

MAIL SERVER

Maturitná práca

OBSAH

ZOZNAM OBRÁZKOV	3
ZOZNAM SKRATIEK	4
ÚVOD	5
1 TEORETICKÁ ČASŤ	6
1.1 Základné pojmy	6
1.1.1 Internet.....	6
1.1.2 Služby v Internete	6
2 POUŽITÉ TECHNOLOGIE	8
2.1 SMTP.....	8
2.2 IMAP	8
2.3 DNS.....	8
2.4 SSL.....	9
2.5 HTTP/HTTPS.....	9
2.6 DKIM	10
3 POUŽITÉ PRODUKTY TRETÍCH STRÁN	11
3.1 Postfix.....	11
3.2 Dovecot	11
3.3 Apache.....	11
3.4 Lets encrypt.....	11
3.5 OpenDKIM.....	12
3.6 RainLoop	12
4 PRAKTICKÁ ČASŤ.....	13
4.1 Prepojenie domény so serverom.....	13
4.2 Konfigurácia postfix-u.....	15
4.3 Konfigurácia Apache web serveru a zaobstaranie SSL certifikátu	16
4.4 Nastavenie SSL certifikátu v postfix-e	17
4.5 Inštalácia Dovecot-u.....	17
4.6 Konfigurácia SPF, DMARC a DKIM	19
4.7 Inštalácia webového klienta.....	24
4.8 Testovanie e-mailovej adresy	25
ZÁVER.....	30
ZOZNAM POUŽITEJ LITERATÚRY	31

ZOZNAM OBRÁZKOV

Obrázok 1: Žiadosť o reverzný DNS záznam. Zdroj: vlastné spracovanie	13
Obrázok 2: Nadstavenie MX DNS záznamu. Zdroj: vlastné spracovanie	13
Obrázok 3: Nadstavenie A DNS záznamu. Zdroj: vlastné spracovanie	14
Obrázok 4: Nadstavenie 2. A DNS záznamu. Zdroj: vlastné spracovanie	14
Obrázok 5: Editácia súboru hosts. Zdroj: vlastné spracovanie	15
Obrázok 6: Nastavenie postfix-u. Zdroj: vlastné spracovanie	15
Obrázok 7: Zdávanie domény. Zdroj: vlastné spracovanie	16
Obrázok 8: Konfigurácia Apache2. Zdroj: vlastné spracovanie	16
Obrázok 9: Implementácia SSL v postfix-e. Zdroj: vlastné spracovanie	17
Obrázok 10: Konfigurácia dovecot-u. Zdroj: vlastné spracovanie	18
Obrázok 11: Implementácia SSL v dovecot-u. Zdroj: vlastné spracovanie	19
Obrázok 12: SPF v DNS. Zdroj: vlastné spracovanie	19
Obrázok 13: Implementácia SPF do postfixu. Zdroj: vlastné spracovanie	20
Obrázok 14: Implementácia SPF do postfixu 2. Zdroj: vlastné spracovanie	20
Obrázok 15: Implementácia DMARC záznamu. Zdroj: vlastné spracovanie	20
Obrázok 16: Konfigurácia OpenDKIM. Zdroj: vlastné spracovanie	21
Obrázok 17: Implementácia OpenDKIM DNS záznamu. Zdroj: vlastné spracovanie	22
Obrázok 18: Konfigurácia OpenDKIM tabuľky s kľúčmi. Zdroj: vlastné spracovanie	22
Obrázok 19: Definovanie dôveryhodných IP adries / domén. Zdroj: vlastné spracovanie	22
Obrázok 20: Zadanie DNS záznamu s DKIM kľúčom. Zdroj: vlastné spracovanie	23
Obrázok 21: Prepojenie DKIM s Postfix-om. Zdroj: vlastné spracovanie	23
Obrázok 22: Získanie mailového klienta. Zdroj: vlastné spracovanie	24
Obrázok 23: Inštalácia mailového klienta pomocou FTP. Zdroj: vlastné spracovanie	24
Obrázok 24: Zadanie mail servera do mailového klienta. Zdroj: vlastné spracovanie	25
Obrázok 25: Testovanie mailu. Zdroj: vlastné spracovanie	26
Obrázok 26: Výsledok testu. Zdroj: vlastné spracovanie	26
Obrázok 27: Test príjmu správ. Zdroj: vlastné spracovanie	27
Obrázok 28: Kontrola príjmu správ. Zdroj: vlastné spracovanie	27
Obrázok 29: Odosielanie správy. Zdroj: vlastné spracovanie	28

Obrázok 30: Kontrola prijatej správy. Zdroj: vlastné spracovanie.....	28
Obrázok 31: Testovanie odozvy servera. Zdroj: vlastné spracovanie	28

ZOZNAM SKRATIEK

SMTP – Jednoduchý protokol na prenos pošty

IMAP - Protokol interaktívneho poštového prístupu

POP – Protokol pošty

DNS - Systém doménových mien

IP – Internetový protokol

SPF - Rámec zásad odosielateľa

DMARC - Autentifikácia správ, podávanie správ a zhoda s doménami

SSL – Bezpečnostná vrstva

HTTP - Hypertextový prenosový protokol

HTTPS - Zabezpečený hypertextový prenosový protokol

DKIM – Mailový identifikátor na základe doménových kľúčov

UNIX - Uniplexed Information and Computing Service

MTA - Agent prenosu pošty

PTR – Pointer

SPAM – Nežiadúca pošta

TXT – Text / Textový

FTP – Protokol pre prenos súborov

PHP - Hypertextový predprocesor

ÚVOD

E-mail je v súčasnosti dôležitou súčasťou komunikácie. Odhaduje sa, že počet e-mailových používateľov presiahne v roku 2020 hranicu 4 miliardy. Jedná sa o ohromné číslo, a preto sa už dávno e-mail nevyužíva len na odosielanie jednoduchých informačných správ, ale svoje miesto si našiel v pracovnej korešpondencii, marketingu, bankovníctve či komunikácii s verejnou správou.

V súčasnosti existuje nepreberné množstvo firiem tzv. e-mailových providerov, ktorí poskytujú e-mail hosting – službu, ktorá prevádzkuje e-mailové servery. Hlavným cieľom našej práce je však vytvorenie vlastného e-mailového servera, ktorý zodpovedá aktuálnym trendom v oblasti zabezpečenia.

Prvá kapitola, nazvaná Teoretická časť, vymedzuje internet a služby v internete súvisiace s elektronickou poštou. V závere prvej kapitoly sú zadefinované aj ďalšie pojmy potrebné pre pochopenie práce v počítačovej sieti.

Druhá kapitola, Použité technológie, nadväzuje na teoretickú časť, a presne vymedzuje jednotlivé protokoly a DNS záznamy, ktoré boli použité v praktickej časti tejto práce.

Praktickej časti práce sa týka aj tretia kapitola, Použité produkty tretích strán, kde sú priblížené konkrétne produkty, ktoré boli použité pri vytvorení vlastného e-mailového servera.

Jednotlivé činnosti potrebné k vytvoreniu vlastného e-mailového servera tvoria obsah poslednej kapitoly s názvom Praktická časť. Približuje kompletnú inštaláciu e-mailového serveru na Linuxe, vrátane niektorých pridružených služieb. Vytvorený e-mailový server je svojim zameraním kombináciou bezpečnosti a rozumnej miery údržby, a jeho vybavenie bude dostatočné pre osobné využitie alebo pre menšiu firmu.

1 TEORETICKÁ ČASŤ

1.1 Základné pojmy

1.1.1 Internet

Internet, hovorovo sieť, net, je médium, ktoré sa stalo súčasťou nášho života. Názov Internet vznikol zo slova INTERconnected NETWORKS, čo znamená prepojené počítačové siete. Počítačová sieť je „množina vzájomne prepojených autonómnych počítačových systémov.“¹ Internet je teda prenosové médium pre prenos územne rozptýlených dát, informácií a takisto pre poskytovanie rôznych služieb.

