Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Implementace routeru s firewallem za pomoci Raspberry Pi

Anna Kleinová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Anna Kleinová

Informatika

Název práce

Implementace routeru s firewallem za pomoci Raspberry Pi

Název anglicky

Implementation of router with firewall using Raspberry Pi

Cíle práce

Cílem práce bude vytvoření bezdrátového routeru s vlastním firewallem na platformě Raspberry Pi, pro důkladné a přehledné monitorování provozu v síti s využitím v soukromé i firemní sféře. Důraz bude kladen na zabezpečení sítě s nastavením vlastních pravidel, proxy a DNS serveru.

Metodika

V práci bude provedeno srovnání a analýza dostupných softwarových a hardwarových komponentů vhodných pro vytvoření bezdrátového routeru za využití Raspberry Pi a jejich následný výběr. Po úvodním výběru komponentů práce se přejde k instalaci a konfiguraci hardwarové a softwarové části pro správný chod routeru, tak aby mohl komunikovat se sítí a zařízeními v síti. Důležitou součástí routeru bude implementovaný firewall, kde budou nastaveny potřebné pravidla pro paketové filtry a síťové služby. Pro lepší přehlednost toků v síti bude k firewallu přidáno webové rozhraní.

Doporučený rozsah práce

30-40 stran

Klíčová slova

Firewall, Router, Raspberry PI, Linux, Proxy, DNS

Doporučené zdroje informací

MONK, Simon. Raspberry Pi Cookbook. 2nd Edition. Newton: O'Reilly, 2016. ISBN 9781491939109.

RASH, Michael. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort. San Francisco: No Starch Press, 2007. ISBN 1593271417.

SHOTS, William. The Linux Command Line: A Complete Introduction. 2nd Edition. San Francisco: No Starch Press, 2019. ISBN 1593279523.

SUEHRING, Steve. Linux Firewalls: Enhancing Security with nftables and Beyond: Enhancing Security with nftables and Beyond. 4th Edition. Boston: Addison-Wesley Professional, 2015. ISBN 0134000021.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 31. 10. 2022

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Implementace routeru s firewallem za pomoci Raspberry Pi" jsem vypracovala 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 autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 15.3.2023

Anna Kleinová

Poděkování

Ráda bych touto cestou poděkovala Ing. Marku Píckovi Ph.D., za vedení bakalářské práce. Dále mé rodině a přátelům, kteří mě podporovali během celého studia.

Implementace routeru s firewallem za pomoci Raspberry Pi

Abstrakt

Tato bakalářská práce se zabývá implementací routeru s firewallem na minipočítači Raspberry Pi 4B s využitím Linux operačního systému do sítě malého rozsahu. Teoretická část této práce je věnována rešerši odborné literatury, aby se bylo možné lépe seznámit s probíraným tématem a jeho sounáležitostmi. Jsou zde tak vysvětlené všechny části, které router s firewallem může obsahovat. Zároveň jsou popsány alternativy podoby systému a důvody proč zrovna hardwarové a softwarové komponenty, které byly zvoleny pro tuto práci byly vybrány. Praktická část práce se zabývá popsáním požadavků vytvořené sítě a její dosavadních specifikací. Hlavní součástí je konfigurace routeru, firewallu a přidaných síťových služeb. Tato část zároveň obsahuje samotné testování nakonfigurovaných komponentů jako DNS, firewall pravidel a propustnosti sítě. V závěru práce je zhodnocena použitelnost systému pro reálné využití.

Klíčová slova: Router, Firewall, Linux, Proxy, DNS, Bezpečnost, Raspberry Pi, DHCP

Implementation of router with firewall using Raspberry Pi

Abstract

This bachelor's thesis deals with the implementation of a router with a firewall on a Raspberry Pi 4B minicomputer using the Linux operating system in a small-scale network. The theoretical part of this thesis is dedicated to the research of professional literature, in order to become better acquainted with the discussed topic and its connections. All the parts that a router with a firewall can contain are explained here. At the same time, the alternatives of the system form and the reasons why the hardware and software components that were chosen for this work are described. The practical part of the work deals with the description of the requirements of the created network and its current specifications. The main part is the configuration of the router, firewall and added network services. This part also contains the actual testing of configured components such as DNS, firewall rules and network throughput. At the end of the work, the applicability of the system for real use is evaluated.

Keywords: Router, Firewall, Linux, DNS, Proxy, Security, Raspberry Pi, DHCP

Obsah

1 Úvod

V době po covidové pandemii je čím dál tím častější pracovat z domova, v takovém případě je potřeba svá data chránit i mimo pracovní prostředí firmy. Internetu je využíváno k práci čím dál tím více a tím tak vystavujeme naše data a identitu v risk. Je dobré se tedy zamyslet nad tím, jak tyto data správně chránit.

Pokud již pracujeme v jakékoliv korporátní firmě, síť, na které vše ve firmě komunikuje je většinou již zabezpečená a spravována IT oddělením firmy. Avšak pokud svojí práci přesuneme na home office o tuto ochranu přijdeme. V tomto případě připadá v úvahu zabezpečit i vlastní síť, abychom se tak uchránili před útoky.

Většina routerů už nějaké vlastní nastavení zabezpečení má, ovšem ne v takové míře, abychom naši síť ochránili dostatečně. Také ne všechny domácnosti samostatný vlastní router vlastní, místo toho je využíváno hojně kombinace routeru s modemem, který je dodán od poskytovatele internetu. Ve většině případu již před vyrobená zařízení mají nainstalovaný po pár měsíců již starý firmware či celkově software, který může nést bezpečnostní rizika bez aktualizace. Těchto zastaralých systému se v napadení používá nejvíce, je dobré udržovat všechna zařízení na nejaktuálnější verzi a každý by měl na tuto skutečnost brát ohled. Nelze počítat pouze s autentizací, že ji nikdo neprolomí. Musíme také počítat s dalšími riziky jakožto šíření virů, vzdálených připojení a jiných infekcí sítě.

Pro správnou ochranu sítě je potřeba nastavit mnohá kritéria a omezení sítě, abychom předešli nevyžádaným akcím. K tomuto poslouží firewall, který aktivně brání průniku podezřelých souboru a komunikací. Můžeme skrze něj nastavit pravidla a blokovat komunikační porty, které by mohli být rizikové. Mimo firewall lze také přidat další síťové služby, kupříkladu proxy serveru, který blokuje nebezpečný obsah stránek a DNS server s cache, který nám zefektivní načítání stránek jejich uložením v mezi paměti.

Technika se stále rozvíjí a více systémů je připojenou k internetu. Mnoho z nás mimo práci má na svém počítači či telefonu řadu intimních informací, které by neměli patřit nikomu jinému. Ať už jsou to bankovní údaje, fotografie nebo rozpracovaný kariérní projekt, musíme aktivně dbát na bezpečnost těchto informací. Měli bychom brát v potaz, že veškerá naše zařízení, jež jsou připojena k síti spolu komunikují. Ne všichni ovšem ví, jaká komunikace se odehrává.

Vlastní router s firewallem nám mimo zabezpečení nabídne kupříkladu i lepší připojení k internetu s možností dalšího vylepšení a optimalizace vnitřní sítě.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je vytvoření bezdrátového routeru s vlastním firewallem na platformě Raspberry Pi s využitím Linux operačního systému, pro důkladné a přehledné monitorování provozu sítě s využitím především v soukromé, ale i firemní sféře. Důraz je kladen na zabezpečení sítě s nastavením vhodných pravidel firewallu, proxy, DHCP a DNS serveru. Dílčím cílem je přidání webového rozhraní pro další správu routeru.

2.2 Metodika

V práci bude provedeno srovnání a analýza dostupných softwarových a hardwarových komponentů vhodných pro vytvoření bezdrátového routeru za využití Raspberry Pi a Linux operačního systému. Proběhne porovnání dostupných variant na trhu a upřesnění varianty vybrané pro tento systém. Také budou brány v potaz veškeré sounáležitosti, které k sestavení systému patří. Důkladnější popis teoretické části jakožto firewallu a routeru, tím i jejich dalších podmnožin. Po úvodním výběru komponentů práce se přejde k instalaci a konfiguraci hardwarové a softwarové části pro správný chod routeru, tak aby mohl komunikovat se sítí a zařízeními v síti. Důležitou součástí routeru bude implementovaný firewall, kde budou nastaveny potřebná pravidla pro paketové filtry a síťové služby pro lepší zabezpečení sítě jakožto celku. Pro lepší přehlednost toků v síti a snadnější správu routeru bude k routeru přidáno webové rozhraní, ve kterém bude možné vzdáleně dále upravovat nastavení routeru a kontrolovat dostupné aktualizace.

V poslední řadě bude provedeno testování firewall pravidel, rychlosti a stability připojení routeru a následné na základě syntézy poznatků z předchozích částí proběhne hodnocení vytvořeného systému.

3 Teoretická východiska

3.1 Raspberry Pi

Raspberry Pi je miniaturní počítač, který se hojně využívá pro mnohé účely, jak v domácnosti, tak ve firemní sféře. Hlavním plusem je právě velikost tohoto počítače, díky níž můžeme počítač využívat bez starostí i v relativně malé domácnosti, kde si nemůžeme dovolit větší elektroniku – například server. Velkým pomocníkem může být například v automatizaci domácnosti neboli smart home, nebo například při ochraně dat v síti, kterým se bude zabývat i tato bakalářská práce.

Pro tuto bakalářskou práci bude využito Raspberry Pi 4, který může být snadněji použit jakožto router oproti jeho předchůdcům. Tento model totiž disponuje dedikovaným ethernet portem a dvěma USB 3.0 porty, díky kterým můžeme připojit síťovou redukci, která bude schopna docílit rychlosti až 1 GB/s LAN. Předchozí verze Raspberry Pi mohly docílit pouze maximálně 300 Mbit/s. Také je na místě zmínit existující rozšiřující desky pro modul Raspberry Pi 4, které mohou vést druhé síťové připojení bez použití sdíleného USB rozhraní. Díky této skutečnosti by mělo být v praxi připojení stabilnější. Využití rozšiřující desky ještě více zredukujeme velikost počítače (Monk, 2022).

V době psaní této bakalářské práce došlo redukci Raspberry Pi na skladech, zapříčiněno především krizí během Covidové pandemie, kvůli které se nadměrně snížila produkce. Právě kvůli této skutečnosti nebylo využito modulu a rozšiřující desky v této bakalářské práci (Upton, 2022).

3.1.1 Raspberry Pi 4B

V této bakalářské práci bude využito v tuto chvíli nejnovějšího modelu Raspberry Pi. 4B, který by dle oficiálních zdrojů měl být v produkci alespoň do ledna 2026. Přesné hardwarové specifikace použitého modelu jsou následující (Raspberry Pi Foundation, 2021):

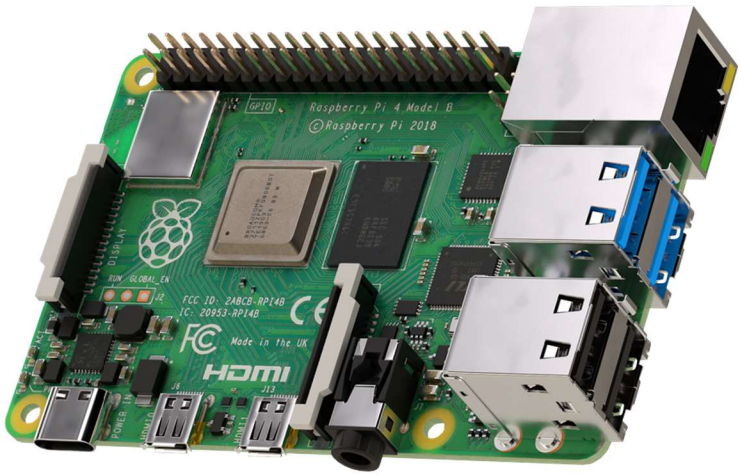
- Čtyřjádrový procesor Broadcom BCM2711 64bit s frekvencí 1.5GHz
- Operační paměť 4GB LPDDR4
- 10/100/1000 Mbit/s Ethernet rozhraní
- Bezdrátová dvoupásmová síť (2.4/5 GHz) dle standardů 802.11b/g/n/ac, Bluetooth 5.0, BLE
- Dva konektory USB 3.0 a dva konektory USB 2.0

- Dvakrát micro HDMI porty s možností až 4K60FPS

Model s těmito specifikacemi lze pořídit v přepočtu za 1650 Kč v MSRP ceně. V důsledku nedostatku na skladech se cena ale může vyšplhat mnohem výše.

