Poczta

Autorstwa Michała Wendta i Macieja Aszyka

Co to jest?

Mail lub jak będziemy go później nazywać poczta elektroniczna to usługa internetowa, umożliwiająca transport wiadomości tekstowych oraz multimedialnych (tzw. listów elektronicznych).

Do czego służy?

W dzisiejszych czasach pocztę elektroniczną możemy dostarczać za pomocą architektury klient-serwer. Wiadomość elektroniczna jest tworzona przy pomocy programu klienta, wysyłana do serwera, dostarczana przez serwer klienta do serwera odbiorcy, by na końcu zostać przekazana do konkretnego odbiorcy.

Jaką ma historię?

Wiadomości wysyłane drogą sieciową swoje początki mają ściśle powiązane z latami sześćdziesiątymi ubiegłego wieku gdy zaczęto używać "time-sharingu" polegającego na udostępnianiu wielu użytkownikom wspólnych zasobów w tym samym czasie.

W latach siedemdziesiątych udało się umożliwić wielu użytkownikom jednoczesną interakcję z jednym komputerem.

Taki podział czasu zdecydowanie obniżył koszty zapewnienia możliwości obliczeniowych oraz umożliwił osobom prywatnym jak i organizacjom dostęp do korzystania z komputera bez posiadania fizycznej postaci komputera oraz promował interaktywne korzystanie z komputerów, a przede wszystkim zapewnił rozwój nowych aplikacji interaktywnych.

Początkowo wielu programistów, którzy w danych czasach mieli utrudnioną komunikację starało się stworzyć swoje własne, najczęściej niekompatybilne ze sobą wzajemnie aplikacje pocztowe. Takich aplikacji używano na mniejszych obszarach jak np. uczelnia lub pojedyncza korporacja.

Wraz z rozwojem technologii wiele z tych aplikacji dołączało stopniowo do skomplikowanej sieci bramek i systemów routingu. To właśnie w tym momencie wiele uniwersytetów w USA stawało się częścią tzw. ARPANET, którego celem było przenoszenie oprogramowania między swoimi systemami. Dzięki tej przenośności udało się zwiększyć wpływ protokołu Simple Mail Transfer Protocol (SMTP).

W okresie późnych lat 80. jak i na początku lat 90. dość powszechne było stwierdzenie że pocztę zdominuje zastrzeżony system komercyjny, lub system poczty elektronicznej X.400, który był częścią profilu rządowych połączeń międzysystemowych (GOSIP). Na szczęście po wygaśnięciu ostatecznych ograniczeń obejmujących przenoszenie ruchu komercyjnego przez Internet w 1995 r. wiele różnych czynników

sprawiło, że obecny pakiet protokołów e-mail tj. SMTP, POP3 oraz IMAP stał się standardem.

Jaki problem rozwiązuje?

Przed rewolucją cyfrową dostępnymi środkami komunikacji asynchronicznej były listy, telegramy oraz fax.Niestety taki sposób komunikacji ma swoje minusy: można je wysyłać tylko i wyłącznie w odpowiednich punktach (oraz posiadać odpowiednie urządzenia w przypadku faksu), cenę[1] (która wciąż wynosi od kilku złotych) oraz czas przesyłu, który nawet w dzisiejszych czasach trwa od prawie dnia a nawet do trzech dni[2] (patrząc na czas narodowego przewoźnika w Polsce) i to w przypadku przesyłek wewnątrzkrajowych. Czas realizacji takich wysyłek na znaczne odległości może wynosić nawet 5 dni roboczych. [3] Odpowiedzią na długą i drogą usługę transportu korespondencji była poczta elektroniczna tzw. Email. Jest to sposób implementacji klasycznego listu do ery cyfryzacji (pozwala przesłać informacje asynchronicznie), którego czas dostawy w praktycznie każdy zakątek świata wynosi mniej niż minutę[3] a cena nie jest ważnym aspektem - (oprócz kosztu dostępu do internetu w danym miejscu oraz urządzenia odbiorczego) obecnie większość większych firm informatycznych usługę poczty oferuje za darmo [4].

