

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství (PEF)



Bakalářská práce

Linuxový server jako antispamový filter

Martin Kolman

© 2019 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Kolman

Informatika

Název práce

Linuxový server jako antispamový filter

Název anglicky

Linux server as antispam filter

Cíle práce

Hlavním cílem této práce bude implementace antispamového serveru na linuxové platformě. Server bude sloužit jako doplněk k existujícím serverům Microsoft Exchange, kterým by měl ulehčit práci. Hlavní funkcionalitu serveru bude zajišťovat sendmail ve spolupráci se spamassassine a clamav. Dílčími cíli této práce budou DNS a webový server. Cílem této práce bude fungující a skutečný server.

Metodika

Nejdříve bude proveden výběr vhodného hardware pro dané řešení s ohledem na plánovanou zátěž. Bude použita linuxová distribuce Debian s emailovým klientem sendmail. Tento klient bude rozšířen o antispamovou ochranu spamassassin a antivirové řešení clamav. Dalšími implementovanými prvky serveru budou DNS a webový server.

V praktické části práce bude popsán celý implementační proces všech služeb a jejich následné ladění, monitorování funkčního systému a zátěžové testy.

Doporučený rozsah práce

30-40 stran

Klíčová slova

Linux, debian, mailserver, sendmail, spamassassin, reversní proxy, email, clamav

Doporučené zdroje informací

KAMENÍK, P. Příkazový řádek v Linuxu. Praha: Computer Press, 2011. ISBN 9788025128190

Sendmail: konfigurace poštovního serveru [online], [cit. 2018-6-6], dostupné z:

<https://www.root.cz/clanky/sendmail-konfigurace-postovniho-serveru/>

SHAH, Steve. Administrace systému Linux: překlad čtvrtého vydání. 1. vyd. Praha: Grada, 2007, ISBN 978-80-247-1694-7.

SCHRODER, Carla. Linux Kuchařka administrátora sítě: první vydání, Computer Press, a.s., 2009, ISBN 978-80-251-2407-9

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 24. 1. 2019

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 1. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 20. 02. 2019

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci Linuxový server jako antispamový filter jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 4.3.2019

Poděkování

Rád bych touto cestou poděkoval Ing. Markovi Píckovi, Ph.D. za pomoc, trpělivost a odborné vedení této bakalářské práce. Dále bych rád poděkoval své manželce Mgr. Kamile Kolmanové za veškerou pomoc, jakožto i hlídání našich dvou dětí, abych mohl studovat a psát tuto práci. Také bych rád poděkoval svým dvěma dcerám Magdaleně a Sáře za jejich trpělivost a pochopení.

Linuxový server jako antispamový filter

Abstrakt

Cílem práce bylo nakonfigurovat antispamový server, který ulehčí práci přetíženým Exchange serverům. Jako takový by měl být schopen odfiltrovat většinu spamových emailů, které do společnosti přijdou a následně je roz distribuovat na vnitřní emailové servery. Dalšími úkoly této práce je DNS, web server a následně celé řešení otestovat.

V teoretické části byla popsána historie Linuxu i GNU, co je to email a jeho historie, spam a jak ho dělíme, Apache SpamAssassin, SPF milter, DNS, root servery, zabezpečení pomocí DNSSEC, DNS Cache poisoning, vývoj aplikace APACHE, reverzní proxy a performance webového serveru.

V praktické části byl nejprve vybrán vhodný hardware s ohledem na zatížení serveru. Byl vybrán server sendmail a jeho nezbytné součásti. Jako antivirová ochrana emailů byl nainstalován antivir ClamAV, antispam Apache SpamAssassin a SPM Milter smf-spf. Jako další krok byl vybrán Bind jako DNS server a Apache jako webový server. Dále byly krok po kroku popsány změny konfiguračních souborů jednotlivých prvků. Toto řešení bylo otestováno s ohledem na bezpečnost a funkcionalitu.

Klíčová slova: Linux, debian, mailserver, sendmail, spamassassin, reversní proxy, email, clamav, bind, apache, spf

Linux as antispam filter

Abstract

The aim of the thesis was to configure an antispam server to help already overloaded Exchange servers. It should be able to filter out most of the spam emails that come to the company and distribute clean emails to internal email servers. Other tasks of this work are setting up DNS, web server and then testing the whole solution.

Theoretical part is focused on the history of Linux and GNU, what is an email and its history, spam, Apache SpamAssassin, SPF Milter, DNS description, root servers, DNSSEC security, DNS Cache poisoning, APACHE development, reverse proxy and web server performance.

In the practical part, the appropriate hardware was chosen with respect to server load. The sendmail server has been selected with necessary components such as Antivirus ClamAV, Apache SpamAssassin as antispam and SPF Milter smf-spf. As a next step, Bind was selected as a DNS server and Apache as a Web server. Changes to the configuration files of each service were described step by step and the whole solution has been tested for security and functionality.

Keywords: Linux, debian, mailserver, sendmail, spamassassin, reverse proxy, email, clamav, bind, apache, spf

Obsah

1 Úvod.....	12
2 Cíl práce a metodika	13
2.1 Cíl práce	13
2.2 Metodika.....	13
3 Přehled související problematiky	14
3.1 Historie Linuxu	14
3.2 Historie GNU	14
3.3 E-Mail.....	15
3.3.1 Omezení velikosti emailové přílohy	15
3.3.2 SPAM.....	15
3.3.2.1 Email spoofing – falšování emailové hlavičky.....	15
3.3.2.2 HOAX.....	16
3.3.2.3 Obchodní nabídky.....	16
3.3.2.4 Viry	16
3.3.3 SpamAssassin	17
3.3.4 ClamAV	17
3.3.5 SPF Milter smf-spf.....	17
3.4 DNS.....	18
3.4.1 ROOT servery	18
3.4.2 Zabezpečení DNS - DNSSEC.....	20
3.4.3 DNS Cache Poisoning.....	20
3.5 APACHE	20
3.5.1 Reverzní proxy	21
3.5.2 Performance	21
4 Vlastní práce	23
4.1 Volba vhodného řešení.....	23
4.1.1 Výběr linuxové distribuce.....	23
4.1.2 Zvolení vhodného hardware	23
4.1.3 Výběr vhodného řešení	24
4.1.4 Obhájení konečné volby	25
4.1.5 Popis fungování jednotlivých prvků	25
4.2 Instalační proces krok po kroku	26
4.3 Instalace systému.....	26
4.3.1 Základní konfigurace a instalace doplňků	30
4.3.2 Konfigurace sítě	31
4.3.3 Instalace a nastavení SSH	32

4.4	Instalace sendmail	33
4.4.1	Instalace ClamAV a Apache SpamAssassin.....	34
4.4.2	Instalace SPF Milteru - smf-spf.....	34
4.4.2.1	Konfigurace a prvotní testování ClamAV	35
4.4.2.2	Počáteční konfigurace Apache SpamAssassin	37
4.4.3	Konfigurace SPF Milteru - smf-spf	44
4.4.4	Konfigurace sendmail	45
4.4.4.1	Access.....	45
4.4.4.2	Mailtable.....	48
4.4.4.3	Aktivace modulů a dokončení instalace	48
4.5	Instalace BIND serveru	50
4.5.1	Úprava named.conf.option.....	50
4.5.2	Úprava named.conf.local	51
4.5.3	Příprava domén	54
4.5.4	Konfigurace je rozdělena na následující možnosti nastavení:	55
4.5.5	Podepsání domén	58
4.6	APACHE Server	62
4.6.1	Konfigurace serveru.....	63
4.6.2	Konfigurace serveru pro reversní proxy	63
4.6.3	Vytvoření první serverové konfigurace	64
4.6.4	Aktivace webové prezentace.....	66
4.7	Závěrečné testování.....	67
4.7.1	Testování emailové komunikace:	67
4.7.2	Testování DNS serveru.....	67
4.7.3	Testování Apache serveru.....	68
4.7.4	Testování zabezpečení serveru	68
5	Závěr.....	69
6	Seznam použitých zdrojů	70

Seznam Tabulek:

Tabulka 1, Seznam 13 root serverů pod správou 12. nezávislých společností	19
---	----

Seznam obrázků:

Obr. č. 1, Popis fungování reverzní proxy,	21
Obr. č. 2, Popis fungování celého řešení	25
Obr. č. 3, Úvodní obrázek instalace	27
Obr. č. 4, Instalace – výběr lokace	28
Obr. č. 5, Rozdělení diskového úložiště	29
Obr. č. 6, Výběr sw prvků serveru	30
Obr. č. 7, Popis výsledné konfigurace sítě	32
Obr. č. 8, Výsledek testování služby clamav-daemon	35
Obr. č. 9, Výsledek testování služby clamav-freshclam	36
Obr. č. 10, Výsledek skenování souboru	36
Obr. č. 11, Výsledek podpisu domény	61
Obr. č. 12, Přehled výpisu emailových logů	67

1 Úvod

I když je v současné době na masivním vzestupu instant messaging (IM), je email stále hlavním komunikačním kanálem. I přes neustále klesající tendenci je v mailové komunikaci spam stále silně zastoupen. Díky snahám firem ušetřit na tiskových řešeních je email využíván i pro elektronizaci dokumentů a bezpapírový styk mezi firmami. I to je jeden z důvodů, proč je důležitá snaha o snížení spamu, který přichází do emailových schránek. Jelikož je email jedním z primárních komunikačních prostředků, je nutné monitorovat a vyhodnocovat, co za obsah do firmy přichází, abychom zabránili spamu a podvodným či hoax zprávám. Čím více totiž takovýchto emailů přijmeme, tím větší riziko ztráty pro firmu i jednotlivce hrozí. Nemusí jít o ztrátu pouze finanční, ale i o ztrátu citlivých dat. Útočníkům se může otevřít přístup do firemní sítě k tajným či citlivým informacím společnosti nebo jednotlivce.

Dalšími důležitými prvky jsou DNS a web server, respektive možnost reverzní proxy a tím i využití více serverů schovaných za jedním. Pokud provozujeme agilní prostředí, potřebujeme mít možnost často měnit DNS záznamy pro webové servery, tak abychom mohli pro zákazníky předvádět naše webové produkty. Otevírá to možnost publikovat webové prezentace externě u zákazníka tak, aby si je zákazník mohl v klidu prohlédnout.

Tato práce si ukládá za cíl vytvořit antispamový server, který bude v rámci možností snižovat riziko přijatých spamů. Zároveň zvýší flexibilitu nastavování DNS záznamů a pomocí reverzního proxy serveru směrování webových aplikací z vnitřní sítě na internet.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce bylo vybrání vhodného antispamového řešení k existujícím emailovým Exchange serverům. Server bude dále sloužit jako DNS a webový server. Server musí být stabilní a dostatečně robustní. Výsledkem práce je plně zabezpečený a funkční antispamový server s dodatečnými funkcemi DNS a web serveru pro ostré nasazení v korporátní síti.

2.2 Metodika

Před samotným začátkem instalace serveru je potřeba vybrat vhodné hardwarové řešení a následně nainstalovat vhodnou linuxovou distribuci. V této práci bude vybrána distribuce Debian, jako jedna z takzvaných „rock stable“ distribucí. Dále bude potřeba mít správně nakonfigurovanou síť s povolenými požadovanými porty pro komunikaci. Tím budeme mít připravený server pro instalaci.

Zvolené řešení bude následně instalováno a konfigurováno krok po kroku dle vybraných prvků. Jako zdroj unikátních spamů budou použité již doručené a stále se opakující spamové zprávy.

Po dokončení konfigurace bude ověřena funkcionálníta jednotlivých na sobě nezávislých řešení jejich postupným otestováním. Vždy po úspěšném ověření bude otestována další funkcionálníta serveru. V případě emailového serveru bude otestována nejen funkcionálníta samotného emailového serveru a jeho schopnost přeposlat emailové zprávy na interní emailové servery, ale i bezpečnostních prvků SpamAssassin, smf-spf a ClamAV. Samotné testování DNS serveru bude zaměřeno na korektní odpovědi serveru a pomoc DNSSEC validátoru. V případě serveru Apache budou testovány jednotlivé webové prezentace na dostupnost a důvěryhodnost SSL pomocí validátoru. Dále budou provedeny testy bezpečnosti samotného serveru.

3 Přehled související problematiky

3.1 Historie Linuxu

Linux začal vyvíjet v roce 1991 student University v Helsinkách, Linus Torvald. Za vznik můžeme poděkovat jeho frustraci z licencování tehdejšího operačního systému MINIX, který byl určen pouze ke školním účelům. Díky tomu začal vyvíjet vlastní jádro operačního systému, z něhož se později stal Linux Kernel. První verze linuxového jádra ve verzi 0.01 byla uveřejněna na internetu 17. září 1991. Linus původně nechtěl pojmenovat svůj projekt jako linux, protože mu to přišlo příliš egoistické a chtěl pro něj název, který sám vytvořil a to „Freax“, což bylo spojení tří významů „free“ jako volný, „freak“ jako bláznivý či podivný a „x“ jako unix. Při požadavku o upload na FTP server (ftp.funet.fi) se tehdejšímu Torvaldovu spolupracovníkovi a dobrovolnému administrátoru FTP serveru Ari Lemmke nezdál název. Proto místo „Freax“ vytvořil složku s názvem „Linux“, aniž by to s Torvaldem jakkoliv konzultoval. Torvald posléze sám uznal, že název Linux byla správná volba. I přes spoustu nedostatků, které tento první systém měl, začal dostávat emailem spousty podnětů, oprav a zdrojových kódů. Torvald jádro dále vyvíjel a současně do něj začal začleňovat příspěvky od ostatních. Vzápětí publikoval zdrojové kódy a další verze již byla publikována v říjnu téhož roku. Od toho okamžiku se na vývoji jádra podíleli tisíce developerů z celého světa. Velice brzy, předběhl Linux ve vývoji svůj vzor MINIX. Z projektu GNU využil Linux spoustu nástrojů používaných na příkazovém řádku, jako například shell bash, kompilátor GCC a další. Linux nikdy nebyl součástí GNU, i když jeho jádro používá licenci GPLv2. [4]

3.2 Historie GNU

V roce 1989 byla Richardem Stallmanem sepsána Licence GPL pro použití s programy poskytovanými jako projekt GNU. Původní GPL byla založena na unifikaci licencí používaných pro časté verze programů, které sice obsahovaly prvky moderního GPL, nicméně byly specifické pro jednotlivé programy. Díky tomu byly nekompatibilní i přes to, že šlo o stejné licence. Důležité rozhodnutí ohledně důvěry v GPL přišlo v roce 1992 od Linuse Torvalda. Použil tuto licenci pro linuxové jádro přechodem z dřívější licence, která mu zakazovala komerční využití. GNU se neomezuje pouze na operační systém. Jeho cílem je využití maximálního množství software pro uživatele, což zahrnuje i aplikační software. [5]

3.3 E-Mail

E-Mail (email) neboli „*Electronic mail*“ je způsob výměny zpráv mezi lidmi, kteří využívají elektronické zařízení. Tuto formu komunikace vymyslel v roce 1960 Ray Tomlinson. První komunikace byla velice omezená a až v polovině 70. let dostala emailová komunikace formu, jakou známe dnes. Dřívější emailová komunikace dokonce vyžadovala, aby oba, jak odesílatel, tak příjemce, byli online, jak je běžné v „instant messaging“. Současná emailová komunikace nicméně již funguje na principu „ulož a přepošli“. Emailový server akceptuje, přepošle, doručí a uloží emailovou zprávu. Díky této posloupnosti není potřeba, aby uživatel nebo jeho počítač byli online.^[16]

3.3.1 Omezení velikosti emailové přílohy

Emailové zprávy mohou obsahovat jednu nebo i více příloh. V principu nejsou žádné technické restrikce pro počet příloh nebo velikost přílohy. Nicméně v praxi jistá omezení jsou, ať již na straně emailových klientů, serverů nebo poskytovatelů internetu. Nejčastěji se setkáváme s limitací velikosti na 25MB pro veřejné emailové servery nebo menší, které jsou častější v komerční sféře.

