 2.1.0 Ok
rcpt to: mm@xxx.poznan.pl
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Test Postfix-a
To: Administrator <administrator@xxx.poznan.pl>
Witaj Administratorze,
Pozdrawiam.

.
250 2.0.0 Ok: queued as 10D5C5E
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Połączenie spoza zaufanych sieci

Brak sprawdzania, czy klient jest uprawniony

Sprawdzanie, czy lokalny odbiorca (domyślnie dozwolony)

Mapy kont i użytkowników

- Relacja: adresy pocztowe a nazwy użytkowników

Mapy kont i użytkowników

- smtpd_sender_login_maps = hash:/etc/postfix/login_maps
- /etc/postfix/main.cf: reject_sender_login_mismatch
- /etc/postfix/login_maps

milostan@host.xxx.poznan.pl	milostan@host.xxx.poznan.pl
mm@xxx.poznan.pl	milostan@host.xxx.poznan.pl
mm@cs.xxx.poznan.pl	milostan@host.xxx.poznan.pl
cert@xxx.poznan.pl	milostan@host.xxx.poznan.pl
Maciej.Milostan@xxx.poznan.pl	milostan@host.xxx.poznan.pl
Jan.Kowalski@xxx.poznan.pl	kowalski@host.xxx.poznan.pl
Jan.Kowalski@host.xxx.poznan.pl	kowalski@host.xxx.poznan.pl
zenek@xxx.poznan.pl	zenek@host.xxx.poznan.pl

- postmap /etc/postfix/login_maps

Przykładowa sesja (fałszerstwo): użytkownik=kowalski,hasło=jan

```
>printf '\0kowalski\0jan'|mimencode
AGtvd2Fsc2tpAGphbg==
>telnet host.xxx.poznan.pl 25
. . .
220 host.xxx.poznan.pl ESMTP Postfix
EHLO client.example.com
250-host.xxx.poznan.pl
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH DIGEST-MD5 PLAIN CRAM-MD5
250 8BITMIME
AUTH PLAIN AGtvd2Fsc2tpAGphbg==
235 Authentication successful
MAIL FROM:Maciej.Milostan@xxx.poznan.pl
250 2.1.0 Ok
RCPT TO:zenek@xxx.poznan.pl
553 5.7.1 <Maciej.Milostan@xxx.poznan.pl>: Sender address rejected: not
    owned by user kowalski@host.xxx.poznan.pl
```

Przykładowa sesja (prawidłowa):

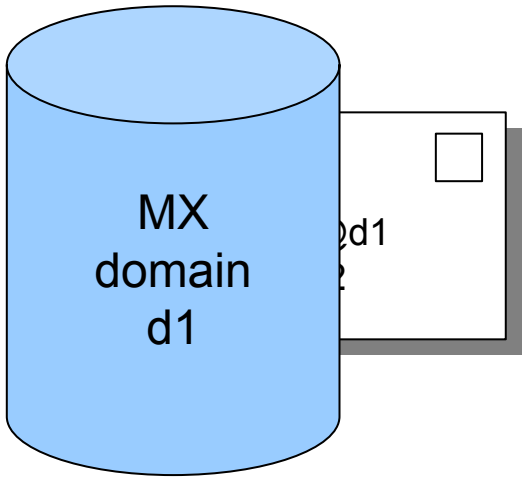
```
>printf '\0kowalski\0jan'|mimencode
AGtvd2Fsc2tpAGphbg==
>telnet host.xxx.poznan.pl 25
220 host.xxx.poznan.pl ESMTP Postfix
EHLO client.example.com
250-host.xxx.poznan.pl
…
250-AUTH DIGEST-MD5 PLAIN CRAM-MD5
250 8BITMIME
AUTH PLAIN AGtvd2Fsc2tpAGphbg==
235 Authentication successful
MAIL FROM:Jan.Kowalski@xxx.poznan.pl
250 2.1.0 Ok
RCPT TO:zenek@xxx.poznan.pl
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
TO:mm@cs.put.poznan.pl
Subject: Test
Test
.
250 2.0.0 Ok: queued as 8FFE65F
```