Dlaczego warto używać akurat tego rozwiązania?

Obecnie istnieje wiele komunikatorów asynchronicznych (WhatsApp, Messenger, Viber etc.), jednakże wymagają one z korzystania z własnych serwerów oraz aplikacji co jest niekorzystne dla użytkowników, którzy chcieliby przechowywać wszystko na własnych zasobach. Dodatkowo mają ograniczony sposób kategoryzacji wiadomości.

W przeciwieństwie do nich, poczta elektroniczna, która pozwala na kategoryzację oraz możliwość stworzenia własnego serwera obsługującego może zostać uznana za najpopularniejszą usługę, dzięki posiadaniu 3,94mld użytkowników w 2019, a do 2024 ma się rozwinąć do 4,48mld[5] - co czyni ją najbardziej popularną usługą komunikacji obecnie.

Klasyfikacja programów pocztowych.

Mimo, iż dla końcowego użytkownika może się wydawać, że korzysta tylko z jednej aplikacji obsługującej pocztę tak naprawdę korzystu z kilku typów aplikacji, które można odpowiednio skategoryzować. Poniżej postanowiliśmy rozważyć trzy główne kategorie.

Mail Transport Agent (MTA)

Czyli agent transportu poczty. Jak nazwa wskazuje - odpowiada on za transfer przesyłanych maili pomiędzy maszynami wykorzystując protokół **SMTP**. Warto też mieć na uwadzę iż proces działania programów typu MTA może się różnić przez stworzenie odpowiednich konfiguracji np. dla prewencji odbierania wiadomości typu SPAM.

Przykładami takich aplikacji są **postfix** oraz **sendmail**.

Porównanie najpopularniejszy MTA

Postfix

- Został zaprojektowany jako w pełni kompatybilnym z Sendmail.
- Jego głównymi zaletami są szybkość, bezpieczeństwo, oraz łatwość konfiguracji.
- W celu poprawy bezpieczeństwa wykorzystano w nim konstrukcję modułową, zapewniającą małym procesom z brakiem uprawnień pewność wykonania poprzez wywoływanie ich przez głównego demona.
- Postfix zapewnia łatwą konfigurację początkową. Wystarczy jedynie kilku drobnych zmian w pliku konfiguracyjnym aby umożliwić akceptowanie połączeń sieciowych z innych hostów niż lokalny komputer.
- W przypadku użytkowników o większych wymaganiach Postfix zapewnia także wiele opcji konfiguracyjnych oraz dodatki dostarczane przez inne firmy czyniąc go w pełni funkcjonalnym i wszechstronnym MTA.
- LDAP jest dostępny w Postfixie i zapewnia źródła różnych tabel wyszukiwania. Dzięki temu LDAP może przechowywać informacji na temat użytkownika hierarchicznie. Ponadto Postfix otrzymuje zapytania LDAP tylko i wyłącznie w razie ich zapotrzebowania. Administratorzy systemu z łatwością mogą przechowywać wszystkie te informacje nie zapisując ich lokalnie.

Sendmail

- Głównym celem jest przesyłanie zabezpieczonych wiadomości, zazwyczaj przy użyciu protokołu SMTP.
- Aktualnie uważa się go za przestarzałego i użytkownicy często zachęcani są do używania innych serwerów takich jak Postfix.
- Najpopularniejszą konfiguracją Sendmaila jest ustawienie jednej maszyny w postaci bramy pocztowej dla wszystkich komputerów w sieci. Jest to szczególnie przydatne dla firm używających tego samego adresu zwrotnego dla całej poczty wychodzącej.
- Trochę inaczej niż w Postfixie, wszystkie poziomy routingu poczty z Sendmaila oraz jego oddzielne pliki konfiguracyjne są wyodrębniane do potężnego klastra LDAP. Z takiego klastra może korzystać wiele różnych *aplikacji.*
- *Tak jak w przypadku Postfix-a, Sendmail także zapewnia możliwość korzystania z protokołu LDAP. Jest on zdecydowanie oddzielony od Sendmaila, ponieważ tutaj także LDAP wysyła do niego tylko i wyłącznie wyniki zapytań we wstępnie zaadresowanych wiadomościach elektronicznych.*