3.3.2 SPAM

Spam je masové šíření nevyžádaného sdělení napříč internetem. Dříve se jednalo výhradně o nevyžádané reklamní emaily, nicméně postupem času tento fenomén postihl i další druhy internetové komunikace, jako jsou diskuzní fóra, komentáře nebo instant messaging. V roce 2018 dosahovalo množství emailového spamu cca 53,5%^[6] z celkového množství emailů. Nejčastěji^[7] jsou zastoupena farmaceutika a seznamky. V současné době je nejčastější zemí původu USA, následována Čínou a Ruskem.

Problémem je i registrace uživatelů na bezpočet webových stránek, kde uvádějí svojí emailovou adresu. Tyto databáze uživatelů mohou být ukradeny, prodány nebo rovnou použity k rozeslání reklamy, hoaxu či nevyžádaných nabídek.

3.3.2.1 Email spoofing – falšování emailové hlavičky

Email spoofing je takový druh zprávy, který se tváří jako zpráva od důvěryhodného zdroje. Což znamená, že se odesílatel snaží vypadat jako někdo jiný. Kupříkladu jako bankovní instituce, známá společnost, ale i třeba kolega z práce. Spamové, ale i phishingové emaily zpravidla používají spoofing ke snaze o oklamání příjemce

o pravdivosti zprávy. V některých případech se může jednat pouze o žert, nicméně v drtivé většině případů se jedná o podvod ať již jednotlivce, společnosti nebo organizované skupiny. Příkladem může být žádost o platbu na neznámý účet, ověření bankovních údajů, přístupu k nějakému účtu, či potvrzení poštovní zásilky.

V těchto případech může být oklamání uživatelů jednodušší, protože se může jednat například o jedno přehozené písmenko v odkazu, čehož si nemusí všimnout ani zkušený uživatelé. Pokud na daný odkaz kliknou, dostanou se na škodlivé stránky nebo spustí škodlivý virus. ^[18]

3.3.2.2 HOAX

Jedná se většinou o poplašnou zprávu, která je, až na plevelení emailových schránek, neškodná a nemá za účel škodit. Jedná se převážně o rozesílání hromadných emailů obsahujících většinou snahu přesvědčit o vlastní důležitosti (naléhavá pomoc, nové nebezpečí, ...), snížení důvěryhodnosti některých institucí (FBI varuje, banka má problémy, zdravotnická organizace zjistila, utajené informace, o kterých média mlčí, ...). Téměř každá zpráva obsahuje požadavek k rozeslání na co největší počet nových příjemců, což je hnacím motorem těchto lavinových emailů, kdy méně zkušený uživatelé rozesílají a sdílejí. ^[8]

3.3.2.3 Obchodní nabídky

Obchodní nabídky jsou bezproblémové, pokud se opravdu jedná o vyžádanou nabídku. Pokud o ni příjemce nestojí, tak se opět jedná o spam. Většinou je na konci emailu uveden odkaz na odhlášení ze seznamu pro zasílání reklamního sdělení, nicméně ne vždy se jedná o jednoduchou záležitost a odhlášení bývá i poměrně zdlouhavé. Díky přehlcení emailové schránky obchodními nabídkami se tak jedná o škodlivý spam, který může v určitých případech zaplnit emailovou schránku a tím ji paralyzuje do zásahu uživatele.

3.3.2.4 Viry

Jedná se o obecný název pro velké množství druhů škodlivého software, který může být uchován v přílohách emailů, součástí emailových zpráv nebo odkazů uvedených v nich, které se nainstalují po kliknutí na ně nebo již samotným zobrazením.

Následně může nakažený počítač rozesílat nákazu na všechny dostupné emailové adresy z počítače, anebo umožnit útočnickovi přímý přístup do počítače a následně z něj

stahovat data. Dalším případem je zablokování počítače, serveru nebo případně zašifrování dat na discích a požadavky na platbu v bitcoinech pro odblokování počítače či odšifrování dat.

3.3.3 SpamAssassin

Jedná se o aplikaci založenou na perlu a určenou ke kontrole příchozí pošty a detekování spamových zpráv. K tomu mu slouží různé techniky detekce založené na Bayesovské filtrování, DNS kontrole, blacklisty a online databáze. Většina defaultních pravidel je založena na regulárních výrazech, které jsou porovnávány s tělem a hlavičkou zprávy. Pravidla jsou v dokumentaci označována jako testy.

Každý test má svojí, hodnotu skóre, která bude přiřazena ke zprávě, pokud odpovídá kritériím testu. Skóre může mít kladné hodnoty označující „SPAM“ nebo negativní „HAM“. Zpráva je porovnávána se všemi testy a aplikace následně spojuje všechny výsledky do globálního skóre, které je přiřazeno ke zprávě. Čím vyšší skóre, tím větší je pravděpodobnost, že se jedná o spam. ^[9]

3.3.4 ClamAV

Clam AntiVirus (ClamAV) je bezplatný, multiplatformní open-source antivirový software, který je schopný detekovat mnoho typů škodlivého software. Hlavním využitím toho řešení je antivirový scanner na poštovních serverech. Poskytuje řadu nástrojů včetně flexibilního a škálovatelného multi-vláknového daemonu. Dále umožňuje skenování z příkazového řádku a pokročilé nástroje pro automatickou aktualizaci databáze aktualizací.

V roce 2007 společnost Sourcefire, která se specializuje na síťovou bezpečnost, oznámila odkoupení antivirového software ClamAV^[11]. Následně v roce 2013 společnost Cisco^[12] zakoupila společnost Sourcefire, jakožto lídra v oblasti inteligentních řešení počítačového zabezpečení. ^[10]

3.3.5 SPF Milter smf-spf

Tento SPF Milter je lehký, tedy nejméně zatěžující systém, rychlý a velice spolehlivý. Jeho přínosem je implementace technologie SPF (Sender Policy Framework), tedy technologie, která ověřuje odesílatelovu IP adresu s MX záznamy dané domény. Tato kontrola umožňuje určit, které počítače mohou odesílat poštu s adresou odesílatele

této domény. Servery příjemce ověří SPF záznam a odmítnou zprávu od neautorizovaného zdroje ještě před tím, než dojde k samotnému stažení těla zprávy. ^{[19][23]}

3.4 DNS

Domain name server zkráceně DNS je hierarchický decentralizovaný názvový systém pro počítače, služby a další zdroje připojené k internetu nebo domácí síti. Od roku 1985 tvoří jeden ze základních prvků funkčnosti internetu. Jedná se o službu, jejíž hlavním úkolem je převod IP adres na uživatelsky příjemnější textové názvy domén.

Prostor doménových jmen tvoří strom s jedním kořenem. Kořen stromu je tzv. kořenová doména, která se zapisuje jako samostatná tečka. Každý uzel stromu obsahuje informace o doméně, která je mu přidělena a odkazy na podřízené domény. Pod kořenem stromu se tedy hierarchicky nacházejí domény nejvyššího řádu TLD (Top Level Domain). Ty se dále dělí na ccTLD (Country-code TLD), tedy národní domény (.cz, .sk, .eu, .it,...), gTLD (generic TLD) tedy generické domény (.com, .info, .info, ...), patří sem i domény .edu, .gov, .int, .mil, .jobs, které jsou poslední dobou považované za sponzorované gTLD. ^[15]

3.4.1 ROOT servery

Jsou to kořenové servery, které jsou naprosto zásadní pro technickou infrastrukturu celého internetu, na které závisí správnost, spolehlivost a bezpečnost operací na internetu.

Zónový soubor, který tyto servery poskytují všem ostatním DNS serverům, popisuje, kde se nacházejí autoritativní servery pro domény nejvyšší úrovně. Kořenový soubor je poměrně malý a je často měněn. Operátoři root serverů soubor pouze zveřejňují. Vydává a upravuje ho pouze organizace IANA (Internet Assigned Numbers Authority) ^[20].

Název root serveru	Operátor	Počet lokalit.
A	Verisign, Inc.	8

B	Information Sciences Institute	2
C	Cogent Communications	10
D	University of Maryland	151
E	NASA Ames Research Center	194
F	Internet Systems Consortium, Inc.	199
G	U.S. DOD Network Information Center	6
H	U.S. Army Research Lab	2
I	Netnod	68
J	Verisign, Inc.	164
K	RIPE NCC	67
L	ICANN	163
M	WIDE Project	9

Tabulka 1, Seznam 13 root serverů pod správou 12. nezávislých společností^[20]

3.4.2 Zabezpečení DNS - DNSSEC

Z počátku nemělo DNS žádný bezpečnostní prvek. Místo toho byl navržen jako škálovatelný distribuovaný systém. DNSSEC (Domain Name System Security Extension) se pokouší přidat zabezpečení komunikace DNS a zároveň zachovat zpětnou kompatibilitu. DNSSEC zavedl do DNS asymetrickou kryptografii. Držitel domény si pro DNSSEC vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem podepíše technické údaje, které o své doméně do DNS vkládá. Pomocí veřejného klíče uloženého u nadřazené autority domény je možnost ověřit pravost podpisu. DNSSEC tedy snižuje riziko podvrhu známého jako „DNS cache poisoning“ neboli „DNS Spoofing“. [21]

3.4.3 DNS Cache Poisoning

DNS Cache poisoning tedy „otrávení mezi-paměti DNS“ jinak taky známá jako DNS spoofing je typ útoku, který zneužívá zranitelná místa v DNS, aby odklonil legální provoz na falešné servery. Jedním z důvodů, proč je otrávení mezipaměti tak nebezpečné je to, že se může šířit ze serveru na server. Pokud je jeden server takto napaden a ostatní poskytovatelé získají informace z tohoto serveru, tak se tato nákaza bude šířit. To se i stalo v roce 2010, kdy čínský „Great firewall“ utekl z hranic Číny a cenzuroval internet v USA, než se podařilo administrátorům tento problém vyřešit. [22]

3.5 APACHE

Apache HTTP Server, zkráceně nazýván Apache, je bezplatný open-source webový server, který je vydáván pod licenci Apache License 2.0. Apache je tvořen a udržován otevřenou komunitou vývojářů pod záštitou ASF (Apache Software Foundation).

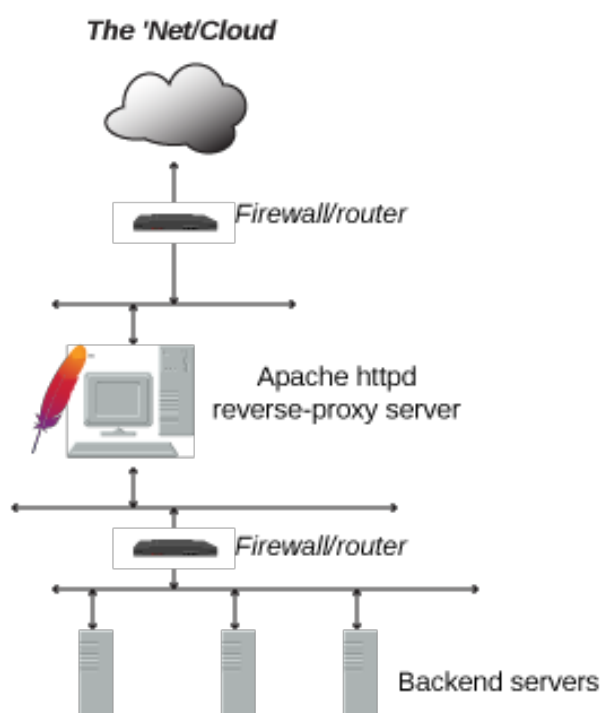
Apache byl původně založený na serveru HTTPd NCSA, vývoj aplikace Apache započal roku 1995 poté, co se práce s kódem NCSA zastavila. Apache tehdy hrál klíčovou úlohu v počátečním růstu WWW (World Wide Web). Apache se stal velice rychle dominantním HTTP serverem.

Převážná většina instancí Apache http Serveru běží na některé z linuxových distribucí. Nicméně současné verze umožňují provoz i na platformě Windows a Unixových distribucích. [17]

3.5.1 Reverzní proxy

Server Apache, kromě standardní funkcionality poskytování webového serveru, umožňuje funkci reverzní proxy. V módu reverzní proxy server nevytváří ani nezpracovává data, ale získává data od jednoho nebo více jiných serverů, které nejsou přímo přístupné z externí sítě. V takovémto případě server získá požadavek od uživatele a ten přesměruje na požadovaný server. Ten vygeneruje požadovanou odpověď a následně jí odešle zpět na server reverzní proxy, který ho zprostředkuje klientovi.

Typické pro takovouto implementaci reverzní proxy je zvýšení zabezpečení, vysoká dostupnost (High Availability - HA), rozdělení zátěže (Load balancer) a centralizovaného systému ověření. Pokud jde o klienta, je tedy jediný poskytovatel server reverzní proxy. Díky tomuto řešení jsou ostatní servery izolované a chráněné z venku od externí sítě.^[24]



Obr. č. 1, Popis fungování reverzní proxy, ^[24]

3.5.2 Performance

Apache ve verzi 2.2 byl pro poskytování statických stránek pomalejší než konkurenční Nginx. K vyřešení tohoto problému vývojáři Apache vytvořili Event MPM (MultiProcessing Module), který umožňuje kombinaci několika procesů a vláken na jeden

proces v asynchronní smyčce. Tato architektura byla implementována ve verzi Apache 2.4.

Apache je navržen tak, aby omezením latence a zvýšením propustnosti jednoduše zpracovával více požadavků, ale zároveň zajistil konzistentní a spolehlivé zpracování požadavků v přiměřených časových rámcích.