Pro úložiště dat bude v případě této práce využito microSD karty. Avšak je možné využít i jiného typu úložiště jako jsou například USB flashdisky nebo externích HDD a SSD. Základním operačním systém využívaným na Raspberry Pi je dodávaný Raspberry Pi OS dříve nazývané Raspbian, kterého také využijeme pro účely této bakalářské práce. Lze využít také široké škály dalších dostupných systémů na tomto minipočítači, například Linux, Windows 10 IoT Core, OpenBSD a NetBSD (Raspberry Pi Trading, 2019).

Obrázek 1: Raspberry Pi 4B



Zdroj: (Raspberry Pi 4 Model B, 2022)

3.1.2 Rozšiřující desky vhodné pro router

Původní plán této práce obsahoval využití rozšiřujících desek společně s Raspberry Pi modulem, který má stejné specifikace jako celý minipočítač, ale bez portů. Z důvodu nedostatku modulů na trhu, a tedy nemožností se k modulu dostat, bylo od této verze práce odstoupeno.

Na trhu jsou dvě prominentní verze rozšiřující desky pro router od výrobců Seeed a DFRobot. Druhá možnost z těchto dvou je právě ta, která měla být použita v této práci dle

původního plánu. Obě zmíněné desky jsou designované pro Raspberry Pi compute module 4. Verze s rozšiřující deskou je mírně nákladnější nežli samotný Raspberry Pi, ale mají i svá pozitiva. Například značná redukce velikosti celého router zařízení a dualní ethernet řešení, díky kterému docílíme stabilnějšímu připojení. Níže jsou blíže představeny obě rozšiřující desky.

Seeed rozšiřující deska je mírně větší nežli ta od DFRobot, avšak i přes to bude značně menší nežli samotný Raspberry Pi 4B. Zabudovaný eth0 je doplněn o další eth1, který je veden skrze USB 3.0 rozhraní. Oproti konkurenční desce nabízí více portů jakožto USB 3.0 nebo také micro HDMI (Seeed Technology, 2022).

Přesné hardwarové specifikace desky od Seeed jsou následující:

- Podpora Raspberry Pi modulu 4
- Ethernet: ETH1: vestavěné v samotném compute modulu
  ETH2: USB 3.0 to GbE Microchip's LAN7800
- USB: 2x USB 3.0
  1x USB 3.0 9-pin rozšíření
  1x USB-C: pro napájení 5V/3A
- Displej: 1x MIPI DSI Konektor
  1x Micro HDMI Konektor

Obrázek 2: Seeed router rozšiřující deska

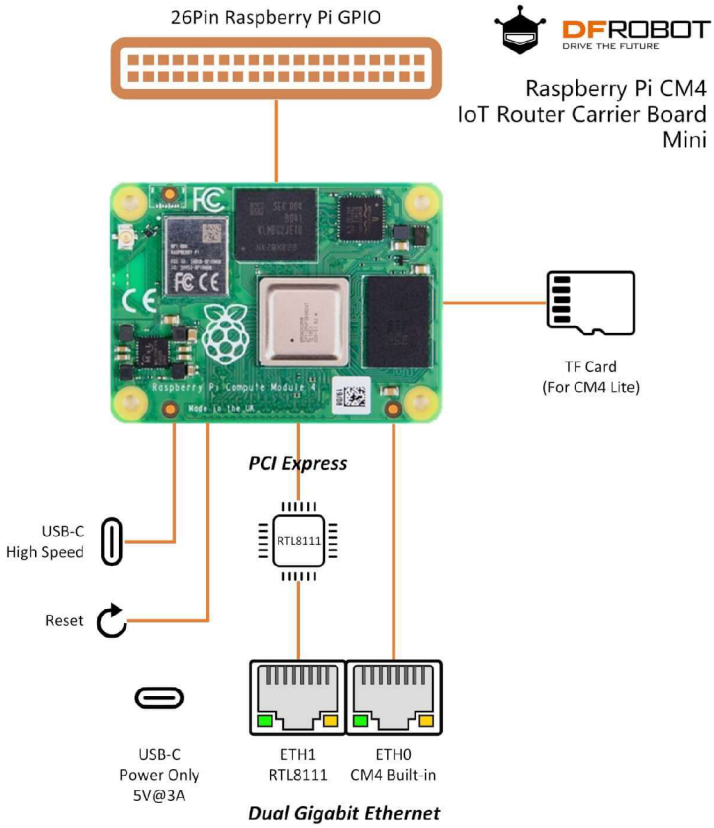
Zdroj: (Geerling, 2021)

DFRobot router rozšiřující deska oproti té od Seeed nepoužívá vedení gigabit sitě skrze USB 3.0 rozhraní, ale skrze PCIe rozhraní, což přináší lepší stabilitu přenosu dat skrze ethernet rozhraní. Tento fakt je znázorněn na obrázku č.2. Rozšiřující desku lze pořídit v přepočtu za 1275 Kč (DFRobot, 2022).

Přesné hardwarové specifikace desky od DFRobot jsou následující:

- Podpora Raspberry Pi modulu 4
- Ethernet: ETH1: vestavěné v samotném compute modulu
  ETH2: PCIE 1000BASE-T NIC
- USB: 1xUSB-C: Pouze pro napájení 5V/3A
  1xUSB-C: USB 2.0 pro normální využití

Obrázek 3: Diagram DFRobot rozšíření



Zdroj: (DFRobot, 2022)

3.2 Operační systém pro router a firewall

Přímo pro cíl vytvoření routeru můžeme využít většinu distribucí Linux, důležitým faktorem pro výběr je možnost nastavení iptables nebo nftables, to lze nalézt téměř u všech distribucí. Vše potřebné pro další nastavení routeru a firewallu je možné na operačním systému Linux doinstalovat. Použít lze ale také přímo specializované a předpřipravené verze operačního systému, která značně usnadní práci s nastavením.

3.2.1 Raspberry Pi OS

Jedná se o operační systém, který je vyvíjen specificky pro minipočítače Raspberry Pi, tudíž by z tohoto důvodu měl být dobře optimalizován a je výrobci doporučován jakoby nejspolehlivější variantou pro základní účely. Operační systém byl postaven na distribuci Debian, po kterém také nesl dřívější název Raspbian. Raspberry Pi OS používá grafické rozhraní (PiXel). V době psaní této bakalářské práce je v produkci verze „Bullseye“, která nahradila předchozí „Buster“ verzi systému (Hattersley, 2023).

Právě tento operační systém bez grafického rozhraní bude použit v této bakalářské práci.

3.2.2 OpenWRT

Operační systém, který je přímo navržen pro účely vytvoření a chodu routeru. Dává možnost vývojářům plnou kontrolu nad firmwarem, a tak se často využívá i na běžných routerech, které lze zakoupit. Nabízí plně otevřený souborový systém se správcem balíčků. OpenWRT má k dispozici více jak 3000 balíčků pro rozšíření systému, díky kterým lze router upravit podle vlastních představ. Nabízí také nainstalované webové rozhraní LuCI pro správu routeru (Russell, 2012).

V době psaní této bakalářské práce je k dispozici nejnovější stabilní verze 22.03 (Spooren, 2022).

3.2.3 Enterprise Linux distribuce

Pokud by se jednalo o systém, který bude použit v korporátní sféře, tedy v podniku, dobrou ne-li správnou volbou může být jedna z Enterprise Linux distribucí. Tyto distribuce jsou předem předpřipravené pro použití v podniku a jejich důležitým plusem je délka podpory použité verze, která ve většině případech dosahá 10 let. Díky tomuto faktu není

třeba operační systém přeinstalovat na nejnovější verzi tak často, jako je tomu u operačních systému pro konzumenty.

Nejznámější Enterprise Linux systémy jsou Red Hat Enterprise Linux, CentOS nebo SUSE Linux (SLED) (SUSE, 2022).

3.2.4 SSH

Pro potřeby routeru a firewallu není nutná instalace systému s desktopovým rozhraním, které je mírně náročnější na běh na slabším hardwaru a zároveň není vhodné mít v tomto případě u zařízení, které má být kompaktní, periferie navíc, jako například monitor. Z tohoto důvodu je vhodnější použít vzdálený přístup z počítače či notebooku přes SSH (Secure Shell).

SSH je zabezpečené šifrování vzdálené komunikace mezi dvěma subjekty, které nahradilo program telnet a r-příkazy na systému Linux, jenž měli bezpečnostní rizika při přenosu hesla, kde mohlo dojít k odposlechnutí. V našem případě komunikace mezi pracovní stanicí a Raspberry Pi. Přes terminál, v textové podobě bez grafického rozhraní, se připojíme vzdáleně k počítači či serveru na jakoukoliv vzdálenost. Můžeme vzdáleně s proti stranou přenášet data, instalovat programy či jinak upravovat vzdálený systém. Toto vše je zabezpečené s pomocí šifrování a povinné autentizace pro přístup k systému (Barrett, 2005).

3.2.5 IPTable vs. NFTables

V operačním systému Linux pro nastavení firewall řešení lze využít existujících programů iptables a nftables.

Iptables je nyní již legacy verzí programu pro správu samostatného paketového netfilter firewallu. Na většině nových distribucí se od iptables již odpouští. Používá koncept samostatných tabulek pro zpracování paketů, které jsou rozděleny do modulů s odlišnou funkcionalitou (Shots, 2019).

Existují tři základní tabulky (Rash, 2007):

- **filter** – základní tabulka firewall filtrovacích pravidel. Zabudované řetězce pravidel obsahuji INPUT, OUTPUT a FORWARD
- **nat** – pravidla pro přístup k veřejné síti. Je určen k překladu zdrojové a cílové adresy přes IP adresu. Zabudované řetězce pravidel obsahují PREROUTING, OUTPUT a POSTROUTING

- **mangle** – pro správu paketů, kontrolováno tabulkou filter. Zabudované řetězce obsahují PREROUTING, INPUT, FORWARD, POSTROUTING a OUTPUT

Od verze kernelu 3.13 je k dispozici novější program nftables, který je vyvíjen stejnou skupinou, která stojí za vývojem iptables. Slučuje do jednoho celku část netfilteru a modulů iptables. Syntaxe se od iptables odlišuje, lze využít skriptování skrze shell, kde je možné si předefinovat kompletní vzhled firewall tabulek bez použití příkazů. Oproti předchůdci nenajdeme žádné předefinované tabulky, administrátor si tak může vytvořit vlastní, které dál nadefinuje podle potřeb. Přechod mezi iptables a nftables je poměrně snadný díky využití nástroje iptables-translate, který převede stará pravidla do nové formy (Suehring, 2015).

Na Raspberry Pi lze využít jak iptable, tak nftable a dalších řešení. V této bakalářské práci bude využito nftables, který je na systému debian/Raspberry Pi OS již před instalován a doporučen vývojáři operačního systému.

3.2.6 Syntaxe NFTables

Pro lepší porozumění přidávání firewall pravidel je dobré znát syntax nftables. První základním prvkem jsou tabulky, které v hierarchii nftables najdeme na nejvyšším stupni, je tedy základním pilířem, od kterého se další prvky odvozují. V nich pak dále nejdeme řetězce a adress family, jakožto inet, ipv4, arp a další (Netfilter Project, 2021).

```
#úprava firewall tabulky
nft [add,list,delete,flush] table [<adress_family>] <table_name>
```

Dalším základním prvkem jsou řetězce, které spojují pravidla v tabulkách. Všechny pakety, které jsou zachycené filtrem řetězce jsou předány pravidlům. Existují dva typy řetězců. Základní řetězce, které fungují jako vstupní body pro pakety přicházející ze síťového zásobníku. Pro vytvoření základního řetězce se použije následují příkaz.

```
#vytvoření základního řetězce
sudo nft add chain [<adress_family>] <table_name> <chain_name> '{type <type>
hook <hook> priority <priority>\; [policy <policy> \;]}'
```

Parametrem **type** můžeme vytvořit následující typy řetězců:

- filter – podporuje arp, bridge, ip, ip6 a inet tabulkové rodiny
- route – označuje pakety, podpora ip a ip6
- nat – pro možnost překladu síťových adres

Parametr **hook** odkazuje na konkrétní fázi paketu, během toho, co je zpracováván jádrem kernel:

- Pro ip a ip6: prerouting, input, forward, output, postrouting.
- Pro arp: input, output
- Pro bridge zpracovává ethernetové pakety procházející bridge zařízeními.
- Pro netdev: ingress

Parametr **priority** představuje řadové číslo řetězců. Poslední parametr **policy** představuje výchozí verdikt pro řízení toku v základním řetězci. Nachází se v něm hodnoty accept a drop (Netfilter Project, 2021).

