EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

Evidenčné číslo: 103004/B/2024/36145806868694788

Využitie mikropočítača ako bezpečnostného prvku malej počítačovej siete

Bakalárska práca

2023/2024 **Jakub Krátky**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

Využitie mikropočítača ako bezpečnostného prvku malej počítačovej siete

Študijný program: Hospodárska informatika

Študijný odbor: Ekonómia a manažment

Školiace pracovisko: Katedra aplikovanej informatiky

Vedúci záverečnej práce: Ing. Peter Procházka, PhD.

Poďakovanie

Ďakujem Ing. Petrovi Procházkovi, PhD. za odborné vedenie pri tvorbe bakalárskej práce a profesionálny prístup a pomoc pri spracovaní a vytváraní práce.

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Jakub Krátky
Študijný program:	hospodárska informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor:	ekonómia a manažment
Typ záverečnej práce:	Bakalárska záverečná práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický

Názov: Využitie mikropočítača ako bezpečnostného prvku malej počítačovej siete.

Anotácia: Študent v BP vytvorí prostredníctvom mikropočítača Raspberry Pi alebo obdobného, zariadenie pre zabezpečenie malej počítačovej siete s využitím viacerých dostupných technológií, tieto medzi sebou porovná a navrhne optimálne riešenie. Výsledný bezpečnostný prvok otestuje, poukáže na jeho výhody a porovná s inými komerčnými riešeniami.

Vedúci:	Ing. Peter Procházka, PhD.
Katedra:	KAI FHI - Katedra aplikovanej informatiky
Vedúci katedry:	Ing. Mgr. Peter Schmidt, PhD.
Dátum zadania:	03.03.2023

Dátum schválenia: 10.03.2023

doc. Ing. Martin Mišút, CSc.
osoba zodpovedná za realizáciu študijného programu

Abstrakt

Krátky, Jakub: *Využitie mikropočítača ako bezpečnostného prvku malej počítačovej siete.* – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky. – Vedúci záverečnej práce: prof. Ing. Peter Procházka, PhD. Bratislava: FHI, 2024, 61 strán.

Bakalárska práca sa zaoberá vývojom bezpečnostného zariadenia pre malé počítačové siete, ktoré je vytvorené na platforme Raspberry Pi alebo podobného mikropočítača. Práca analyzuje viaceré dostupné technológie na zabezpečenie sietí, porovnáva ich a navrhuje optimálne riešenie pre zabezpečenie. Cieľom práce bolo vytvoriť efektívny a ekonomicky výhodný bezpečnostný sieťový prvok, ktorý bol následne otestovaný a porovnaný s komerčnými riešeniami. Výsledky práce ukázali, že navrhnuté zariadenie poskytuje adekvátnu úroveň bezpečnosti a predstavuje konkurencieschopnú alternatívu k existujúcim komerčným produktom.

Kľúčové slová: Počítačová sieť, OpenWRT, Linux

Abstrakt

Krátky, Jakub: *The use of a microcomputer as a security element of a small computer network.* – University of Economics in Bratislava. Faculty of Economic Informatics; Department of Applied Informatics FHI. – Supervisor of the final thesis: prof. Ing. Peter Procházka, PhD. Bratislava: FHI, 2024, 61 pages.

This bachelor's thesis focuses on the development of a security device for small computer networks, based on the Raspberry Pi platform or a similar microcomputer. The work analyzes various available network solutions, compares them, and proposes an optimal solution for protection. The aim was to create an effective and economically viable security element, which was subsequently tested and compared with commercial solutions. The test results demonstrated that the proposed device provides an adequate level of security and represents a competitive alternative to existing commercial products.