4 Vlastní práce

4.1 Volba vhodného řešení

Nejdříve je potřeba si uvědomit, k čemu bude server sloužit a jaká bude jeho primární funkce. Server bude primárně používán jako antispamový a antivirový filter pro emailové zprávy. Jeho sekundární použití bude Bind a Apache server plnící funkci web serveru a aplikačního proxy serveru. Musí být tedy počítáno s takovou HW konfigurací, která bude schopna pojmout všechny funkcionality.

4.1.1 Výběr linuxové distribuce

Vhodných linuxových distribucí pro serverové řešení je několik. Mezi nejrozšířenější zástupce serverových řešení jsou společně s jejich odnožemi Debian (Ubuntu), Redhat (Fedora, Centos), SuSe SLES (OpenSuse). Výsledná volba padla na operační systém Debian ve verzi 9, s kódovým označením „Stretch“. Obsahuje prověřené a stabilní balíčky programů, dostatečné zabezpečení a pravidelné aktualizace. Důvody nasazení této distribuce jsou následující:

- Vysoká stabilita systému.
- Jedná se o open source.
- Velká podpora komunity bez efektu „Vendor Lock“.
- Jednoduchá a intuitivní správa balíčků.
- Dostupné nepřehledné množství software.
- Veliký důraz na bezpečnost.
- Přizpůsobení prostředí - (ostatní linuxové servery mají OS Debian).

4.1.2 Zvolení vhodného hardware

Byla zvolena linuxová distribuce Debian 9, jejíž minimální požadavky jsou nenáročné, RAM (Minimal) 64MB, RAM (Optimal) 256MB, Hard disk 1GB. Debian je možné provozovat jak na x86 tak na x64 bitové architektuře procesorů Intel nebo AMD. Při vlastním výběru hardware serveru je potřeba se zaměřit na požadovanou funkcionalitu a předpokládanou zatížitelnost serveru podle počtu uživatelů a počtu provozovaných funkcionalit serveru. Každá další funkcionalita zvyšuje hardwarové požadavky na server.

Pro naše potřeby byl dostupný server od HPE Proliant DL 120 v provedení rack, osazený jedním 12 jádrovým procesorem Intel Xeon E5 v4 2.2GHz, 16GB RAM, dvěma 1Gb síťovými kartami a čtyřmi 500GB 2,5“ pevnými disky v zapojení RAID 10 s celkovým využitelným prostorem 1TB. RAID 10 byl vybrán pro svoji vyšší rychlost, jelikož přes tento server bude procházet velké množství emailů. Tím pádem bude potřeba vyšší rychlost na discích kvůli procházení malých souborů.

4.1.3 Výběr vhodného řešení

Po zvolení operačního systému a hardware bylo potřeba vybrat jeho další součásti. Jako první je třeba zvolit vhodné řešení MTA (Mail Transfer Agent). Variant MTA využívajících SMTP (Simple Mail Protocol) je mnoho a mezi nejznámější patří SendMail, Postfix, Exim, Qmail. Tato varianta bude využívána pouze pro přenos emailových zpráv a jejich čištění, nikoliv pro samotnou správu emailových schránek. Byla proto vybrána nejstarší varianta SendMail, která je ale také nejlépe zdokumentovaná, má obrovskou podporu komunity, nejlepší logování průběhu jednotlivých událostí a v neposlední řadě možnost rozšířitelnosti o mnoho dodatečných funkcí.

Vybrané řešení bude doplněno antispamovým filtrem v kombinaci s antivirovým filtrem. Jako antispamový filter bylo vybráno řešení Apache SpamAssassin. O Antivirovou ochranu se bude starat ClamAV antivirus, který má ve firmě Sourcefire, respektive CISCO, silnou podporu. O kontrolu SPF záznamů se bude starat SPF Milter smf-spf.

Další funkcí bude DNS server. Pro samotnou funkcionalitu bude instalována aplikace BIND. Tento standardní DNS server nahradí současné DNS řešení na straně poskytovatele, aby bylo možné agilně měnit DNS záznamy pro potřeby reversní proxy.

Poslední, ale neméně důležitou funkcí, kterou bude potřeba zvolit, je webový server. Ve výsledku bylo rozhodováno mezi dvěma webovými servery Apache a NGINX. Nakonec byl vybrán jako webový server Apache, který je nejlépe zdokumentován, umožňuje připojení portování dalších modulů a v neposlední řadě autorova osobní zkušenost s tímto webovým serverem. Server jako takový bude použit pouze pro několik statických webových prezentací a jako hlavní, k čemu bude sloužit, bude reversní proxy. Přes reversní proxy budou vypublikovány interní aplikace do externí sítě.

4.1.4 Obhájení konečné volby

Při výběru všech částí systémů byl kladen vysoký důraz na stabilitu, bezpečnost a rychlost. Bylo použito takové řešení, které je nejlépe zadokumentováno a nejvíce podporováno, ať již z hlediska instalace, konfigurace či samotné správy celého řešení a jedná se o konfigurace odzkoušené. SendMail je nejstarší, robustní, nejlépe zdokumentovaný a hodí se pro použití ve velkých organizacích. Totéž se dá říci o dalších vybraných prvcích toho serveru.

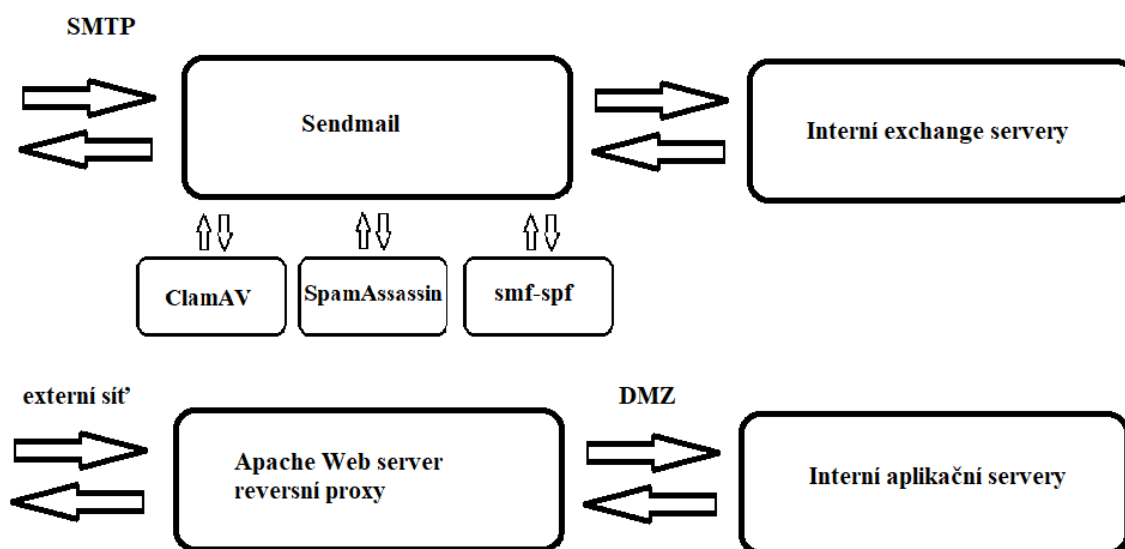
4.1.5 Popis fungování jednotlivých prvků

Jako výsledné řešení MTA byl zvolen sendmail, který bude tvořit SMTP server. O bezpečnost se bude starat antivirus ClamAV společně s antispamovým filtrem Apache SpamAssassin a smf-spf jako SPF Milter.

Jako DNS server byla zvolena varianta BIND serveru, který bude sloužit pro agilní potřeby nastavování webových služeb reverzního proxy serveru a pohodlné nastavování z jednoho místa.

Pro řešení webových služeb a reverzního proxy serveru byl zvolen webový server Apache, aby bylo možno bezpečně publikovat interní aplikace bez nutnosti připojení interních serverů do externí sítě.

Pro všechny popsané funkcionality je potřeba nastavit prostupy do vnitřní sítě, aby bylo umožněno komunikovat s vnitřními servery společnosti.



Obr. č. 2, Popis fungování celého řešení

4.2 Instalační proces krok po kroku

Proto, aby mohly být nainstalovány jednotlivé funkcionality serveru, je potřeba nainstalovat základ celého řešení. Základem bude čistá instalace systému Debian a několika nezbytných součástí, bez kterých by instalace nemohla začít. Podstatné bude nastavení počítačové sítě s propustností jednotlivých portů pro vzdálenou správu systému pomocí ssh, přijímání emailů a odesílání emailů, webové služby a DNS server.

Na sever nejdříve bude nainstalován Sendmail, spamassasin, smf-spf a ClamAv s jejich vzájemným provázáním. Následně budou nakonfigurovány adresy interních exchange serverů, kam bude nasměrováno přeposílání zkontrolovaných emailů a prověřených emailů.

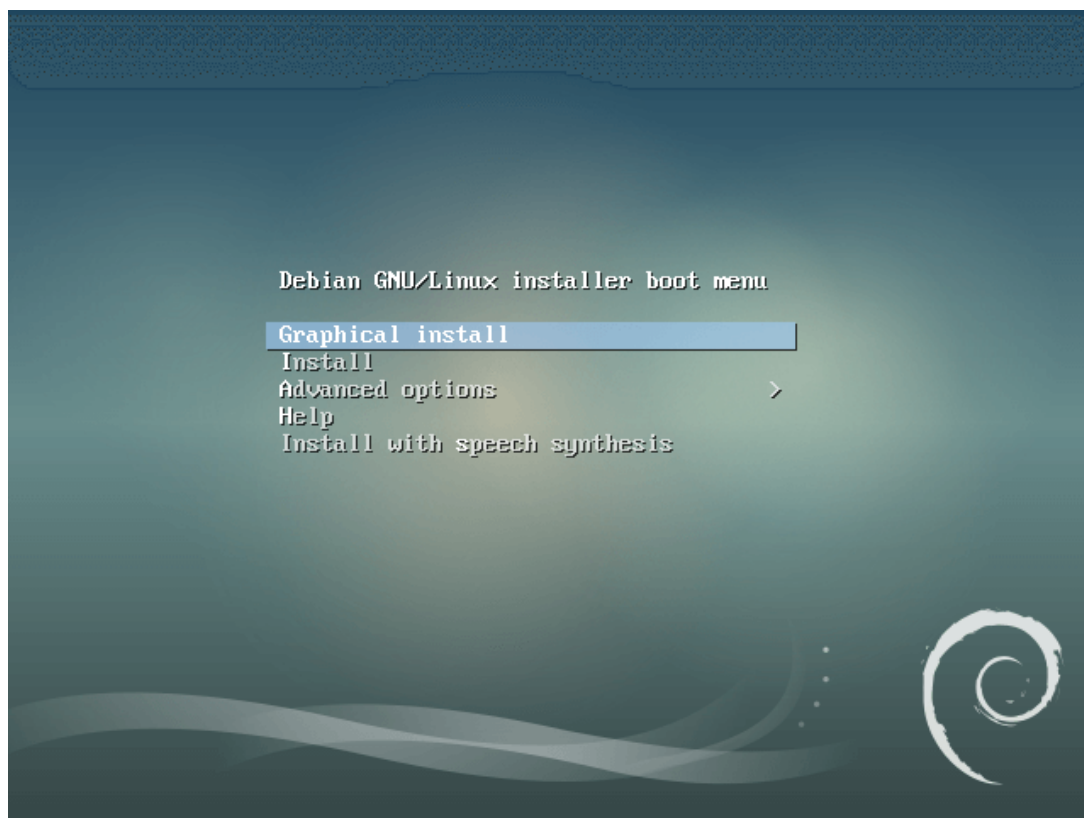
Další funkcionalitou bude Bind server. Po jeho základní konfiguraci bude provedeno jeho zabezpečení pomocí DNSSEC, kdy pomocí vygenerovaného certifikátu a jeho veřejného klíče dojde k ověření zabezpečení celého DNS serveru.

Jako poslední dojde k nainstalování webového serveru Apache, kde vytvářením jednotlivých webových konfiguračních souborů dojde k publikování interních aplikací do externí sítě.

Závěrem bude celé řešení otestováno, jak na funkcionalitu, tak i na bezpečnost.

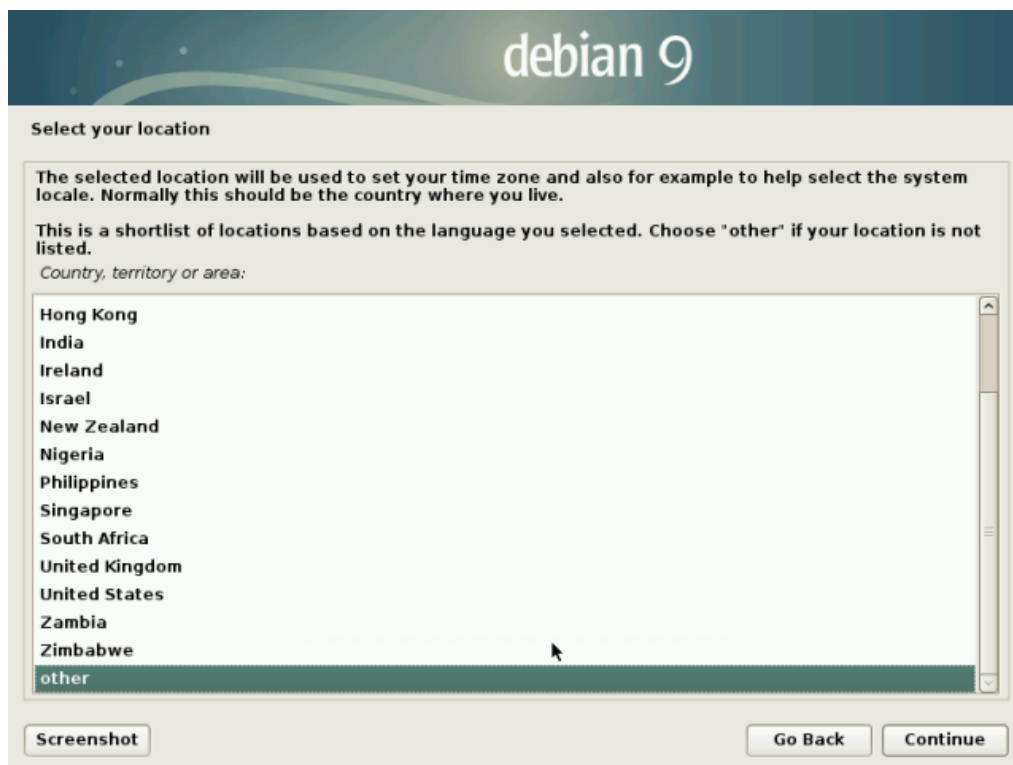
4.3 Instalace systému

Po vložení instalačního média nás Debian uvítá grafickým menu. Úvodní menu je v angličtině a dá nám několik možností Graphical Install s pokročilým grafickým průvodcem instalace, Install se základním grafickým rozhraním, možnost Advanced options, pod kterou nalezneme možnost expertní instalace, Rescue mode nebo Automated Install. Další z možností jsou Help a Install with speech synthesis.



