Osobní poštovní server

Ondřej Caletka

cesnet

3. března 2019

O sdružení CESNET

n×100 Gb/s
n×10 Gb/s
uzel (PoP)
uživatel (user)
100 Gb/s
10 Gb/s
1–2,5 Gb/s
<1 Gb/s

Motivace

Zdroj: Attuned Photography

Zadání

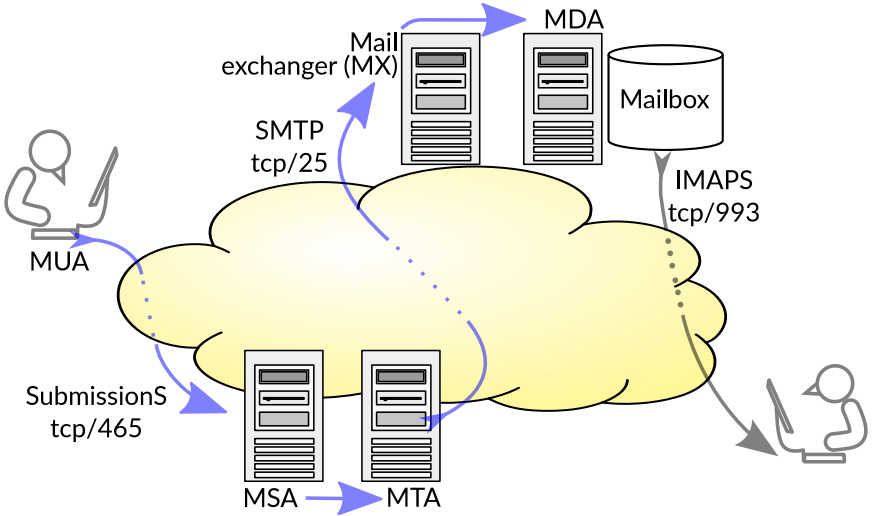
- vlastní poštovní schránka na vlastní doméně
- přístup z poštovních klientů standardními protokoly IMAPS a SubmissionS
- očekávaný provoz desítek zpráv denně
- aspoň základní ochrana před spamem

Minimální požadavky

- vlastní linuxový server s IPv4 (i IPv6) konektivitou
- možnost nastavit reverzní záznamy k IP adresám

cesnet

Jak to vlastně funguje

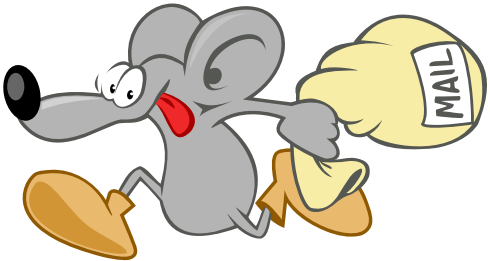


cesnet

Autor: Ale2006-from-en CC-BY-SA

Postfix

- všestranný poštovní server
- použijeme jako MSA, MTA, MX, MDA



cesnet

Dovecot

- jednoduchý server pro IMAP
- vysoce konfigurovatelná autentizace
- poskytuje autentizaci uživatelů i pro Postfix

cesnet

Ukládání e-mailových zpráv

- unixové nebo virtuální účty
- formát schránky mbox nebo maildir
- > volíme unixové schránky a formát maildir

mbox

- schránka je soubor
- INBOX je ve `/var/spool/mail/<user>`
- ostatní schránky někde v `$HOME`
- zamykání, fragmentace

maildir

- zpráva je soubor
- všechny schránky jsou v `$HOME`
- atomické přesuny

cesnet

Výchozí chování (Debian)

- postfix přijímá a odesílá poštu pro sebe
- používá self-signed certifikát
- podporuje jen SMTP
- ukládá do mboxů