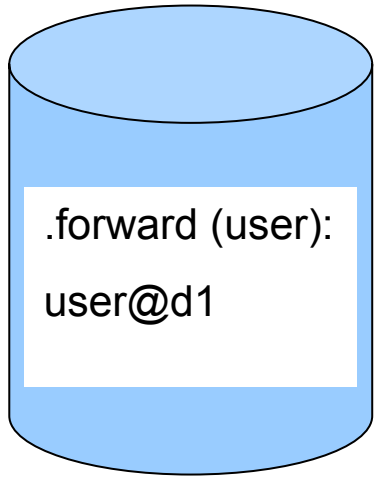
Mapy kont i użytkowników – przykładowa sesja (bez autoryzacji)

```
>telnet host.xxx.poznan.pl 25
. . .
220 host.xxx.poznan.pl ESMTP Postfix
EHLO client.example.com
250-host.xxx.poznan.pl
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH DIGEST-MD5 PLAIN CRAM-MD5
250 8BITMIME
MAIL FROM:Maciej.Milostan@xxx.poznan.pl
250 2.1.0 Ok
RCPT TO:zenek@xxx.poznan.pl
553 5.7.1 <Maciej.Milostan@xxx.poznan.pl>: Sender address rejected:
    not logged in
```

Wada tego rozwiązania

- Potencjalny problem z forwardami





REJECT

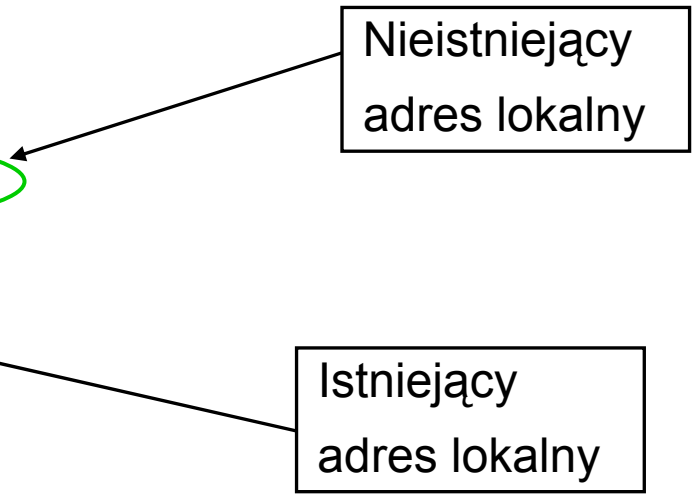
(user@d1 nie zautoryzował się)

Problemy

- Pocztę na zewnątrz mogą wysyłać tylko użytkownicy sieci/hostów wyspecyfikowanych w *mynetworks*
- Spamerzy mogą podszywać się pod wewnętrznych użytkowników
- Wewnętrzni (zautoryzowani) użytkownicy mogą fałszować adresy nadawców (niekoniecznie lokalnych) i wysyłać do dowolnych odbiorców
- Spamerzy mogą podszywać się pod nieistniejących użytkowników

Przykładowa sesja bez check_sender_access

220 host.xxx.poznan.pl ESMTP Postfix
helo mm
250 host.xxx.poznan.pl
mail from:zzz@xxx.poznan.pl
250 2.1.0 Ok
rcpt to:mm@xxx.poznan.pl
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
To:mm@xxx.poznan.pl
.
250 2.0.0 Ok: queued as 55ECC5B



Przykładowa sesja bez check_sender_access

220 host.xxx.poznan.pl ESMTP Postfix

helo mm

250 host.xxx.poznan.pl

mail from:zzz@xxx.poznan.pl

250 2.1.0 Ok

rcpt to:milos@man.poznan.pl

554 5.7.1 <milos@man.poznan.pl>: Relay access denied

Nieistniejący adres lokalny

Istniejący adres zewnętrzny

Ograniczanie możliwości wysyłania

- Jak uniemożliwić wysyłanie z nieistniejących lokalnych adresów?

check_sender_access *type:table*

smtpd_recipient_restrictions =
permit_mynetworks,
reject_sender_login_mismatch,
check_sender_access hash:/etc/postfix/access,
reject_unauth_destination

smtpd_recipient_restrictions = …
check_sender_access hash:/etc/postfix/access

milostan@host.xxx.poznan.pl	**OK**
mm@xxx.poznan.pl	**OK**
mm@cs.xxx.poznan.pl	**OK**
cert@xxx.poznan.pl	**OK**
Maciej.Milostan@xxx.poznan.pl	**OK**
Jan.Kowalski@xxx.poznan.pl	**OK**
Jan.Kowalski@host.xxx.poznan.pl	**OK**
zenek@xxx.poznan.pl	**OK**
host.xxx.poznan.pl	**REJECT**
xxx.poznan.pl	**REJECT**

- parent_domain_matches_subdomains

>postconf -d |grep parent_domain_matches_subdomains

parent_domain_matches_subdomains =
debug_peer_list,fast_flush_domains,mynetworks,permit_mx_backup_networks,qmqpd_authorized_clients,relay_domains,
smtpd_access_maps