1.1.2 Služby v Internete

Služby, ktoré sú v Internete poskytované sú na báze architektúry klient/server. „Klient je softvérový proces, ktorý požaduje služby od iného softvérového procesu, server je softvérový proces, ktorý poskytuje službu (služby), ako odozvu na požiadavku klienta (klientov) nezávisle od hardvérovej platformy.“²

Vo svojej práci sa budeme zaoberať týmito službami Internetu:

- a) elektronická pošta (e-mail) – je rýchly spôsob výmeny elektronických správ medzi dvomi alebo viacerými užívateľmi. Programové prostriedky, ktoré umožňujú realizovať elektronickú poštu majú zvyčajne dve časti:
 - používateľskú – používateľ služby má na svojom počítači nainštalovaný program (klient), ktorý komunikuje so serverom, počítač nemusí byť stále v prevádzke,
 - prenosovú – „prenosový agent je spravidla uložený na počítači, ktorý je trvalo v prevádzke, aby bolo možné správu vždy doručiť.“³ To znamená, že pracuje v reálnom čase (server). Má vyhradený pamäťový priestor na uloženie správ.

- b) World Wide Web (www) – je „služba Internetu, predstavujúca distribuovaný, hypertextovo orientovaný informačný systém, ktorý umožňuje transparentný prístup k rôznym zdrojom. Základnou jednotkou informácie je dokument, často

¹ ZÁVODNÝ, P.: Počítačové siete v hospodárskej praxi. Bratislava : Vydavateľstvo Ekonóm, 2005, s. 8.

² ZÁVODNÝ, P.: Počítačové siete v hospodárskej praxi. Bratislava : Vydavateľstvo Ekonóm, 2005, s. 90.

³ ZÁVODNÝ, P.: Počítačové siete v hospodárskej praxi. Bratislava : Vydavateľstvo Ekonóm, 2005, s. 92.

nazývaný aj webová stránka,⁴ ktorá obvykle obsahuje odkazy na ďalšie dokumenty rozptýlené po Internete.

Na to, aby mohla prebiehať výmena informácií v počítačovej sieti, je potrebný súbor pravidiel tzv. protokolov. Súvisia s architektúrou počítačovej siete, pričom základným prvkom architektúry je vrstva. V každej vrstve sa pomocou príslušných protokolov zabezpečuje niektorá zo sieťových služieb. Aby sa budovali jednotné počítačové siete, boli Medzinárodnou organizáciou pre normalizáciu ISO (International Standards Organisation) navrhnuté medzinárodné normy a štandardy prepojenia otvorených systémov sedemvrstvovým referenčným modelom OSI/ISO.

⁴ ZÁVODNÝ, P.: Počítačové siete v hospodárskej praxi. Bratislava : Vydavateľstvo Ekonóm, 2005, s. 98.

2 POUŽITÉ TECHNOLOGIE

2.1 SMTP

SMTP (Simple Mail Transfer Protocol) je „jeden zo sady protokolov TCP/IP. Riadi výmenu elektronickej pošty“⁵.

2.2 IMAP

IMAP (Internet Message Access Protocol) je internetový protokol, ktorý umožňuje prístup k e-mailovým schránkam. IMAP správy neukladá do počítača používateľa, ale ich umožňuje čítať zo servera, čím umožňuje prístup k správam z akéhokoľvek zariadenia. Ukladanie správ na strane servera má za následok väčšiu náročnosť na kapacitné požiadavky servera, a tým pádom aj vyššie finančné zaťaženie prevádzkovateľa servera, na rozdiel od protokolu POP3, ktorý umožňuje ukladať správy na strane klienta a správy zo servera odstraňuje.

2.3 DNS

DNS (Domain Name System) je doménový systém, ktorý slúži ako prekladač domén na IP adresy. IP adresy majú číselný charakter a sú pridelené každému uzlu (počítač, server, modem a pod.) v počítačovej sieti. DNS sa teda využíva predovšetkým pre webové stránky, kde sa doménové meno prevedie na IP adresu. Takisto sa využíva aj pri iných službách, napr. e-mailoch, kde okrem iného prispieva k tomu, že po zadaní „menopouzivatela@domena.tld“ príde e-mail tej správnej osobe. Týmto sa značne zjednodušuje používanie internetových služieb ako takých. DNS takisto vytvára tzv. DNS záznamy a poskytuje záznamy lokálne.

Existuje viacero typov DNS záznamov a každý z nich má určité špecifické vlastnosti:

- A záznamy – typ DNS záznamu, ktorý priradí doméne IP adresu z ktorej sa má načítavať obsah. IP Adresa musí byť vo formáte IPv4.
- AAAA záznamy – typ DNS záznamu, ktorý priradí doméne IPv6 adresu, z ktorej sa má načítavať obsah.

⁵HORÁK, J.:Bezpečnosť malých počítačových sítí (praktické rady a návody). Praha : Grada Publishing, 2003, s.180.

- MX záznamy – „MX záznamy (mail exchanger) slúžia na určenie serveru, ktorý má spracovávať e-maily pre vašu doménu.“⁶
- NS záznamy – slúžia na určenie adresy, z ktorej má doména čerpať ďalšie DNS záznamy.
- CNAME záznamy – slúžia na určenie vzorového DNS záznamu. Najprv sa stiahne vzorový DNS záznam, a pokiaľ neexistuje, tak sa postupuje podľa MX, A, AAAA a pod.
- TXT záznamy – slúžia na pridanie textových informácií do DNS záznamu.
- SPF záznamy – záznam, ktorý zaznamenáva odosielaciu politiku servera. Vo svojej podstate slúži ako jedno z mnohých opatrení proti SPAM-u.
- DMARC záznam – určuje, kam má e-mail ísť, pokiaľ je adresát neexistujúci alebo nedostupný. Taktiež sa tým zavádza určitá prijímacia politika, a to či neoverený e-mail má ísť do spamu alebo má byť odmietnutý či prijatý.

2.4 SSL

SSL (Secure Sockets Layer) „je šifrovací protokol, ktorý slúži na šifrovanie komunikácie medzi počítačmi.“⁷ v sieti a jeho hlavnou úlohou je zabezpečiť, aby žiadna tretia strana nemohla vidieť dáta, ktoré sa prenášajú. SSL sa využíva v drvivej väčšine pri weboch, ale aj pri e-mailoch. V raných vekoch SSL mávalo 40 bitovú šifru, dnes je štandardom 128 bitová šifra, ale napr. v bankovom sektore sa dá bežne stretnúť s 256 bitovou šifrou.

2.5 HTTP/HTTPS

HTTP (Hypertext Transfer Protocol Secure) je hypertextový protokol, ktorý v Internete slúži na prenos dát. Slúži teda ako služba, prostredníctvom ktorej môže server

⁶ DNS záznamy. [online]. [cit. 2019.11.19]. Dostupné na: <<https://www.websupport.sk/support/kb-categories/dns-zaznamy/>>.

⁷ What is SSL?. [online]. [cit. 2019.11.22]. Dostupné na: <<https://www.ssl.com/faqs/faq-what-is-ssl/>>.

hostovať webovú stránku. Samozrejme aj HTTP má svoju kryptovanú verziu, a to HTTPS, kde sa využíva protokol SSL.

2.6 DKIM

DKIM (Domain Keys Identified Mail) „je e-mailová autentifikačná technika, ktorá umožňuje príjemcovi overiť či e-mail bol skutočne zaslaný z domény skutočného odosielateľa.“⁸ To sa robí za pomoci digitálneho podpisu.

⁸What is DKIM?. [online]. [cit. 2019.11.20]. Dostupné na: <<https://www.dmarcanalyzer.com/dkim/>>.

3 POUŽITÉ PRODUKTY TRETÍCH STRÁN

3.1 Postfix

Postfix je softvér, ktorý smeruje a doručuje elektronickú poštu. Postfix je open-source a beží na všetkých operačných systémoch založených na UNIX-e. Ako SMTP server, postfix poskytuje určitý stupeň ochrany voči spam-botom. Samozrejme je možné (a doporučené) kombinovať s anti-spam asistentmi.

3.2 Dovecot

Dovecot „je open-source IMAP a POP 3 e-mailový server pre LINUX / UNIX operačné systémy“⁹, ktorý umožňuje používateľom pristupovať do e-mailových schránok či ich spravovať.