Fetchmail

- Zaimplementowano w nim wiele funkcjonalności pomagających w szybszej obsłudze jak na przykład oddzielenie procesu pobierania wiadomości z serwera zdalnego od procesu czytania i organizowania wiadomości.
- Może przekazywać wiadomości elektroniczne na serwer SMTP. Używa dowolnej liczby protokołów do szybkiego łączenia oraz pobierania wszystkich wiadomości do pliku pocztowego .
- Zaprojektowano go dla użytkowników korzystających z dial-up.
- Ciekawym rozwiązanie, którego nie widzieliśmy w poprzednich aplikacjach jest umożliwienie używania Fetchmail bez pliku konfiguracyjnego. W takim przypadku użytkownik jest zmuszony do użycia opcji wiersza poleceń, co może nie być najwygodniejsze dla przeciętnego użytkownika, ale nadal pozostaje możliwością. Przydaje się to raczej w celu jednorazowego użycia polecenia z innymi ustawieniami niż zazwyczaj.

Mail Delivery Agent (MDA)

Najprościej rzecz mówiąc - jest to program, który rozdziela pocztę przychodzącą na serwer do odpowiednich użytkowników (kont) na maszynie.

Warto też dodać, że niektóre programy typu MTA (np postfix, sendmail) realizują tę usługę dodatkowo.

Przykładem takiej aplikacji jest **procmail**.

Mail User Agent (MUA)

Jest to po prostu klient pocztowy służący do obsługi poczty przez klienta pocztowego.

Przykłady to **mailix**, **Mozilla Thunderbird**.

Protokół SMTP.

Opis protokołu.

Czyli Simple Mail Transfer Protocol - jest to protokół służący do przesyłania wiadomości elektronicznych. W momencie wysyłania maila program przekazuje go do serwera obsługującego, który obsługuje proces komunikacji (przekazania) danych pomiędzy serwerem wychodzącym (nadawcą) a serwerem odbierającym (adresata)[6]

Opis działania protokołu SMTP

Rozpoczynamy połączenie z serwerem (polecenie HELO):

220 serwer ESMTP Exim 4.43 Thu, 12 Nov 2020 12:00:55 +0100

HELO serwer.email.com

Serwer odpowiada wiadomością powitalną:

250 uzytkownik.internet.com Hello uzytkownik at uzytkownik.internet.com [1.1.1.1]

Podajemy adres nadawcy (polecenie MAIL FROM):

MAIL FROM: <nadawca@example.org>

Serwer odpowiada wiadomością potwierdzającą

250 OK

Podajemy adres odbiorcy (polecenie RCPT TO):

RCPT TO: <odbiorca@example.org>

Serwer odpowiada wiadomością potwierdzającą:

250 Accepted

Wpisujemy treść naszej wiadomości (polecenie DATA):

DATA

354 Enter message, ending with "." on a line by itself

Date: 12 Nov 20 12:12:12

From: nadawca@example.org

To: odbiorca@example.org
Subject: temat naszej wiadomości
treść naszej przykładowej wiadomości
.

Serwer odpowiada wiadomością potwierdzającą:

250 Ok: queued as 12345

Kończymy sesję (polecenie QUIT):

QUIT

Serwer odpowiada wiadomością pożegnalną:

221 Bye
221 serwer.email.com closing connection

Porównanie najpopularniejszych serwerów.[7]

Nazwa	Platforma	Protokoły	SSL	Licencja
Postfix	Linux, Unix,MacOs	SMTP,Dovecot, UW IMAP, SMTP	Tak	IBM Public License
SendMail	Linux,Unix,Mac Os	SMTP,Dovecot, UW IMAP, SMTP	Tak	SendmailLicense
Microsoft Exchange Server	Windows Server	POP3, IMAP, SMTP	Tak	Własnościowa
Qmail	Linux, Unix, MacOs	SMTP,Dovecot, UW IMAP, SMTP, POP3	Tak	Public Domain
Exim	Linux, Windows (cygwin), MacOs	SMTP,Dovecot, UW IMAP, SMTP	Tak	GPLv2+

Protokoły dostępu do poczty

Są to protokoły wykorzystywane do odbierania poczty przez klientów z serwerów. Dwa główne, najczęściej wykorzystywane z nich to **POP** i **IMAP**. Warto dodać, że domyślnym serwerem dla tych protokołów w systemie Fedora jest **Dovecot**.