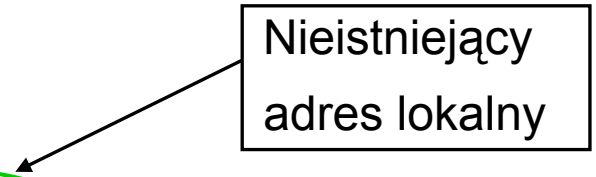
Przykładowa sesja

220 host.xxx.poznan.pl ESMTP Postfix

helo mm

250 host.xxx.poznan.pl

mail from:zzz@xxx.poznan.pl



250 2.1.0 Ok

rcpt to:mm@xxx.poznan.pl

554 5.7.1 <zzz@xxx.poznan.pl>: Sender address rejected: Access denied

quit

221 2.0.0 Bye

Czarne listy

- Dodajemy na końcu smtpd_recipient_restrictions
  reject_rhsbl_client blackhole.securitysage.com,
  reject_rhsbl_sender blackhole.securitysage.com,
  reject_rbl_client relays.ordb.org,
  reject_rbl_client blackholes.easynet.nl,
  reject_rbl_client cbl.abuseat.org,
  reject_rbl_client proxies.blackholes.wirehub.net,
  reject_rbl_client bl.spamcop.net,
  reject_rbl_client sbl.spamhaus.org,
  reject_rbl_client opm.blitzed.org,
  reject_rbl_client dnsbl.njabl.org,
  reject_rbl_client list.dsbl.org,
  reject_rbl_client multihop.dsbl.org,

Czarne listy

- Zewnętrzna kontrola
- Czasami dodawane są całe klasy adresowe
- Problem z usuwaniem wpisanych hostów
- Adresy popularnych dostawców znajdują się często na wielu listach. Dla przykładu:
  - Adresy TP S.A. / Orange
  - Adresy Polskiej Telefonii Cyfrowej
  - Adresy Polkomtela

Analiza nagłówków i zawartości

- **header_checks(5)**
- **header_checks = regexp:/etc/postfix/maps/header_checks**

  /^HEADER: .*content_to_act_on/ ACTION
  /^Subject: .*Make Money Fast!/ REJECT
- **mime_header_checks = regexp:/etc/postfix/maps/mime_header_checks**

  /name=[^>]*\.(bat|com|exe|dll)/ REJECT
- **body_checks = regexp:/etc/postfix/maps/body_checks**

  /content_to_act_on/ ACTION

Inne restrykcje

- reject_unauth_destination,
  reject_invalid_hostname,
  reject_unauth_pipelining,
  reject_non_fqdn_sender,
  reject_unknown_sender_domain,
  reject_non_fqdn_recipient,
  reject_unknown_recipient_domain,

- check_client_access
  hash:/etc/postfix/maps/access_client,
  check_helo_access
  hash:/etc/postfix/maps/access_helo,
  check_sender_access
  hash:/etc/postfix/maps/access_sender,
  check_recipient_access
  hash:/etc/postfix/maps/access_recipient,

Przepisywanie adresów (canonical rewriting)

- Jak wymusić standaryzację adresów?

canonical_maps = hash:/etc/postfix/canonical

sender_canonical_maps =
hash:/etc/postfix/sender_canonical
recipient_canonical_maps =
hash:/etc/postfix/recipient_canonical

```
mm                  Maciej.Milostan@xxx.poznan.pl
Kowalski Jan.Kowalski@xxx.poznan.pl
...
```

Zewnętrzne filtry (before queue)

Internet ->
Postfix SMTP server ->
Before queue filter ->
Postfix SMTP server ->
Postfix cleanup server ->
smtp
Postfix queue -< local
virtual

Wady i zalety filtrów przedkolejkowych

- Poczta jest odrzucana, zanim skończy się sesja z klientem
- Wydłużenie czasu odpowiedzi serwera przy połączeniach SMTP wynikające z konieczności filtrowania „on-line”
- Duże wymagania pamięciowe niektórych filtrów wymuszają ograniczenie liczby ich instancji, w efekcie jeszcze bardziej wydłużając czas obsługi