Druhým řetězcem je regulární řetězec, který nefunguje jako filter, ale jakoby jump targets. Napomáhají s organizací a přehledností nftables. Pro vytvoření regulárního řetězce se použije následující příkaz.

```
#úpravá regulárního řetězce
sudo nft [add, delete, flush] chain [<adress_name>] <table_name> <chain_name>
```

Poslední součástí jsou samotná pravidla. Ta již filtrované pakety podle řetězců přijímají a provádějí s nimi akce na základě toho, zda odpovídají konkrétním kritériím. Každé pravidlo se rozděluje na dvě části. První část má žádný nebo jeden výrazů, které udávají kritéria pro pravidla. Druhá část má jeden nebo více výroků, které udávají akci, která bude vykonána, pokud se paket bude rovnat výroku v pravidlu. Výrazy i výroky se vyhodnocují zleva doprava (Stickman, 2023).

Pro vytvoření pravidla se použije následující příkaz.

```
sudo nft add rule <adress_famiy> <table_name> <chain_name> tcp dport 22
counter accept
```

3.3 Router

Jedná se o mezičlánek mezí privátní sítí a dalším zařízením jako je například počítač nebo herní konzole. Jinými slovy je prostředkem pro routovaní. Je určen k propojení všech zařízení v domácnosti a v pracovním prostředí s využitím IP adresy. Umožňuje tak bezpečný přenos dat a efektivní provoz v síti (Tanenbaum, 2010).

Router by se snadno mohl zaměnit s modemem, který sice může být součástí celku, ale také samostatným subjektem. Modem je především pro připojení do veřejné sítě od poskytovatele internetového připojení.

Se správně nastaveným routerem můžeme zabránit kybernetickým útokům, ale také chránit před infikováním zařízení v síti viry a malwary.

Routery se dělí do jednotlivých typů, které jsou popsány v následujících bodech.

- **Wireless router** – Za použití ethernet kabelu se router připojí k modemu. Data jsou přenášena z binárního kódu do radiových signálů, které jsou bezdrátově přenášeny za pomocí antény. Vytvářejí tak WLAN připojení, které komunikuje bezdrátově. Ve většině případech se dá bezdrátový router použít také jako drátový, pokud nám chybí dostatek LAN portů lze využít dodatečného hardwaru v podobě switche (Cisco, 2023).
- **Wired router** – Router je také připojen do modemu pomocí ethernet kabelu. Avšak oproti bezdrátovému routeru jsou zařízení připojena dalším ethernet kabelem do portu, tím vytváří LAN síť (Cisco, 2023).
- **Core router** – Většinou využíván korporátními společnostmi, které potřebují přenést velké množství dat po rozsáhlé síti. Jsou tak jádrem lokální sítě, ale nekomunikují s externí sítí (Cloudflare, 2023).
- **Edge router** – Komunikuje mezi core routerem a externí sítí. Využívají k tomu protokol BGP pro posílání a přijímáni dat z LAN a WAN sítě. Modem lze také chápat jako edge router (Cisco, 2023).
- **Virtuální router** – Za pomocí software lze router virtualizovat jako službu v cloud prostředí. Díky tomuto jsou dobrou volbou pro velké společnosti s komplexní sítí v podniku (Cloudflare, 2023).

3.3.1 Možná bezpečnostní rizika

Firmware, který je nainstalován na routeru může mít bezpečnostní rizika, kterých lze využít k narušení integrity systému. Útočníci si jsou často těchto rizik vědomi. V tomto případě je dobré udržovat firmware routeru v nejnovější verzi, kde jsou adresovaná a opravena rizika předchozích verzí (Cisco, 2023).

Další možným rizikem může být DDoS útok nebo také brute-force útok, kdy je router napaden více zařízeními, dochází tak k přehlcení a router v tu chvíli přestává fungovat.

3.3.2 Routing

Směrování, které úzce souvisí s routerem, jak je z názvu patrné. V TCP/IP se nachází na třetí vrstvě. Existují dva základní typy vnitřního dynamického směrování (Bouška, 2007):

- **Distance-vector routing protokol** – routovací tabulka obsahuje informace o vzdálenosti do specifické sítě. Tabulka je periodicky zasílána sousedům, kteří si svoji

tabulku upraví a tu opět odešlou dál. Pro výpočet nejlepší cesty se používá jedna nebo více metrik, jako je například počet hopů. Nejlepší cesta se počítá pomocí Dual algoritmu. Upraveným typem distance-vector protokolu je path-vector protocol. Spadají sem protokoly RIPv1, RIPv2 a IGPR.

- **Link-state routing protokol** – Komplexní databáze síťové topologie, která je vytvořena pomocí LSA, vyměňují si link-state advertisements. LSA jsou vyvolány jakoukoliv událostí v síti, do svého okolí zároveň odesílá Hello pakety, kde zasílá informace o sobě, rychle reaguje na změny topologie. Avšak tím spotřebovává více pásma a zdrojů na routeru, metrika je komplexní, nejlepší cesta se počítá pomocí Dijkstrova algoritmu shortest path first (SPF). Spadají sem protokoly OSPF a IS-IS.

Posledním typem jsou hybridní směrovací protokoly, které spojují nejlepší vlastnosti dvou předchozích protokolů do jednoho celku (Aweya, 2021).
Dále je také potřeba zmínit statické neboli neadaptivní směrování, které je například mezi ISP a firmami, kde není nutné, aby běžel složitý směrovací protokol, a tak zbytečně zatěžoval síť.

Další varianty jsou dynamické a defaultní směrování. Dynamické je schopné se přizpůsobit situaci, naopak defaultní, pokud není jiná cesta, je vždy použito v té výchozí, jak již název napovídá (Medhi, 2017).

3.4 Směrovací protokoly

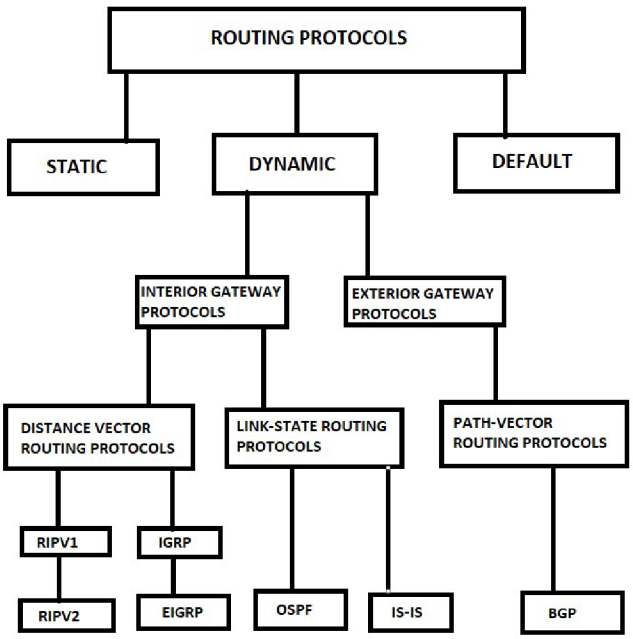
Směrování pomáhá s přenosem informací po síti a mezi dalšími zařízeními. Pro router jsou tyto protokoly zásadní, protože díky nim má router aktuální informace a nemusí se manuálně aktualizovat jeho routovací tabulky (Liu, 2009).

Routovací tabulka je určena pro zaznamenání použitých cest nebo vrstev, podle nichž jsou dále pakety směrovány. Následující body ukazují detailněji jednotlivé dynamické směrovací protokoly. Na konci této kapitoly je pro lepší přehlednost zobrazeno graficky sounáležitosti těchto protokolů na obrázku č.4.

- **Open Shortest Path First (OSPF)**: Jako první otevírá nejbližší možnou cestu, pracuje nad doménovým rozdělením sítí. Má neomezení počet hopů a jedná se IGP protokol, který běží pouze na daném systému. Funguje na principu sousedů, jak bylo již zmíněno u link-state protokolu. Je tak ideální volbou pro velkou síť (Cisco Networking Academy, 2014).

- **Intermediate System – Intermediate System (IS-IS)**: Je postaven na metodologii ISO. Poskytuje rychlou konvergenci a škálovatelnosti. Je efektivní při využívání šířky pásma sítě (Cisco, 2022).
- **Interior Gateway Routing Protocol (IGRP)**: V této době se již protokol IGRP nepoužívá, robustnější nežli původní protokol RIP. Specifikuje, jakým způsobem budou vyměněné informace o směrování mezi bránami v rámci jedné nezávislé sítě. Tyto informace pak dále můžou protokoly použít pro další směrováni (Cisco Networking Academy, 2014).
- **Exterior Gateway Protocol (EGP)**: Volí cestu mezí sousedními sítěmi, tento protokol najdeme jako mezičlánek při přenosu mezi systémy. Pod tímto protokolem najdeme protokol BGP (Cisco, 2022).
- **Border Gateway Protocol (BGP)**: Spadá pod path vector routing protokoly. Funguje mezi různými sítěmi jakožto EGP protokol. Tím se odlišuje od ostatních zmíněných protokolů, které fungují pouze uvnitř routeru. Můžeme jej najít především ve spojení s edge routery (Cisco, 2022).
- **Enhanced Interior Gateway Routing Protocol (EIGRP)**: Jedná se o hybridní směrovací protokol, který byl vytvořen společností Cisco. Maximální počet skoků je 255. Pokud router není schopen najít cestu s pomocí směrovací tabulky, zeptá se na cestu sousedů, kteří si informaci předávají, dokud cesta není nalezena. Informují mezi sebou pouze o změně, a tak si nepředávají kompletní směrovací tabulku (Cisco Networking Academy, 2014).
- **Routing Information Protocol (RIP)**: Jeden z nejstarších směrovacích protokolů. Dnes se používá pouze RIPv2, které podporuje stejný počet skoků jako první verze neboli 15 a rozšiřuje podporu IPv6 (Cisco Networking Academy, 2014).

Obrázek 4: Směrovací protokoly



Zdroj: (Networking Learning, 2021)

3.5 Síťové protokoly

Díky těmto protokolům získává síťová architektura definici pro komunikaci a přenos dat mezi zařízeními v síti. Určují tak dostupné služby, kterých můžeme na síti využívat. Fungují jakožto soubor pravidel a chování pro komunikaci mezi zařízeními. V síťové komunikaci využíváme vrstvení, v každé vrstvě najdeme jiné protokoly. Protokoly jsou neustále vyvíjeny proto jsou zveřejňovány formou RFC dokumentů. Mezi nejzákladnější síťové protokoly náleží TCP/IP, který stojí za během internetu nebo například emailová komunikace s POP3, SMTP a IMAP protokoly (Dostálek, 2008).

3.5.1 TCP/IP a ISO OSI

TCP/IP soubor protokolů pro správný chod internetu na našem zařízení. Jméno nese po dvou protokolech, které se v celku nachází.

- **IP –** základní síťový protokol, každé zařízení má přiřazenou IP adresu, díky které lze rozeznat destinaci pro přenos dat.
- **DHCP** – používá se pro dynamické rozdělování IP adres, které jsou limitovány rozsahem.