Keywords: Computer network, OpenWRT, Linux

Zoznam ilustrácií

Zoznam skratiek

1. ACK - Acknowledgement (Potvrdenie prijatia)
2. DNS - Domain Name System (Systém doménových mien)
3. DoH - DNS over HTTPS (DNS cez HTTPS)
4. DoS - Denial of Service (Odmietnutie služby)
5. FTP - File Transfer Protocol (Protokol prenosu súborov)
6. GPIO - General Purpose Input/Output (Všeobecné vstupy/výstupy)
7. HTTP - Hypertext Transfer Protocol (Protokol prenosu hypertextu)
8. HTTPS - HTTP Secure (Zabezpečený HTTP)
9. I2C - Inter-Integrated Circuit (Sériová počítačová zbernica)
10. IP - Internet Protocol (Internetový protokol)
11. IPS - Intrusion Prevention System (Systém prevencie proti vniknutiu)
12. ISO - International Organization for Standardization (Medzinárodná organizácia pre štandardizáciu)
13. LEDE - Linux Embedded Development Environment
14. NAT - Network Address Translation (Preklad sieťových adries)
15. NGFW - Next-Generation Firewall (Firewall novej generácie)
16. OSI - Open Systems Interconnection (Model medzisystémovej komunikácie)
17. QoS - Quality of Service (Kvalita služby)
18. SFTP - SSH File Transfer Protocol (Protokol prenosu súborov cez SSH)
19. SPI - Software in the Public Interest (Softvér pre verejný záujem)
20. SSH - Secure Shell (Zabezpečená shell obálka)
21. TCP - Transmission Control Protocol (Protokol riadenia prenosu)
22. TLS - Transport Layer Security (Bezpečnosť transportnej vrstvy)
23. TOS - Type Of Service (Typ služby)
24. TTL - Time To Live (Čas života)
25. UDP - User Datagram Protocol (Protokol užívateľských datagramov)
26. USB - Universal Serial Bus (Univerzálna sériová zbernicová architektúra)
27. VPN - Virtual Private Network (Virtuálna privátna sieť)
28. WAN - Wide Area Network (Rozsiahla sieť)

Úvod

V súčasnej dobe, keď digitalizácia preniká do všetkých sfér našich životov, sa bezpečnosť počítačových sietí stáva neoddeliteľnou súčasťou každodenného fungovania malých podnikov a domácností. Malé podniky často nemajú dostatok prostriedkov na nákup drahých komerčných bezpečnostných riešení, čo ich robí zraniteľnými voči kybernetickým útokom. Tento fakt poukazuje na potrebu cenovo dostupných, ale efektívnych bezpečnostných riešení. Cieľom tejto bakalárskej práce je vytvoriť, otestovať a porovnať rôzne bezpečnostné prístupy na ochranu malých sietí s využitím mikropočítača Raspberry Pi, ktorý poskytuje unikátnu kombináciu nízkej ceny, dostupnosti a flexibilného výkonu.

V práce sme sa zamerali na návrh a realizáciu sieťového prvku, ktorý bude schopný integrovať a optimalizovať rôzne dostupné technológie pre zabezpečenie a vylepšenie siete. Výsledné zariadenie otestujeme a jeho výhody a nevýhody budú porovnané s komerčne dostupnými alternatívami. Táto práca nielenže prispieva k zvýšeniu bezpečnosti malých počítačových sietí, ale poskytuje aj dôležité usmernenia a odporúčania pre ich zabezpečenie.

Pri výbere témy sme boli motivovaní osobným záujmom o kybernetickú bezpečnosť a výzvami, ktorým čelia malé siete v súčasnom digitálnom prostredí. Rastúci trend internetu vecí (IoT) a inteligentných zariadení v domácnostiach a malých firmách predstavuje ďalšie bezpečnostné riziká, ktoré si vyžadujú nové a prispôsobené riešenia. V súlade s tým, sa naša práca snaží prispieť k lepšiemu porozumeniu a implementácii bezpečnostných technológií, ktoré sú prístupné a efektívne pre širokú verejnosť. Táto bakalárska práca má potenciál poskytnúť prínos v oblasti zvyšovania kybernetickej odolnosti malých počítačových sietí, a tým prispieť k ich stabilnejšiemu a bezpečnejšiemu fungovaniu v náročnom digitálnom prostredí. Význam práce spočíva vo vytvorení modelu, ktorý by mohol byť príkladom pre implementáciu cenovo efektívnych bezpečnostných opatrení, ktoré môžu mať významný dopad na zabezpečenie malých sietí po celom svete.