Konfiguracja filtrów przedkolejkowych

- Postfix komunikuje się z filtrami poprzez protokół SMTP

Internet ->

Postfix SMTP server on port 25 ->

filter on localhost port 10025 ->

Postfix SMTP server on localhost port 10026 ->

Postfix cleanup server ->

Postfix incoming queue

Konfiguracja: /etc/postfix/master.cf

```
# ==========================================================
# service type  private unpriv  chroot  wakeup  maxproc command
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================

                                    rver. Receive mail from the network and
                                    ilter on localhost port 10025.
#
smtp      inet  n       -       n       -       20      smtpd
    -o smtpd_proxy_filter=127.0.0.1:10025
    -o smtpd_client_connection_count_limit=10
#
# After-filter SMTP server. Receive mail from the content filter
# on localhost port 10026.
#
127.0.0.1:10026 inet n  -       n       -       -       smtpd
    -o smtpd_authorized_xforward_hosts=127.0.0.0/8
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=
    -o mynetworks=127.0.0.0/8
    -o receive_override_options=no_unknown_recipient_checks
```

Adres i port filtra

Ograniczenie liczby sesji z domyślnych 100 do 20

Jeden klient może zużyć max. 10 procesów filtra

Adres i port, na którym Postfix odbiera filtrowaną pocztę

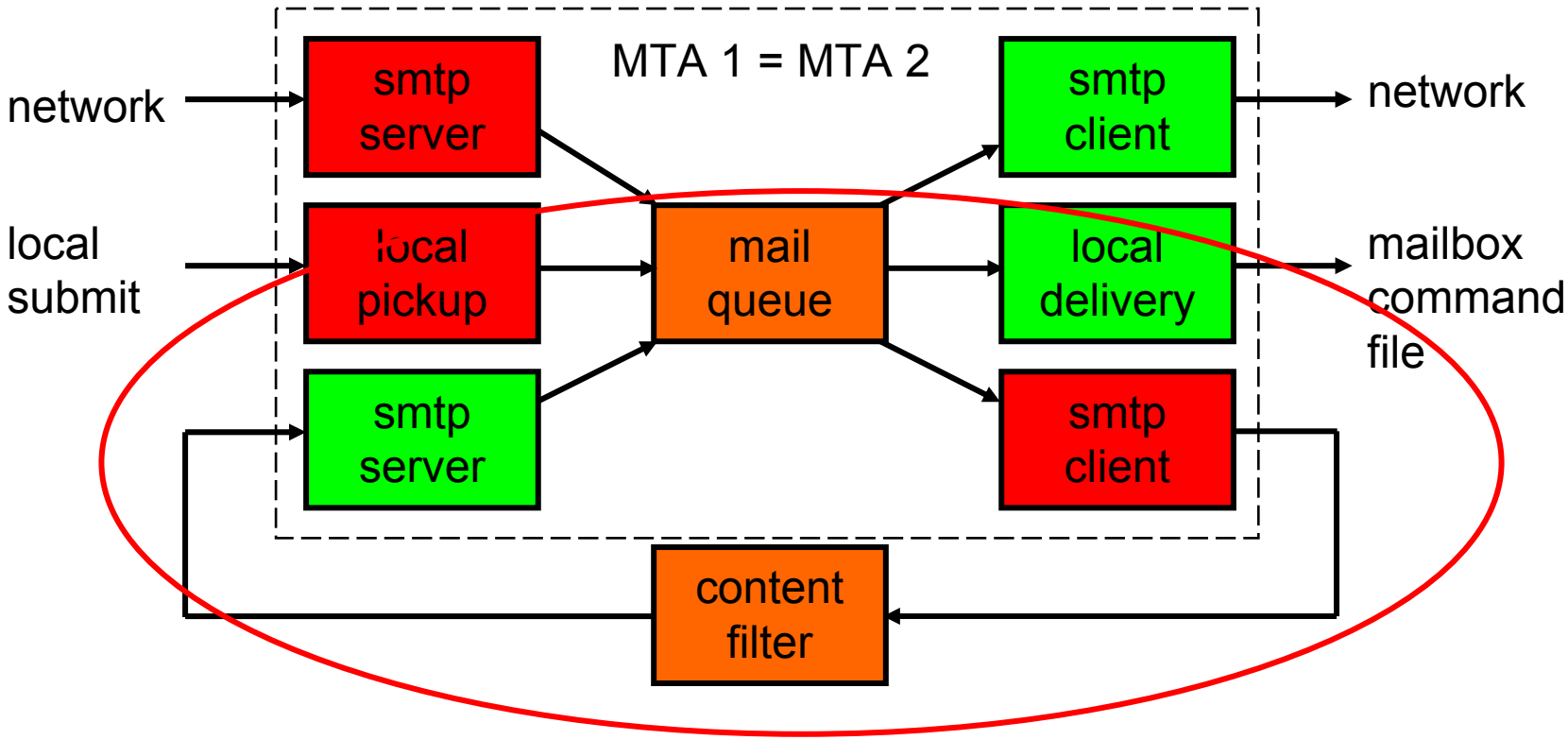
Umożliwia logowanie oryginalnych nagłówków

Uwaga: nie używać spacji wokół znaków "=" lub ",".