3.3 Apache

Apache „je open-source najpoužívanejší webový server na operačných systémoch Linux.“¹⁰, ktorý dokáže hostovať jednu či viacero webových stránok na protokole HTTP/HTTPS. Taktiež má podporu nespočetného množstva programovacích jazykov a veľkého množstva prídavných modulov.

3.4 Lets encrypt

Lets encrypt je autorita podpisujúca SSL certifikáty, ktoré môžu byť použité napr. na webových, či e-mailových serveroch. Lets encrypt je dotovaná neziskovou organizáciou „ISRG“, vďaka čomu je možné generovať SSL certifikáty úplne zadarmo.

⁹DOVECOT. [online]. [cit. 2019.11.13]. Dostupné na: < <https://www.dovecot.org/>>.

¹⁰HTTPD - Apache2 Web Server. [online]. [cit. 2019.11.25]. Dostupné na: < <https://help.ubuntu.com/lts/serverguide/httpd.html>> .

3.5 OpenDKIM

OpenDKIM je open-source implementácia DKIM autorizačného systému na overenie odosielateľa e-mailu. OpenDKIM obsahuje DKIM službu ako takú, a takisto aj komunikačný filter, ktorý sa dá prepojiť s MTA (napr. postfix).

3.6 RainLoop

RainLoop „je open-source webový klient založený na PHP, ktorý je zdarma.“¹¹ Má jednoduchý vzhľad, dokáže si poradiť s väčším množstvom používateľov, a to aj napriek tomu, že nepotrebuje napojenie na databázu, samozrejme, napojenie na databázu je možné. Je moderný, bezpečný a je veľmi modulárny, čo znamená, že existuje veľa prídavkov, ktoré sa dajú doinštalovať.

¹¹RAINLOOP FEATURES. [online]. [cit. 2019.11.29]. Dostupné na:

< <https://www.rainloop.net/features/> >.

4 PRAKTICKÁ ČASŤ

Úlohou tejto časti je sa zaoberať praktickou stránkou, tvorenia, konfigurovania a testovania emailového servera.

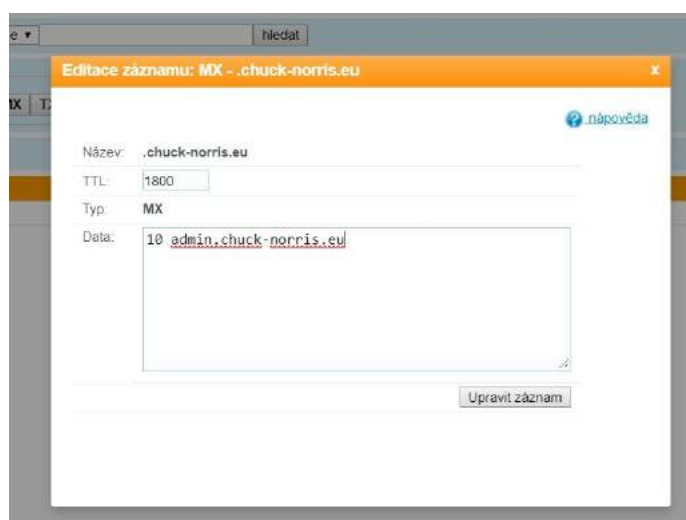
4.1 Prepojenie domény so serverom

Aby e-maily neputovali rovno do SPAM-u, je potrebné urobiť sériu opatrení. Jednou a hlavnou časťou je nastavenie PTR – reverzného záznamu. Tento záznam sa nachádza v DNS servera a odkazuje na doménu. Slúži na overenie, či IP adresa zodpovedá názvu domény. Bohužiaľ, mnoho hostiteľov z bezpečnostných dôvodov neumožňujú klientom nastaviť reverzný záznam, a preto o to treba požiadať.



Obrázok 1: Žiadosť o reverzný DNS záznam. Zdroj: vlastné spracovanie.

Následne je potrebné nastaviť MX a A záznam na strane domény. Do MX záznamu zadáme číslo 10. Toto číslo označuje prioritu. V našom prípade používame iba jeden server, ale ak by ich bolo viac, tak by sa využíval server s nižšou prioritou, a po jeho páde by sa automaticky používal ten s vyšším číslom. Následne zadáme doménu budúceho SMTP servera.



Obrázok 2: Nastavenie MX DNS záznamu. Zdroj: vlastné spracovanie.

Vytvoríme dva A záznamy. Prvý bude pre doménu chuck-norris.eu a odkazovať na IP adresu servera.



Obrázok 3: Nadstavenie A DNS záznamu. Zdroj: vlastné spracovanie.

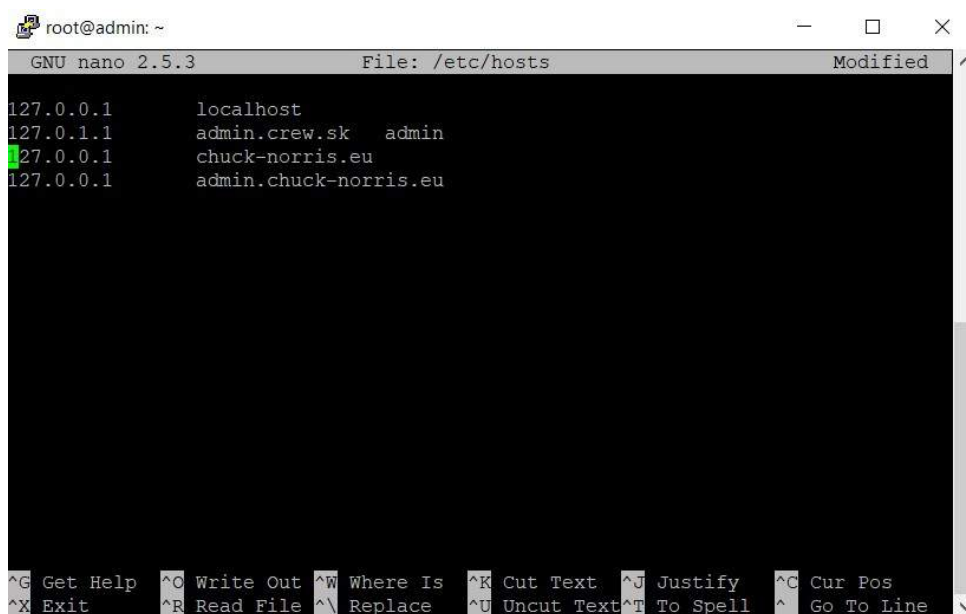
Druhý pre doménu admin.chuck-norris.eu taktiež s odkazom na IP adresu servera.



Obrázok 4: Nadstavenie 2. A DNS záznamu. Zdroj: vlastné spracovanie.

Následne je potrebné napojiť sa na virtuálny server a nastaviť hostiteľské mená. "Hostiteľské meno je názov miestneho počítača. Užitočné hlavne v prípadoch, kedy si nie sme istý podobou názvu"¹². Pre pripojenie bude používaný program „Putty“. Súbor s nastavením hostiteľských mien upravíme pomocou príkazu: „sudo nano /etc/hosts“. Každý doméne, ktorú sme nastavili v A záznamoch, priradíme lokálnu IP adresu.

¹² MINASI, M.: Windows XP Professional. Praha : Grada Publishing, 2002. s.790.