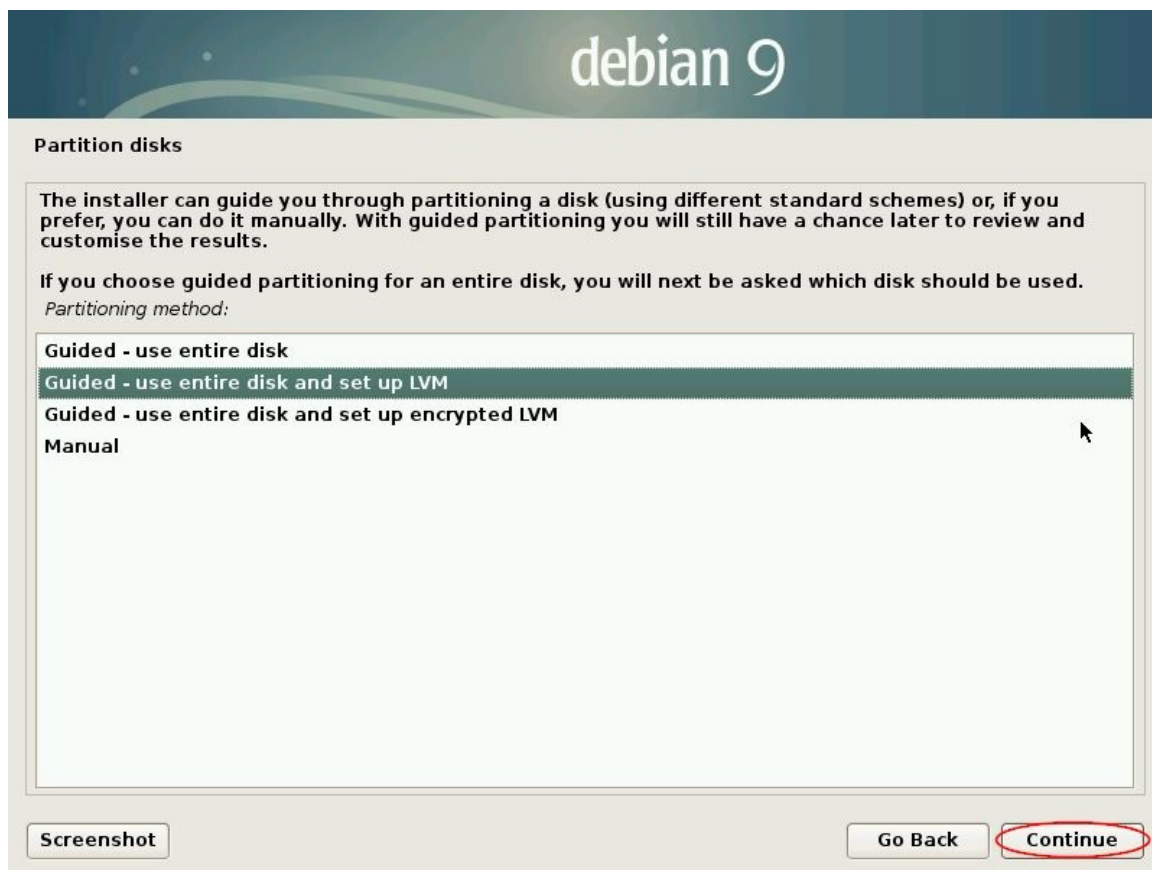
Obr. č. 3, Úvodní obrázek instalace

Po výběru typu instalace, v tomto případě Graphical install, nám instalace nabídne možnost vybrat si jazyk instalace, který bude poté nastaven zároveň jako výchozí jazyk prostředí. Po jeho výběru nám instalace nabídne možnost výběru naší lokality. Česká republika se skrývá až pod vybráním možnosti „other -> Europe -> Czech Republic“.



Obr. č. 4, Instalace – výběr lokace

Dále si vybereme jazyk klávesnice a její rozložení. V následujícím kroku nám instalační průvodce nabídne konfiguraci síťového rozhraní, kde nastavíme hostname a domain name. V dalším kroku nás systém vyzve ke zvolení hesla superuživatele root a vytvoření nového uživatele. Nyní nám systém dá na výběr možnost rozdělení disku, buď s průvodcem, nebo manuálně. Zvolíme možnost Průvodce a použití celého disku s možností LVM (Logical Volume Management), jenž nám nabízí větší variabilitu správy diskového prostoru, než konvenční metody dělení disků.



Obr. č. 5, Rozdělení diskového úložiště

Po potvrzení tohoto kroku již probíhá samotná instalace základní části operačního systému, která trvá pár minut. Po dokončení instalace nakonfigurujeme „*package manager*“, kde nám pomocí geolokace IP adres nabídne zemi, kde se nachází, s obecným doporučením, že servery *ftp.<your country code>.debian.org* jsou tou nejlepší volbou. Následuje příprava, která probíhá automaticky a trvá asi dvě minuty. Nyní přichází na řadu volba instalace software a to, zda požadujeme desktopové rozhraní s možností výběru několika verzí, Gnome, Xfce, KDE, Cinnamon, MATE, LXDE a možnosti „web server“, „print server“, „SSH server“, „standard system utilities“. Ponecháme pouze „standard system utilities“ a potvrzením naší volby dojde k samotné instalaci.



Obr. č. 6, Výběr sw prvků serveru

Ta již probíhá bez našeho zásahu a trvá pouhých několik minut. Na závěr se nás instalátor zeptá ještě na instalaci „GRUB boot loader“, kterou potvrdíme a vybereme disk, na který jsme instalovali systém. Potvrzením volby dojde k dokončení instalace a restartu serveru

4.3.1 Základní konfigurace a instalace doplňků

Po dokončení instalace základního systému je potřeba doinstalovat a nastavit několik základních aplikací. V současné době je naštěstí instalace pomocí balíčkovacího systému, který za uživatele vyřeší instalaci závislostí a potřebných balíčků. Vybrané aplikace a služby jsou následně nainstalovány ve výchozím nastavení. Pro lepší budoucí konfiguraci jednotlivých aplikací konfiguračních souborů bude nainstalována aplikace VIM^[1], která i v základním nastavení graficky zvýrazňuje syntaxe jednotlivých nastavení a konfigurace s ním je uživatelsky příjemnější. Abychom nemuseli neustále přepínat uživatele je nutné se pomocí příkazu „su“ přepnout do módu superuživatele a následně přidat uživatele do skupiny „sudo“. To bude provedeno příkazem „*usermode*“^[2]:

```
„usermod -a -G sudo <username>“
```

Dále je potřeba přidat řádek v „*/etc/sudoers*“, což bude provedeno spuštěním následujícího příkazu a přidáním jednoho řádku^[1]:

```
„visudo“
```

```
„<username> ALL=(ALL) ALL“
```

Všechny instalace bychom měli začít nejdříve příkazem:

```
„sudo apt-get update“
```

```
„sudo apt-get upgrade“
```

Pomocí příkazu „*sudo apt-get install vim -y*“ bude provedena instalace a v rámci několik sec. proběhne samotné nainstalování balíčku.

4.3.2 Konfigurace sítě

Jelikož po základní instalaci je síťová karta nastavena na DHCP, je nutné toto nastavení upravit. Pomocí příkazu „*ip link show*“ budou zobrazeny veškeré dostupné síťové prvky. Systém obsahuje dvě síťové karty, které budou zobrazeny společně s „lo“ a to „*eth0*“ a „*eth1*“. Jelikož je od tohoto serveru požadována vysoká dostupnost, bude každá síťová karta zapojena do samostatného switchu a bude potřeba nastavit network teaming, neboli bonding. Pro tuto funkcionalitu bude nutná instalace balíčku „*ifenslave*“, která se provede příkazem „*sudo apt-get install ifenslave*“. Instalace nám oznámí doinstalování dodatečného balíčku „*net-tools*“, volbu potvrdíme a po několika vteřinách dojde k dokončení instalace. Pro zavedení do systému je potřeba, aby se v módu jádra spustil modul „*bonding*“. Nyní je nutné přidat řádek do konfiguračního souboru modulů pomocí příkazu „*sudo vim /etc/modules*“. Pomocí klávesy „a“ je umožněn insertní mód, ve kterém

bude přidán řádek s požadovanou hodnotou. Po dokončení editace dojde k opuštění insertního módu stiskem klávesy „ESC“. Následně pomocí příkazu „:wq“ bude zapsána konfigurace a ukončení editace souboru. Aby bylo možné samotnou funkcionalitu začít využívat, je potřebné provést několik následujících kroků. Nejdříve bude vypnuta služba sítě pomocí příkazu „sudo /etc/init.d/networking stop“. Nyní je potřeba do systému zavést modul bonding, což bude provedeno příkazem „modprobe bonding“. Nyní bude provedena samotná konfigurace síťového rozhraní. Zadáním příkazu „sudo vim /etc/network/interfaces“ bude upravena konfigurace síťových karet tak, aby mohli fungovat v modu „active-backup“.^[3]

```
# eth0 is manually configured, and slave to the "bond0" bonded NIC
auto eth0
iface eth0 inet manual
    bond-master bond0
    bond-primary eth0

# eth1 ditto, thus creating a 2-link bond.
auto eth1
iface eth1 inet manual
    bond-master bond0

# bond0 is the bonding NIC and can be used like any other normal NIC.
# bond0 is configured using static network information.
auto bond0
iface bond0 inet static
    address 185.91.165.51
    gateway 185.91.165.50
    netmask 255.255.255.240
    dns-nameservers 185.91.165.51
    dns-search eltodo.cz
    bond-mode active-backup
    bond-miimon 100
    bond-slaves none
```

Obr. č. 7, Popis výsledné konfigurace sítě

4.3.3 Instalace a nastavení SSH

Nezbytnou součástí tohoto serveru bude také možnost připojit se na tento server vzdáleně pomocí ssh. Nejdřív je potřeba danou funkcionalitu doinstalovat. Nainstalování openssh serveru a klientské části bude provedeno spuštěním následujícího příkazu:

```
„sudo apt-get install openssh-server -y“
```

Následně bude potřeba změnit několik hodnot v konfiguraci pomocí příkazu:

```
„sudo vim /etc/ssh/sshd_config“
```

Změna se provádí odkomentováním řádku - smazáním znaku „#“, čímž dojde k aktivování daného konfiguračního řádku a můžeme v něm provést další úpravy.

<i>Port 4489</i>	<i>- změna standardního portu na port 4489</i>
<i>PermitRootLogin no</i>	<i>- zamezení ssh přihlášení uživateli root</i>

Dále je třeba provést změny následujícím způsobem:

```
„sudo service ssh restart“
```

Nyní je možné se přihlásit na server pomocí ssh jako uživatel. Po přihlášení na server pomocí ssh je potřeba spouštět služby pomocí příkazu „sudo“ nebo příkazem „su“ se přepnout do modu superuživatele. ^[3]

4.4 Instalace sendmail

Nyní je možné začít s instalací nejdůležitějšího prvku toho serveru a to je sendmail. Samotná instalace probíhá standardním způsobem, kdy nám systém doinstaluje potřebné závislé balíčky.

```
„sudo apt-get install sendmail -y“
```

Následně proběhne samotná instalace, během které dojde k vytvoření základní konfigurace sendmailu s vytvořením konfiguračních souborů, které jsou ve výchozím nastavení. Ve výchozím nastavení sendmail odmítá veškerou poštu, která není určena pro vlastní stroj nebo není uvedena v konfiguračním souboru „/etc/mail/local-host-names“.

4.4.1 Instalace ClamAV a Apache SpamAssassin

Před započítím veškerých konfigurací je zapotřebí, aby byly nainstalovány i jejich podpůrné funkce ClamAV a Apache SpamAssassin.

```
sudo apt-get clamav clamav-daemon clamav-milter spamassassin spampd spamc  
spamass-milter -y
```

Celá instalace proběhne během několika vteřin. Nyní je potřeba otestovat a nastavit jednotlivé prvky.

4.4.2 Instalace SPF Milteru - smf-spf

Pro samotnou instalaci je potřeba nejdříve stáhnout aplikaci, jelikož nemá vlastní balíček. To bude provedeno pomocí příkazu:

```
wget https://github.com/jcbf/smf-spf/archive/master.zip
```

Tento milter pro svojí funkci vyžaduje knihovnu libspf2, kterou je potřeba nejprve stáhnout:

```
wget https://github.com/shevek/libspf2/archive/master.zip
```

Po dokončení stahování, které proběhne během několika vteřin, bude provedeno rozbalení staženého balíčku a instalace pomocí následujících příkazů:

```
mkdir /home/user/temp  
unzip /home/user/temp/master.zip -d /home/user/temp  
cd /home/user/temp/libspf2-master/  
./configure  
make  
make check  
make install
```

Po doinstalování tohoto balíčku je možné pokračovat v instalaci samotného milteru.

Nejdříve je tedy potřeba stažený zip rozbalit do dočasného adresáře pro instalaci, což bude provedeno následující sérií příkazů:

```
unzip ./master.zip -d ~/temp
cd /home/user/temp/smf-spf-master/
make
make install
```

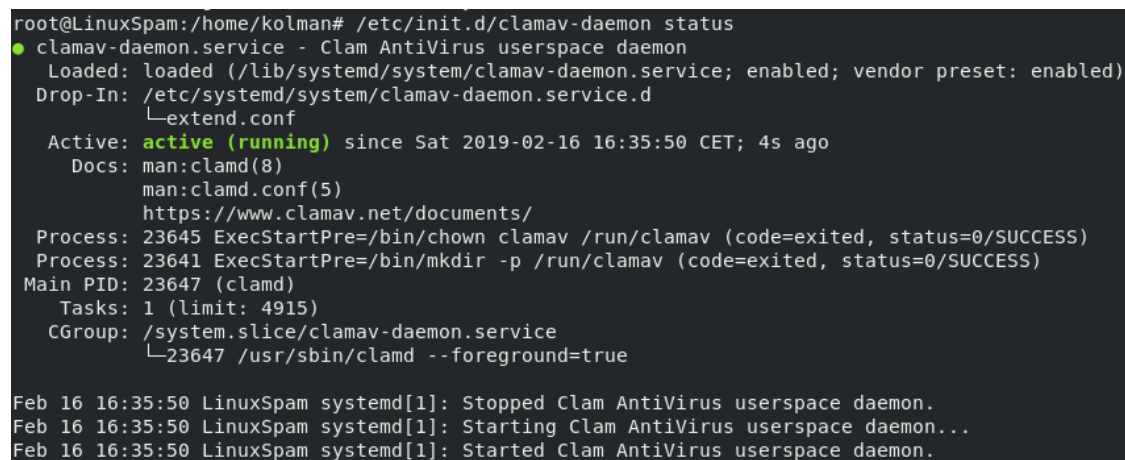
Posledním příkazem dojde k vytvoření potřebného uživatele a skupiny „*smfs:smfs*“. Následně nás instalace vyzve, abychom zkontrolovali a případně editovali konfigurační soubor „*/etc/mail/smf/smf-spf.conf*“.