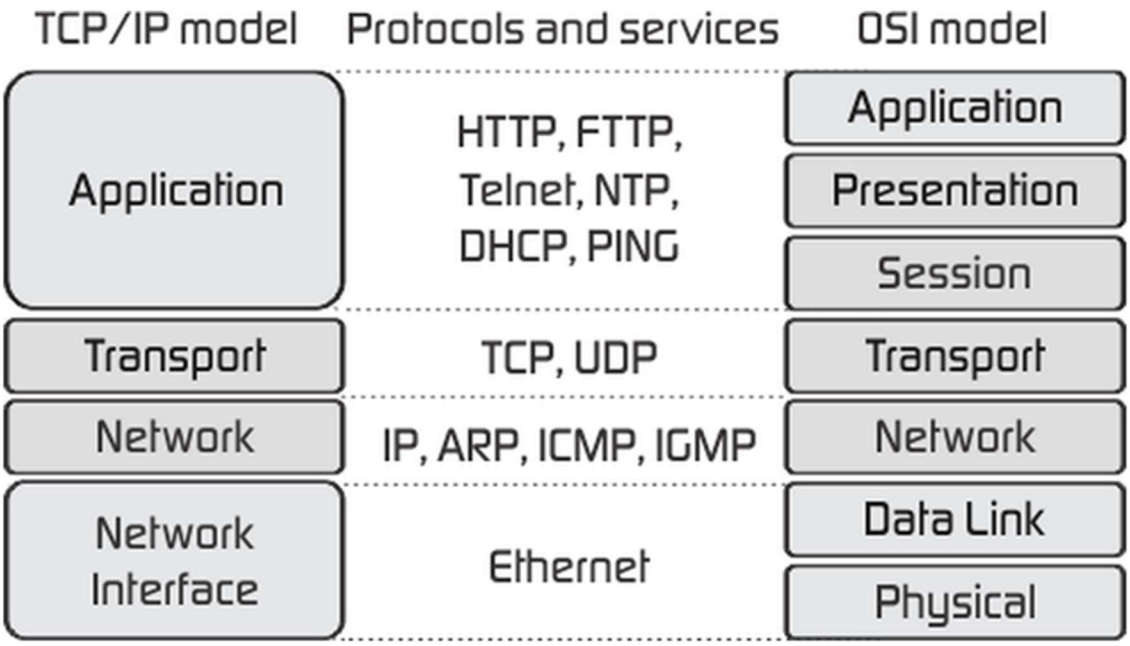
- **TCP –** vytváří virtuální okruh mezi koncovými aplikacemi obousměrně. Kontroluje přenos dat.

Jedná se o otevřenou standardizaci, kterou je možné použít na široké škále zařízení. Protokoly TCP/IP používají 4 vrstvy, nenachází se zde linková a fyzická vrstva (Dostálek, 2008).

Naproti tomu model OSI, který je veden pod mezinárodním standardizačním úřadem (OSI), využívá 7 vrstev. Každá vrstva obsahuje více protokolů, které jsou funkcionalitou specifické pro danou vrstvu. Pokud se procesy nacházejí na stejné vrstvě, tak využívají stejných protokolů. Zde se jedná o standardizaci architektury pro fungování sítě. Kromě vrstev aplikační, transportní a síťové se nacházejí v modelu OSI následující (Hunt, 2002):

- **Prezenční vrstva** – aplikace jenž spolupracují se musejí dohodnout na tom, jak budou data reprezentována. Představují tak rutinu pro zastupování neboli reprezentaci dat.
- **Relační vrstva** – spravuje relace mezi spolupracujícími aplikacemi. V TCP/IP se s relacemi nepracuje, místo relací se setkáme s popisem cesty pomocí portů a soketů, které se používají ke komunikaci mezi aplikacemi.
- **Fyzická vrstva** – definuje charakteristiky hardwaru, který je potřeba pro přenos signálu. Najdeme zde tak informace o využitých pinech a úrovní napětí. Příkladem může být standart lokální propojení sítě skrze IEEE 802.11.
- **Linková vrstva** – zaručuje doručení dat přes základní fyzickou síť pomocí linkové vrstvy. Většina RFC, které se týkají linkové vrstvy, popisují, jak může IP využít existující protokoly datových spojů.
- **Aplikační vrstva** – vrstva přístupná uživatelům. Všechny procesy, s kterými uživatel přímo interaguje.
- **Transportní vrstva** – zaručuje, že data, které jsou přenášena se dostanou k protistraně v nezměněném stavu, tedy přesně tak byla odeslána. V TCP/IP k této funkci můžeme využít TCP, ale také UDP, které nekontroluje správné dodání dat.
- **Síťová vrstva** – odděluje informace o síti od dalších vrstev, ty jsou řešené v této vrstvě a do vrchní se již neposílají. Oddělení dojde díky IP, který tyto informace izoluje a zprostředkuje adresaci a dodání dat.

Obrázek 5: TCP/IP a ISO OSI vrstvy s protokoly



Zdroj: (TCP/IP model vs OSI model, 2013)

3.6 Firewall

Obecně se jedná o v pomyslnou zeď, která zabraňuje útokům na naše zařízení, díky nastaveným pravidlům a filtrům. Mohli bychom tak firewall brát jako opevnění před útokem naše vlastnictví v podobě dat a svobody. Brání tak napadení z veřejné i privátní internetové sítě, podle nastavení firewall kontroluje obě strany připojení. Můžeme tak blokovat jednotlivé porty a IP adresy, které by mohly být využity proti našemu prospěchu. V této bakalářské práci bude firewall nastaven přímo na router, tím by se mělo předejít infikování celé domácí či firemní sítě.

3.7 Rozdělení firewallů

Pro rozdělení typů firewallů je dobré porozumět vrstvám TCP/IP a modelu OSI s kterým firewall blízce souvisí a pohybuje se v jeho vrstvách.

3.7.1 Paketové filtry

Nejprimitivnější z typů firewallu, fungují na úrovni síťové a transportní vrstvy modelu OSI. Pakety jsou jednotlivé celky dat, které jsou přenášeny po síti.

Rozhodují, zda paket bude přenesen dle informací nalezených z IP nebo TCP/UDP. Filtr filtruje pouze samotné pakety a nemonitoruje TCP relace. Z tohoto důvodu nelze přes paketové filtry zachytit falešné pakety, které díky ACK označení v názvu paketu obejdou zabezpečení (spoofing). Výhodou je rychlost, avšak bezpečnost díky spoofingu není ideální. Blokují či přijímají pakety dle IP adresy, portů a typu protokolů (Shinder, 2008).

3.7.2 Stavový firewall

Rozšiřuje původní paketový filtr a pokouší se adresovat jeho rizika, přitom je dán zřetel na zachování stejné rychlosti. Oproti paketovému filtru kontroluje relace, tak aby mohl zjistit legitimnost paketů s pomocí spojovací tabulky, kde se vytvoří zápis při první synchronizaci na začátku TCP relace. Relace jsou periodicky pozastavovány.

Kromě TCP relací lze stavový firewall použít k UDP komunikaci, která sama o sobě žádné stavy neprodukuje. Komunikace se při inicializaci také přidá do spojovací tabulky, poté bude další komunikace z nedůvěryhodné sítě akceptována pouze v případě, že se v tabulce nachází.

V aplikační vrstvě lze stavový firewall uplatnit u FTP, který využívá portu 21 při připojení uživatele a dále pak pro kontrolu port 20 (Shinder, 2008).

3.7.3 Aplikační brány

Fungují jako prostředníci v síťových relacích. Připojení jsou kontrolována v aplikační vrstvě, kde aplikační brána posoudí, zda uživatel může postupovat dále. Z tohoto hlediska je aplikační brána bezpečnější nežli paketové filtry, avšak tím ztrácí po stránce výkonu. Aplikační brány musí být samostatně vyvíjeny a jejich přidání a úprava je mnohem složitější, nežli tomu bylo u předchozích firewallů. Z tohoto důvodu jsou aplikační brány využívány méně (Shinder, 2008).

3.8 Síťové služby

Služby, které nám mohou obohatit využití sítě, dovolují nám komunikovat na velké vzdálenosti a přenášet velké množství dat. Tyto služby mohou být využívány přímo na dalších zařízeních jak už fyzických, tak virtuálních. K službám uživatel nemá přímí přístup, i když je využívá. Hlavní důvodem služeb je zjednodušení instalace a nastavení zařízení v síti.

3.8.1 DNS

Hierarchický systém, který překládá hostitelské jméno jakožto text do IP adresy. Funguje tedy jakoby překladač, aby adresa byla lépe čitelná. Nemá žádnou centrální databázi, místo toho jsou domény rozdělovány mezi několik poskytovatelů. Hierarchie DNS by se mohla přirovnat k souborovému systému v UNIX, kde se nachází „root domain" jakožto nejvyšší stupeň v hierarchii. Domény jsou tak rozděleny na TLD (domény nejvyššího řádu), které jsou dále rozdělený podle umístění a organizace, najdeme zde domény jako .com, .gov a .mil. Dále na domény druhého řádu a na subdomény, která se přidává před doménu řádu druhého.

V UNIX systémech se s DNS můžeme setkat ve spojení s BIND (Barkley Internet Name Domain) softwarem, ten DNS rozděluje na dvě části resolver, který posílá dotazy a name server, který na dotazy odpovídá (Hunt, 2002).

3.8.2 VPN

Používá se pro připojení do zabezpečené soukromé sítě skrze šifrovaný tunel, přes který poté probíhá veškerá komunikace po síti. Můžeme tak maskovat naší reálnou IP adresu, která se s využitím VPN změní, chrání tak naše soukromí. Máme pak tedy přístup i ke stránkám, které bychom díky našemu umístění jinak neměli neboli můžeme tak obejít geolokační blokaci nebo cenzuru. Nevýhodou pak může být horší rychlost a latence připojení, jelikož vlastně využíváme jiné vzdálené sítě, ale stála jsme omezováni naší sítí.

Pro připojení přes VPN lze využít široké škály programů jako OpenVPN a NordVPN, ale v této době je možné využít i zabudované VPN v systému Windows (Mediati, 2014).

3.8.3 DHCP

Tato služba se nejčastěji nachází na routerech nebo přímo na serverech. Automaticky přiděluje IP adresy, výchozí brány, maskuje podsítě a pracuje s DNS. IP adresy stále za využití IPv4 jsou přiřazeny ke každému klientovi, periodicky je však adresa odebrána, aby mohla být znovu použita pro jiný klient a původní ji již nebude mít možnost využít. Rozlišuje tak známá a neznámá zařízení, pro taková zařízení jsou pak aplikována jiná pravidla. Komunikace probíhá na portech 68, jakožto klient a 67, který naslouchá přímo DHCP (BasuMallick, 2022).

3.9 Proxy server

Důležitou součástí firewallu pro filtrování obsahu jakožto URL a stránek. Funguje jako prostředník mezi klientem, který posílá požadavek pro zobrazení webového dokumentu a dalším serverem, na kterém se dokument nachází. Díky konfiguraci proxy můžeme blokovat a filtrovat obsah jenž je nevhodný či výhradně obtěžující. Filtrováním můžeme také rozumět úpravou finální stránky, odebrání například reklam ze stránky. Navštívené stránky si uchovávají do cache paměti. Probíhá tak nejprve kontrola, zda stránka již v paměti není uložena, pokud ano posílá zpět staženou kopii místo toho, aby se poslala přímo aktuální stránka. Díky tomuto faktu se může zvýšit rychlost načítání stránek a také jejich bezpečnost (BasuMallick, 2023).

V této bakalářské práci bude využito Squid proxy, která je optimalizovaná pro Unixové systémy a je podporována ve vybraném webovém rozhraní.

3.9.1 Reverzní proxy

Webové stránky se po navštívení ukládají lokálně. Proxy kontroluje, zda lokálně uložená stránka je aktuální, nebo na ni již proběhli změny. Kvůli této skutečnosti tak nemusí vůbec proběhnout připojení k dalšímu serveru. Kontrola dokumentu probíhá skrze http hlavičku (Saini, 2011).

3.9.2 Forward proxy

Jsou používané pro přenos dat mezi skupinami uživatelů v interní síti. Jakmile je zaslán požadavek od odesílatele, proxy server zkontroluje, zda má v připojení pokračovat nebo ne. Přesměrovává tak provoz. Pod forward proxy můžeme najít i open proxy server, který je přístupný pro veřejnost. Umožnuje schování IP adresy uživatelů pro procházení webu (Saini, 2011).

4 Vlastní práce

4.1 Průběh vlastní práce

Realizace vlastní práce bude probíhat dle popsaných postupů v metodice práce. Nejprve bude provedena instalace lite verze Rasperry Pi OS na microSD kartu, kde se provedou první úpravy vlastností systému jakožto hostname a možnost SSH připojení. Základní instalace operačního systému neobsahuje veškeré balíčky, které budou potřeba pro realizaci práce, tedy dodatečné služby budou doinstalovány a nastaveny pro správných chod routeru. Po instalaci dodatečných služeb bude přidáno webové rozhraní pro lepší přehlednost a jednoduší správu systému.

V poslední části budou zhodnoceny praktické výsledky práce a využití systému v reálných podmínkách. Součástí bude provedení měření propustnosti síťových prvků a funkčnosti firewall pravidel.