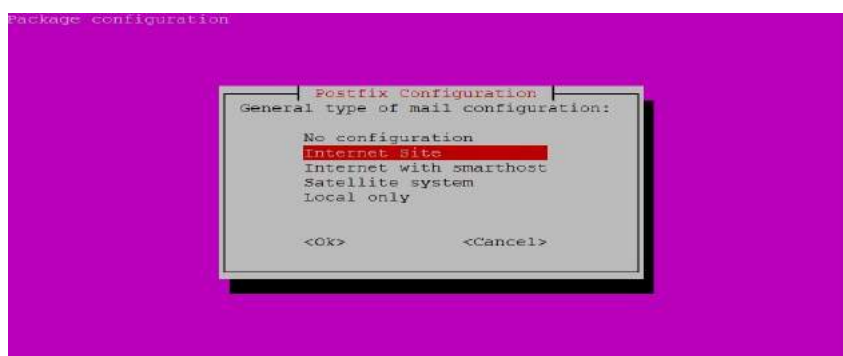
```
root@admin: ~
GNU nano 2.5.3 File: /etc/hosts Modified
127.0.0.1 localhost
127.0.1.1 admin.crew.sk admin
127.0.0.1 chuck-norris.eu
127.0.0.1 admin.chuck-norris.eu
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Obrázok 5: Editácia súboru hosts. Zdroj: vlastné spracovanie.

4.2 Konfigurácia postfix-u

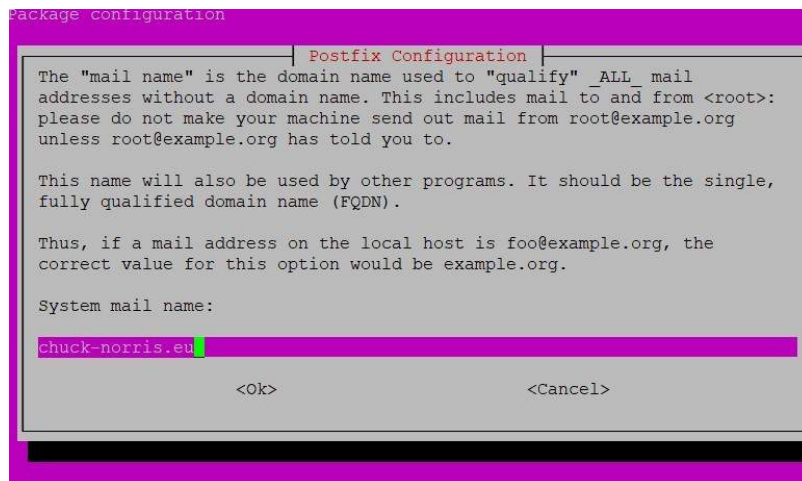
Postfix ako taký už je vopred nainštalovaný. Preto je ho potrebné prekonfigurovať, a to pomocou „sudo dpkg-reconfigure postfix“.

Následne vyskočí okno s otázkou, aký typ servera chceme použiť. Keďže chceme používať plne funkčný e-mailový server prostredníctvom Internetu, vyberieme druhú možnosť.



Obrázok 6: Nastavenie postfix-u. Zdroj: vlastné spracovanie.

V nasledujúcom kroku zadáme doménu.

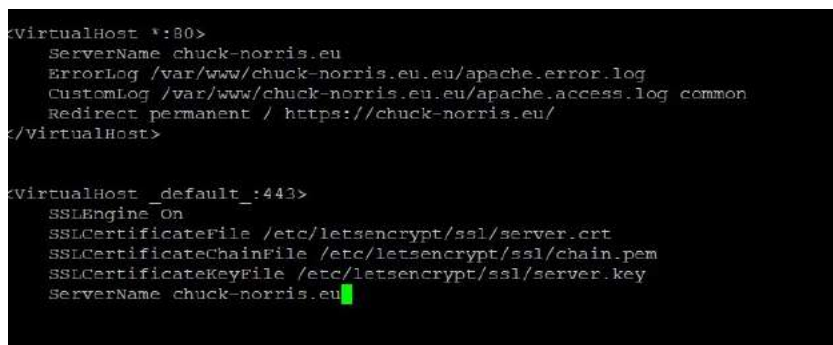


Obrázok 7: Zdávanie domény. Zdroj: vlastné spracovanie.

Taktiež je nevyhnutné otvoriť port 25 pre správne fungovanie postfixu. To zariadime pomocou príkazu: „sudo ufw allow 25/tcp“.

4.3 Konfigurácia Apache web serveru a zaobstaranie SSL certifikátu

Apache server je už predinštalovaný spolu s Ubuntu, takže ho nie je potrebné inštalovať. Šifrovaním človek nikdy nič nepokazí. Preto je dobré si zaobstarat' SSL certifikát. Ten zaobstaráme pomocou aplikácie „Certbot“. Aplikáciu Cerbot nainštalujeme pomocou príkazu „sudo apt install certbot“. Certifikát zaobstaráme pomocou príkazu: „sudo certbot --apache --agree-tos --redirect --hsts --staple-ocsp --email admin@chuck-norris.eu -d admin.chuck-norris.eu“. Po vygenerovaní cerifikátu je potrebné nastaviť apache webserver. Nastavenie stránok otvoríme pomocou „sudo nano /etc/apache2/sites-available/000-default.conf“. Do apache konfiguračného súboru zadáme aj SSL certifikát.



Obrázok 8: Konfigurácia Apache2. Zdroj: vlastné spracovanie.

4.4 Nastavenie SSL certifikátu v postfix-e

Teraz je potrebné postfix nakonfigurovať tak, aby dokázal odosielať zašifrované správy. Konfiguračný súbor si otvoríme pomocou príkazu: „sudo nano /etc/postfix/main.cf“. Zadáme cestu k certifikátu. Zmenu vykonáme pomocou „sudo postfix reload“.

```
# TLS parameters

smtpd_tls_cert_file=/etc/letsencrypt/live/admin.chuck-norris.eu/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/admin.chuck-norris.eu/privkey.pem
smtpd_tls_security_level = may
smtpd_tls_protocols = !SSLv2, !SSLv3 !TLSv1
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache

smtpd_use_tls=yes
```

Obrázok 9: Implementácia SSL v postfix-e. Zdroj: vlastné spracovanie

4.5 Inštalácia Dovecot-u

Dovecot a potrebnú IMAP knižnicu nainštalujeme pomocou príkazu „sudo apt install dovecot-core dovecot-imapd“. Inštaláciu otestujeme pomocou príkazu: „sudo dovecot – version“. Výstup je: „2.2.22 (fe789d2)“ tzn. dovecot je nainštalovaný a beží. Teraz je potrebné otvoriť porty nevyhnutné na prevádzku, a to port 80, 8080, 587, 443, 143, 465, 993, 25, 110, 995, . To zabezpečíme pomocou rady príkazov:

- sudo ufw allow 80/tcp
- sudo ufw allow 8080/tc
- sudo ufw allow 587/tcp
- sudo ufw allow 443/tcp
- sudo ufw allow 143/tcp
- sudo ufw allow 465/tcp
- sudo ufw allow 993/tc
- sudo ufw allow 25/tc
- sudo ufw allow 110/tc
- sudo ufw allow 995/tc

Každý z týchto portov je používaný aplikáciami na špecifické využitie.

Port 80 je natívny http port.

Port 8080 je alternatívny http port.

Port 587 je port primárne používaný emailovými agentmi na odchádzajúcu poštu.

Port 443 je natívny port pre šifrovaný http protokol (https).

Port 143 je natívny IMAP port pre nešifrovanú poštu.

Port 465 je port používaný na odosielanie šifrovanej pošty.

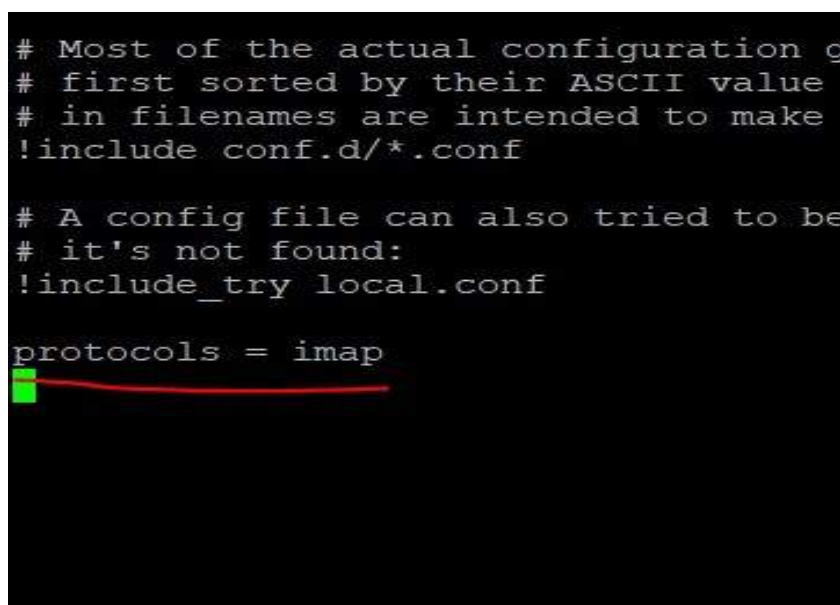
Port 993 je natívny IMAP port pre šifrovanú poštu.

Port 25 je natívny port pre SMTP nešifrovanú komunikáciu.

Port 110 je natívny port pre POP3 nešifrovanú komunikáciu.

Port 995 je natívny port pre POP3 šifrovanú komunikáciu.

Následne je potrebné dovecot nakonfigurovať tak, aby prijímal IMAP protokol a to pomocou „sudo nano /etc/dovecot/dovecot.conf“, kde na koniec pridáme „protocols = imap“.