Změna na maildir

```
# postconf -e "home_mailbox = Maildir/"
# postfix reload
# editor /etc/dovecot/conf.d/10-mail.conf
  mail_location = maildir:~/Maildir
```

cesnet

TLS certifikát

- nejsnáze pomocí Let's Encrypt
- ověření přes web nebo DNS
- stejný certifikát pro SMTP, IMAPS i SubmissionS
- vytvoříme TLSA záznam pro SMTP certifikát (typ 3 1 1)
- v Dovecotu je TLS ve výchozím stavu vypnuto
- můžeme vypnout nešifrovaný IMAP nastavením portu na 0

cesnet

Zprovoznění SubmissionS a SASL

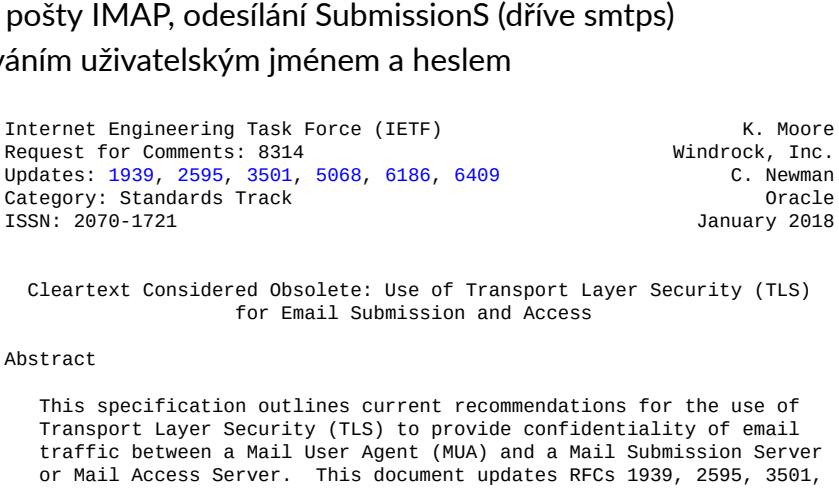
- Dovecot vytvoří UNIX socket v spool adresáři Postfixu
- Autentizaci povolujeme jen na portu 465 - Submissions

Zprovoznění SubmissionS

```
# editor /etc/dovecot/conf.d/10-master.conf
  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {…
# postconf -e "smtpd_sasl_type = dovecot"
# postconf -e "smtpd_sasl_path = private/auth"
# editor /etc/postfix/master.cf
  smtps     inet  n   -   y   -   -   smtpd
  …
  -o smtpd_sasl_auth_enable=yes
```

Nastavení MUA

- příjem pošty IMAP, odesílání SubmissionS (dříve smtps)
- ověřováním uživatelským jménem a heslem



Internet Engineering Task Force (IETF) — K. Moore
Request for Comments: 8314 — Windrock, Inc.
Updates: 1939, 2595, 3501, 5068, 6186, 6409 — C. Newman
Category: Standards Track — Oracle
ISSN: 2070-1721 — January 2018

Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access

Abstract

This specification outlines current recommendations for the use of Transport Layer Security (TLS) to provide confidentiality of email traffic between a Mail User Agent (MUA) and a Mail Submission Server or Mail Access Server. This document updates RFCs 1939, 2595, 3501, 5068, 6186, and 6409.

cesnet

Bezpečné předávání pošty

- ve výchozím nastavení se v odchozím směru nešifruje
- pro DANE je třeba bezpečný validující resolver (na loopbacku)

```
# postconf -e "smtp_dns_support_level = dnssec"
# postconf -e "smtp_tls_security_level = dane"
# postconf -e "smtp_tls_loglevel = 1"
```

cesnet

Speciální heslo jen pro poštu

- pro uložení do nejrůznějších zařízení
- chrání před zneužitím uživatelského účtu jinde než v poště

```
# editor /etc/dovecot/conf.d/10-auth.conf
  !include auth-passwdfile.conf.ext
# doveadm pw -p heslo
{CRAM-MD5}95650…9b184c
# cat > /etc/dovecot/users
user:{CRAM-MD5}95650…9b184c:1000:1000::/home/user:
sender_only:{CRAM-MD5}95…:65534:65534::/nonexistent:
```

cesnet

Procmail

- umožňuje filtrovat poštu na serveru
- postupně vytlačován ve prospěch sieve

```
# cat >/etc/procmailrc
MAILDIR=$HOME/Maildir/
DEFAULT=$MAILDIR
# postconf -e 'mailbox_command = procmail -a "$EXTENSION"'
```

cesnet

Ukázka konfigurace /.procmailrc

```
MAILDIR=$HOME/.maildir/
DEFAULT=$MAILDIR
LOGFILE=$HOME/procmail.log
EXT=$1

:0
* ^X-Cron-Env
.Cron/

:0
* ^Subject: DenyHosts Report
.Cron.DenyHosts/
```