4.2 Požadované předpoklady a služby

Síť, na které se bude router s firewallem nacházet je menšího rozsahu, obsahuje pouze malé množství ostatních zařízení jakožto počítačů, konzolí, chytrých telefonů, televize a dalších. Valná většina zařízení bude připojena přes bezdrátové připojení, avšak některá zařízení bezdrátové připojení nepodporují, tato zařízení mohou být připojena drátově s využitím malého switche skrze RJ45 síťový port. Momentální stav rychlosti sítě je předveden v příloze B. Předpokládá se zrychlení bezdrátového připojení a zlepšení zabezpečení sítě.

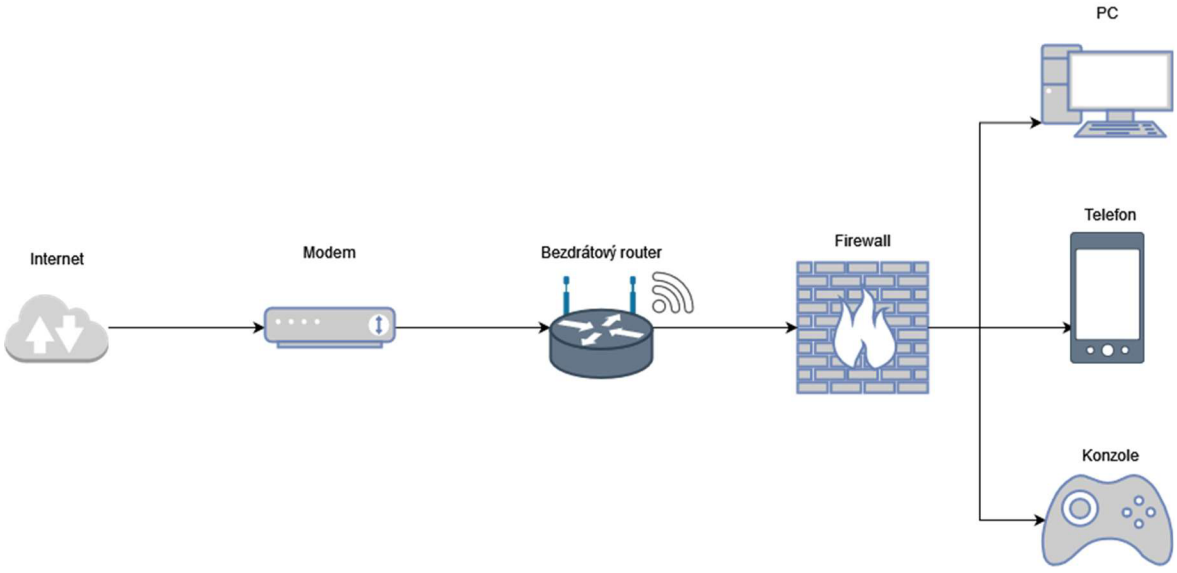
Předpokládané služby systému budou obsahovat následující:

- Bezdrátový přístup – zrychlení dosavadního řešení
- DNS server – stránky budou ukládány do mezi paměti
- DHCP – přidávání dynamických IP adres na wlan rozhraní
- Webové rozhraní – pro další správu routeru
- Proxy server – filtrování stránek
- Firewall – nastavena pravidla pro chod routeru a bezpečnostní pravidla proti útokům

4.3 Architektura sítě

Raspberry Pi jakožto finální systém bude fungovat jako router s bezdrátovým přístupovým bodem a také firewall řešení s využitím nftables. Obsahuje tři síťová rozhraní, první vestavěné wifi rozhraní dle standardů 802.11b/g/n/ac, které poslouží pro bezdrátový přístupový bod, dále na základní desce najdeme síťovou kartu, do které bude vedeno internetové připojení od ISP. V poslední řadě se přes USB 3.0 rozhraní využije k testování gigabit externí síťové karty. Diagram cílové vlastní sítě je znázorněn na obrázku č.6.

Obrázek 6: Diagram sítě



4.4 Věci potřebné pro realizace vlastní práce

Pro realizaci této bakalářské práce bude potřeba samotného minipočítače Raspberry Pi 4B, který bude rozšířen o další hardwarové části.

Počítač bude usazen do miniaturní počítačové skříně s aktivním chlazením, pro lepší výkon při vícečetných výpočtech, kde by mohlo dojít k poklesu efektivity z důvodu vysoké teploty. Skříň ochrání počítač před prachem a dalšími faktory, které by mohli počítač poškodit, tak aby se předešlo ohnutí pinů a poškození portů.

Pro běh systému bude použito micro SD karty ve velikosti 32 GB, kde bude nainstalován operační systém Raspberry Pi OS a další služby jakožto proxy, DHCP a DNS.

Pro testování stability drátového připojení bude použito redukce z USB 3.0 na port RJ45, jelikož počítač má na základní desce k dispozici pouze jeden síťový port. Avšak díky

USB 3.0 rozhraní by mělo být možné docílit až rychlosti jednoho gigabitu. Tohoto celého kroku by se dalo předejít použitím modulu Raspberry Pi 4 a rozšiřující desky, ve chvíli psaní této bakalářské práce je téměř nereálné sehnat zmíněný modul z důvodu nedostatku zboží na trhu, kvůli snížené produkci.

K samotnému připojení k routeru bude využito SSH připojení. Jelikož se jedná o zařízení, které nutně nepotřebuje pro chod další periferie jako je monitor, klávesnice a myš z logického principu, tak bude nainstalována verze operačního systému bez grafického rozhraní.

4.5 Instalace Raspberry Pi OS

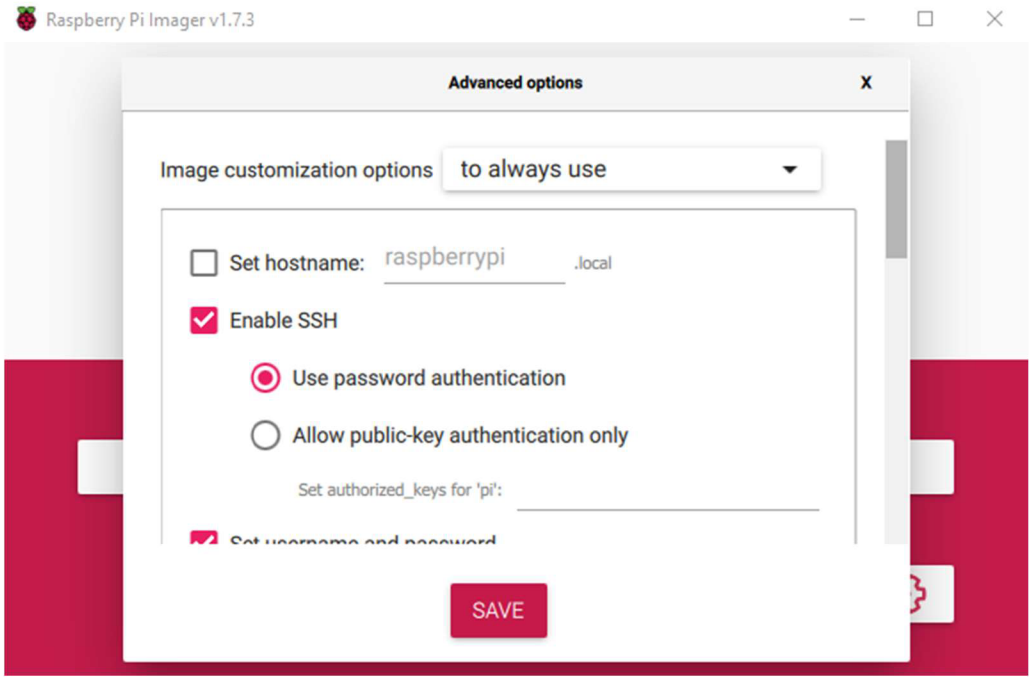
Aby se mohlo přejít k nastavení samotného routeru a firewallu bude potřeba nainstalovat samostatný podklad na kterém vše bude fungovat. Tím bude právě Raspberry Pi OS bez grafického rozhraní, tedy lite verzi 64bit.

4.5.1 Raspberry Pi Imager

Pro instalaci samotného operačního systému je potřeba nejdříve stáhnout a nainstalovat nástroj Raspberry Pi Imager pro přidání operačního systému na microSD kartu, tento krok může být proveden skrze počítač či notebook, kde se nachází přístup ke čtečce microSD karet.

V Raspberry Pi Imageru bylo před instalací upraveno pokročilé nastavení, kde je možné nastavit, aby operační systém byl od začátku připravený na SSH připojení. Současně je nastaven hostname zařízení pro jednoduší připojení a lepší přehled v síti. Nastaveny jsou dále autentifikační údaje uživatele **root**. V pokročilém nastavení lze dále nastavit klávesnici a připojení k wifi, které nebude potřeba, zabudovaná wifi bude použita pro bezdrátovou funkci routeru.

Obrázek 7: Raspberry Pi Imager



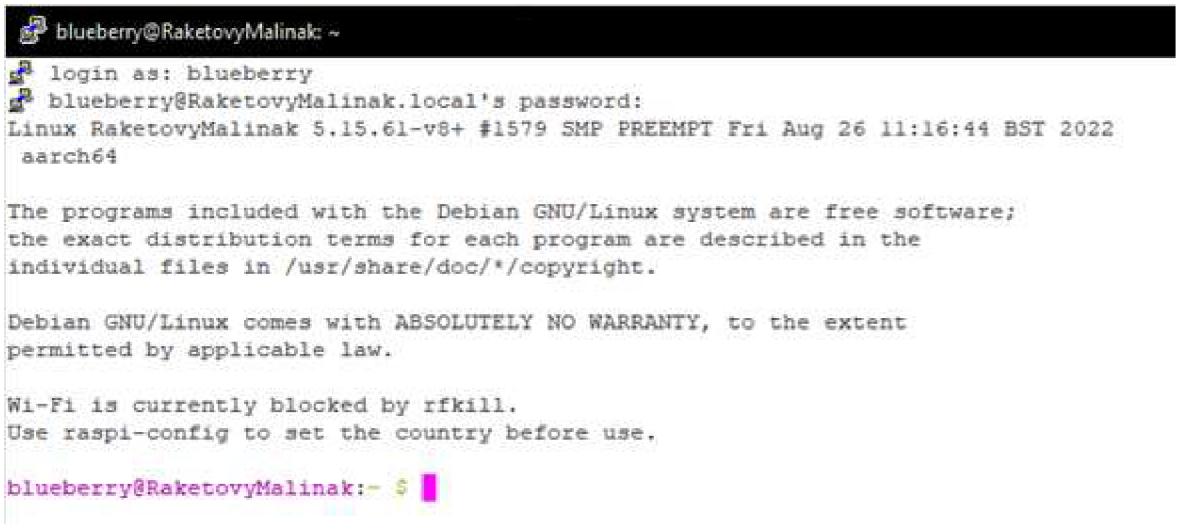
Po instalaci operačního systému na microSD kartu je karta vložena do Raspberry Pi. Po zapnutí systém sám nastaví předdefinovaná nastavení, která byla zvolena v pokročilém nastavení imageru, poté je ihned připraven k použití. Nyní je možné pokračovat s iniciálním nastavením systému.

4.5.2 Připojení přes SSH

SSH připojení je možné již od začátku díky počátečnímu nastavení. Avšak bude potřeba samotného programu pro SSH připojení. V případě této práce bude využito programu PuTTy.

Jelikož bylo nastaven hostname zařízení, nebude potřeba hledat IP adresu přes kterou je nutné se připojit, stačí nám k tomu pouze hostname.

Obrázek 8: Iniciální připojení k Raspberry Pi



4.6 Instalace bezdrátového routeru

Nyní se přejde k nastavení samotného bezdrátového routeru. Nejdůležitější součástí nastavení bude instalace dodatečných služeb pro správný chod routeru. Jelikož se jedná o bezdrátový router, bude v tomto případě využito zabudovaného wifi rozhraní pro vytvoření bezdrátového přístupu. Při prvním spuštění je nutné Wifi nakonfigurovat, aby mohla být nakonfigurována pro bezdrátové použití. V neposlední řadě je potřeba nainstalovat dodatečné služby pro DNS a bezdrátový přístup.

4.6.1 Instalace služeb a jejich nastavení

Budou nainstalovány dodatečné služby pro správný chod bezdrátového routeru. Instalované služby budou Hostapd pro vytvoření bezdrátové přístupového bodu a DNSmasq software pro nastavení DNS a částečně DHCP.