Inne parametry konfiguracyjne

- smtpd_proxy_timeout (domyślnie: 100s): limit czasu połączenia z przedkolejkowymi filtrami zawartości (ang. before-queue content filter), włącznie z czasem przesyłania komend i danych. Wszystkie błędy (ang. proxy errors) są logowane w pliku logu poczty (ang. maillog). Ze względów ochrony prywatności zdalni klienci SMTP w przypadku przekroczenia tego limitu otrzymują błąd „451 Error: queue file write error” (Błąd zapisu do kolejki). Nie jest wskazane ujawnianie szczegółów wewnętrznej konfiguracji nieznanym osobom z zewnątrz.
- smtpd_proxy_ehlo (domyślnie: $myhostname)

Zewnętrzne filtry (after queue)



Zewnętrzne filtry (after queue): przekazywanie poczty do filtra

- /etc/postfix/main.cf:

```
content_filter = scan:localhost:10025
receive_override_options = no_address_mappings
```

- /etc/postfix/master.cf:

```
# ==========================================================
# service type  private unpriv  chroot  wakeup  maxproc command
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================
  scan      unix    -       -       n       -       10      smtp
    -o smtp_send_xforward_command=yes
    -o disable_mime_output_conversion=yes
    -o smtp_generic_maps=
```

Zewnętrzne filtry: uruchamianie filtra spawn vs. standalone

/etc/postfix/master.cf:

```
# ==========================================================================
# service       type  private unpriv  chroot  wakeup  maxproc command
#                     (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
   localhost:10025 inet  n       n       n       -       10      spawn
      user=filter argv=/path/to/filter localhost 10026
```

- "filter" – dedykowany użytkownik
- command_time_limit – ogranicza czas działania filtra
- Filtry nasłuchujące cały czas należy uruchamiać bez użycia usługi spawn

Odbieranie poczty z filtra

```
#/etc/postfix/master.cf
# ==========================================================================
# service       type  private unpriv  chroot  wakeup  maxproc command
#                     (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
localhost:10026 inet  n       -       n       -       -       smtpd
-o content_filter=
-o receive_override_options=no_unknown_recipient_checks,no_header_body_checks,no_milters
 -o smtpd_helo_restrictions=
 -o smtpd_client_restrictions=
 -o smtpd_sender_restrictions=
 -o smtpd_recipient_restrictions=permit_mynetworks,reject
 -o mynetworks=127.0.0.0/8
 -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Wyłączenie filtrowania poczty wracającej z filtra, inne ustawienie może spowodować zapętlenie

Nie chcemy sprawdzać tego, co już zostało sprawdzone

Nie wyspecyfikowano: no_address_mappings, gdyż mapowanie nie było wykonane wcześniej w wyniku użycia parametru receive_override_options w /etc/postfix/master.cf

Kwestie wydajności filtrów (after queue)

- Za mała liczba procesów filtrów powoduje gromadzenie poczty w kolejce (active queue)
- Za duża liczba procesów powoduje nadmierną konsumpcję zasobów i opóźnianie dostarczania poczty z powodu braku odpowiedzi z filtra
- Dopasowywanie wartości parametrów odbywa się metodą prób i błędów
- Analiza wydajności jest „upośledzona” ze względu na współdzielenie kolejki przez wiadomości przefiltrowane i nieprzefiltrowane

Analiza wydajności i usuwanie wiadomości z kolejki

- Narzędzie qshape(1) (zobacz też: QSHAPE_README)

> qshape deferred

> qshape incoming active deferred

> qshape hold

> qshape maildrop

- mailq
- postsuper –d <message id>

> mailq|grep MAILER-DAEMON|awk "{print substr(\$1,0,7)}"|postsuper -d –

> postsuper –d ALL (usuwa wszystkie wiadomości z kolejki, po ALL można podać nazwę kolejki)

- Wymuszanie dostarczania: postfix flush

Zewnętrzne filtry – amavisd-new

- Amavisd-new
  - Interfejs pomiędzy MTA filtrami
  - Ułatwia integrację programów antywirusowych
  - Napisany w PERLu, ale charakteryzujący się dość dobrą wydajnością
  - Standardowo dystrybuowany razem z modułem do SpamAssassina

Amavisd-new a Postfix

- /etc/main.cf:

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

- /etc/master.cf:

```
smtp-amavis     unix    -       -       y       -       2       smtp
  -o smtp_data_done_timeout=1200
  -o disable_dns_lookups=no
127.0.0.1:10023 inet    n       -       y       -       -       smtpd
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o strict_rfc821_envelopes=yes
```

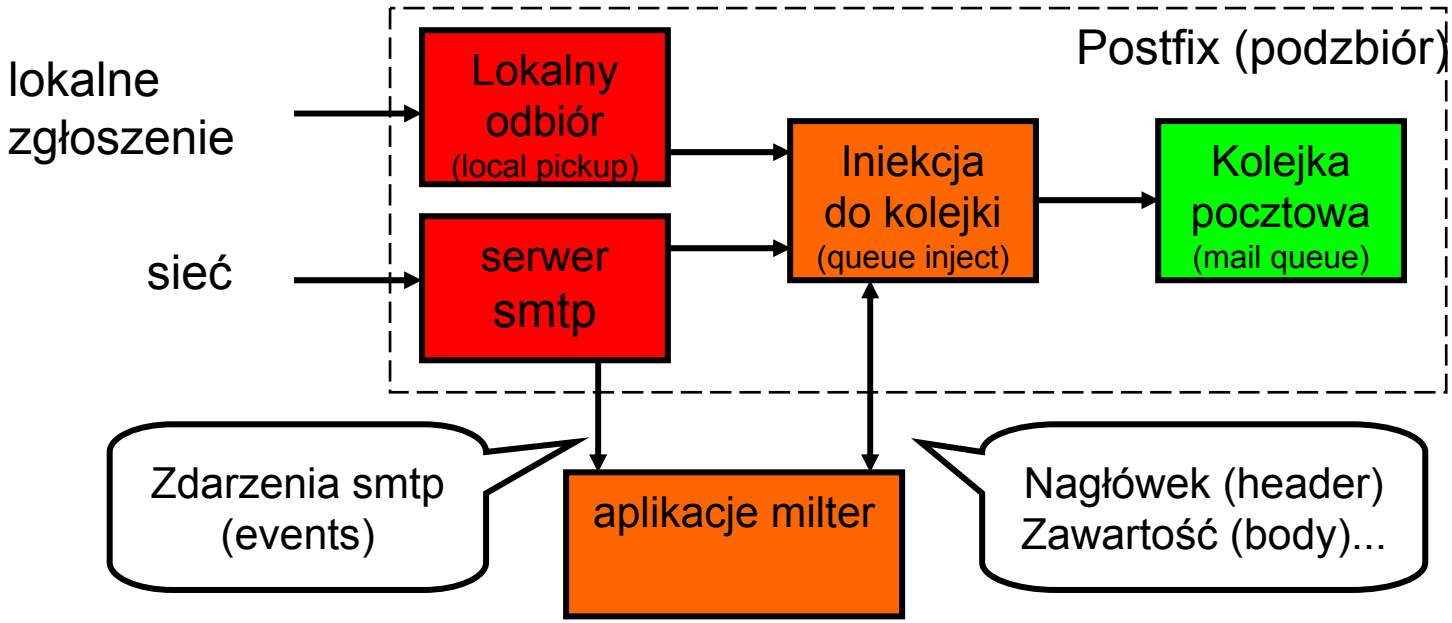
- /etc/amavisd.conf:

```
$forward_method = 'smtp:[127.0.0.1]:10023';
```

Dodatkowy filtr antwyirusowy lub antyspamowy

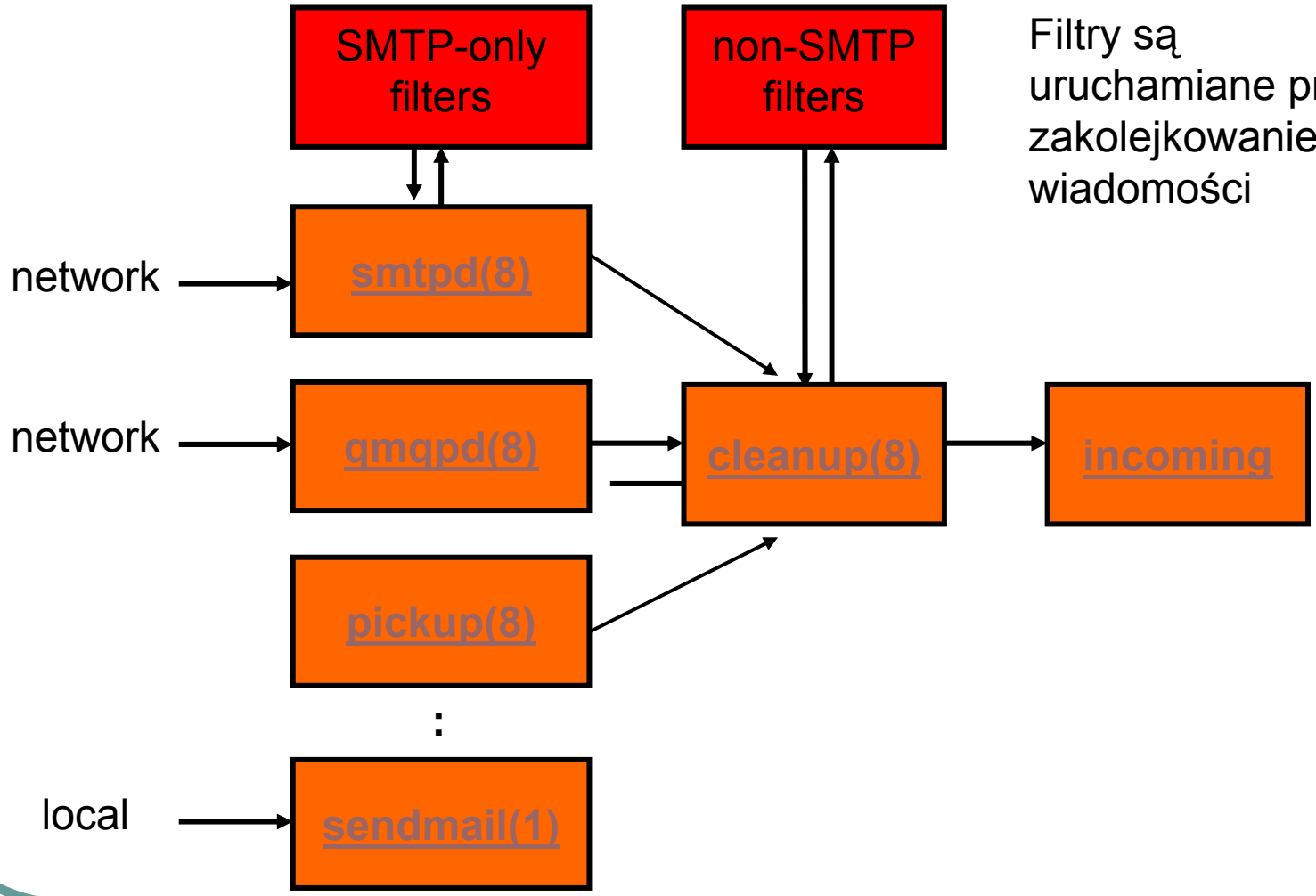
- Amavis posiada wsparcie dla wielu popularnych produktów antywirusowych
- Jeżeli filtr działa w oparciu o SMTP, to można go dodać w sposób analogiczny do przedstawionego dla amavisa. W tym celu należy dodać kolejne demony SMTP odbierające pocztę z kolejnych filtrów. Dla tych demonów parametr content-filter wskazuje na następny filtr. Kolejne filtry przekazują pocztę do kolejnych demonów SMTP.
- Dla ostatniego demona SMTP opcja
  -o content-filter= musi zostać ustawiona na wartość pustą

Filtry Milter a Postfix



- Czerwony = brudny, zielony = czysty

Milter a Postfix



Milter a Postfix

- Filtry są pisane w językach C, JAVA i Perl
- W przypadku C potrzebna jest biblioteka implementująca protokół Sendmail 8 Milter
- Postfix nie dostarcza takiej biblioteki - trzeba skorzystać z biblioteki dostarczanej przez Sendmaila (libmilter)
- Biblioteka jest zwykle dostępna w pakiecie sendmail-devel, ew. można pobrać źródła i skompilować samemu

Instalacja przykładowego filtra

- Kompilacja dkim-milter (analogcznie sid-milter)

$ **gzcat dkim-milter-*x.y.z*.tar.gz | tar xf**

$ **cd dkim-milter-*x.y.z***

$ **make**

[...*dużo komunikatów*...]

- Uruchamianie

 # /some/where/dkim-filter -u *userid* -p inet:*portnumber*@localhost ...*other options*...

Wartość *userid* nieużywana przez inne aplikacje (nie "postfix", nie "www", itd.)

Konfiguracja Postfix-a

- /etc/postfix/main.cf:

Milters for mail that arrives via the smtpd(8) server.

smtpd_milters = **inet:**localhost:*portnumber* ...*other filters*...

unix:*pathname*

inet:*host*:*port*

Milters for non-SMTP mail.

non_smtpd_milters = inet:localhost:*portnumber* ...*other filters*...

Obsługa błędów, protokół etc.

- accept, reject, tempfail.
  milter_default_action = tempfail
- milter_protocol = 2
- UWAGA: Implementacja Miltera w Postfix-ie jest nie pełna (niektóre opcje nie działają). Zobacz: limitations.
  Dla przykładu Postfix wspiera tylko wersję 2.4 protokołu Miltera.

SPF a Postfix

- Sender Policy Framework
- Próba kontroli fałszowanych e-maili
- Daje możliwość specyfikowania legitymowanych źródeł poczty
- Implementowany jako rekordy DNS-owe
- Protokół opracowany przez grupę ochotników
- Rozwijany od 2003 roku

Jak sprawdzać rekordy SPF

C:\>**nslookup**

Serwer domyślny: dns.server.domain

Address: 150.254.x.x

>**set type=TXT**

>**wp.pl**

wp.pl text =
  "v=spf1 ip4:212.77.96.0/19 mx -all"