4.4.2.1 Konfigurace a prvotní testování ClamAV

Nyní je potřeba ověřit samotnou funkcionalitu antiviru a jeho součástí.

Pomocí následujícího příkazu zkontrolujeme status obou nainstalovaných služeb. Jak samotného „*clamav-daemonu*“, tak i „*clamav-freshclam*“, který se stará o aktualizace antivirové databáze.

```
„/etc/init.d/clamav-daemon status“
„/etc/init.d/clamav-freshclam status“
```



```
root@LinuxSpam:/home/kolman# /etc/init.d/clamav-daemon status
● clamav-daemon.service - Clam AntiVirus userspace daemon
   Loaded: loaded (/lib/systemd/system/clamav-daemon.service; enabled; vendor preset: enabled)
   Drop-In: /etc/systemd/system/clamav-daemon.service.d
            └─extend.conf
   Active: active (running) since Sat 2019-02-16 16:35:50 CET; 4s ago
     Docs: man:clamd(8)
            man:clamd.conf(5)
            https://www.clamav.net/documents/
   Process: 23645 ExecStartPre=/bin/chown clamav /run/clamav (code=exited, status=0/SUCCESS)
   Process: 23641 ExecStartPre=/bin/mkdir -p /run/clamav (code=exited, status=0/SUCCESS)
  Main PID: 23647 (clamd)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/clamav-daemon.service
           └─23647 /usr/sbin/clamd --foreground=true

Feb 16 16:35:50 LinuxSpam systemd[1]: Stopped Clam AntiVirus userspace daemon.
Feb 16 16:35:50 LinuxSpam systemd[1]: Starting Clam AntiVirus userspace daemon...
Feb 16 16:35:50 LinuxSpam systemd[1]: Started Clam AntiVirus userspace daemon.
```

Obr. č. 8, Výsledek testování služby clamav-daemon

```

root@LinuxSpam:/home/kolman# /etc/init.d/clamav-freshclam status
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2019-02-16 15:50:41 CET; 45min ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://www.clamav.net/documents
  Main PID: 23129 (freshclam)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/clamav-freshclam.service
           └─23129 /usr/bin/freshclam -d --foreground=true

Feb 16 15:50:41 LinuxSpam systemd[1]: Started ClamAV virus database updater.
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> ClamAV update proce... 2019
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> ^Your ClamAV instal...ATED!
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> ^Local version: 0.1...101.1
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> DON'T PANIC! Read h...lamav
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> main.cvd is up to d...mgr)
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> daily.cvd is up to ...nman)
Feb 16 15:50:41 LinuxSpam freshclam[23129]: Sat Feb 16 15:50:41 2019 -> bytecode.cvd is up ... neo)
Hint: Some lines were ellipsized, use -l to show in full.

```

Obr. č. 9, Výsledek testování služby clamav-freshclam

Bude provedeno testování jednoduchého souboru na přítomnost škodlivého software pomocí příkazu:

```
„clamscan <scanovany_soubor>
```

Dle velikosti souboru by měl být výsledek scanování do několika vteřin.

```

/home/send.txt: OK

----- SCAN SUMMARY -----
Known viruses: 6810817
Engine version: 0.100.2
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.01 MB
Data read: 0.00 MB (ratio 2.00:1)
Time: 21.426 sec (0 m 21 s)

```

Obr. č. 10, Výsledek skenování souboru

4.4.2.2 Počáteční konfigurace Apache SpamAssassin

Jako první je potřeba naučit SpamAssassin Bayesian klasifikaci. To bude provedeno nastavením „*sa-learn*“ respektive s následující úpravou příkazu:

```
„sudo sa-learn --spam /var/cache/spamassassin/bayes_db/bayes“
```

```
„sudo sa-learn --ham /var/cache/spamassassin/bayes_db/bayes“
```

Nyní je potřeba provést konfiguraci „*/etc/spamassassin/local.cf*“.

Konfigurace je rozdělena do několika základních možností.^[25]

WHITELIST_FROM – používá se pro whitelisting emailových adres nebo celých serverů. Těmto zprávám je přiřazeno nejlepší skóre, tedy co nejnižší až záporné.

BLACKLIST_FROM – používá se pro blokování jednotlivých emailových adres, domén nebo serverů – zprávám se poté přiřadí nejhorší skóre a jsou zablokovány.

TRUSTED_NETWORKS – důvěryhodné sítě nebo servery.

HEADER – zprávy jsou blokovány nebo povolovány na základě předmětu zprávy. Dá se zde využít buď přímo text zprávy, nebo lze používat regulární výrazy, pokud se ve zprávách mění kupříkladu číselná hodnota.

BODY – to samé jako v případě „HEADER“, nicméně zde se jedná o tělo zprávy.

REWRITE_HEADER SUBJECT – označení spamové zprávy Kupř. (*****SPAM*****, [SPAM], atd.).

REPORT_SAFE – možnost nastavit 0, 1 a 2.

0 – do předmětu zprávy zapíše to, co je obsahem „*rewrite_header subject*“.

1 – přidá 2 přílohy, dokument s detaily spamového pravidla a jako přílohu podezřelý email.

2 – opět 2 přílohy, nicméně v těle emailu se objeví text spamového pravidla.

USE_BAYES –volby 0|1 tedy vypnutí či zapnutí veškerých operací spojených s Bayesem.

USE_AUTO_WHITELIST –volby 0|1 pro vypnutí nebo zapnutí automatického přidávání na whitelist.

BAYES_AUTO_LEART –volby 0|1 pro vypnutí nebo zapnutí bayesova učícího systému.

BAYES_PATH – nastavená cesta k databázím pro určení, zda se jedná o spam|ham.

BAYES_FILE_MODE – nastavení oprávnění (bitů) souborů používaných pro Bayesovské databáze.

SKIP_RBL_CHECKS – volby 0|1 SpamAssassin provede kontrolu RBL (Real-time BlackHole List), volba 1 se používá pouze, pokud kontrolu RBL provádí poskytovatel internetového připojení.

USE_RAZOR2 – volby 0|1 pro vypnutí nebo zapnutí funkce, při zapnutí je potřeba doinstalování klientského programu pro ověření spamů proti internetové databázi.

USE_PYZOR – stejné jako u USE_RAZOR2 pouze s jinou databází.

USE_DCC – stejné jako u USE_RAZOR2 pouze s jinou databází.^[30]

Samotná úprava konfiguračního souboru je poté následující:

```
rewrite_header Subject [SPAM]    #přidá k podezřelým zprávám označení [SPAM]
required_hits 5                  #kolikrát se zpráva musí objevit, než ji systém začne
považovat za spam
report_safe 0                    # typ zápisu do zprávy
use_bayes 1
use_auto_whitelist 1
#Enable Bayes auto-learning
bayes_auto_learn 1
bayes_path /var/cache/spamassassin/bayes_db/bayes
bayes_file_mode 0777
# Enable or disable network checks
skip_rbl_checks 0
use_razor2 0
use_dcc 1
use_pyzor 0

# whitelisting emailových adres.
whitelist_from emailserver@pop3.amadeus.net
whitelist_from dispecer@eltodo.cz
whitelist_from vmwareteam@connect.vmware.com
whitelist_from noreply@ready2go.cz
whitelist_from MBX_KTC.ITSM.CZ@kapsch.net # dispecink
whitelist_from *@prace.eltodo.cz
whitelist_from prace-admin@eltodo.cz
```

```

whitelist_from izm@eltdo.cz
whitelist_from czech.electronicstatement@citi.com
whitelist_from stanislav.holy@citi.com
whitelist_from webformular@eltdo.cz
whitelist_from vyplatni-pasky-automat@eltdo.cz
whitelist_from *@siemens.com
whitelist_from *@iora.cz
whitelist_from *@commerzbank.com
whitelist_from *@gmx.at # GrandHotel-ambassador - zákazník
whitelist_from *@gmx.de # Grandhotel-ambassador - zákazník
whitelist_from *@invent-europe.com # Grandhotel-ambassador - zákazník
whitelist_from *@hrs.de # Grandhotel-ambassador - zákazník
whitelist_from *@jetbrains.com
whitelist_from mail.netvis.eu
whitelist_from *.netvis.local

# Odfiltrovani ruskeho spamu.
header SUBJ_RUSS_CHAR      Subject:raw =~ /koi8-r/i
describe SUBJ_RUSS_CHAR    has Russian char encoding
score SUBJ_RUSS_CHAR      3.5

#Blokování spamu dle subjektu emailu.
header SUBJ_S1      Subject =~ /^Urgent Alert/i
describe SUBJ_S1    Subject: SPAM
score SUBJ_S1      100

header SUBJ_S2      Subject =~ /^Insufficient funds/i
describe SUBJ_S2    Subject: SPAM
score SUBJ_S2      100

header SUBJ_S3      Subject =~ /^Attention Required/i
describe SUBJ_S3    Subject: SPAM
score SUBJ_S3      100

```

header SUBJ_S4 Subject =~ /^DSCF\d{4}\d{6}\.gif/i

describe SUBJ_S4 Subject: SPAM

score SUBJ_S4 100

header SUBJ_S5 Subject =~ /^For Your Consideration/i

describe SUBJ_S5 Subject: SPAM

score SUBJ_S5 100

header SUBJ_S6 Subject =~ /^Order \#\d{7}/i

describe SUBJ_S6 Subject: SPAM

score SUBJ_S6 100

header SUBJ_S7 Subject =~ /^Recent order/i

describe SUBJ_S7 Subject: SPAM

score SUBJ_S7 100

header SUBJ_S8 Subject =~ /^Payment Information/i

describe SUBJ_S8 Subject: SPAM

score SUBJ_S8 100

Blokování spamu na základě obsahu těla zprávy.

body BODY_B1 /Váš emailem adresa právě vyhrál \€ 150,000/i

describe BODY_B1 SPAM

score BODY_B1 100

body BODY_B2 /El Gordo Award 4th \11\2015 Gratulujeme Email právě vyhrál 150,000,00 Euro bylo mezi vítěze měsíce vyhraná částka Of 150,000,00 účastníků Euro.All byly vybrány náhodně z World Wide Web Facebook stránkách prostřednictvím počítače čerpá ystemTo souboru pro vaše tvrzení, kontaktujte prosím naše důvěrník agent okamžitě tete tuto zprávu pro rychlé a naléhavé propuštění vašeho fondu./i

describe BODY_B2 SPAM

score BODY_B2 100

body BODY_B3 /Jmenuji se Dr. John Edward Lloyds Banking group plc Londýn, Velká Británie. Mám právní úkon pro tebe, jsem dostal e-mailovou informaci prostřednictvím vaší/i

describe BODY_B3 SPAM

score BODY_B3 100

body BODY_B4 /Hello Hledam na seriozni vztah\. Laska kucharstvi a sledovani televize\. Bych chtěla\, kdyby bys mohl odpovedet/i

describe BODY_B4 SPAM

score BODY_B4 100

body BODY_B5 /Dear Client\! Our delivery department could not accept your operation due to a problem with your current account\. In order to avoid falling into arrears and getting charged\, please fill out the document in the attachment as soon as possible and send it to us\./i

describe BODY_B5 SPAM

score BODY_B5 100

body BODY_B6 /we have received your payment but the amount was not full\. Probably\, this occurred due to taxes we take from the amount\. All the details are in the attachment \- please check it out\./i

describe BODY_B6 SPAM

score BODY_B6 100

body BODY_B7 /our HR Department told us they haven\'t received the receipt you\'d promised to send them.Fines may apply from the third party\. We are sending you the details in the attachment\./i

describe BODY_B7 SPAM

score BODY_B7 100

body BODY_B8 /You made it last week\. Please check it out as soon as possible\. The receipt with all info is in the attached file\./i

describe BODY_B8 SPAM

score BODY_B8 100

body BODY_B9 /Unfortunately\, you have forgotten to specify insurance payments\. Soq, we cannot accept the payment without them\./i

describe BODY_B9 SPAM

score BODY_B9 100

body BODY_B10 /The error occurred during payment\. Sending you details of the transaction\. Please pay the remaining amount as soon as possible\./i

describe BODY_B10 SPAM

score BODY_B10 100

body BODY_B11 /The counteragent has conducted the checking and found no confirmed payment for the recent order\..Please process the payment/i

describe BODY_B11 SPAM

score BODY_B11 100

body BODY_B12 /Starting tomorrow\, fines will be charged\. Please make appropriate payments\./i

describe BODY_B12 SPAM

score BODY_B12 100

body BODY_B13 /Sending you the scan of the software license agreement
\(Order \#\./i

describe BODY_B13 SPAM

score BODY_B13 100

#Důvěryhodné sítě / server.

siemens

trusted_networks 194.138.37.40 194.138.37.39 192.35.17.2

Mpro

trusted_networks 194.169.252.4

trusted_networks 194.169.252.67

TDext

```
trusted_networks 46.167.233.8
# EWatch
trusted_networks 88.146.197.73
# ONLIO
trusted_networks 217.31.53.21
# Vegacloud
trusted_networks 62.240.162.14
# VMware
trusted_networks 209.167.231.112
trusted_networks 209.167.231.113

# Black list emailový adres
blacklist_from *@logisticsmanager.msgfocus.com
blacklist_from mikus1200@azet.sk
blacklist_from aamski2@tig.com.au
blacklist_from aceman@winshop.com.au
blacklist_from acs@senet.com.au
blacklist_from admin@buzzwaxx.com
blacklist_from agalvin@tassie.net.au
blacklist_from ahogan@bigpond.net.au
blacklist_from airnorth@octa4.net.au
blacklist_from aiti@cs.mu.oz.au
```

Výše uvedená konfigurace je použita z Exchange serverů a z často se opakujících emailových zpráv. Výpis blacklistovaných emailových zpráv byl zkrácen na několik příkladů. Jinak daný seznam emailových adres je o několik stran delší.