Po instalaci služeb budou služby nastaveny skrze soubor pro nastavení. První služba, která byla nastavena je hostapd. Nastavení lze kdykoliv upravit, takže nemusí být finální.

```
sudo nano /etc/hostapd/hostapd.conf

#do souboru nastavení je přidán následující text pro nastavení bezdrátového
přístupového bodu

interface=wlan0

#nastavení pásma sítě a=5GHz, g=2,4GHz
hw_mode=a

#Channel musí odpovídat nastavenému pásmu
channel=36

#QoS podpora, nutné pro plnou rychlost na 802.11n/ac/ax
wmm_enabled=1


#Podpora pro standarty 802.11n/ac
ieee80211n=1
ieee80211ac=1

#Nastavení kodu země a limitu, pro danou zemi
country_code=CZ
ieee80211d=1

#Nastavení jména wifi a zabezpečení
ssid=RaketovyMalinak
wpa_passphrase=test1234
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
```

Dále bude nastavena služba hostapd tak, aby se při každém spuštění routeru spustila automaticky a nemusela být spouštěna manuálně.

```
sudo nano /etc/default/hostapd

#Řádek přidán do souboru nastavení pro automatické spouštění
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Jelikož základní chování Linux systému je izolovat síťové karty, pokud jich je v zařízení více, a to by znemožnilo použití wifi pro bezdrátový přístup, je potřeba zapnout IP forwarding. Poté by již měl být nově vytvoření přístupový bod viditelný v aktivních wifi připojeních na dalších zařízeních.

```
sudo nano /etc/sysctl.conf


#Odkomentován následující řádek pro povolení směrování paketů
net.ipv4.ip_forward=1
```

4.6.2 Konfigurace DHCP a DNS serveru

Před nastavením DNS serveru bude nejdříve potřeba nastavit statickou IP adresu Raspberry Pi routeru. K tomu bude využit DHCP server, jehož soubor nastavení je upraven následovně.

```
# přidano pro vytvoření statické adresy routeru pro wlan0 rozhraní a
vypnutí wpa_supplicant, tak aby byl brán hostpad místo něj

nohook wpa_supplicant
interface wlan0
static ip_address=192.168.42.10/24
static routers=192.168.42.1
```

V předešlé kapitole byla společně s hostapd nainstalována i služba DNSmasq, kterou bude využita pro vytvoření a konfiguraci DNS serveru, aby se tímto mohla zlepšit rychlost připojení. DNS server bude použit jakožto caching nameserver. K nastavení DNS serveru lze také využít balíčku BIND, kterého v této bakalářské práci nevyužijeme. DNSmasq byl vybrán pro tuto práci, jelikož se jedná o méně náročný software a je vhodný pro sítě menšího rozměru. I v tomto případě bude potřeba upravit soubor nastavení. Zde požadujeme nastavení následujících specifikací:

- Nastavení DNS serveru tak, aby nepřenášel jména bez tečky (.). Všechna tato jména zůstanou pouze v lokální síti.
- Zastavení čtení upstream nameserverů ze souboru nastavení /etc/resolv.conf, místo toho využije konfigurace DNSmasq.
- Zabránění zpětnému vyhledávání místního rozsahu IP na upstream DNS servery. Předejde se tím tak úniku místní sítě na upstream servery.
- Zvýšení velikosti cache paměti, pro zredukovaní času DNS lookup, což výrazně vylepší rychlost sítě.
- Použije se Google DNS serverů pro upstream nameservery.

Soubor nastavení bude tedy obsahovat následující:

```
#nastavení je seřazeno dle předchozího popisu
domain-needed
no-resolv
bogus-priv
cache-size=1000
server=8.8.8.8
server=8.8.4.4


#doplňující nastavení pro DHCP na wlan0 rozhraní
interface=wlan0
bind-dynamic
dhcp-range=192.168.42.100,192.168.42.200,255.255.255.0,2h
```

4.7 Nastavení firewallu

K nastavení firewallu se v této práci využije Linux aplikace nftables, která je v operačním systému již předinstalovaná jakožto výchozí aplikace pro firewall. Není tedy důvod použít legacy verze iptables, která nepřináší jakékoliv výhody oproti nftables. Stejného nastavení lze také docílit skrze iptables. Nftables má oproti iptables jednoduší syntaxi, sjednocená pravidla pro IPv4 a IPv6 skrze jeden příkaz (nft) a celkově lepší výkon, kde u iptables výkon degraduje s počtem přidaných pravidel. Nftables zůstává konzistentní. Během upravování pravidel také program zůstane stále aktivní a změny jsou uloženy ihned bez přerušení stávajícího nastavení. Budou nastavena a popsaná blíže základní pravidla, která budou pro router použita. Pravidla budou nastavena s využitím skriptu napsaném v shell. Skript s bližším popsáním pravidel lze nalézt v příloze A.

4.7.1 Konfigurace routeru přes NFTables

Pro následující pravidla byla vytvořena tabulka router, která obsahuje veškeré řetězce s pravidly pro router, které byly v této práci použity.

Na Raspberry Pi jsou prvotně přidána pravidla pro překlad protokolu pro bezdrátové připojení a přeposílání internetového provozu, tak aby bylo možno se k internetu připojit i z jiného zařízení skrze wifi síť.

Na routeru je nainstalován proxy server, který je třeba nastavit pro přesměrování HTTP komunikace, která probíhá na portu 80 skrze proxy server. Pravidla budou nastavena jakožto prerouting, tedy tak aby pakety byly změněny ještě před routing částí.

Tato pravidla jsou pouze pro správnou funkci samotného routeru a proxy serveru, proto byla nastavena pravidla s policy accept.

Výsledná tabulka obsahující veškeré řetězce a pravidla bude následovná.

```
table ip router {
        chain POSTROUTING {
                type nat hook postrouting priority filter; policy accept;
                oifname "eth0" counter packets 0 bytes 0 masquerade
        }

        chain FORWARD {
                type filter hook forward priority filter; policy accept;
                iifname "wlan0" oifname "eth0" counter packets 0 bytes 0
accept
                iifname "eth0" oifname "wlan0" ct state established,related
                counter packets 0 bytes 0 accept
        }

        chain PREROUTING {
                type nat hook prerouting priority filter; policy accept;
                iifname "wlan0" tcp dport 80 counter packets 0 bytes 0 dnat
to 192.168.42.1:3128
                iifname "eth0" tcp dport 80 counter packets 0 bytes 0
redirect to :3128
        }
}
```

4.7.2 Ochrana před DDoS útokem a dalšími

K firewall nastavení budou přidána pravidla pro zmírnění případného DDoS útoku na router. Předpoklady pro ochranu proti takovému útoku jsou následující:

- Příchozí pakety, co obsahují fragmenty budou zahozeny. Pokud není ošetřeno, může dojít ke ztrátě dat.
- Filtrování bogon IP adres
- Poškozené příchozí XMAS pakety budou zahozeny.
- Poškozené příchozí pakety NULL budou zahozeny.
- Blokování nových paketů, co nejsou SYN.

Výsledné tabulky s řetězci a pravidly pro toto nastavení budou následovné.

```
table netdev filter {
        chain INGRESS {
                type filter hook ingress device eth0 priority -500;
                ip frag-off & 0x1fff != 0 counter packets 0 bytes 0 drop
                ip saddr { \
                                0.0.0.0/8, \
                                10.0.0.0/8, \
                                100.64.0.0/10, \
                                127.0.0.0/8, \
                                169.254.0.0/16, \
                                172.16.0.0/12, \
                                192.0.0.0/24, \
                                192.0.2.0/24, \
                                192.168.0.0/16, \
                                198.18.0.0/15, \
                                198.51.100.0/24, \
                                203.0.113.0/24, \
                                224.0.0.0/3 \
                        } \
                        counter packets 0 bytes 0 drop
                tcp flags & (fin|psh|urg) == fin|psh|urg counter packets 0 by-
tes 0 drop
                tcp flags & (fin|syn|rst|psh|ack|urg) == 0x0 counter packets 0
bytes 0 drop
                tcp flags syn \
                        tcp option maxseg size 1-535 \
                        counter packets 0 bytes 0 drop
        }
}

table inet mangle {
        chain PREROUTING {
                type filter hook prerouting priority -150;
                ct state invalid counter packets 0 bytes 0 drop
                tcp flags & (fin|syn|rst|ack) != syn \
                        ct state new \
                        counter packets 0 bytes 0 drop
        }
}
```

4.8 Konfigurace webového rozhraní

Nyní se přejde k přidání webového monitoru pro snadnější úpravu a sledování chodu sítě. Administrátor tak nebude muset při každém zásahu nebo kontrole zacházet do systému skrze SSH připojení, aby se mohlo nastavení upravit skrze konzoli.

V této bakalářské práci bude využito nástroje Webmin, který bude schopen ukázat veškerá nastavení na našem routeru a zároveň zde budeme moci zkontrolovat využití systému. Je tak pomocníkem při správě vytvořeného zařízení.

4.8.1 Webmin instalace a nastavení

Nástroj byl nainstalován skrze automatický skript, který nastavil oficiální úložiště a GPG klíče přímo na Raspberry Pi systém, toto usnadní aktualizace Webmin nástroje do budoucna. Prvně je provedena instalace repositáře, který je pravidelně aktualizován.

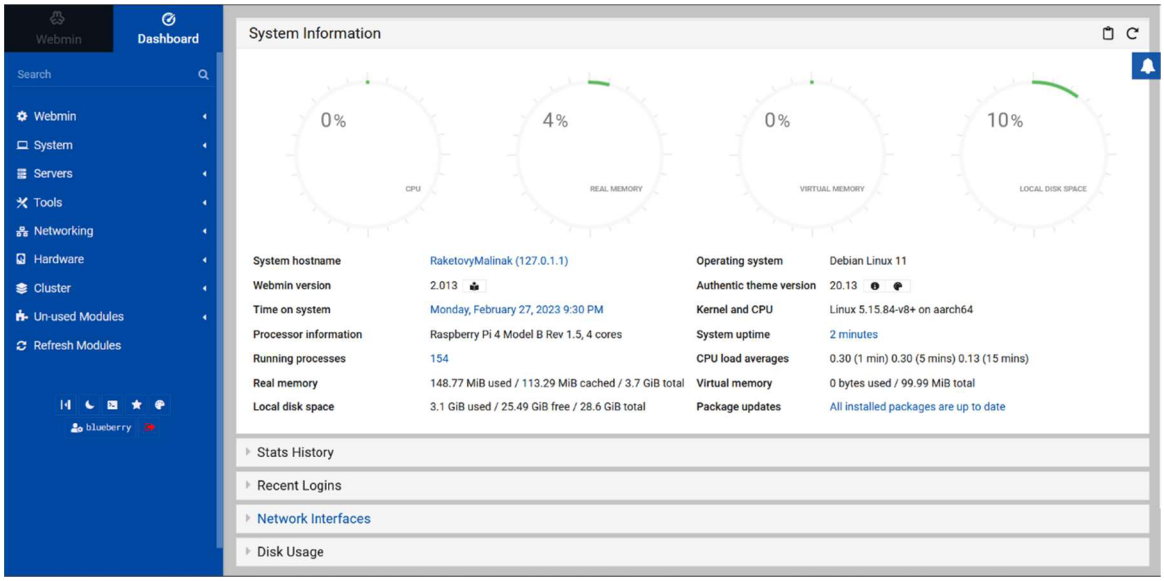
```
#použitý příkaz pro skript instalace repozitáře

curl -o setup-repos.sh
https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh
```

Webmin webové rozhraní využívá portu 10000. Po nainstalování nástroje se tak lze k webovému rozhraní dostat skrze URL adresu s IP adresou routeru: **http://<IP>:10000**

Skrze webový monitor je možné upravovat veškerá nastavení, která by jinak musela být upravována skrze terminál. Pro tuto bakalářskou práci je důležitá **Networking** část rozhraní, kde lze upravovat firewall pravidla a sledovat propustnost sítě. Zároveň je možné přidat doplňující software, který je možné upravovat skrze implementované rozhraní.

Obrázek 9: Dashboard Webmin webového rozhraní



4.8.2 Přidání proxy a webového filteru

Webmin rozhraní podporuje proxy software, který bude použit v této práci, tím je možné obě součásti propojit. To hrálo hlavní roli ve výběru proxy. V této práci je využito proxy Squid a filteru SquidGuard. Předpokladem je blokování nežádaného obsahu stránek a

logování všech navštívených stránek. Ke Squid proxy je do rozhraní přidán doplňek **Calamaris,** který usnadní monitorování proxy a přidá lepší přehlednost logováni.
Do souboru nastavení pro Squid proxy je přidáno nasledující.