```
# Most of the actual configuration of dovecot is done in
# first sorted by their ASCII value
# in filenames are intended to make
!include conf.d/*.conf

# A config file can also be tried to be included, if
# it's not found:
!include_try local.conf

protocols = imap
```

Obrázok 10: Konfigurácia dovecot-u. Zdroj: vlastné spracovanie.

Aj Dovecot potrebuje nastaviť SSL certifikát. Konfiguračný súbor otvoríme pomocou „sudo nano /etc/dovecot/conf.d/10-ssl.conf“ a zadáme príkazy nevyhnutne potrebné na správne fungovanie.

```
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = required

ssl_cert = </etc/letsencrypt/live/admin.chuck-norris.eu/fullchain.pem
ssl_key = </etc/letsencrypt/live/admin.chuck-norris.eu/privkey.pem
```

Obrázok 11: Implementácia SSL v dovecot-u. Zdroj: vlastné spracovanie.

4.6 Konfigurácia SPF, DMARC a DKIM

Ako prvé nakonfigurujeme SPF a to tak, že pridáme TXT DNS záznam na doménu s textom „v=spf1 mx ~all“.

Název:	<input type="text" value="admin"/>	.chuck-norris.eu
TTL:	<input type="text" value="1800"/>	
Typ:	<input type="text" value="A"/>	
Data:	<input type="text" value="v=spf1 mx ~all"/>	
<input type="button" value="Uložiť záznam"/>		

Obrázok 12: SPF v DNS. Zdroj: vlastné spracovanie.

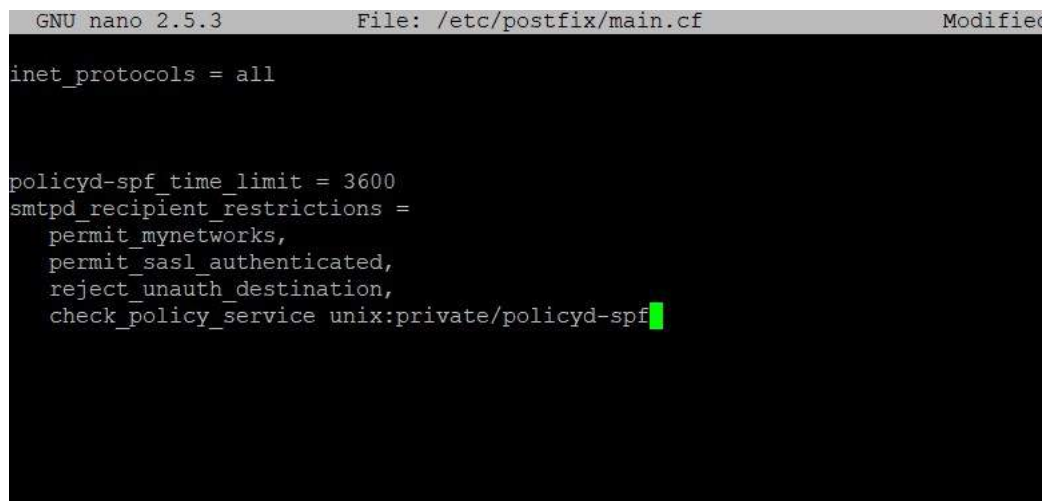
Teraz SPF nainštalujeme na server, a to príkazom: „sudo apt install postfix-policyd-spf-python“. Následne je potrebné SPF nastaviť aj v Postfix-e, a to otvorením konfiguračného súboru pomocou príkazu: „sudo nano /etc/postfix/master.cf“ s tým, že na koniec súboru zadáme príkaz potrebný na akceptáciu SPF.

```
policyd-spf unix - n n - 0 spawn
user=policyd-spf argv=/usr/bin/policyd-spf
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ _ Go To Line

Obrázok 13: Implementácia SPF do postfixu. Zdroj: vlastné spracovanie.

Ďalej je potrebné nastaviť hlavný konfiguračný súbor postfix-u. Ten otvoríme pomocou „sudo nano /etc/postfix/main.cf“ a na jeho úplný koniec zadáme potrebné príkazy.

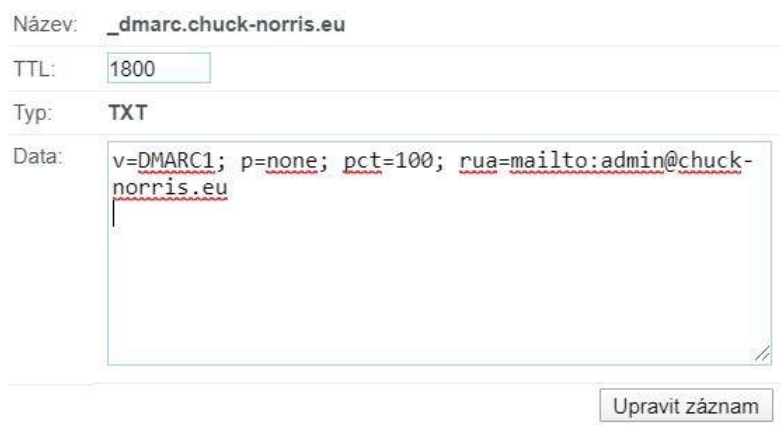


```
GNU nano 2.5.3 File: /etc/postfix/main.cf Modified
inet_protocols = all

policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_unauth_destination,
  check_policy_service unix:private/policyd-spf
```

Obrázok 14: Implementácia SPF do postfixu 2. Zdroj: vlastné spracovanie.

Postfix reštartujeme pomocou „sudo service postfix restart“. Po úspešnej konfigurácii SPF je potrebné vytvoriť DMARC záznam. Ten vytvoríme ako TXT DNS záznam.



Název:	<u>_dmarc.chuck-norris.eu</u>
TTL:	1800
Typ:	TXT
Data:	v=DMARC1; p=none; pct=100; rua=mailto:admin@chuck-norris.eu

Upravit záznam

Obrázok 15: Implementácia DMARC záznamu. Zdroj: vlastné spracovanie.

Pre zabezpečenie DKIM podpisu využijeme aplikáciu „OPEN-DKIM“. Tú nainštalujeme pomocou príkazu: „sudo apt install opendkim opendkim-tools“. Následne je potrebné pridať postfix pod DKIM. To zariadime tak, že užívateľa postfix pridáme do skupiny opendkim. To zariadime pomocou príkazu: „sudo gpasswd -a postfix opendkim“. Následne

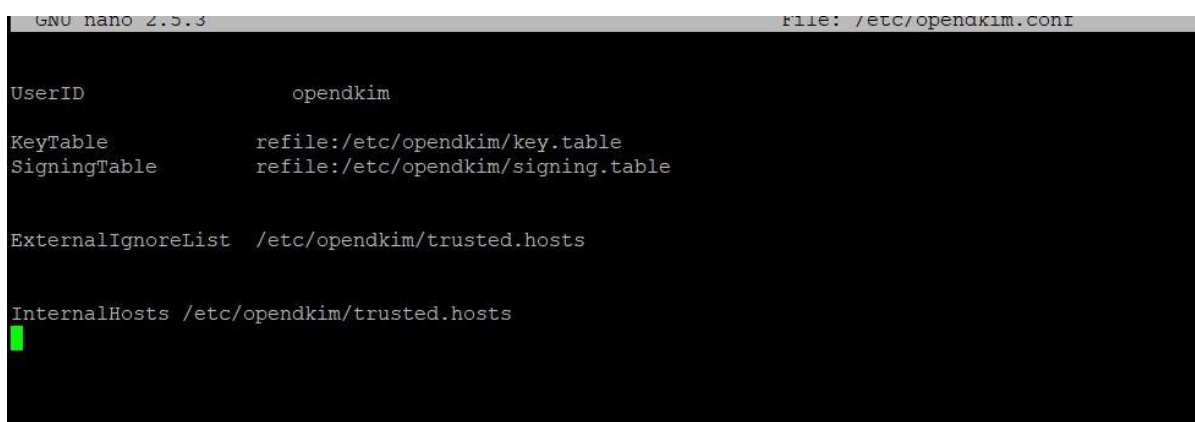
nastavíme konfiguračný súbor „opendkim.conf“ a to pomocou príkazu: „sudo nano /etc/opendkim.conf“. Do konfiguračného súboru zadáme:

Canonicalization simple

Mode sv

SubDomains no

Následne na koniec konfiguračného súboru definujem cestu k doménam, kľúčom a užívateľskú skupinu.



```
GNU nano 2.5.3 file: /etc/opendkim.conf
UserID                opendkim
KeyTable              refile:/etc/opendkim/key.table
SigningTable          refile:/etc/opendkim/signing.table

ExternalIgnoreList    /etc/opendkim/trusted.hosts

InternalHosts         /etc/opendkim/trusted.hosts
```

Obrázok 16: Konfigurácia OpenDKIM. Zdroj: vlastné spracovanie.

Ďalej je nevyhnutné vytvoriť umiestnenia pre OpenDKIM. Ako prvé vytvoríme koreňovú zložku pre OpenDKIM a to pomocou príkazu:

„sudo mkdir /etc/opendkim“ a zmeníme jej vlastníka pomocou príkazu: „sudo chown -R opendkim:opendkim /etc/opendkim“.

Potom vytvoríme zložku keys v koreňovej zložke opendkim a to pomocou príkazu: „sudo mkdir /etc/opendkim/keys“ a zmeníme zapisovaciu politiku pomocou príkazu: „sudo chmod go-rw /etc/opendkim/keys“.

Ďalej vytvoríme podpisovú tabuľku a to pomocou príkazu: „sudo nano /etc/opendkim/signing.table“.

Do tejto tabuľky zadáme doménu a priradím k nej DNS záznam, ktorý ma vyhľadávať.

```
GNU nano 2.5.3 File: /etc/openssl/signi
*@chuck-norris.eu default._domainkey.chuck-norris.eu
```

Obrázok 17: Implementácia OpenDKIM DNS záznamu. Zdroj: vlastné spracovanie.

Potom vytvoríme tabuľku s kľúčmi a to pomocou príkazu: „sudo nano /etc/openssl/key.table“, do ktorej zapíšeme lokáciu kľúčou.

```
GNU nano 2.5.3 File: /etc/openssl/key.table
default._domainkey.chuck-norris.eu.com chuck-norris.eu:/etc/openssl/keys/chuck-norris.eu/default.private
```

Obrázok 18: Konfigurácia OpenDKIM tabuľky s kľúčmi. Zdroj: vlastné spracovanie.

V neposlednej rade vytvoríme súbor „trusted.hosts“, ktorý definuje adresy a domény, ktoré budú akceptované.

```
GNU nano 2.5.3 File: /etc/openssl/trusted.hosts
127.0.0.1
localhost
*.chuck-norris.eu
```

Obrázok 19: Definovanie dôveryhodných IP adries / domén. Zdroj: vlastné spracovanie.

Teraz je potrebné vygenerovať súkromné kľúče. Najprv im ale musíme vytvoriť umiestnenie. To vykonáme pomocou príkazu: „sudo mkdir /etc/openssl/keys/chuck-norris.eu“. Konkrétne kľúče vygenerujeme pomocou príkazu:

„sudo openssl-genkey -b 2048 -d chuck-norris.eu -D /etc/openssl/keys/chuck-norris.eu -s default -v“.

Následne nastavíme vlastníka kľúčov príkazom: „sudo chown openssl:openssl /etc/openssl/keys/chuck-norris.eu/default.private“. Celý kľúč zadáme do DNS záznamu:

Název:	default._domainkey.chuck-norris.eu
TTL:	1800
Typ:	TXT
Data:	v=DKIM1;k=rsa;p=MIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwUFkhrEvgnjNTpIB/xM+zs3L+hcmJL+qRVxqBIq7h7EuF3+lG9c+hQ5EkQTKayS9ij1xQGLBltjuIfzdLQrBnjZ+vmqBvxZxMDPTiEFL2ghiG70+0eQMOC538s6+2lh2/XZi/ZR3FulZsyV9jnT0BVBMN4QJSryGyn2jxwiiWyFVyCoR5ZQfg6QyLEjRh9GKFbNKsHKOjXY4XJ40KhWPwepN7FYVDMdE04mA w12HILO10Bowy1i2GSTnYprsIRMLFkeVLKqWpzD7DnwmihA2 VwkytIkVFofhl+bd8g89mti9vRPEpCuHg8BUj2Q2wpLyrrl6
Upraviť záznam	

Obrázok 20: Zadanie DNS záznamu s DKIM kľúčom. Zdroj: vlastné spracovanie.

Ako posledný krok je zapotreby prepojiť DKIM s postfix-om. Otvoríme konfiguračný súbor postfixu cez príkaz „sudo nano /etc/postfix/main.cf“ a za sekciu „smtpd_recipient_restriction“ pridáme cestu k DKIM.

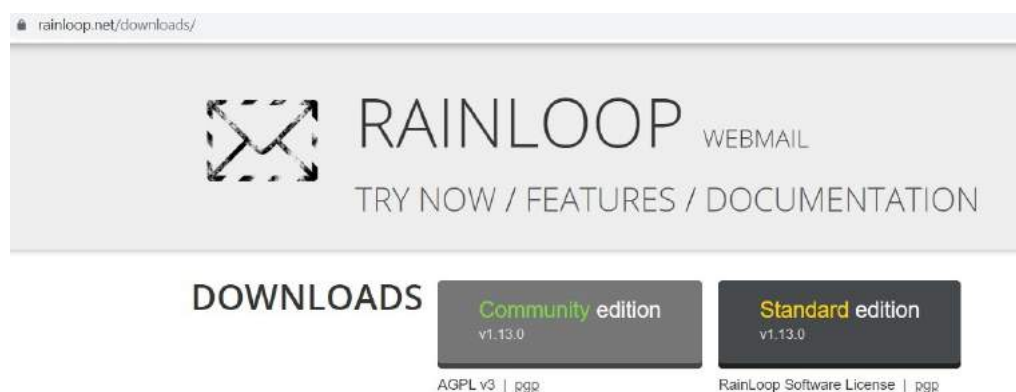
```
GNU nano 2.5.3
smtpd_recipient_restriction = accept
smtpd_protocol = 6
smtpd_milters = local:/openssl/openssl.sock
non_smtpd_milters = $smtpd_milters
```

Obrázok 21: Prepojenie DKIM s Postfix-om. Zdroj: vlastné spracovanie.

Po úspešnej konfigurácii reštartujeme OpenDKIM aj Postfix a to cez príkaz:
„sudo systemctl restart opendkim postfix“.

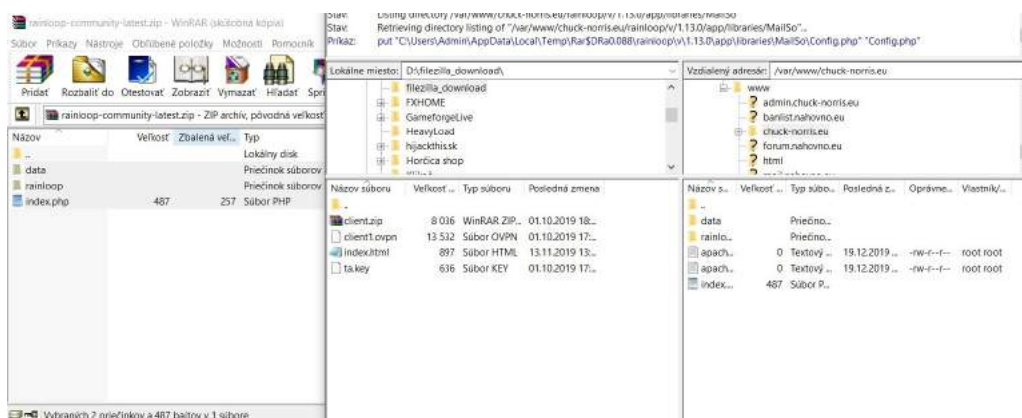
4.7 Inštalácia webového klienta

Ako webového klienta budeme použiť RainLoop. RainLoop stiahneme z oficiálnej stránky, zo sekcie „downloads“, kde vyberieme komunitnú edíciu, pre prípad budúceho módovania.