1 Súčasný stav riešenej problematiky

Raspberry Pi je mikropočítač, hlavnou výhodou je nízka cena ale aj malá veľkosť vzhľadom na dostupný výpočtový výkon. Zariadenia boli vytvorené britskou spoločnosťou Raspberry Pi Foundation, organizáciou, ktorá sa zameriava najmä na vzdelávanie spoločnosti v oblasti výpočtovej techniky. Dôraz kladie aj na dostupnosťou ich hardvéru, teda pomerne nízkou cenou sa zasluhujú aj o uľahčenie prístupu k výpočtovej technike . Raspberry Pi bolo na trhu predstavené v roku 2012 a od jeho predstavenia v roku 2012 bolo vytvorených mnoho vylepšených verzií nasledujúcich filozofiu prvého zariadenia [1].

1.1 Opis platformy Raspberry Pi

Mikropočítače od tejto spoločnosti sú využívané po celom svete, či už na hobby domáce účely, v rámci školstva, ako osobný počítač ale aj ako nástroj automatizácie pre podniky. Zariadenie je teda kompaktný, nízko nákladový počítač, ktorého ceny sa aktuálne pohybujú v rozmedzí 35 EUR až 85 EUR, v závislosti od zakupovanej verzie. Raspberry operuje na základe open-source filozofie. Na zariadeniach je teda možné spustiť viacero open-source operačných systémov. Zariadenie ponúka aj vlastný operačný systém vyvinutý priamo pre tento hardvér, nazýva sa Raspberry Pi. Tento operačný systém je možné použiť pre každý model s výnimkou Raspberry Pico.[1] Raspberry Pi OS je linuxová distribúcia vhodná pre bežné použitie na zariadeniach a je voľne dostupná. Operačný systém sa neustále vyvíja, pričom dôraz je kladený na zlepšenie stability a výkonu Debian balíkov na platforme [2].

1.1.1 Softvér Raspberry Pi

Operačný systém ponúka viac ako 35 000 predkompilovaných softvérových balíkov, ktoré sú pripravené na jednoduchú inštaláciu. Zvláštny dôraz je kladený na podporu programovacích jazykov ako Python, C a Scratch, zabezpečujúc kompatibilitu aj s ďalšími populárnymi programovacími jazykmi. Okrem toho je mikropočítač kompatibilný s rôznymi inými operačnými systémami, čo je zdokumentované na oficiálnej stránke. Medzi tieto systémy patria Arch Linux Arm, Ubuntu MATE, RISC OS, a Windows 10 IoT Core. Ďalej existujú špecializované distribúcie, napríklad pre multimediálne použitie na platforme KODI, ktoré rozširujú možnosti využitia Raspberry Pi.

Operačný systém môže byť nainštalovaný na microSD karte, USB kľúči alebo externom hard disku, pripojenom prostredníctvom USB portu. Raspberry Pi 4 podporuje rôzne distribúcie Linuxu, ako napríklad Raspbian. Tým sa otvára priestor pre vývoj softvéru v prostredí Python, C++ a ďalších programovacích jazykov [2] .

1.1.2 Hardvér Raspberry Pi 4

Svojou kompaktnou veľkosťou a rozsiahlou funkcionalitou poskytuje toto zariadenie ideálnu platformu pre rôzne projekty v oblasti informatiky a elektroniky. Tento mikro počítač prináša niekoľko výrazných vylepšení oproti svojim predchodcom. Procesor Raspberry Pi 4 tvorí štvorjadrový procesor ARM Cortex-A72 s frekvenciou až 1,5 GHz, čo zabezpečuje robustný výkon pre bežné výpočtové úlohy. Spoločnosť ponúka varianty s 2GB, 4GB a 8GB operačnou pamäťou, čo umožňuje plynulý beh aplikácií a multitasking [3] .