```
#Nastavena funkčnost na HTTP pouze pro síť Wifi s rozsahem 42.X

acl localnet src 192.168.42.0/24
http_access allow localnet
```

Další součástí je webový filter SquidGuard, který je doplňkem samotné proxy. Skrze filtr mohou být zablokovány nevhodné stránky, které jsou nežádoucí na specifické síti.
I zde je potřeba upravit soubor nastavení. Do filtru je možné přidat vlastní stránky, které by měli být zablokovány nebo stáhnout již nastavený blacklist. Zde je využito právě této možnosti. Adresy z databáze tak budou zablokovány a uživatel dostane předdefinovanou HTML stránku s notifikací, že stránka není přístupná.

```
 dbhome /var/lib/squidguard/db logdir /var/log/squidguard dest violence {
domainlist blacklists/violence/domains
urllist blacklists/violence/urls
log violenceaccess
}
acl {
default
{
pass !violence
redirect http://localhost/block.html
} }
```

4.9 Testování

V rámci metodiky poslední část praktické práce je samotné testování přidaných služeb, firewall pravidel a propustnosti sítě skrze bezdrátový router.

4.9.1 DNS

DNS server je otestován pomocí příkazu **dig,** který se musí separátně nainstalovat. Zde je potřeba dbát na aktualizace balíčkovacího systému, bez kterých stažení neprojde. Na následujících obrázcích je ukázán test DNS server, kde můžeme pomocí **Query time** posoudit, že DNS server opravdu funguje a stránky jsou uložené v mezi paměti.

Obrázek 10: Testování funkčnosti DNS

```
blueberry@RaketovyMalinak:~ $ dig pef.czu.cz @localhost

; <<>> DiG 9.16.37-Debian <<>> pef.czu.cz @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19741
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pef.czu.cz.                    IN      A

;; ANSWER SECTION:
pef.czu.cz.             3600    IN      A       193.84.47.38

;; Query time: 19 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Feb 22 17:15:53 CET 2023
;; MSG SIZE  rcvd: 55
```

Obrázek 11: Výsledek testování DNS

```
blueberry@RaketovyMalinak:~ $ dig pef.czu.cz @localhost

; <<>> DiG 9.16.37-Debian <<>> pef.czu.cz @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 79
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;pef.czu.cz.                    IN      A

;; ANSWER SECTION:
pef.czu.cz.             3560    IN      A       193.84.47.38

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Wed Feb 22 17:16:33 CET 2023
;; MSG SIZE  rcvd: 55
```

4.9.2 Firewall pravidla

Nastavená firewall pravidla budou testována v následující části. K testování bylo při vytváření pravidel přidán **counter** pro počítání celkového počtu paketů a bajtů, které od posledního spuštění prošly skrz síť.

Ve vytvořené tabulce router byla testována nastavená pravidla pro přenos internetového provozu, funkčnost pravidel je ukázána na obrázku č.12.

Obrázek 12: Test přenosu internetového provozu

```
blueberry@RaketovyMalinak:~ $ sudo nft list ruleset
table ip router {
        chain POSTROUTING {
                type nat hook postrouting priority filter; policy accept;
                oifname "eth0" counter packets 211 bytes 20096 masquerade
        }

        chain FORWARD {
                type filter hook forward priority filter; policy accept;
                iifname "wlan0" oifname "eth0" counter packets 34801 bytes 36096862 accept
                iifname "eth0" oifname "wlan0" ct state established,related counter packets 36733 bytes 43410553 accept
        }
}
```

Následující pravidla byla nastavena pro nainstalovaný proxy server squid, tak aby http requesty, které náleží portu 80 procházely skrze proxy server. Test pravidel je ukázán na obrázku č.13.

Obrázek 13: Test proxy serveru