Obrázok 22: Získanie mailového klienta. Zdroj: vlastné spracovanie.

Inštalčný balíček RainLoop webového klienta nahráme do koreňového priečinku webu „chuck-norris.eu“.



Obrázok 23: Inštalácia mailového klienta pomocou FTP. Zdroj: vlastné spracovanie.

Následne sa prihlásime do administrátorského panelu, kde nastavíme prihlasovaciu doménu.

The screenshot shows a web interface for adding a domain. The title is "Pridať doménu 'chuck-norris.eu'". There is a text input field for the domain name containing "chuck-norris.eu". A message box states: "This domain configuration will allow you to work with *@chuck-norris.eu email addresses." Below this, there are two columns for IMAP and SMTP settings. The IMAP section has a "Server" field with "admin.chuck-norris.eu" and a "Port" field with "143". The "Bezpečné" dropdown is set to "STARTTLS". There is an unchecked checkbox for "Použiť skrátené prihlásenie" and a link for "Nastavenia Sieve (beta)". The SMTP section has a "Server" field with "admin.chuck-norris.eu" and a "Port" field with "587". The "Bezpečné" dropdown is set to "STARTTLS". There is an unchecked checkbox for "Použiť skrátené prihlásenie", a checked checkbox for "Použiť overenie", and an unchecked checkbox for "Použiť php mail() funkciu (beta)". At the bottom, there are buttons for "Test", "Zoznam povolených", "Zatvoriť", and "Pridať".

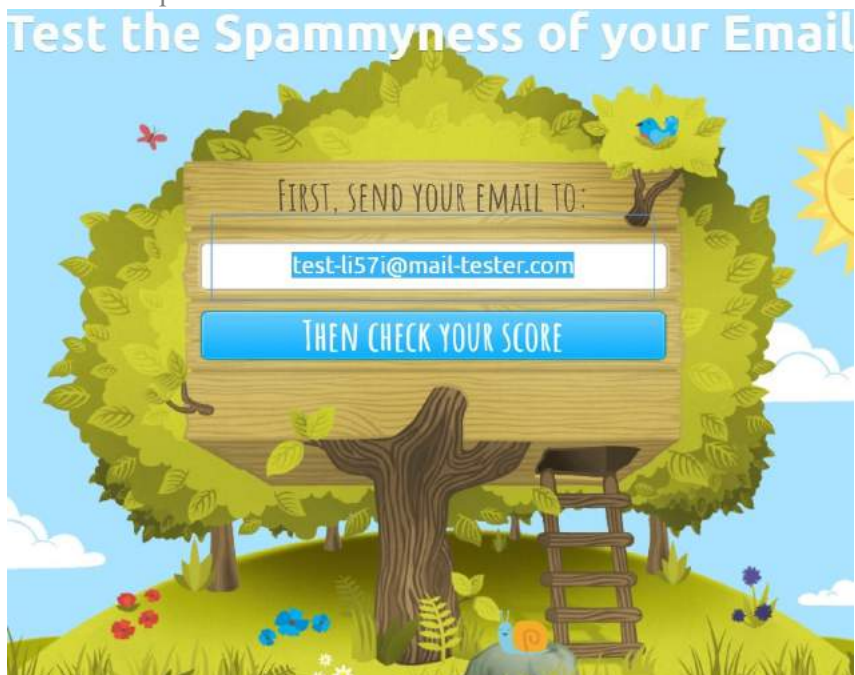
Obrázok 24: Zadanie mail servera do mailového klienta. Zdroj: vlastné spracovanie.

Teraz je potreba vytvoriť užívateľa. Toho vytvoríme pomocou príkazu: „sudo adduser gmail“. Po úspešnom pridaní užívateľa sa prihlásime.

4.8 Testovanie e-mailovej adresy

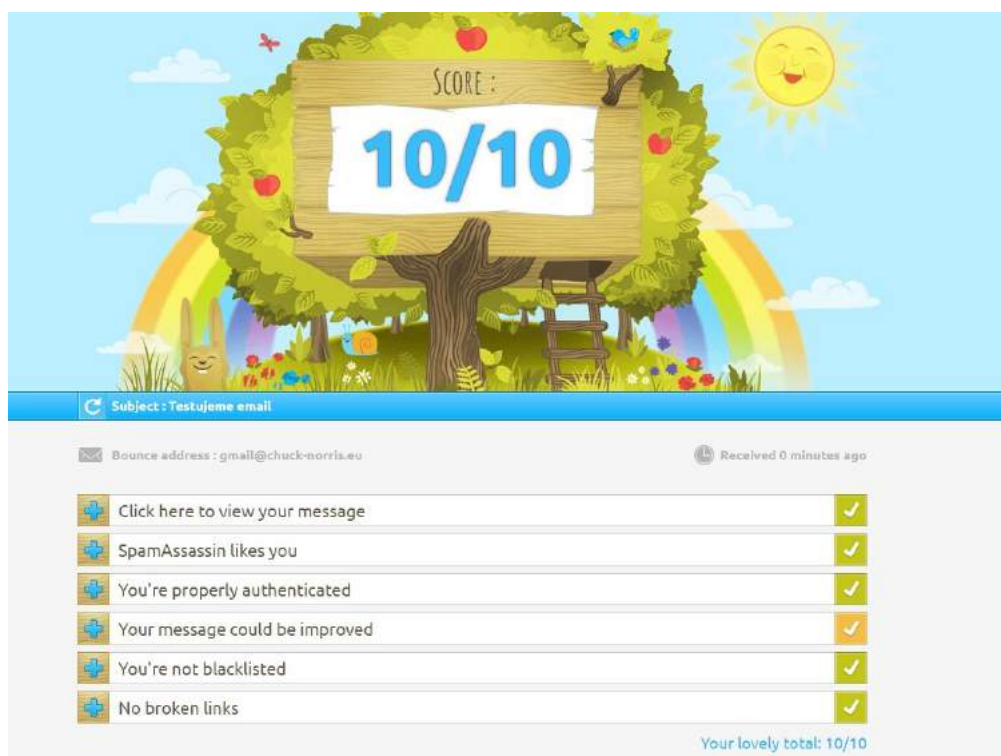
Mail otestujeme cez službu „mail-tester.com“.

Mail-tester.com je opensource freemium služba zaoberajúca sa hlavne testovaním emailových serverov a doplnkom k nim. Funguje na jednoduchom princípe, a to tak, že vygeneruje náhodnú emailovú schránku, na ktorú ich klient odošle správu, ktorú následne služba oboduje na stupnici od 0 do 10. Pokiaľ má človek na prvý pohľad bezproblémový server, služba ho oboduje maximálnym počtom bodov.



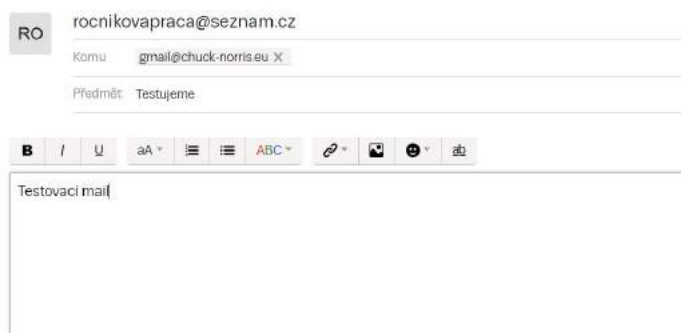
Obrázok 25: Testovanie mailu. Zdroj: vlastné spracovanie.

Zašleme email na zadanú adresu.