Zariadenie ponúka možnosť nastavenia taktu procesora, čo poskytuje dodatočnú flexibilitu pre pokročilých používateľov a vývojárov. Avšak by sa malo brať do úvahy, že zvyšovanie taktu procesora môže viesť k zvýšeniu teploty čipu a vyššej energetickej spotrebe. Nastavovanie taktu je proces, ktorý vyžaduje opatrný prístup a pozornosť k detailom. Preto je dôležité zvážiť termálnu účinnosť a stabilitu systému pri takýchto úpravách. Jednou z kľúčových vlastností je aj dostatočný počet portov a rozhraní pre pripojenie ďalších zariadení. Patria sem dva porty USB 3.0 pre rýchle prenosy dát, dva USB 2.0 porty, dva MicroHDMI porty, gigabitový Ethernet port pre stabilné pripojenie k sieti a slot na microSD kartu pre ukladanie operačného systému a dát. Raspberry Pi 4 podporuje bezdrôtové pripojenie cez integrovaný Wi-Fi a Bluetooth, čo pridáva flexibilitu pre bezdrôtovú komunikáciu a pripojenie periférií. Na základnej doske zariadenia sú tiež umiestnené GPIO piny, ktoré umožňujú pripojenie rôznych senzorov a periférií pre rozsiahle experimenty v oblasti elektroniky [3].

1.2 Základy sieťových technológií

V ére digitalizácie a globálnej konektivity sa sieťová komunikácia stáva stredobodom moderných technológií, ktoré ovplyvňujú každodenný život, ako aj širšie ekonomické a sociálne štruktúry. Počítačové siete a internet sú základmi, ktoré umožňujú nielen prenos dát a informácií medzi rôznymi geografickými regiónmi v reálnom čase, ale tiež podporujú kritickú infraštruktúru a služby, ktoré sú nevyhnutné pre fungovanie moderných spoločností.

S rastúcou závislosťou na technológiách je nevyhnutné pochopiť základné princípy a protokoly, ktoré riadia sieťovú komunikáciu. Táto kapitola je venovaná dvom hlavným modelom, ktoré sú základom pre pochopenie a návrh sieťových systémov. Model OSI (Open Systems Interconnection) a Model TCP/IP (Transmission Control Protocol/Internet Protocol). Oba modely poskytujú rámec pre analýzu a dizajn sieťových protokolov, ktoré sú základnými stavebnými blokmi pre dátovú komunikáciu cez počítačové siete.

Pochopenie týchto modelov je kľúčové nielen pre študentov a profesionálov v oblasti informačných technológií a kybernetickej bezpečnosti, ale tiež pre kohokoľvek, kto sa zaujíma o vývoj a správu sieťových systémov. Prehľad týchto modelov a súvisiacich protokolov umožní čitateľom lepšie pochopiť, ako sú dáta organizované, spravované, zabezpečené a prenášané v sieťových prostrediach. Navyše, vzhľadom na neustále sa meniace hrozby v kybernetickom priestore, je dôkladné porozumenie týchto základov nevyhnutné pre návrh a implementáciu efektívnych bezpečnostných riešení.

V nasledujúcich sekciách sme sa zaoberali jednotlivými vrstvami modelu OSI a modelu TCP/IP, čím sme poskytli ucelený prehľad o ich funkcionalitách a dôležitosti v rámci sieťovej architektúry. Tiež skúmame rôzne protokoly, ktoré operujú na týchto vrstvách, a diskutujeme o ich bezpečnostných aspektoch, ktoré sú nevyhnutné pre zabezpečenie dôvernosti, integrity a dostupnosti prenášaných dát.

1.2.1 Model OSI a TCP/IP

Model OSI a Model TCP/IP sú dve základné štruktúry používané na popis funkcií sieťových protokolov vo vrstvách [4]. Tieto modely poskytujú rámec pre porozumenie a implementáciu rôznych sieťových technológií a protokolov. **Model OSI** bol vyvinutý organizáciou ISO (International Organization for Standardization) a popisuje sieťovú komunikáciu v siedmich vrstvách [5].