Další konfigurační soubor, který je potřeba upravit, je „*/etc/spamassassin/v310.pre*“, kde je nutné smazáním znaku „#“ odkomentovat následující řádky pro aktivaci auto-whitelist checks a kontrolu zpráv proti online databázi spamu.

```
„loadplugin Mail::SpamAssassin::Plugin::AWL“
„loadplugin Mail::SpamAssassin::Plugin::DCC“
```

Nyní je potřeba spamassassin aktivovat, což bude provedeno pomocí následujícího příkazu:

```
„sudo systemctl enable spamassassin.service“
```

Celou konfiguraci je potřeba také otestovat následujícím příkazem:

```
„sudo spamassassin -lint“
```

Pokud jsou konfigurační soubory v pořádku, tak příkaz nevrátí žádnou hodnotu. Jinak dojde k vypsání jednotlivých chyb.

4.4.3 Konfigurace SPF Milteru - smf-spf

Prvotní konfiguraci instalace je potřeba provést v „*/etc/mail/smfs/smf-spf.conf*“.

V tomto souboru je potřeba udělat několik následujících úprav pro whitelisting jednotlivých domén, od kterých chceme, aby se přes tento server mohli odesílat emailové zprávy a neprošli by přes SPF test.^[23]

```
WhitelistIP 127.0.0.0/8
WhitelistIP 172.16.0.0/16
WhitelistIP 172.28.0.0/16
WhitelistIP 192.168.0.0/16

#Povolí přeposílání z linuxspam
WhitelistIP 185.91.165.51/32
# Povolí přeposílání z linuxu.
WhitelistIP 194.228.220.82/32
# Povolí přeposílání z proxy-hvoz.
WhitelistIP 195.113.161.178/32
# Povolí odesílání hlášení poruch z webu.
WhitelistIP 217.31.53.21/32
```

```
# Povolí odesílání z M-Pro.  
WhitelistIP 194.169.252.4/32  
WhitelistIP 194.169.252.67/32  
#TDex  
WhitelistIP 46.167.233.8/32  
#EWatch  
WhitelistIP 46.167.233.11/32  
#Vegacloud  
WhitelistIP 62.240.162.14/32  
#poruchy ricany  
WhitelistIP 89.187.143.49/32  
#Dispecer  
WhitelistIP 217.31.53.17/32
```

4.4.4 Konfigurace sendmail

Konfigurace sendmailu je rozdělena do několika kroků, respektive je rozdělena úpravou jednotlivých konfiguračních souborů.

4.4.4.1 Access

Nejdříve provedeme úpravu v souboru „*/etc/mail/access*“, což je přístupová databáze celého sendmailu.

Samotná konfigurace je rozdělena na následující možnosti nastavení:

CONNECT - host, na kterém běží sendmail

RELAY – umožní předávání pošty – uvedený host může přes tento server posílat emaily

REJECT – přesný opak RELAY, odmítne veškerou poštu od daného hosta nebo na danou emailovou adresu

OK – v tomto případě může host posílat poštu pouze na tento stroj

TRY_TLS: spatny.server NO - používá se pokud je problém s nesprávně nakonfigurovaným serverem. [26]

V tomto souboru byly provedeny následující změny:

```
#Ve výchozím nastavení je umožněno odesílat emaily pouze danému stroji.
```

```
Connect:localhost.localdomain    RELAY
Connect:localhost                 RELAY
Connect:127.0.0.1                 RELAY
Connect:127.0.1.1                 RELAY
Connect:linuxspam                 RELAY
Connect:linuxspam.eltodo.cz       RELAY
Connect:185.91.165.51             RELAY
```

```
# Domény, pro které přijímáme emaily a přeposíláme dál.
```

```
To:eltodo.cz                      RELAY
To:eltodo.sk                      RELAY
To:vegacom.cz                    RELAY
To:energovod.cz                  RELAY
To:elektrosignal.cz              RELAY
To:misel.cz                      RELAY
To:sagasta.cz                    RELAY
To:grandhotel-ambassador.cz      RELAY
To:grandhotel-ambassador.eu      RELAY
To:grandhotel-ambassador.com     RELAY
To:o-es.cz                       RELAY
To:autoreply.vegacom.cz         RELAY
To:vegacloud.cz                  RELAY
```

```
# Počítače, které mohou posílat emaily přes tento server.
```

```
# Exchange1
```

```
Connect:172.16.1.23              RELAY
```

```
# Exchange2
```

```
Connect:172.16.1.12              RELAY
```

```
# MYQ
```

```
Connect:172.16.1.5               RELAY
```

```
#ERP Servery
```

```
Connect:172.16.1.100             RELAY
Connect:172.16.1.101             RELAY
Connect:172.16.1.102             RELAY
Connect:172.16.1.103             RELAY
Connect:172.16.1.104             RELAY
```

```

# Nagios
    Connect:172.16.1.50          RELAY
# Nastavení limitů
    GreetPause:127             0
    ClientRate:127             0
    ClientConn:127             0
# Localnet
    GreetPause:172.16          0
    GreetPause:192.168         0
    ClientRate:172.16          0
    ClientRate:192.168         0
    ClientConn:172.16          0
    ClientConn:192.168         0
# # Backup MX
    GreetPause:194.228.41.114  0
    ClientRate:194.228.41.114  0
    ClientConn:194.228.41.114  0
# Gateway
    GreetPause:194.228.220.92  0
    ClientRate:194.228.220.92  0
    ClientConn:194.228.220.92  0
# OTE-CR
    GreetPause:62.77.71.218    0
    ClientRate:62.77.71.218    0
    ClientConn:62.77.71.218    0
# Problem s TLS
    Try_TLS:itsystem.cz        NO
    Try_TLS:prestice-mesto.cz  NO
    Try_TLS:mestopacov.cz      NO
    Try_TLS:fortel.cz          NO
    Try_TLS:znacky-plzen.cz    NO
    Try_TLS:sbd8.cz            NO
    Try_TLS:egpi.cz            NO
    Try_TLS:mepnet.cz          NO
    Try_TLS:ms10.mepnet.cz     NO
    Try_TLS:ms11.mepnet.cz     NO
    Try_TLS:praha.eu           NO

```

Try_TLS:avexim.cz	NO
Try_TLS:hotice.cz	NO
# Zablokováno z externích sítí	
To:hr_info@eltodo.cz	REJECT

4.4.4.2 Mailertable

Protože tento server neslouží pro ukládání pošty, ale rovnou po přefiltrování poštu odesílá dále, je potřeba v souboru „*/etc/mail/mailertable*“ provést následující úpravy, které pokrývají veškeré spravované domény. [26]

eltodo.cz	esmtplib:internal-mail.eltodo.cz
eltodo.sk	esmtplib:internal-mail.eltodo.cz
energovod.cz	esmtplib:internal-mail.eltodo.cz
elektrosignal.cz	esmtplib:internal-mail.eltodo.cz
linuxspam.eltodo.cz	esmtplib:linuxspam.eltodo.cz
vegacom.cz	esmtplib:internal-mail.eltodo.cz
autoreply.vegacom.cz	esmtplib:172.16.1.51
vegacloud.cz	esmtplib:internal-mail.eltodo.cz
sagasta.cz	esmtplib:internal-mail.eltodo.cz
grandhotel-ambassador.cz	esmtplib:internal-mail.eltodo.cz
o-es.cz	esmtplib:internal-mail.eltodo.cz

4.4.4.3 Aktivace modulů a dokončení instalace

Aby sendmail začal využívat nainstalované bezpečnostní a antispamové moduly, je potřeba jejich aktivace. Aktivace bude provedena editací, respektive přidáním řádků do soubodu:

„/etc/mail/sendmail.mc“

Aktivace smf-spf bude provedena přidáním následujících řádků:

```
define(`confMILTER_MACROS_HELO', confMILTER_MACROS_HELO`,  
{verify}')dnl  
INPUT_MAIL_FILTER(`smf-spf', `S=unix:/var/run/smfs/smf-spf.sock,  
T=S:30s;R:1m')dnl
```

Aktivace ClamAV bude provedena přidáním následujících řádků:

```
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav/clamav-milterctl, F=T,  
T=S:4m;R:4m')dnl
```

Aktivace ClamAV bude provedena přidáním následujících řádků:

```
INPUT_MAIL_FILTER(`spamassassin', `S=local:/var/run/spamass/spamass.sock, F=,  
T=C:15m;S:4;R:4m;E:10m')dnl
```

Na závěr je potřeba již pouze spustit dokončení instalace sendmailu, které bude provedeno následujícím příkazem:

```
„sudo sendmailconfig“
```

Potvrzením voleb příkazu dojde k dokončení instalace a spuštění celého řešení sendmail s nainstalovanými prvky Apache SpamAssassin, ClamAV a smf-spf.

Posledním krokem je zajištění pravidelné aktualizace databáze SpamAssassinu. Abychom mohli pravidelně aktualizovat, využijeme „*crontab*“, do kterého přidáme následující řádek. Tím zajistíme pravidelnou denní aktualizaci ve 3 hodiny:

```
00 3 * * * root /user/bin/sa-update && /etc/init.d/spamassassin reload &&  
/etc/init.d/spamass-milter restart
```

4.5 Instalace BIND serveru

Samotná instalace serveru je jednoduchá a bude provedena ve výchozí konfiguraci příkazem:

```
„sudo apt-get install -y bind9“
```

Nyní je potřeba celý server nakonfigurovat pro interní potřeby společnosti, což bude provedeno úpravou jednotlivých konfiguračních souborů.^[13]

4.5.1 Úprava `named.conf.options`

Jako první je potřeba provést úpravu v tomto konfiguračním souboru, který je stěžejní k fungování DNS serveru. Zde se nastavuje pracovní adresář celého serveru. Port, na kterém server naslouchá, povolené dotazy a servery, na které přeposíláme konfiguraci. Úprava bude provedena následujícím způsobem:

```
„sudo vim /etc/bind/named.conf.options“
```

Samotná konfigurace je rozdělena na následující možnosti nastavení:

DUMP-FILE – určuje absolutní cestu, kde má BIND uloženou cache, databázi s odpověďmi na `rndc dumpdb`.

STATISTICS-FILE - absolutní nebo relativní cesta k adresáři, kam BIND ukládá statistiky příkazu `rndc stats`.

MEM STATISTICS-FILE – absolutní nebo relativní cesta k adresáři, kam BIND ukládá statistiky využití paměti.

DNSSEC-ENABLED – tato volba označuje, že je používána zabezpečená služba DNS

ALLOW-QUERY – tato volba definuje seznam IP adres, na které se smí dotazovat tento server.^[26] Naším cílem není veřejný DNS server, a proto zde budou pouze naše DNS servery a servery poskytovatele internetového připojení. V tomto konfiguračním souboru budou provedeny následující změny:

```

options {
    directory "/var/cache/bind";
    dump-file      "/var/cache/bind/data/cache_dump.db";
    statistics-file  "/var/cache/bind/data/named_stats.txt";
    memstatistics-file  "/var/cache/bind/data/named_mem_stats.txt";
    dnssec-validation yes;
    dnssec-enable yes;
    recursion yes
    allow-query      { 127.0.0.1; 185.91.165.51; 194.228.220.80/28; 172.16.1.1;
172.16.1.10; 172.16.1.4; 172.16.1.22; 172.16.101.0/24; 90.183.17.222; 90.182.56.211;
82.208.45.102; 192.168.3.1; 192.168.4.1; 192.168.21.1; 195.113.161.178; };
    auth-nxdomain no; # conform to RFC1035
    listen-on { any; };
    listen-on-v6 { any; };
};

```

4.5.2 Úprava named.conf.local

V tomto souboru budou vyspecifikovány veškeré firemní směrové (forward) a zpětné (revers) zóny DNS serveru. Tato úprava bude provedená následující příkazem:

```
„sudo vim /etc/bind/named.conf.local“
```

Samotná úprava souboru bude vypadat následujícím způsobem, kde první části jsou směrové a poslední dva bloky jsou reversní:

```

zone "eltodo.cz" {
    type master;
    file "eltodo.cz/eltodo.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 195.113.161.178; 194.228.2.1; 194.228.220.83;
194.228.220.88; };
    notify yes;
};

```

```
zone "net.eltodo.cz" {
    type master;
    file "net.eltodo.cz/net.eltodo.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
    notify yes;
};

zone "ext.eltodo.cz" {
    type master;
    file "ext.eltodo.cz/ext.eltodo.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
    notify yes;
};

zone "vegacom.cz" {
    type master;
    file "vegacom.cz/vegacom.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 195.113.161.178; 194.228.2.1; 194.228.220.83;
194.228.220.88; };
    notify yes;
};

zone "dohled.vegacom.cz" {
    type master;
    file "dohled.vegacom.cz/dohled.vegacom.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
```

```

    notify yes;
};

zone "energovod.cz" {
    type master;
    file "energovod.cz/energovod.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 193.85.1.115; 194.228.220.88; 195.113.161.178; };
    notify yes;
};

zone "elektrosignal.cz" {
    type master;
    file "elektrosignal.cz/elektrosignal.cz.signed";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
    notify yes;
};

zone "elektrosignal.com" {
// Do teto domeny je smerovan test dostupnosti externiho DNS ze SCOM //
    type master;
    file "elektrosignal.com";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
    notify yes;
};

zone "optun.cz" {
    type master;
    file "optun.cz/optun.cz.signed";
    allow-query { any; };

```

```

    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
    notify yes;
};

zone "orpheum.cz" {
    type master;
    file "generic.cz";
    allow-query { any; };
    allow-transfer { 185.91.165.51; 194.228.2.1; 194.228.220.83; 194.228.220.88;
195.113.161.178; };
    notify yes;
};

zone "16.172.in-addr.arpa" IN {
    type forward;
    forwarders { 172.16.1.1; 172.16.1.4; 172.16.1.22; };
};

zone "168.192.in-addr.arpa" IN {
    type forward;
    forwarders { 172.16.1.1; 172.16.1.4; 172.16.1.22; };
};

```

4.5.3 Příprava domén

Jelikož se náš server bude starat o více domén, je potřeba připravit pro každou doménu vlastní adresář s konfiguračními soubory. Potřebná souborová a adresářová struktura je patrná z předchozí části v konfiguračním souboru „*/etc/bind/named.conf.local*“. Pomocí následujícího příkazu bude vytvořena požadovaná adresářová struktura:

```
„sudo mkdir /var/cache/bind/<požadovaný_adresář>“
```

4.5.4 Konfigurace je rozdělena na následující možnosti nastavení:

\$TTL – Time-To-Live – v kontextu DNS definuje dobu ve vteřinách, po jakou může být záznam uchovávan v mezipaměti na ostatních resolversch. Nedoporučuje se používat „0“ tedy žádná cache z důvodu zpětné kompatibility DNS serverů.

TXT – určuje, které IP adresy mohou odesílat za danou doménu emailové zprávy.

SOA^[14] – Star of Authority – definuje globální parametry dané domény. V dané doméně je možné použít pouze jeden SOA záznam. Záznam jako takový obsahuje následující záznamy.