POP (POP3) - Post Office Protocol

Jest to protokół zgodny z standardem MIME, który pozwala na odbieranie załączników. Jego główne cechy to:

- większość klientów wykorzystujących go usuwa z serwera po pobraniu (choć można zmienić to w konfiguracji)

- wymaga pobrania całych wiadomości (brak możliwości pominięcia niczego, uciążliwe dla słabego połączenia internetowego)
- brak możliwości kategoryzacji wiadomości
- ~~wymaga stałego połączenia z internetem~~
- najlepiej sprawdza się, gdy użytkownik korzysta tylko z jednej maszyny lub dostęp do serwera jest ograniczony
- pozwala na wykorzystanie bezpiecznego połączenia (SSL)

Obecnie wykorzystywaną wersją **POP** jest **POP3**.

IMAP - Internet Message Access Protocol

Zaprojektowany jako następca POP. Jego główne cechy to

- możliwość organizacji emaili na serwerze (tworzenia folderów, zmienianie ich nazw oraz ich usuwania bez pobierania ich)
- pobiera tylko pliki nagłówkowe do wyświetlenia (można pobrać treść emaili, które nas interesują)
- klienci IMAP zazwyczaj zapisują emaile wcześniej odczytane (bez konieczności powtarzania pobierania ich z serwera)
- idealnie sprawdza się w warunkach gdy klient korzysta z wielu maszyn na raz
- brak konieczności pobierania treści do każdej wiadomości (co pozwala korzystać bez uciążliwości dla wolniejszych połączeń)
- możliwe wykorzystanie SSL

Filtry antyspamowe i antywirusowe dla serwerów SMTP

Filtry antyspamowe mają za zadanie filtrowanie wiadomości przychodzących, które prawdopodobnie zawierają treści niechciane przez użytkownika lub są masowo wysyłanymi treściami reklamowymi. Przykładami takich filtrów są **SpamAssassin, ASSP, Dspam.**

Natomiast filtry antywirusowe służą do skanowania wiadomości w przeszukiwaniu programów niebezpiecznych dla komputera tj. wirusów i zapobiegania uruchomieniu im. Obecnie na rynku istnieje wiele rozwiązań, dla przykładu **Dr. Web, ClamAV.**

Jeżeli chcemy wykorzystywać wiele usług do filtrowania naszych wiadomości musimy mieć wrapper, który będzie używał wielu narzędzi do filtrowania wiadomości. Narzędziem, które świetnie współpracuje z Postfixem nazywa się **Amavis**.

Istnieją również inne metody blokowania spamu, niektóre z nich to:

- filtracja rekordów PTR
- ustawienie filtrowania HELO/EHLO przy nagłówkach
- włączenie greylistowania (liczenie na to, iż spamer wysyła wiadomość tylko raz, tj w przypadku niedostarczenia za pierwszym razem wiadomości nie ponowi żadnej próby)

Część praktyczna: instalacja i konfiguracja

Instalacja wymaga uprawnień roota.

W tym celu logujemy się na konto root-a poleceniem:
su
lub używamy komendy **sudo** przed każdym poleceniem. (W tej instrukcji będziemy używali wcześniej zalogowanego konta root-a).
Przed instalacją serwera poczty należy mieć poprawnie skonfigurowaną usługę DNS.

Etap I: DNS

W pliku konfiguracyjnym BINDa (tj. np /var/named/primary/XYZ) na końcu dodajemy kod:

@ IN TXT "v=spf1 mx ip4:192.168.XXX.YYY ~all"
@ IN MX 10 poczta
poczta IN A 192.168.XXX.YYY

Gdzie XXX.YYY relatywnie do swojej maszyny.