- **Fyzická vrstva**
  - Zaoberá sa prenosom surových bitov cez fyzické médium ako sú káble (medené, optické) alebo bezdrôtové signály.
  - Zabezpečenie fyzickej vrstvy zahŕňa ochranu hardvéru, zariadení a médií pred fyzickým poškodením alebo neoprávneným prístupom.
- **Vrstva dátového spojenia**
  - Zabezpečuje bezchybný prenos dát cez fyzické spojenie. Vykonáva taktiez opravu chýb z fyzickej vrstvy, reguluje tok dát a umožňuje adresovanie na úrovni siete.
  - Implementuje techniky ako MAC (Media Access Control) adresovanie a kontrolu prístupu k médium (napr. Ethernet).
- **Sieťová vrstva**
  - Zodpovedná za smerovanie paketov cez rôzne siete. Zabezpečuje adresáciu, smerovanie a doručenie paketov medzi hostiteľmi, ktorí nie sú priamo spojení.
  - Implementuje bezpečnostné funkcie ako sú IPsec a VPN na ochranu dát prenášaných cez internet a iné siete.
- **Transportná vrstva**
  - Zabezpečuje rýchlu prenosovú službu. Riadi *end-to-end* komunikáciu, zabezpečuje segmentáciu dát, správu spojení a kontrolu preťaženia.
  - Používa protokoly ako TCP a UDP, kde TCP poskytuje mechanizmy na riadenie prenosu, zatiaľ čo UDP poskytuje jednoduchšie služby.

- **Relačná vrstva**
  - Riadi spojenia a relácie medzi aplikáciami. Zabezpečuje ich správne otvorenie, používanie a ukončenie.
  - Podporuje autentizáciu a obnovu relácií, spravuje spojenia tak, aby boli dáta v bezpečí pred prerušením.
- **Prezentačná vrstva**
  - Zaoberá sa formátovaním dát a ich prezentáciou. Prekladá dáta medzi formátmi, ktoré aplikácia prijíma a sieťovým formátom, zabezpečuje šifrovanie a kompresiu dát.
  - Kľúčová vrstva pre šifrovanie a dešifrovanie informácií poskytovaných aplikačnej vrstve.
- **Aplikačná vrstva**
  - Priamy kontakt s koncovým používateľom alebo aplikáciou, poskytuje špecializované protokoly ako HTTP, FTP, SMTP a iné.
  - Zabezpečuje autentizáciu koncového používateľa a kontrolu prístupu k sieťovým zdrojom

Tieto vrstvy modelu OSI zabezpečujú, že sieťová komunikácia je usporiadaná a že každá časť sieťovej komunikácie je jasne definovaná s príslušnými bezpečnostnými opatreniami. Toto rozdelenie umožňuje odborníkom na bezpečnosť lepšie zameranie sa na potenciálne hrozby
a zraniteľnosti na každej úrovni.

Model TCP/IP je zjednodušený model používaný pre internet, ktorý má štyri vrstvy [4]:

- Linková vrstva - Zodpovedá za rámcovanie paketov pre fyzické médium.
- Internetová vrstva - Zabezpečuje smerovanie paketov IP adresami.
- Transportná vrstva - Obsahuje protokoly ako TCP a UDP, ktoré riadia prenos dát
- Aplikačná vrstva - Obsahuje protokoly ako HTTP, FTP, ktoré umožňujú aplikáciám komunikovať cez sieť.

Zrozumiteľné a dôsledné zabezpečenie protokolov ako HTTP, FTP a SSH je vhodné pre ochranu dát a infraštruktúry organizácií pred kybernetickými hrozbami. Implementácia

bezpečnostných opatrení, ako sú šifrovanie, autentifikácia a monitorovanie, je kľúčová pre zabezpečenie týchto protokolov.

Model OSI a TCP/IP poskytujú štrukturovaný prístup k pochopeniu a implementácii týchto bezpečnostných techník na rôznych úrovniach sieťovej architektúry, čo umožňuje efektívne ochranné stratégie na ochranu sieťových zdrojov a dát [6].

1.2.2 Sieťové protokoly

Protokoly v internetových sieťach sú súbory pravidiel, ktoré umožňujú rôznym zariadeniam komunikovať medzi sebou cez digitálne siete. Predstavujú štandardizovaný spôsob, ako zariadenia vymieňajú informácie a dáta. Tieto pravidlá zahŕňajú formátovanie, synchronizáciu, sekvenovanie a chybové kontroly prenášaných dát. Protokoly sú kritické pre fungovanie internetu a ďalších sieťových technológií, pretože zabezpečujú, že dáta odoslané z jedného bodu sú správne prijaté a interpretované v inom bode siete [5].