cesnet

Spamassassin

- funguje velmi dobře bez dalšího nastavování
- snadno se integruje přímo do procmailu
- konfigurace po prvním spuštění v `~/.procmailrc`

```
:0fw: spamassassin.lock
* < 512000
| spamassassin

:0
* ^X-Spam-Status: Yes
.spam/
```

cesnet

SPF, DMARC, DKIM

- pro menší pravděpodobnost, že skončíme ve spamu
- pomocí SPF deklarujeme povolené servery
- kvůli přeposílání pošty nepoužíváme hard fail
- jsme-li přihlášeni v poštovních konferencích, nenastavujeme DMARC politiku
- podepisováním pomocí DKIM nic nezkazíme

Příklad SPF a DMARC záznamu

```
example.com.          IN  TXT "v=spf1 +mx ~all"
_dmarc.example.com.   IN  TXT "v=DMARC1; p=none"
dkim2018._domainkey.example.com. IN TXT "v=DKIM1…
```

cesnet

OpenDKIM

```
# cd /etc/dkimkeys
# opendkim-genkey --bits 2048 --selector="dkim2019"
# editor /etc/opendkim.conf
  Domain                  example.com
  Selector                dkim2019
  KeyFile                 /etc/dkimkeys/dkim2019.key
  Canonicalization        relaxed
  Socket             local:/var/spool/postfix/opendkim.sock
# postconf -e "smtpd_milters = unix:opendkim.sock"
# postconf -e "non_smtpd_milters = unix:opendkim.sock"
```

cesnet

Testování telnetem

```
220 SMTP server ready
EHLO local.machine.example
250 server.example.net
MAIL FROM: <jdoe@machine.example>
250 2.1.0 Ok
RCPT TO: <mary@example.net>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: John Doe <jdoe@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
.
250 2.0.0 Ok: queued as C5D1822AF6
QUIT
221 2.0.0 Bye
```

cesnet

Testování DANE for SMTP

Bez TLSA záznamu – Untrusted

```
$ /usr/sbin/posttls-finger -c seznam.cz
posttls-finger: mx1.seznam.cz:25: Matched subjectAltName: mx1.seznam.cz
posttls-finger: certificate verification failed for mx1.seznam.cz:25:
                untrusted issuer /C=US/O=thawte, Inc./OU=Certification
                Services Division/OU=(c) 2006 thawte, Inc. - For
                authorized use only/CN=thawte Primary Root CA
posttls-finger: Untrusted TLS connection established to mx1.seznam.cz:25:
                TLSv1.2 with cipher AES128-SHA (128/128 bits)
```

S TLSA záznamem – Verified

```
$ /usr/sbin/posttls-finger -c cesnet.cz
posttls-finger: using DANE RR: _25._tcp.… IN TLSA 2 0 1 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: postino.cesnet.cz:25: depth=1 matched trust anchor certificate
                sha256 digest 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: Verified TLS connection established to postino.cesnet.cz:25:
                TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits)
```

`https://dane.sys4.de`

cesnet

Další možná vylepšení

- záložní MX server
  - pro dlouhé výpadky (>3 dny)
  - měl by odmítat poštu pro neexistující adresy
- greylisting
  - zdržování legitimní pošty
  - méně účinné než Spamassassin
- real-time DNS blacklist
  - při malém objemu zpráv nedává smysl
- postfwd
  - pokročilý firewall
  - lze například limitovat počet zpráv za účet za hodinu

cesnet

Závěrečné myšlenky

- tiché zahazování e-mailů je zlo
  - přijmu-li e-mail do fronty, odpovídám za jeho doručení, případně odeslání nedoručenky
  - takže je potřeba občas **projít složku spam**
- dohlížejte délku fronty
  - pro osobní e-mailový server jsou zásadní i jednotky zpráv
  - prudký nárůst obvykle znamená **zneužití přihlašovacích údajů** ke spammingu
  - pomalý nárůst může být způsoben **chybou v DANE** na straně příjemce
- certifikát pro SMTP server raději RSA
  - spousta zastaralých odesílatelů ECDSA nepodporuje
  - většina provede downgrade, jeden exemplář zprávu nedoručil

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.