Etap II: Instalacja pakietów.

Instalujemy odpowiednie oprogramowanie.
dnf -y install postfix
dnf -y install dovecot
dnf -y install mailx

Etap III: POSTFIX

Konfiguracja postfixa odbywa się w pliku **/etc/postfix/main.cf**

Odpowiednia numeracja dla oryginalnego, niezmienionego pliku konfiguracyjnego bez żadnych zmian.

Numer linii	Zawartość po zmianie	Komentarz
95	myhostname = poczta.domlabXXX.studmat.uni.torun.pl	Gdzie XXX to końcówka IP maszyny
102	mydomain = domlabXXX.studmat.uni.torun.pl	j/w
118	myorigin = $mydomain	-
135	inet_interfaces = all	-

138	inet_protocols = ipv4	Zakładam, że konfiguracja DNS działa po IPv4
183	mydestination = $myhostname, localhost.$mydomain, localhost, **$mydomain**	Dodajemy na końcu $mydomain (Dla spostrzegawczych istnieje już $mydomain wcześniej, jednakże jest połączony z localhost, dodajemy, żeby obsługiwał jeszcze samą domenę.)
283	mynetworks = 192.168.134.0/24, 127.0.0.0/8	Ustawiamy parametry na naszą sieć.
438	home_mailbox = Maildir/	Ustawiamy domyślny folder do przechowywania poczty dla użytkownika
593	smtpd_banner = $myhostname ESMTP	

Dodatkowo na końcu dodajemy:
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
smtpd_recipient_restrictions = permit_mynetworks, permit_auth_destination, permit_sasl_authenticated, reject
message_size_limit = 10485760
mailbox_size_limit = 1073741824

Włączenie usługi POSTFIX odbywa się za pomocą komendy:
systemctl enable --now postfix

Jeżeli na serwerze działa usługa firewalla to dodajemy do wyjątków
firewall-cmd --add-service=smtp --permanent
firewall-cmd --reload

W przypadku problemów w działania usługi.

W takim wypadku możemy przejrzeć plik logów usługi mailowej. Znajduje się on pod ścieżką:
/var/log/maillog
Poniższy przykład pokazuje gdy poprawnie wyślemy emaila na inną maszynę.

Nov 11 16:15:14 localhost postfix/pickup[44736]: 4FFB183A1B8: uid=1000 from=<maciej>
Nov 11 16:15:14 localhost postfix/cleanup[44914]: 4FFB183A1B8:
message-id=<20201111151514.4FFB183A1B8@poczta.domlab225.studmat.uni.torun.pl>

Nov 11 16:15:14 localhost postfix/qmgr[37420]: 4FFB183A1B8:
from=<maciej@domlab225.studmat.uni.torun.pl>, size=516, nrcpt=1 (queue active)

Nov 11 16:15:14 localhost postfix/smtp[44916]: 4FFB183A1B8:
to=<testuser@domlab125.studmat.uni.torun.pl>,
relay=domlab125.studmat.uni.torun.pl[192.168.134.125]:25, delay=0.1,
delays=0.04/0/0.04/0.02, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 635F3B1353)

Nov 11 16:15:14 localhost postfix/qmgr[37420]: 4FFB183A1B8: removed

Nov 11 16:17:27 localhost postfix/anvil[44955]: statistics: max connection rate 1/60s for
(smtp:172.18.24.22) at Nov 11 16:14:05

Nov 11 16:17:27 localhost postfix/anvil[44955]: statistics: max connection count 1 for
(smtp:172.18.24.22) at Nov 11 16:14:05

Nov 11 16:17:27 localhost postfix/anvil[44955]: statistics: max cache size 1 at Nov 11
16:14:05

ETAP IV: DOVECOT

Dla oryginalnych, niezmienionych plików konfiguracyjnych:

Numer linii	Zawartość po zmianie	Komentarz
Plik: **/etc/dovecot/dovecot.conf**		
30	listen = *, ::	Odkomentować linię
Plik: **/etc/dovecot/conf.d/10-auth.conf**		
10	disable_plaintext_auth = no	Pozwalamy na plain text auth
100	auth_mechanism = plain login	-
Plik: **/etc/dovecot/conf.d/10-mail.conf**		
30	mail_location = maildir:~/Maildir	Zmiana ścieżki lokacji maili, w którym będą przechowywane maile użytkownika. Gdy tego

		nie zrobimy będą przechowywane w **/var/spool/mail/$user**
Plik: **/etc/dovecot/conf.d/10-master.conf**		

107-109	unix_listener /var/spool/postfix/private/auth {
	mode = 0666
	user = postfix
	group = postfix
	}
		Linijki należy odkomentować oraz przypisać odpowiednie wartości do zmiennych

Plik: **/etc/dovecot/conf.d/10-ssl.conf**		
8	ssl = yes	(nie wymaga SSL)

Usługę uruchamiamy za pomocą komendy:
systemctl enable --now dovecot

Jeżeli na serwerze działa firewall to dodajemy do wyjątków:
firewall-cmd --add-service={pop3,imap} --permanent
firewall-cmd --reload

ETAP V: KONFIGURACJA KLIENTA

I. Ustawienie ścieżki poczty w systemie na ~/Maildir
echo 'export MAIL=$HOME/Maildir' >> /etc/profile.d/mail.sh
W przypadku braku chęci restartowania maszyny można lokalnie dla danego użytkownika użyć polecenia:
export MAIL=$HOME/Maildir

II. Tworzenie nowego konta pocztowego.

Odbywa się za pomocą stworzenia nowego użytkownika w systemie, tj:
useradd NAZWA
passwd NAZWA

III. Konfiguracja klienta.

Na lokalnej maszynie klient jest od razu dostępny do działania (polecenie **mail**)

Konfiguracja klienta na maszynie zewnętrznej (np Mozilla Thunderbird):

Jako, iż używany DNS na komputerze osobistym nie zawiera wpisu na naszą domenę, tj **domlabXXX.studmat.uni.torun.pl** należy ją dodać do pliku HOSTS ręcznie.
Plik ten znajduje się w folderze dostępnym pod ścieżką
%SystemRoot%\System32\drivers\etc

W pliku należy dodać wpis:
192.168.YYY.XXX domlabXXX.studmat.uni.torun.pl

Po dodaniu takiego wpisu (mając połączenie VPN z siecią wewnętrzną WMiI) Thunderbird automatycznie pobierze konfiguracje potrzebną do obsługi poczty z serwera. Jedynie trzeba ręcznie potwierdzić certyfikaty.

FILTRY ANTYSPAMOWE I ANTYWIRUSOWE

W tym wypadku wybrałem odpowiednio: SpamAssassin i ClamAV, jako iż współpracują z postfixem oraz są OpenSource. Żeby używać dwóch narzędzi na raz potrzebujemy wrappera, który będzie przepuszczał przez wiele filtrów na raz. W tym wypadku skorzystamy z pakietu **Amavis.**
Instalujemy je:
dnf -y install amavisd-new clamd

Warto mieć na uwadzę, iż Amavis nie potrzebuje osobnej instalacji pakietu SpamAssassin, gdyż jest zintegrowany.

DEAMON CALMD

/etc/clam.d/scan.conf

Powinniśmy mieć w nim takie pola (lub nie, wtedy trzeba dopisać własnoręcznie)

ID linii	Zawartość	Komentarz
~14	LogFile /var/log/clamd.scan	Odkomentować linijkę. Wskazuje plik do logów.
~77	PidFile /var/run/clamd.scan/clamd.pid	Odkomentować. Pozwala zapamiętać w logach ID procesu. Dodać główny katalog jako /var/
~81	TemporaryDirectory	Odkomentować, wskazuje

	/var/tmp	folder roboczy dla antywirusa.
~96	LocalSocket /var/run/clamd.scan/clamd.sock	Wskazuje na socket, na którym działa nasz deamon. Dodać główny katalog jako /var/
~112	TCPSocket 3310	--

Po czym musimy dać prawa naszemu deamonowi do logu:
chown clamscan. /var/log/clamd.scan