- MNAME – primární název serveru dané zóny, tedy serveru, na kterém běží BIND
- SERIAL – sériové číslo dané zóny. Pokud sekundární název serveru podřízený tomuto pozoruje zvýšení sériového čísla, předpokládá, že zóna byla aktualizována a zahájí její přenos a aktualizaci.
- REFRESH – počet vteřin, po které by měli ostatní DNS servery dotazovat master záznam pro SOA a detekovat změny zóny
- RETRY – počet vteřin, kdy by měli ostatní servery požadovat opětovnou odpověď na sériové číslo z master serveru, pokud nedostanou odpověď – doporučeno 7200 sec.
- EXPIRE – počet vteřin, po kterých ostatní servery přestanou odpovídat požadavkům na tuto zónu, pokud jim master server neodpoví. Tato hodnota musí být větší než hodnoty refresh a retry, doporučení je min. 3600000, tedy 1000 hodin.
- DEFAULT_TTL – nastavuje se na stejnou hodnotu jako expire, neurčuje výchozí hodnotu „ttl“

NS – Name Server – tedy jmenný server. Vyjmenované autoritativní servery dané zóny

CNAME – mapuje alias nebo přezdívku na skutečný nebo kanonický název, který může být i mimo aktuální zónu.

A - adresní záznam, jedná se o adresu stanice / serveru

_AUTODISCOVER._TCP – umožňuje jednoduší konfiguraci klientů pro starší Exchange servery.^[27]

Níže bude uveden, jako příklad, výpis jednoho konfiguračního souboru:

```
$TTL 18000
@           IN      SOA   linuxspam.eltodo.cz. root.spamlinux.eltodo.cz. (
                2013022601 ; serial
                3600 ; refresh
                3600 ; retry
                129600 ; expire
                129600 ; default_ttl
                )
           IN      NS    linuxspam.eltodo.cz.
           IN      MX    10   linuxspam.eltodo.cz.
           IN      TXT   "v=spf1 ip4:185.91.165.51 ip4:194.228.220.82
ip4:194.228.220.88 ip4:195.113.161.178 -all"
           IN      TXT   "MS=ms63756800"
           IN      A     217.31.53.21

www        IN      CNAME  eltodo.cz.
linuxspam  IN      A      185.91.165.51
linux      IN      A      194.228.220.82
prace     IN      A      87.236.196.206
www.prace  IN      A      87.236.196.206
profil    IN      A      87.236.196.206
crm       IN      A      194.228.220.83
www       IN      A      87.236.196.206
polepy    IN      A      194.228.220.83
sdt       IN      A      194.228.220.84
trenazer  IN      A      195.113.161.181
sim       IN      A      194.228.220.83
crl       IN      A      194.228.220.82
crl       IN      A      194.228.220.88
rudna     IN      A      194.228.40.170
edsftp    IN      A      90.176.143.76
ty nec.net IN      A      88.101.158.242
```



```

vpn      IN      A      80.188.202.86 ; VPN pristup
ciscoasa IN      A      80.188.202.86
web1     IN      A      194.228.220.88
vpnhvoz  IN      A      90.183.17.222
hv.proxy IN      A      192.168.32.11
abalon   IN      A      194.228.220.86
astra    IN      A      194.228.220.91
dag1     IN      A      194.228.220.93
cas1     IN      A      194.228.220.94
internal-mail IN    A      192.168.6.9
internal-mail IN    A      172.16.1.12
internal-mail IN    A      172.16.1.23
dataroom IN      A      194.228.220.87
zet      IN      A      46.36.35.34
nomriz   IN      A      46.36.35.34
satel    IN      A      46.36.35.34
stratdet IN      A      81.0.216.37
ustrednaHk IN    A      193.86.140.71
unir     IN      A      85.255.2.156
navapl   IN      A      194.228.220.82
share    IN      A      194.228.220.82
owncloud IN      A      194.228.220.82

```

; CNAME záznamy

```

standard IN    CNAME linuxspam
dalpo    IN    CNAME linuxspam
inep     IN    CNAME linuxspam
znalsys  IN    CNAME linuxspam
safetun  IN    CNAME linuxspam
kvet     IN    CNAME linuxspam
podpora  IN    CNAME linuxspam
www.podpora IN  CNAME linuxspam
prilepy  IN    CNAME linuxspam
rymice   IN    CNAME linuxspam

```

```

rymarov      IN      CNAME  linuxspam
strelice     IN      CNAME  linuxspam
tomms        IN      CNAME  linuxspam
egis         IN      CNAME  linuxspam
vesint       IN      CNAME  linuxspam
ezadost      IN      CNAME  linuxspam
vgctelco    IN      CNAME  linuxspam
mailing      IN      CNAME  linuxspam
amos         IN      CNAME  linuxspam
alarmy       IN      CNAME  linuxspam
baska        IN      CNAME  linuxspam
unhost       IN      CNAME  linuxspam
si           IN      CNAME  linuxspam

_autodiscover._tcp      IN      SRV 0 0 443  abalon.eltodo.cz.
_autodiscover._tcp      IN      SRV 0 0 443  exhvoz.eltodo.cz.
_autodiscover._tcp      IN      SRV 0 0 443  astra.eltodo.cz.
_autodiscover._tcp      IN      SRV 0 0 443  cas1.eltodo.cz.

```

4.5.5 Podepsání domén

Aby byl náš DNS server bezpečný a tedy i důvěryhodný, je nutné ho zabezpečit pomocí DNSSEC. K tomu je potřeba aktivovat funkcionalitu „*dnssec-enable yes*“ v „*named.conf.option*“. Jelikož budeme podepisovat více domén, bude pro tyto účely stvořen následující skript „*podepsani_domen.sh*“. V tomto souboru je potřeba vytvořit klíče a následně jimi podepsat doménu. Samotný skript bude vypadat takto:

```

#!/bin/bash

# elektrosignal.cz
cd /var/cache/bind/elektrosignal.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu elektrosignal.cz"
dnssec-signzone -S -N unixtime -3 $nahoda elektrosignal.cz

```

```
rndc reload elektrosignal.cz

# optun.cz
cd /var/cache/bind/optun.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu optun.cz"
dnssec-signzone -S -N unixtime -3 $nahoda optun.cz
rndc reload optun.cz

# eltodo.cz
cd /var/cache/bind/eltodo.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu eltodo.cz"
dnssec-signzone -S -N unixtime -3 $nahoda eltodo.cz
rndc reload eltodo.cz

# net.eltodo.cz
cd /var/cache/bind/net.eltodo.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu net.eltodo.cz"
dnssec-signzone -S -N unixtime -3 $nahoda net.eltodo.cz
rndc reload net.eltodo.cz

# ext.eltodo.cz
cd /var/cache/bind/ext.eltodo.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu ext.eltodo.cz"
dnssec-signzone -S -N unixtime -3 $nahoda ext.eltodo.cz
rndc reload ext.eltodo.cz

# vegacom.cz
cd /var/cache/bind/vegacom.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu vegacom.cz"
```

```

dnssec-signzone -S -N unixtime -3 $nahoda vegacom.cz
rndc reload vegacom.cz

# ext.vegacom.cz
cd /var/cache/bind/ext.vegacom.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu ext.vegacom.cz"
dnssec-signzone -S -N unixtime -3 $nahoda ext.vegacom.cz
rndc reload ext.vegacom.cz

# ext.vegacom.cz
cd /var/cache/bind/dohled.vegacom.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu dohled.vegacom.cz"
dnssec-signzone -S -N unixtime -3 $nahoda dohled.vegacom.cz
rndc reload dohled.vegacom.cz

# energovod.cz
cd /var/cache/bind/energovod.cz
nahoda=$(cat /dev/urandom | tr -cd 'a-f0-9' | head -c 32)
echo -e "\n\nPodepisuji doménu energovod.cz"
dnssec-signzone -S -N unixtime -3 $nahoda energovod.cz
rndc reload energovod.cz

```

Aby bylo možné soubor spustit, je potřeba mu nastavit práva, která to umožňují, což bude provedeno příkazem „*chmod*“: ^[1]

```
„chmod 711 /root/bin/podepsani_domen.sh“
```

Před samotným spuštěním skriptu je potřeba vytvořit pár certifikátů pro každou doménu.

To bude provedeno pomocí nástroje „*dnssec-keygen*“ s následujícími přepínači

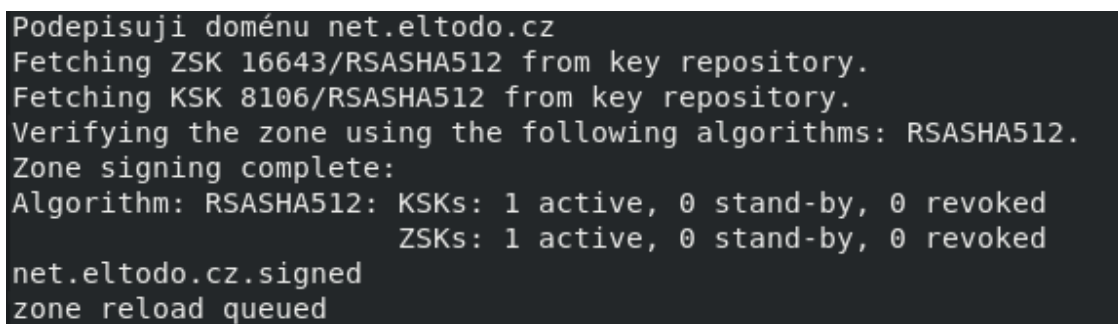
- *r* – určuje nám zdroj náhodnosti /dev/urandom nebo ekvivalentní zařízení, ve výchozím nastavení zdrojem náhodnosti volí klávesnice

- a – vybírá šifrovací algoritmus RSASHA1, DSA, DH (Diffie Hellman) nebo HMAC-MDA5
- b – specifikuje počet bitů v klíči. Jeho velikost závisí na použitém šifrovacím algoritmu.
- n – určuje typ vlastníka klíče. Hodnota názvu musí být ZONE, HOST/ENTITY, USER/OTHER
- f – nastaví zadaný příznak (flag) do pole flag pro záznam DSNKEY.^[28]

Pro naše potřeby je tedy nutné vytvořit pro každou doménu vlastní pár klíčů, což bude provedeno pomocí následujících příkazů v jednotlivých adresářích domén:

```
dnssec-keygen -r /dev/urandom -a RSASHA512 -b 2048 -3 -n ZONE <nazevdomeny.cz>
dnssec-keygen -r /dev/urandom -a RSASHA512 -b 2048 -3 -n ZONE -f ZONE
<nazevdomeny.cz>
```

Po vygenerování doménových klíčů dojde ke spuštění samotného skriptu „*podepsani_domen.sh*“. Po dokončení skriptu, který by měl doběhnout během několika vteřin, bychom měli vidět, že jednotlivé domény jsou v pořádku podepsány.



```
Podepisuji doménu net.eltodo.cz
Fetching ZSK 16643/RSASHA512 from key repository.
Fetching KSK 8106/RSASHA512 from key repository.
Verifying the zone using the following algorithms: RSASHA512.
Zone signing complete:
Algorithm: RSASHA512: KSKs: 1 active, 0 stand-by, 0 revoked
                    ZSKs: 1 active, 0 stand-by, 0 revoked
net.eltodo.cz.signed
zone reload queued
```

Obr. č. 11, Výsledek podpisu domény

Dalším krokem bude spouštění daného skriptu každé pondělí v 1 hodinu ráno, abychom zajistili stálou aktuálnost DNSSEC a tedy vysokou bezpečnost našeho serveru.

To bude zajištěno úpravou „*/etc/crontab*“, kam bude přidán následující řádek:

```
00 1 * * 1 root /root/bin/podepsani_domen.sh
```

Před samotnou úpravou DNS záznamů na straně poskytovatele našeho doménového registrátora je ještě potřeba zaktivovat službu BIND serveru, aby se spouštěla automaticky po zapnutí serveru. To bude provedeno následujícím příkazem:

```
systemctl enable bind9.service
```

a nastartováním serveru:

```
systemctl start bind9.service
```

Nyní je potřeba provést úpravu na straně registrátora domény, kdy změníme DNS server na tento server. Po této změně trvá DNS serverům až 24 hodin, než se změna propíše. Nicméně v CZ je propsání poměrně rychlé, v řádu minut. Následně bychom měli provést otestování funkcionality. Otestování jako takové proběhne v závěru, po dokončení instalace a konfigurace všech prvků serveru.

4.6 APACHE Server

Samotná instalace serveru je jednoduchá a bude provedena ve výchozí konfiguraci příkazem:

```
„sudo apt-get install -y apache2“
```

Po dokončení instalace je server automaticky spuštěn, což bude ověřeno příkazem:

```
„sudo systemctl status apache2.service“
```

4.6.1 Konfigurace serveru

První soubor, ve kterém je potřeba provést úprava konfigurace, je „ports.conf“, který umožní přidat nestandardní porty pro webové servery. Samotná úprava konfiguračního souboru vypadá následovně:^[29]

```
NameVirtualHost *:80
NameVirtualHost *:443
NameVirtualHost *:8888
Listen 80
Listen 8888

<IfModule ssl_module>
    Listen 443
    Listen 8042
    Listen 10443
    Listen 10444
</IfModule>
<IfModule mod_gnutls.c>
    Listen 443
    Listen 8042
    Listen 10443
    Listen 10444
</IfModule ssl_module>
```

4.6.2 Konfigurace serveru pro reversní proxy

Server jako takový se nedostane do vnitřní sítě, pokud mu to nebude umožněno. Server má na firemním firewallu vždy nastaven požadovaný přístup mezi tímto serverem a serverem poskytujícím webovou prezentaci nebo aplikaci. Kvůli síťovému nastavení serveru tento server nezná vnitřní adresy. Je tedy potřeba serveru nastavit vnitřní servery. To bude provedeno úpravou konfiguračního souboru „/etc/hosts“ přidáním následujících řádků:

```
185.91.165.51 linuxspam.eltodo.cz linuxspam
194.228.220.82 linux.eltodo.cz linux
172.16.1.1    dhcp-n1.eltodo.cz dhcp-n1
172.16.1.4   arthur.eltodo.cz arthur
172.16.1.12  abalon.eltodo.cz abalon
172.16.1.23  astra.eltodo.cz astra
172.16.1.128 owncloud.eltodo.cz owncloud
172.16.1.128 share.eltodo.cz      share
```

4.6.3 Vytvoření první serverové konfigurace

Samotná konfigurace je rozdělena na několik možností nastavení:

REDIRECT – přesměrování stránky jinam, kupříkladu z HTTP na HTTPS

SSENGINE – zapíná SSL funkcionalitu pro danou konfiguraci

SSLVERIFYCLIENT – nastavení ověření certifikátu klienta

SSLCERTIFICATEKEYFILE – nastavuje plnou cestu k privátnímu klíči certifikátu použitému pro tento server

SSLCERTIFICATECHAINFILE – nastavuje cestu k řetězovému certifikátu certifikačních autorit

SSLCERTIFICATEFILE – nastavuje plnou cestu k SSL certifikátu

SSLCIPHERSUITE – tato komplexní směrnice používá šifrovací řetězec oddělený dvojtečkou, který se skládá ze speciální šifry a konfiguruje šifrovací balíček, pomocí kterého mohou klienti přistupovat k webu pomocí SSL.