```
        chain PREROUTING {
                type nat hook prerouting priority filter; policy accept;
                iifname "wlan0" tcp dport 80 counter packets 110 bytes 5720 dnat to 192.168.42.1:3128
                iifname "eth0" tcp dport 80 counter packets 0 bytes 0 redirect to :3128
        }
}
```

4.9.3 Propustnost sítě

Propustnost sítě bude testována pomocí měření propočítání průměru rychlostí. Testovaní proběhlo skrze lan, wlan a samotný router. Vytvořený router s firewallem byl testován na síti malého rozsahu s následujícími parametry:

- Připojení k internetu bylo uskutečněno skrze ethernet kabel a port eth0, udávaná rychlost ISP činí 300/300 Mbit s agregací 1:1.
- Vnitřní bezdrátová síť byla uskutečněna pomocí vbudované Raspberry Pi Wifi v pásmu 2,4 a 5GHz s nastavenou podporou pro standarty 802.11n/ac.

Během testování byla naměřena propustnost sítě s pomocí nástroje **iperf3**. Každá tabulka měření obsahuje deset jednotlivých měřeních a jejich výsledný průměr. K testování bylo využito notebooku Lenovo s duální Wifi 2,4/5GHz a PC s gigabit vestavěnou kartou Intel I225-V.

Naměřeny byly následující výsledky pro vybrané možnosti připojení.

Hodnoty naměřené skrze rozhraní wlan0 na frekvenci 2,4GHz (Tabulka 1).

Tabulka 1: Test propustnosti pro wlan0 2,4GHz

Měření	Objem přenesených dat (MB)	Propustnost (Mbits/s)
1	63,0	52,8
2	61,6	51,7
3	60,6	50,8
4	62,5	52,4
5	64,9	54,4
6	64,1	53,8
7	62,2	52,2
8	62,5	52,4
9	63,8	53,5
10	63,9	53,5
Průměr	**62,91**	**52,75**

Hodnoty naměřené skrze rozhraní wlan0 na frekvenci 5GHz (Tabulka 2).

Tabulka 2: Test propustnosti pro wlan0 5GHz

Měření	Objem přenesených dat (MB)	Propustnost (Mbits/s)
1	80,1	67,2
2	79,8	66,9
3	80,2	67,3
4	80,5	67,5
5	80,4	67,3
6	80,2	67,3
7	80,9	67,8
8	80,0	67,1
9	80,6	67,6
10	80,4	67,4
Průměr	**80,31**	**67,34**

Hodnoty naměřené skrze rozhraní wlan0 na frekvenci 5GHz pomocí internetové stránky www.speedtest.net skrze Vodafone server (Tabulka 3)

Tabulka 3: Test reálné rychlosti připojení pro wlan0 5GHz

Měření	Download (Mbits/s)	Upload (Mbits/s)
1	60,6	66,0
2	61,1	67,1
3	62,3	67,3
4	62,6	66,6
5	64,7	67,0
6	63,3	67,8
7	63,9	67,6
8	65,9	67,1
9	61,4	67,1
10	65,4	66,4
Průměr	**63,12**	**67**

Hodnoty naměřené skrze rozhraní wlan0 na frekvenci 2,4GHz pomocí internetové stránky www.speedtest.net (Tabulka 4)

Tabulka 4: Test reálné rychlosti připojení pro wlan0 2,4GHz

Měření	Download (Mbits/s)	Upload (Mbits/s)
1	35,2	44,8
2	41,8	49,1
3	38,6	48,3
4	40,8	40,0
5	41,2	47,4
6	41,9	48,0
7	37,9	47,1
8	44,0	47,9
9	38,9	48,1
10	41,1	46,2
Průměr	**40,14**	**46,69**

Hodnoty naměřené skrze rozhraní eth0 (Tabulka 6).

Tabulka 5: Test propustnosti pro eth0

Měření	Objem přenesených dat (GB)	Propustnost (Mbits/s)
1	1,10	946
2	1,09	942
3	1,10	944
4	1,10	945
5	1,09	934
6	1,10	947
7	1,10	945
8	1,09	947
9	1,10	946
10	1,10	945
Průměr	**1,097**	**944,1**

Hodnoty naměřené skrze rozhraní eth0 pomocí internetové stránky www.speedtest.net skrze Vodafone server (Tabulka 5)

Tabulka 6: Test realné rychlosti připojení pro eth0

Měření	Download (Mbits/s)	Upload (Mbits/s)
1	284,0	216,9
2	279,0	194,6
3	287,6	218,7
4	291,3	199,6
5	283,1	212,5
6	277,4	215,0
7	272,2	207,0
8	263,5	212,9
9	270,5	200,5
10	255,4	209,2
Průměr	**276,4**	**208,69**

5 Zhodnocení výsledků

Z výsledného měření propustnosti bylo zjištěno, že vytvořená wifi síť na routeru s firewallem je schopna dosahovat propustnosti průměrně 67,24 Mbit/s, tedy méně, nežli je skutečná rychlost poskytovaná od ISP na testované síti. Rychlost je tedy omezena propustností vytvořeného routeru. Avšak pokud bychom měli tuto rychlost porovnat s průměrnou rychlostí wifi připojení v ČR, tak je tento router stále vhodným řešením pro bezdrátový přenos dat. Průměrná rychlost wifi připojení v ČR byla naměřena 27,92 Mbit/s (DSL.cz, 2023). Zároveň se pro dosavadní síť jedná o značné vylepšení pro bezdrátové připojení, kde byla před implementací naměřena průměrná rychlost bezdrátového připojení pouze cca 27 Mbit/s. Rychlost wifi připojení skrze vytvořený router by mohla být vylepšena přidáním kupříkladu gigabit USB wifi přijímače.

Co se týče drátového připojení skrze vytvořený router, toto připojení je schopno docílit průměrně až rychlosti 944,1 Mbit/s a je tedy vhodné i pro sítě s mnohem rychlejším připojením, nežli bylo zde využito. V tomto případě by router mohl být využit jakožto drátový s využitím dodatečných přístupových bodů. Je tak v tomto ohledu adekvátní variantou i pro podnikové využití.

Firewall pravidla mohou být nadále upravována skrze vytvořený firewall skript. Jedná se o snadnější úpravu nežli skrze příkazy a je tak i snadno přenositelný na další zařízení. Během testování propustnosti síťových prvků nedošlo k pozorování zpomalení rychlosti připojení s přidávanými firewall pravidly. Můžeme tak usoudit, že využití nftables jakožto firewall řešení v takovémto měřítku nemá žádné negativní dopady na výkon sítě.

6 Závěr

Na závěr práce je vhodné zhodnotit průběh práce a splněné cíle, které na začátku byly vyznačeny.

Hlavním cílem této práce bylo vytvoření funkčního bezdrátového routeru s firewallem na platformě Raspberry Pi pro lepší zabezpečení a rychlejší bezdrátové připojení sítě. Funkčnost implementovaného systému byla potvrzena v testovací fázi této práce. S ohledem na předchozí specifikace sítě lze uznat, že nově vytvořené řešení vydává mnohem lepší výkony než dosavadní řešení na testované síti. Rychlost wifi připojení se zlepšila více jak dvakrát tolik. Před implementací firewallu síť nebyla nijak zabezpečena, zvedla se tak i bezpečnost vnitřní sítě. V tomto směru byly hlavní cíle splněny.

Dalšími součástmi cíle bylo rozšíření síťových služeb o DNS a Proxy server, které na router byly také přidány a testovány v poslední fázi vlastní práce. Zároveň bylo k routeru přidáno webové rozhraní, skrze jenž lze router nadále spravovat na lokální síti.

Samotná implementace zařízení proběhla úspěšně, během práce bylo lépe porozuměno funkčnosti sítě a jejím nastavením. Zároveň totéž platí o znalosti se zabezpečením sítě a bližšímu seznámení s Linux operačním systémem.

Závěrem je dobré zmínit, že systém s takovýmito specifikacemi by mohl být dále rozšiřován o více síťových služeb. V budoucnu by tak mohla z této práce, díky novým nabitým znalostem, vzniknout mnohem rozsáhlejší síť s řadou vylepšení.

7 Seznam použitých zdrojů

RASPBERRY PI FOUNDATION, 2021. Raspberry pi 4 product brief. *Raspberrypi* [online]. Cambridge: Raspberry Pi Trading [cit. 2023-03-08]. Dostupné z: https://datasheets.raspberrypi.com/rpi4/raspberry-pi-4-product-brief.pdf

MONK, Simon, 2022. *Raspberry Pi Cookbook*. 4th edition. Newton: O'Reilly. ISBN 9781098130923.

HATTERSLEY, Lucy, ed., 2023. *Raspberry Pi Handbook 2023*. Cambridge: Raspberry Pi. ISBN 978-1-912047-42-0.

SPOOREN, Paul, 2022. Releases. *Github* [online]. Leipzig: GitHub [cit. 2023-03-08]. Dostupné z: https://github.com/openwrt/openwrt/releases

SUSE, 2022. Enterprise Linux. *Suse* [online]. Nuremberg: SUSE [cit. 2023-03-08]. Dostupné z: https://www.suse.com/suse-defines/definition/enterprise-linux/

BARRETT, Daniel J., Richard E. SILVERMAN a Robert G. BYRNES, 2005. *SSH, The Secure Shell: The Definitive Guide*. 2nd edition. Cambridge: O'Reilly Media. ISBN 978-0596008956.

SUEHRING, Steve, 2015. *Linux Firewalls: Enhancing Security with nftables and Beyond*. 4th edition. Boston: Addison-Wesley Professional. ISBN 978-0134000022.

RASH, Michael, 2007. *Linux Firewalls: Attack Detection and Response with iptables*. San Francisco: No Starch Press. ISBN 978-1593271411.

UPTON, Eben, 2022. Production and supply-chain update. *Raspberrypi* [online]. Cambridge: Raspberry pi foundation [cit. 2023-03-07]. Dostupné z: https://www.raspberrypi.com/news/production-and-supply-chain-update/

RUSSELL, Jesse, ed., 2012. *Openwrt*. 2nd edition. Moscow: Book on Demand. ISBN 9785511971179.

STICKMAN, Nathaniel, 2023. Get Started with nftables. *Linode* [online]. Philadelphia: Linode [cit. 2023-03-08]. Dostupné z: https://www.linode.com/docs/guides/how-to-use-nftables/

NETFILTER PROJECT, 2021. Quick reference-nftables in 10 minutes. *Nftables wiki* [online]. Netfilter Project [cit. 2023-03-08]. Dostupné z: https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes

TANENBAUM, Andrew a David WETHERALL, 2010. *Computer Networks*. 5th edition. London: Pearson. ISBN 978-0132126953.

CISCO, 2023. What is a Router?. *Cisco* [online]. San Jose: Cisco [cit. 2023-03-08]. Dostupné z: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html#~types-of-routers

CLOUDFLARE, 2023. Router definition. *Cloudflare* [online]. San Francisco: Cloudflare [cit. 2023-03-08]. Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-a-router/

BOUŠKA, Petr, 2007. TCP/IP - Routing - směrování. *Samuraj-cz* [online]. Praha: Samuraj [cit. 2023-03-14]. Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-routing-smerovani/

WEYA, James, 2021. *IP Routing Protocols Fundamentals and Distance-Vector Routing Protocols*. Boca Raton: CRC Press. ISBN 9780367709624.

LIU, Dale, 2009. *Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit*. Waltham: Syngress. ISBN 978-1597493062.

CISCO NETWORKING ACADEMY, 2014. *Routing Protocols Companion Guide*. Indianapolis: Cisco Press. ISBN 978-1-58713-323-7.

CISCO, 2022. Intermediate System-to-Intermediate System (IS-IS). *Cisco* [online]. San Jose: Cisco Systems [cit. 2023-03-08]. Dostupné z: https://www.cisco.com/c/en/us/products/ios-nx-os-software/intermediate-system-to-intermediate-system-is-is/index.html

DOSTÁLEK, Libor a Alena KABELOVÁ, 2008. *Velký průvodce protokoly TCP/IP a systémem DNS*. Brno: Computer Press. ISBN 978-80-251-2236-5.

SHINDER, Thomas W., 2008. *The Best Damn Firewall Book Period*. 2nd edition. Waltham: Syngress. ISBN 978-1597492188.

HUNT, Craig, 2002. *TCP/IP Network Administration*. 3rd edition. Sebastopol: O'Reilly Media. ISBN 9780596002978.

SHOTS, William. The Linux Command Line: A Complete Introduction. 2nd edition. San Francisco: No Starch Press, 2019. ISBN 1593279523.

SAINI, Kulbir, 2011. *Squid Proxy Server 3.1: Beginner's Guide*. Birmingham: Packt Publishing. ISBN 978-1849513906.

DFROBOT, 2022. Raspberry Pi Compute Module 4 IoT Router Carrier Board Mini. *DFRobot* [online]. Shanghai: DFRobot [cit. 2023-03-08]. Dostupné z: https://www.dfrobot.com/product-2242.html

SEEED TECHNOLOGY, 2022. Dual Gigabit Ethernet NICs Carrier Board for Raspberry Pi Compute Module 4. *Seeedstudio* [online]. Shenzhen: Seeed Technology Co. [cit. 2023-03-08]. Dostupné z: https://www.seeedstudio.com/Rapberry-Pi-CM4-Dual-GbE-Carrier-Board-p-4874.html

RASPBERRY PI TRADING, 2019. *Raspberry Pi Projects Book 5*. Cambridge: Raspberry Pi Trading. ISBN 978-1-912047-70-3.

Raspberry Pi 4 Model B, 2022. *Inno-maker* [online]. Shenzhen: inno-maker [cit. 2023-03-08]. Dostupné z: https://www.inno-maker.com/product/raspberry-pi-4-model-b/

GEERLING, Jeff, 2021. Test Seeed Studio's Dual Gigabit CM4 Carrier Board. *Github* [online]. San Francisco: GitHub [cit. 2023-03-08]. Dostupné z: https://github.com/geerlingguy/raspberry-pi-pcie-devices/issues/137
NETWORKING LEARNING, 2021. Introduction of Routing Protocol. *Networking learning* [online]. Networking Learning [cit. 2023-03-08]. Dostupné z: https://www.networkinglearning.com/2021/07/introduction-of-routing-protocol.html

TCP/IP model vs OSI model, 2013. *Fiberbit* [online]. Miaoli City: AD-net Technology Co. [cit. 2023-03-08]. Dostupné z: https://fiberbit.com.tw/tcpip-model-vs-osi-model/

MEDHI, Deep a Karthik RAMASAMY, 2017. *Network Routing - Algorithms, Protocols, and Architectures*. 2nd edition. Burlington: Morgan Kaufmann. ISBN 9780128007372.

DSL.CZ, 2023. Naměřené rychlosti internetu na DSL.cz v lednu 2023. *Dsl* [online]. Praha: DSL.cz [cit. 2023-03-10]. Dostupné z: https://www.dsl.cz/clanky/namerene-rychlosti-internetu-na-dsl-cz-v-lednu-2023

MEDIATI, Nick, 2014. Everything You Need to Know About VPNs. *Techsoup* [online]. San Francisco: TechSoup Globa [cit. 2023-03-13]. Dostupné z: https://www.techsoup.org/Support/articles-and-how-tos/everything-you-need-to-know-about-vpns

BASUMALLICK, Chiradeep, 2022. What is DHCP (Dynamic Host Configuration Protocol)? Meaning, Working, and Features. *Spiceworks* [online]. Austin: Spiceworks [cit. 2023-03-13]. Dostupné z: https://www.spiceworks.com/tech/networking/articles/what-is-dhcp/

BASUMALLICK, Chiradeep, 2023. What Is a Proxy Server? Working, Types, Benefits, and Challenges. *Spiceworks* [online]. Austin: Spiceworks [cit. 2023-03-13]. Dostupné z: https://www.spiceworks.com/tech/data-center/articles/proxy-server/

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

Wifi – Wireless Fidelity

LAN – Local Area Network

WLAN – Wireless Local Network

USB – Universal Serial Bus

GB – Gigabyte

MB – Megabyte

MHz – Megahertz

GHz – Gigahertz

NAT – Network Address Translation

ARP – Address Resolution Protocol

IP – Internet Protocol

UDP – User Datagram Protocol

SSH – Secure Shell

VPN – Virtual Private Network

URL – Uniform Resource Locator

DNS – Domain Name System

DDoS – Distributed Denial of Service

TLD – Top Level Domain

ACK – Acknowledgement Code

FTP – File Transfer Protocol

BIND – Berkeley Internet Name Domain

OS – Operating system

TCP/IP – Transmission Control Protocol/Internet Protocol

ISO OSI – International Standards Organization Open Systems Interconnection

DHCP – Dynamic Host Configuration Protocol

SD karta – Secure Digital karta

GPG – GNU Privacy Guard

RAM – Random Access Memory

UNIX – UNiplexed Information Computing System

HDMI – High-Definition Multimedia Interface

MIPI DSI – Mobile Industry Processor Interface Display Serial Interface

ISP – Internet Service Provider

Přílohy

Příloha A: Finální firewall skript

```
#!/usr/sbin/nft -f

#smazání všech dosavadních pravidel
flush ruleset
#definování proměnné lan pro lokální rozsah IP adres
define lan = 192.168.2.2-192.168.2.20

table netdev filter {
        chain ingress {
                type filter hook ingress device eth0 priority -500;
                # fragmenty zahozeny
                ip frag-off & 0x1fff != 0 counter drop
                # bogon IPv4 adresy
                ip saddr { \
                                0.0.0.0/8, \
                                10.0.0.0/8, \
                                100.64.0.0/10, \
                                127.0.0.0/8, \
                                169.254.0.0/16, \
                                172.16.0.0/12, \
                                192.0.0.0/24, \
                                192.0.2.0/24, \
                                192.168.0.0/16, \
                                198.18.0.0/15, \
                                198.51.100.0/24, \
                                203.0.113.0/24, \
                                224.0.0.0/3 \
                        } \
                        counter drop
                # odhození poškozených xmas paketů
                tcp flags & (fin|psh|urg) == fin|psh|urg counter drop
                # odhození poškozených null paketů
                tcp flags & (fin|syn|rst|psh|ack|urg) == 0x0 counter drop
                # nastavena maximalní velikost segmentu TCP
                tcp flags syn \
                        tcp option maxseg size 1-535 \
                        counter drop
        }
}

table inet filter {
        chain input {
                type filter hook input priority 0;
                # povolení loopback/ACL
                iifname lo accept
                # established/related připojení
                ct state established, related accept
                # zahození invalid připojení
                ct state invalid drop
                # ping flood DoS ochrana
                ip6 nexthdr icmpv6 icmpv6 type echo-request limit rate
2/second accept
                ip protocol icmp icmp type echo-request limit rate 2/second
accept
                # povelení portů na lokální síti
                tcp dport [ssh, 443, 10000] ip saddr $lan accept
        }

        chain forward {
```

```
                type filter hook forward priority 0; policy accept;
                iifname "wlan0" oifname "eth0" counter accept

        }

        chain output {
                type filter hook output priority 0;
                # ssh pouze pro tento systém
                tcp dport ssh reject with icmp type port-unreachable
        }
}

table inet mangle {
        chain prerouting {
                type filter hook prerouting priority -150;
                # zahození invalid připojení
                ct state invalid counter drop
                # blokování nových paketů, které nejsou SYN
                tcp flags & (fin|syn|rst|ack) != syn \
                        ct state new \
                        counter drop

        }
}

table ip router {
        chain postrouting {
                type nat hook postrouting priority 0; policy accept;

                oifname "eth0" counter masquerade

                }

       chain prerouting {
                type filter hook prerouting priority 0; policy accept;
                # Squid přemostění komunikace
                iifname "wlan0" tcp dport 80 counter dnat to
192.168.42.1:3128
                iifname "eth0" tcp dport 80 counter redirect to :3128

        }
}
```

Příloha B: Testování reálné rychlosti předchozího řešení

Testována reálná rychlost předchozího řešení na síti. Rychlost byla testována skrze stránku www.speedtest.net a Vodafone server. Dosavadní řešení nabízelo pouze pásmo 2,4GHz s následujícími výsledky.

Měření	Download (Mbits/s)	Upload (Mbits/s)
1	28,0	15,5
2	29,1	9,1
3	27,0	10,3
4	28,1	11,9
5	20,6	13,6
6	19,2	13,4
7	16,8	12,7
8	34,1	11,0
9	35,3	18,6
10	31,2	19,0
Průměr	**26, 94 ± 5,91**	**13,51 ± 3,15**

Z výsledků lze usoudit, že dosavadní řešení nenabízelo velmi stabilní připojení. Zároveň ani ne výkonnější, co se reálné rychlosti týče.