SELINUX

Domyślnie SELinux będzie nam blokował możliwość skanowania. Dlatego trzeba dodać do wyjątków za pomocą komend:
restorecon -v /var/log/clamd.scan
setsebool -P antivirus_can_scan_system on

AMAVISD

Plik konfiguracyjny to **/etc/amavisd/amavisd.conf**

ID linii	Linia	Komentarz
~15	$mydomain = 'domlabXXX.studmat.uni.torun.pl'	Odkomentować zmienną oraz zmienić wartość na domenę wskazaną w konfiguracji Postfixa
~140	$myhostname = 'poczta.domlabXXX.studmat.uni.torun.pl'	J/w. Wskazujemy hosta z postfixa
~155	$notify_method $forward_method	Odkomentować te dwie zmienne.
~370	['ClamAV-clamd', \&ask_daemon, ["CONTSCAN {}\n", "**/var/run/clamd.scan/clamd.sock**"], qr/\bOK$/m, qr/\bFOUND$/m, qr/^.*?: (?!Infected Archive)(.*) FOUND$/m],	W tym wypadku sprawdzamy czy adres wykorzystywanego SOCKETa jest identyczny jak w Clamd (potłuszczone). Jeżeli nie to zmieniamy.

POSTFIX

W pliku **/etc/postfix/main.cf** musimy wskazać postfixowi, iż maile powinien wysyłać na nasz socket, który będzie je filtrował. Robimy to za pomocą dodania na koniec pliku opcji:
content_filter=smtp-amavis:[127.0.0.1]:10024

Natomiast w pliku /etc/postfix/master.cf musimy wskazać konfigurację naszego połączenia:

```
smtp-amavis unix -    -    n    -    2 smtp
   -o smtp_data_done_timeout=1200
   -o smtp_send_xforward_command=yes
   -o disable_dns_lookups=yes
127.0.0.1:10025 inet n    -    n    -    - smtpd
   -o content_filter=
   -o local_recipient_maps=
   -o relay_recipient_maps=
   -o smtpd_restriction_classes=
   -o smtpd_client_restrictions=
   -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
   -o smtpd_error_sleep_time=0
   -o smtpd_soft_error_limit=1001
   -o smtpd_hard_error_limit=1000
```

Skoro już mamy wszystko skonfigurowane można uruchomić usługi:

```
systemctl start clamd@scan
systemctl start amavisd
systemctl restart postfix
```

UWAGA: Może się zdarzyć tak, iż dostaniemy błąd **ClamAV-clamd socket connection refused** (np sprawdzając **systemctl status postfix** po wysłaniu jakiegoś maila). Należy wtedy zmienić prawa dostępu do folderu oraz socketu na amavisda, tj:

```
chown avamis:avamis clamd.scan #ścieżka z wcześniejszej konfiguracji
```

Jeżeli wszystko dobrze zrobiliśmy to nasze wiadomości powinny być skanowane, np:

Source of: imap://testuser@domlab225.studmat.uni.torun.pl:143/fetch%3EUID%3E.INBOX%3E20 - Mozilla Thunderbird

File Edit View Help

```
Return-Path: <testuser@domlab125.studmat.uni.torun.pl>
X-Original-To: testuser@domlab225.studmat.uni.torun.pl
Delivered-To: testuser@domlab225.studmat.uni.torun.pl
Received: from localhost (localhost [127.0.0.1])
    by poczta.domlab225.studmat.uni.torun.pl (Postfix) with ESMTP id 19A5183A0D2
    for <testuser@domlab225.studmat.uni.torun.pl>; Wed, 11 Nov 2020 23:49:09 +0100 (CET)
X-Virus-Scanned: amavisd-new at domlab225.studmat.uni.torun.pl
Received: from poczta.domlab225.studmat.uni.torun.pl ([127.0.0.1])
    by localhost (poczta.domlab225.studmat.uni.torun.pl [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id KYFZ4l8uZAlH
    for <testuser@domlab225.studmat.uni.torun.pl>;
    Wed, 11 Nov 2020 23:48:54 +0100 (CET)
Received: from poczta.domlab125.studmat.uni.torun.pl (lab125.domlab225.studmat.uni.torun.pl [19
    by poczta.domlab225.studmat.uni.torun.pl (Postfix) with ESMTPS id 3E9FB83A0D1
    for <testuser@domlab225.studmat.uni.torun.pl>; Wed, 11 Nov 2020 23:48:54 +0100 (CET)
Received: by poczta.domlab125.studmat.uni.torun.pl (Postfix, from userid 1001)
    id 000BE11C91B; Wed, 11 Nov 2020 23:48:53 +0100 (CET)
Date: Wed, 11 Nov 2020 23:48:53 +0100
To: testuser@domlab225.studmat.uni.torun.pl
Subject: TestZAntyWirusem
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20201111224854.000BE11C91B@poczta.domlab125.studmat.uni.torun.pl>
From: testuser@domlab125.studmat.uni.torun.pl

Witaj swiecie.
```