SSLPROTOCOL – pomocí této směrnice se nastavuje povolení jednotlivých protokolů – od SSL až po TLSv1.3. ^[29]

Samotná konfigurace poté vypadá po spuštění následujícího příkazu takto:

```
„sudo vim /etc/apache/sites-available/001-share.eltodo.cz“
```

```
<VirtualHost *:80>
    ServerAdmin ITSupport@eltodo.cz
    ServerName owncloud.eltodo.cz
    Redirect "/" "https://owncloud.eltodo.cz/"
```



```

ErrorLog ${APACHE_LOG_DIR}/owncloud.eltodo.cz-error_log
CustomLog ${APACHE_LOG_DIR}/owncloud.eltodo.cz-access_log common
</VirtualHost>
<VirtualHost *:443>
    ServerAdmin ITSupport@eltodo.cz
    DocumentRoot /var/www_virtual/owncloud.eltodo.cz
    ServerName owncloud.eltodo.cz
    ErrorLog ${APACHE_LOG_DIR}/owncloud.eltodo.cz-error_log
    CustomLog ${APACHE_LOG_DIR}/owncloud.eltodo.cz-access_log common

    SSLEngine on
    SSLProxyEngine on
    SSLVerifyClient none
    SSLCertificateFile      /etc/apache2/ssl/new_geo_eltodo.cer
    SSLCertificateKeyFile   /etc/apache2/ssl/new_geo_eltodo.key
    SSLCertificateChainFile /etc/apache2/ssl/digi_root.crt

    SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-
GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256

    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1

    # Always set these headers.
    Header always set Access-Control-Allow-Origin "*"
    Header always set Access-Control-Allow-Methods "POST, GET, OPTIONS,
DELETE, PUT"
    Header always set Access-Control-Max-Age "1000"
    Header always set Access-Control-Allow-Headers "x-requested-with, Content-Type,
origin, authorization, accept, client-security-token"

    # Added a rewrite to respond with a 200 SUCCESS on every OPTIONS request.

```

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} OPTIONS
RewriteRule ^(.*)$ $1 [R=200,L]

# ProxyRequests Off
<Proxy *>
    Order deny,allow
    Deny from all
</Proxy>
# ProxyVia On

ProxyPass / https://owncloud.eltodo.cz/

<Location / >
    ProxyPassReverse /
    Order allow,deny
    Allow from all
</Location>
</VirtualHost>
```

Po dokončení konfigurace je potřeba vytvořit adresář pro danou webovou prezentaci. To bude provedeno příkazem:

```
„sudo mkdir /var/www_virtual/share.eltodo.cz
```

4.6.4 Aktivace webové prezentace

Na základě této konfigurace je potřeba, aby byla provedena aktivace dané webové stránky. To provedeme jednoduše spuštěním dvou příkazů:

```
„ln -s /etc/apache2/sites-available/001-share.eltodo.cz /etc/sites-enabled/001-  
share.eltodo.cz
```

```
„sudo systemctl restart apache2.service“
```

4.7 Závěrečné testování

4.7.1 Testování emailové komunikace:

Samotné testování funkčnosti jednotlivých prvků bude provedeno jednoduchou kontrolou, zda funguje emailová komunikace. A zda došlo ke snížení počtu spamových zpráv.

Abychom zjistili, jestli dané řešení funguje a jeho jednotlivé prvky kontrolují zprávy, provedeme kontrolou logů následujícím příkazem:

```
„tail -f /var/log/mail.log“
```

Tento příkaz nám zobrazuje aktuální provoz na emailovém serveru a přírůstky v LOG souborech. Abychom ověřili podrobnosti o zprávách, je potřeba si vytáhnout náhodně zprávu pomocí unikátního čísla zprávy, což bude provedeno následujícím způsobem:

```
„grep <kód_zprávy> /var/log/mail.log“
```

```
root@linuxspam: /home#grep x1L6A4o0003501 /var/log/mail.log
Feb 21 07:10:04 linux sm-mta[3501]: x1L6A4o0003501: from=<root@linuxspam.eltodo.cz>, size=3281, class=0, nrcpts=1, msgid=<201902210610.x1L6A4Ge003500@linuxspam.eltodo.cz>, proto=ESMTP, daemon=MTA-v4, relay=localhost [127.0.0.1]
Feb 21 07:10:04 linux sm-mta[3501]: x1L6A4o0003501: Milter add: header: X-Virus-Scanned: clamav-milter 0.99.4 at linux
Feb 21 07:10:04 linux sm-mta[3501]: x1L6A4o0003501: Milter add: header: X-Virus-Status: Clean
Feb 21 07:10:04 linux sendmail[3500]: x1L6A4Ge003500: to=root, ctladdr=root (0/0), delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=33017, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (x1L6A4o0003501 Message accepted for delivery)
Feb 21 07:10:05 linux sm-mta[3502]: x1L6A4o0003501: to=kolmanm@eltodo.cz, ctladdr=<root@linuxspam.eltodo.cz> (0/0), delay=00:00:01, xdelay=00:00:01, mailer=esmtpl, pri=33566, relay=internal-mail.eltodo.cz. [172.16.1.23], dsn=2.0.0, stat=Sent (<201902210610.x1L6A4Ge003500@linuxspam.eltodo.cz> [InternalId=2729944] Queued mail for delivery)
```

Obr. č. 12, Přehled výpisu emailových logů

Jak je z testu patrné, proběhnou veškeré testy a pošta se odešle na interní Exchange servery k doručení.

4.7.2 Testování DNS serveru

Nejjednodušší testování bylo provedeno z venkovní sítě ověřením některého ze serverů, které jsou v naší doméně. Pomocí příkazu „ping“, z externí sítě, byly provedeny dotazy na jednotlivé DNS záznamy, které jsou zaznamenány na tomto serveru. Samotné ověření

funkcionality DNSSEC bylo poté potřeba ověřit pomocí validátorů. Byly použity dva validátory pro zajištění nezávislosti testování:

<https://dnsviz.net>

<https://dnssec-analyzer.verisignlabs.com>

4.7.3 Testování Apache serveru

Základní testování bylo provedeno vizuální kontrolou jednotlivých webových prezentací a to jak z vnitřní sítě, tak i z externí sítě. Následně bylo provedeno testování pomocí webové stránky „<https://www.ssllabs.com>“. Tato stránka umožňuje otestování zadané webové prezentace, kde v testech bylo získáno hodnocení „A“. Tedy dostatečné SSL zabezpečení a důvěryhodnost webové stránky.

4.7.4 Testování zabezpečení serveru

Testování bylo provedeno formou vzdáleného připojení pomocí aplikace Telnet. Aby se server nestal terčem útoků, nesmí být open relay. Tedy přes tento server mohou odesílat pouze servery, které jsou uvedené v konfiguraci. Server neumožnil odeslání emailové zprávy pomocí protokolu SMTP a tím bylo ověřeno, že server není open relay. Dále byl server testován pomocí aplikace „*nmap*“, kde bylo ověřeno otevření pouze potřebných portů pro tento server. Tímto testováním byla ověřena funkcionality celého řešení a server úspěšně prošel.

5 Závěr

Hlavním cílem bylo řešení Antispamového serveru založeného na systému Linux jako ústředního prvku mailové komunikace s antivirovou kontrolou. Dalším cílem této práce byla instalace a konfigurace DNS serveru v kombinaci se serverem reversní proxy pro agilní publikování vnitropodnikových webových prezentací s možností konfigurace z jednoho místa.

Hlavní i dílčí cíle byly naplněny realizací na fyzický server. Tím se podařilo vyhodnotit potřeby společnosti s minimem vynaložených nákladů, snížit zatížení starších exchange serverů spamem a zvýšit zabezpečení nasazením antivirové kontroly. Podrobná instalace systému, jakožto i jednotlivých částí řešení, byla detailně popsána spolu s vysvětlením jednotlivých kroků a možností nastavení.

Výsledné řešení je plně funkční, pořizovací náklady na toto řešení se rovnají pouze pořizovací ceně serveru. Hlavním přínosem práce je plně funkční a nakonfigurovaný antispamový server, který bude společností dále využíván pro publikování vlastních webových prezentací z vnitřních serverů do externí sítě. S tím bude nadále pomáhat i vlastní DNS server. Díky tomuto řešení bude publikování webových prezentací rychlejší a pohodlnější pro konfiguraci z jednoho místa.

6 Seznam použitých zdrojů

- [1] KAMENÍK, P. Příkazový řádek v Linuxu. Praha: Computer Press, 2011. [cit. 05.02.2019]. ISBN 9788025128190
- [2] SHAH, Steve. Administrace systému Linux: překlad čtvrtého vydání. 1. vyd. Praha: Grada, 2007, [cit. 05.02.2019]. ISBN 978-80-247-1694-7
- [3] SCHRODER, Carla. Linux Kuchařka administrátora sítě: první vydání, Computer Press, a.s., 2009, [cit. 05.02.2019]. ISBN 978-80-251-2407-9

Internetové zdroje:

- [4] History of Linux [online]. [cit. 05.02.2019]. Dostupné z: https://en.wikipedia.org/wiki/History_of_Linux.
- [5] GNU Operating system [online]. [cit. 05.02.2019]. Dostupné z: <https://www.gnu.org>
- [6] Global spam volume as percentage of total e-mail traffic from January 2014 to September 2018, by month [online]. [cit. 05.02.2019]. Dostupné z: <https://www.statista.com/statistics/420391/spam-email-traffic-share>
- [7] The World's Worst Spam Enabling Countries [online]. [cit. 05.02.2019]. Dostupné z: <https://spamhaus.org/statistics/countries>
- [8] Co je to HOAX [online]. [cit. 05.02.2019]. Dostupné z: <http://hoax.cz/hoax/co-je-to-hoax>
- [9] Apache SpamAssassin - Wikipedia. [online]. [cit. 05.02.2019]. Dostupné z: https://en.wikipedia.org/wiki/Apache_SpamAssassin
- [10] ClamavNet [online]. Copyright © 2004 [cit. 06.02.2019]. Dostupné z: <https://www.clamav.net/documents/clamav-overview>
- [11] SourceFire Acquires ClamAV | InfoWorld. InfoWorld - Technology insight for the enterprise [online]. [cit. 05.02.2019]. Copyright © 2019 IDG Communications, Inc. [cit. 05.02.2019]. Dostupné z: <https://www.infoworld.com/article/2636039/open-source-software/sourcefire-acquires-clamav.html>
- [12] Cisco Announces Agreement to Acquire Sourcefire | The Network | The Network. Cisco Newsroom | The Network [online]. [cit. 05.02.2019]. Dostupné z:

- <<https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1225204>>
- [13] Debian 9: Install BIND for DNS server | Narrow Escape | Hiroom2 [online]. [cit. 05.02.2019]. Dostupné z: <<https://www.hiroom2.com/2017/06/27/debian-9-install-dns-server>>
- [14] SOA record – Wikipedia. [online]. [cit. 05.02.2019]. Dostupné z: <https://en.wikipedia.org/wiki/SOA_record>
- [15] Domain Name System - Wikipedia. [online]. [cit. 05.02.2019]. Dostupné z: <https://en.wikipedia.org/wiki/Domain_Name_System>
- [16] Email - Wikipedia. [online]. [cit. 05.02.2019]. Dostupné z: <<https://en.wikipedia.org/wiki/Email>>
- [17] Apache HTTP Server - Wikipedia. [online]. [cit. 05.02.2019]. Dostupné z: <https://en.wikipedia.org/wiki/Apache_HTTP_Server>
- [18] Email spoofing - Wikipedia. [online]. [cit. 12.02.2019]. Dostupné z: <https://en.wikipedia.org/wiki/Email_spoofing>
- [19] Sender Policy Framework - Wikipedia. [online]. [cit. 12.02.2019]. Dostupné z: <https://en.wikipedia.org/wiki/Sender_Policy_Framework>
- [20] Internet Assigned Numbers Authority. Internet Assigned Numbers Authority [online]. [cit. 12.02.2019]. Dostupné z: <<https://www.iana.org>>
- [21] CZ.NIC - O DNSSEC. CZ.NIC [online]. Copyright © 2019 CZ.NIC, z. s. p. o. [cit. 23.02.2019]. [cit. 12.02.2019]. Dostupné z: <<https://www.nic.cz/page/513/about-dnssec/>>
- [22] DNS spoofing - Wikipedia. [online]. [cit. 12.02.2019]. Dostupné z: <https://en.wikipedia.org/wiki/DNS_spoofing>
- [23] GitHub - jcbf/smf-spf. GitHub [online]. Copyright © 2019 [cit. 24.02.2019]. Dostupné z: <<https://github.com/jcbf/smf-spf>>
- [24] Reverse Proxy Guide - Apache HTTP Server Version 2.4. Welcome! - The Apache HTTP Server Project [online]. [cit. 24.02.2019]. Dostupné z: <https://httpd.apache.org/docs/2.4/howto/reverse_proxy.html>
- [25] Mail::SpamAssassin::Conf - SpamAssassin configuration file. [online]. [cit. 24.02.2019]. Dostupné z: <https://spamassassin.apache.org/full/3.1.x/doc/Mail_SpamAssassin_Conf.html>
- [26] INSTALLATION AND OPERATION GUIDE | Sendmail [online]. [cit. 04.02.2019]. Dostupné z: <<https://www.sendmail.org/~ca/email/doc8.12/op.html>>

- [27] Bind9 - Debian Wiki. Debian Wiki [online]. [cit. 04.02.2019]. Dostupné z:
<<https://wiki.debian.org/Bind9>>
- [28] DNSSEC key generation tool - Linux man page. Linux Documentation [online]. Copyright © 2004, 2005, 2007 [cit. 04.02.2019]. Dostupné z:
<<https://linux.die.net/man/8/dnssec-keygen>>
- [29] The Apache HTTP Server Project [online]. [cit. 04.02.2019]. Dostupné z:
<https://httpd.apache.org/docs/2.4/>
- [30] Mail::SpamAssassin - Spam detector and markup engine. [online]. [cit. 24.02.2019]. Dostupné z:
<https://spamassassin.apache.org/full/3.1.x/doc/Mail_SpamAssassin.html>