Transmission Control (TCP) je zodpovedný za zabezpečenie spoľahlivého, usporiadaného a chybovo opraveného prenosu medzi hostiteľmi v sieti. Funguje na princípe spojenia, čo znamená, že komunikácia začína naviazaním spojenia a končí jeho ukončením. Každý TCP segment obsahuje kontrolný súčet pre detekciu chýb, sekvenčné čísla pre usporiadanie dát a potvrdzovacie čísla pre potvrdenie ich prijatia [5]. Bežné porty a bezpečnostné riziká sú:

- Port 80: HTTP pre nezašifrovaný webový prenos.
- Port 443: HTTPS pre šifrovanú komunikáciu.
- Port 21: FTP pre prenos súborov.
- Port 22: SSH pre zabezpečené prihlásenie a iné bezpečné prenosy.

- SYN Flood Attack: Využíva TCP handshake k zahlteniu cieľového systému zaslaním množstva SYN paketov bez dokončenia spojenia.
- Session Hijacking: Útočník môže prevziať kontrolu nad TCP spojením zmenou sekvenčných čísel.
- Man-in-the-Middle Attacks: Útočník odpočúva alebo manipuluje s komunikáciou medzi dvoma stranami.

User Datagram Protocol (UDP) je jednoduchší protokol, ktorý odosiela segmenty bez potvrdenia o prijatí alebo poradí. Je vhodný pre aplikácie, kde je rýchlosť dôležitejšia než spoľahlivosť, ako sú video streamy alebo online hry. Bežné porty a bezpečnostné riziká sú:

- Port 53: DNS pre vyhľadávanie internetových domén.
- Port 123: NTP pre synchronizáciu času.
- Port 69: TFTP, jednoduchý protokol pre prenos súborov.
- UDP Flood: Útočník môže generovať obrovské množstvo UDP paketov smerovaných na určité porty, čím spôsobí DoS.
- Reflection Attacks: Využíva verejne prístupné UDP servery na zosilnenie útoku tým, že falšuje zdrojové IP adresy.

Internet Protocol (IP) zabezpečuje adresovanie a smerovanie dátových paketov medzi sieťami. Každý IP paket obsahuje zdrojovú a cieľovú IP adresu, ktoré smerujú pakety cez rôzne siete na ich cieľové miesto. Útočník môže falšovať IP adresu, aby maskoval svoju identitu alebo vyvolal neoprávnený prístup k zdrojom.

HTTP (Hypertext Transfer Protocol) je základným protokolom pre prenos hypertextových dokumentov na World Wide Web. HTTPS (HTTP Secure) pridáva šifrovanie, ktoré zabezpečuje integritu a súkromie dát prenášaných cez internet.**)**

FTP (File Transfer Protocol) je určený pre prenos súborov, ktorý umožňuje užívateľom sťahovať a nahrávať súbory zo a na server. Pre lepšie zabezpečenie spojenia je dostupná aj verzia SFTP (SFTP Secure File Transfer Protocol).

SSH (Secure Shell) poskytuje zabezpečenie vzdialeného prístupu k počítaču alebo serveru. SSH používa silné šifrovanie na ochranu komunikácie pred odpočúvaním a umožňuje bezpečný prenos súborov a ďalších dát. SSH je protokol určený na bezpečné pripojenie a správu vzdialených počítačov alebo serverov. Tento protokol využíva šifrovanie a autentifikáciu na zabezpečenie dát, ktoré sa prenášajú medzi zariadeniami. Jedným z konkrétnych príkladov využitia SSH je pripojenie k Raspberry Pi routeru, ktorý slúži ako základná sieťová jednotka s možnosťou rôznych konfigurácií a úprav. SSH poskytuje možnosť presmerovania bežného portu, známe ako port forwarding, čo umožňuje prenos dát medzi sieťami, ktoré by inak neboli priamo dostupné [7].

SSH funguje na základe TCP/IP protokolu, ktorý zabezpečuje formátovanie, adresovanie a prenos paketov cez sieť. Kryptografia verejných kľúčov, ktorú SSH využíva, umožňuje bezpečnú výmenu dát medzi zariadeniami. SSH vyžaduje autentifikáciu používateľov, ktorá sa najčastejšie uskutočňuje pomocou kombinácie prihlasovacieho mena a hesla, alebo prostredníctvom pokročilejších metód ako sú kľúče. Tento komplexný prístup zabezpečuje, že vzdialené prístupy a operácie sú chránené pred neželanými zásahmi.