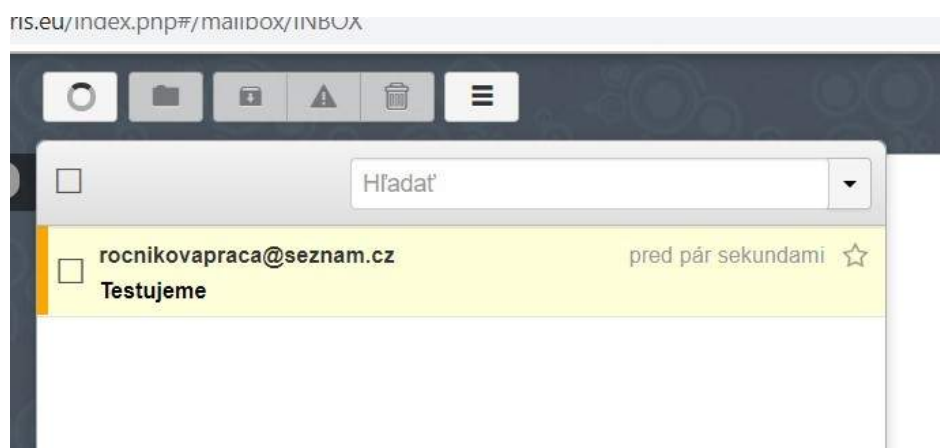
Obrázok 26: Výsledok testu. Zdroj: vlastné spracovanie.

Mail obdržal plné skóre, to znamená, že SSL,DKIM,SPF,DMARC atp. je nastavené správne. Teraz je najvyšší čas odskúšať mail v praxi. Vytvorili sme si testovací e-mail v službe seznam.cz. Ako prvé odskúšame príjem správ, to znamená, že z mailovej adresy „rocnikovapraca@seznam.cz „ odošleme správu na „gmail@chuck-norris.eu“.



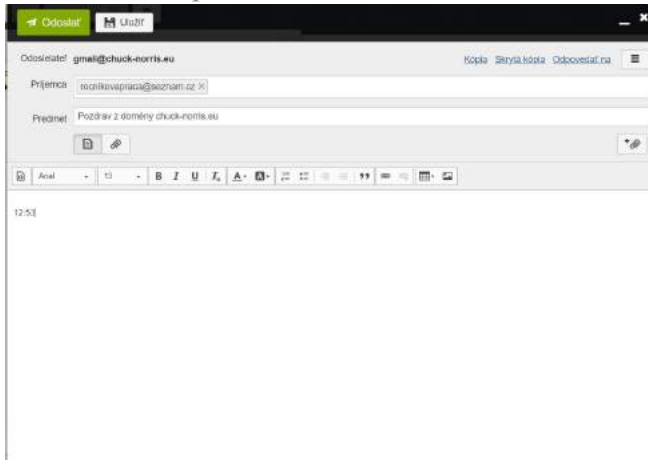
Obrázok 27:Test príjmu správ. Zdroj: vlastné spracovanie.

Následne skontrolujeme, či email úspšne dorazil. A áno, skutočne dorazil.

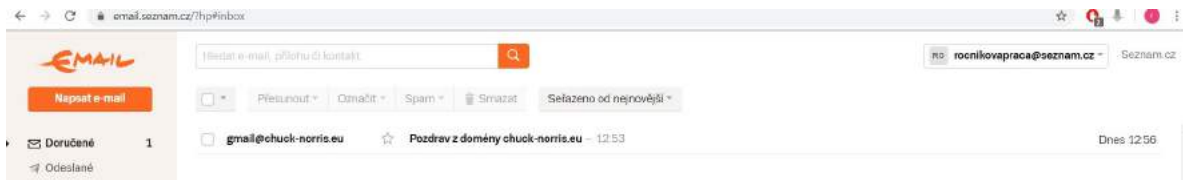


Obrázok 28:Kontrola príjmu správ. Zdroj: vlastné spracovanie

Teraz to odtestujeme opačne, zašleme správu z „gmail@chuck-norris.eu“ na adresu „rocnikovapraca@seznam.cz“.



Obrázok 29: Odosielanie správy. Zdroj: vlastné spracovanie.



Obrázok 30: Kontrola prijatej správy. Zdroj: vlastné spracovanie.

Email úspešne prišiel a čo je hlavné neskončil v SPAMe.

Nasledujúci hlavný faktor, ktorý ale treba otestovať je odozva servera, respektíve odozva jednotlivých funkcionalít, ako napríklad CONNECT, ANSWER, HELLO, TLS, CERT, FROM a podobne. Samo o sebe doba odozvy nemá ani taký význam, ale niektoré emailové anti-spamové systémy môžu identifikovať server s vyššou odozvou ako server nežiadúci. Pre otestovanie odozvy použijeme službu „checktls.com“.

CheckTLS Confidence Factor for "admin.chuck-norris.eu": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
admin.chuck-norris.eu [185.91.116.166:25]	0	OK (108ms)	OK (373ms)	OK (108ms)	OK (108ms)	OK (300ms)	OK (110ms)	OK (122ms)
Average		100%	100%	100%	100%	100%	100%	100%

Obrázok 31: Testovanie odozvy servera. Zdroj: vlastné spracovanie

Testovanie dopadlo v poriadku, hodnoty sú v norme. Server by nemal byť odmietnutý na základe vysokej odozvy.

ZÁVER

Služba elektronickej pošty je v Internete poskytovaná na báze architektúry klient/server. Používateľské prostredie na strane klienta bolo vytvorené prostredníctvom webového e-mailového klienta RainLoop, ktorý využíva protokol IMAP4. Funkcia prenosového agenta je vykonávaná prostredníctvom softvéru Postfix, ktorý je uložený na počítači, ktorý je trvalo v prevádzke, aby bolo možné správu vždy doručiť tzn. na serveri.

Náklady na virtuálny privátny server (VPS) sú nižšie, ako náklady na prevádzku vlastného fyzického serveru, a preto bol pre našu prácu použitý virtuálny privátny server od poskytovateľa ORELSOFT.cz. Zvolili sme si operačný systém Ubuntu 16.04. Ďalšou požiadavkou bola vlastná doména. Pre potreby tejto práce sme zaregistrovali doménu chuck-norris.eu u poskytovateľa Wedos.sk.

V praktickej časti tejto práce sme zrealizovali vlastný e-mailový server pre osobnú potrebu alebo pre malé firmy, ktorý zodpovedá aktuálnym trendom v oblasti zabezpečenia. Vytvorený vlastný e-mailový server je plne funkčný, a je ho možné využívať na prenos správ.

ZOZNAM POUŽITEJ LITERATÚRY

Knižné zdroje:

1. HORÁK, J.:Bezpečnosť malých počítačových sítí (praktické rady a návody). Praha : Grada Publishing, 2003. 200 s. ISBN 80-247-0663-6.
2. MINASI,M.: Windows XP Professional. Praha : Grada Publishing, 2002. 800s. ISBN 80-247-0326-2
3. ZÁVODNÝ, P.: Počítačové siete v hospodárskej praxi. Bratislava : Ekonóm, 2005. 234 s. ISBN 80-225-1979-0.

Internetové zdroje:

1. A Technology Market Research Fir. [online]. [cit. 2019.11.15]. Dostupné na: <<http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf>>.
2. DNS záznamy. [online]. [cit. 2019.11.19]. Dostupné na: <<https://www.websupport.sk/support/kb-categories/dns-zaznamy/>>.
3. DOVECOT. [online]. [cit. 2019.11.13]. Dostupné na: <<https://www.dovecot.org/>>.
4. HTTPD - Apache2 Web Server. [online]. [cit. 2019.11.25]. Dostupné na: <<https://help.ubuntu.com/lts/serverguide/httpd.html> >.
5. RAINLOOP FEATURES. [online]. [cit. 2019.11.29]. Dostupné na: <<https://www.rainloop.net/features/>>.
6. What is DKIM?. [online]. [cit. 2019.11.20]. Dostupné na: <<https://www.dmarcanalyzer.com/dkim/>>.
7. What is SSL?. [online]. [cit. 2019.11.22]. Dostupné na: <<https://www.ssl.com/faqs/faq-what-is-ssl/>>.