SPF a Postfix

- Mechanizmy SPF
  - all | ip4 | ip6 | a | mx | ptr | exists | include
- Modyfikatory (modifiers)
  - redirect | exp
- Kwalifikatory
  - "+"Pass
  - "-"Fail
  - "~"SoftFail
  - "?"Neutral

SPF a Postfix

- Kolejność ewaluacji mechanizmów (od lewej do prawej)
  - "v=spf1 -all"
  - "v=spf1 a -all"
  - "v=spf1 a mx -all"
  - "v=spf1 +a +mx -all"

Ewaluacja rekordów SPF

Wynik	*Wyjaśnienie*	*Zamierzony efekt (Intended action)*
Przepuść (Pass)	Rekord SPF określa adres hosta uprawnionego do wysyłania.	**akceptacja (accept)**
Odrzuć (Fail)	Rekord SPF określa adres hosta jako nieuprawniony do wysyłania	**odrzucenie (reject)**
„Miękkie" odrzucenie (SoftFail)	Rekord SPF określa adres hosta jako nieuprawniony do wysyłania, ale jest to stan przejściowy	**akceptacja z oznaczaniem (accept but mark)**
Neutralny (Neutral)	Rekord SPF określa ściśle, że nic nie można powiedzieć na temat ważności	**akceptacja (accept)**
Żaden (None)	The domain does not have an SPF record or the SPF record does not evaluate to a result	**akceptacja (accept)**
Błąd (PermError)	Wystąpił permanentny błąd (np. źle sformatowany rekord)	**Nieokreślona (unspecified)**
Błąd przejściowy (TempError)	Nastąpił przejściowy błąd	**Akceptacja albo odrzucenie (accept or reject)**

Zaawansowany przykład

> **gmail.com**

gmail.com text =

"v=spf1 redirect=_spf.google.com”

>**_spf.google.com**

_spf.google.com text =

"v=spf1 ip4:216.239.32.0/19
ip4:64.233.160.0/19 ip4:66.249.80.0/20
ip4:72.14.192.0/18 ip4:209.85.128.0/17
ip4:66.102.0.0/20 ip4:74.125.0.0/16 ?all"

SPF a Postfix

- **Milter**
- **postfix-policyd-spf-perl**

/etc/postfix/master.cf

policy unix - n n - - spawn user=nobody
argv=/usr/bin/perl /usr/lib/postfix/policyd-spf-perl

/etc/postfix/main.cf

smtpd_recipient_restrictions =[…]
reject_unauth_destination,check_policy_service
unix:private/policy

Uwaga: ta opcja musi wystąpić przed check_policy_service, w innym przypadku host może stać się open relayem

Podsumowanie

- Postfix jako MTA o bezpiecznej architekturze
- Duże możliwości konfiguracyjne
- Liczne filtry podstawowe
- Możliwość wprowadzania własnych rozszerzeń na różnych etapach przetwarzania
- Obszerna dokumentacja i liczne przykłady dostępne w sieci Internet

Kontakty i pytania

Kontakt:

Maciej Miłostan

milos@man.poznan.pl

Zespół bezpieczeństwa PCSS

security@man.poznan.pl

WWW:

http://security.psnc.pl

http://www.man.poznan.pl

DZIĘKUJĘ ZA UWAGĘ

Przerwa

- Wszystkich obecnych zapraszam na krótką przerwę
- Dalszy ciąg nastąpi za 10 minut