Natomiast jeżeli dostaniemy spam to zostanie on usunięty (do zobaczenia w maillogu)

```
Nov 11 23:43:49 localhost postfix/smtpd[1616]: connect from lab125.domlab225.studmat.uni.torun.pl[192.168.134.125]
Nov 11 23:43:50 localhost postfix/smtpd[1616]: 00F4183A0DA: client=lab125.domlab225.studmat.uni.torun.pl[192.168.134.125]
Nov 11 23:43:50 localhost postfix/cleanup[1619]: 00F4183A0DA: message-id=<20201111224349.BAC5611C920@poczta.domlab125.studmat.uni.torun.pl>
Nov 11 23:43:50 localhost postfix/qmgr[1155]: 00F4183A0DA: from=<testuser@domlab125.studmat.uni.torun.pl>, size=861, nrcpt=1 (queue active)
Nov 11 23:43:50 localhost postfix/smtpd[1616]: disconnect from lab125.domlab225.studmat.uni.torun.pl[192.168.134.125] ehlo=2 starttls=1 mail=1 rcpt=1 data=1
 quit=1 commands=7
Nov 11 23:44:05 localhost amavis[1063]: (01063-04) Blocked SPAM {DiscardedInternal,Quarantined}, MYNETS LOCAL [192.168.134.125]:53406 <testuser@domlab125.st
udmat.uni.torun.pl> -> <testuser@domlab225.studmat.uni.torun.pl>, Queue-ID: 00F4183A0DA, Message-ID: <20201111224349.BAC5611C920@poczta.domlab125.studmat.un
i.torun.pl>, mail_id: HTuNnmNvKgAC, Hits: 999.001, size: 861, 15575 ms
Nov 11 23:44:05 localhost postfix/smtp[1620]: 00F4183A0DA: to=<testuser@domlab225.studmat.uni.torun.pl>, relay=127.0.0.1[127.0.0.1]:10024, delay=16, delays=
0.03/0.05/0.03/16, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=01063-04 - span)
Nov 11 23:44:05 localhost postfix/qmgr[1155]: 00F4183A0DA: removed
[root@localhost clamd.scan]# systemctl status postfix
```

Bibliografia:

[1] https://www.poczta-polska.pl/biznes/korespondencja/listy-zwykle/
[2] https://www.poczta-polska.pl/paczki-i-listy/przesylki-zagraniczne/listy/list-zwykly/
[3] https://www.hcidata.info/email-delivery.htm
[4] https://blog.hubspot.com/marketing/free-email-accounts
[5]https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide
[6]https://pomoc.home.pl/baza-wiedzy/co-to-jest-nazwa-poczta-smtp
[7]https://en.wikipedia.org/wiki/Comparison_of_mail_servers
https://docs.fedoraproject.org/en-US/fedora/rawhide/system-administrators-guide/servers/Mail_Servers/
https://en.wikipedia.org/wiki/History_of_email
https://en.wikipedia.org/wiki/Time-sharing
https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
https://www.server-world.info/en/note?os=Fedora_31&p=mail&f=1
https://help.ubuntu.com/community/PostfixAmavisNew
https://www.linuxbabe.com/mail-server/block-email-spam-postfix