V rámci bakalárskej práce sme nástroj Secure Shell (SSH) využili ako kľúčový nástroj pre vzdialenú správu a konfiguráciu zariadenia. SSH nám poskytlo spoľahlivý a bezpečný spôsob pripojenia k týmto zariadeniam cez nezabezpečenú sieť, čo umožňuje vykonávať rôzne úlohy z akéhokoľvek miesta s prístupom na internet. SSH umožňuje pripojiť sa k Raspberry Pi routeru a vykonávať rôzne úlohy ako nastavovanie siete, aktualizáciu softvéru, konfiguráciu firewallu a ďalšie úpravy nastavení. Nástroj umožňuje administrátorom sledovať stav a prevádzku Raspberry Pi routeru pomocou príkazov na diaľku. To zahŕňa zobrazenie systémových logov, kontrolu využitia zdrojov a ďalšie diagnostické úlohy. V prípade problémov so zariadením je možné rýchlo reagovať a diagnostikovať problémy, napríklad skontrolovať sieťové pripojenia, overiť konfiguráciu alebo spustiť opravné príkazy [7].

1.2.3 Pakety

Paket v kontexte počítačových sietí je základnou jednotkou dát, ktorá sa prenáša cez sieť. Keď dáta opúšťajú zariadenie (napríklad počítač alebo smartphone), sú rozdelené na menšie kusy známe ako pakety. Tieto pakety sú potom posielané cez sieť do cieľového zariadenia, kde sú znovu zložené do pôvodnej formy. Tento proces umožňuje efektívne a flexibilné riadenie dát cez komplexné siete [8].

- Štruktúra paketu: Paket sa skladá z dvoch hlavných častí: hlavičky a nákladu (payload).
- Hlavička: Obsahuje metadáta potrebné pre správne smerovanie a doručenie paketu. Tieto metadáta zahŕňajú zdrojovú a cieľovú adresu, sekvenčné čísla, protokolové informácie a ďalšie kontrolné mechanizmy potrebné na správne spracovanie paketu v sieti.

- Náklad (Payload): Táto časť obsahuje skutočné dáta posielané užívateľom. V závislosti od aplikácie môže obsahovať text, obrázky, video, alebo iné typy dát [9].

Pakety sú posielané cez sieť pomocou smerovačov a prepínačov, ktoré rozhodujú o najefektívnejšej ceste pre každý paket. Každý paket môže cestovať rozdielnou trasou a doraziť v rôznom poradí. Protokoly ako TCP zaisťujú, že pakety sú správne usporiadané a všetky chýbajúce alebo poškodené pakety sú znovu vyžiadané a doručené.

TCP pakety (Transmission Control Protocol) obsahujú viaceré technické komponenty, ktoré umožňujú spoľahlivé zdieľanie dát. UDP pakety (User Datagram Protcol) majú jednoduchšiu hlavičku a obsahujú menej polí, čo umožňuje rýchlejšie spracovanie. Hlavička v prípade IP paketov (Internet Protocol) riadi smerovanie a dodanie paketov v sieti.

Tieto technické aspekty sú základom pre správne pochopenie základov, ako sieťové protokoly TCP, UDP a IP fungujú a interagujú v rozsiahlom prostredí siete, ako je internet. Vďaka nim je možné efektívne riadiť dátový tok, zabezpečiť spoľahlivosť prenosu, alebo naopak optimalizovať rýchlosť v prípade menej kritických aplikácií [9].

1.3 Doménový menný systém

Doménový menný systém (DNS) predstavuje kľúčovú súčasť fungovania internetu, umožňujúcu preklad doménových mien na IP adresy a opačne. V tejto kapitole sa dôkladne zameriavame na jednotlivé mechanizmy, ktoré zabezpečujú túto funkcionalitu a ktoré tvoria základný kameň celého DNS systému.

Rozlíšenie doménových mien na IP adresy: DNS umožňuje preklad doménových mien, ktoré sú ľahko zapamätateľné pre ľudí, na IP adresy, ktoré sú potrebné pre komunikáciu v počítačovej sieti. Tento proces začína na úrovni resolverov, ktoré posielajú dotazy na nameservery a interpretujú ich odpovede. Mechanizmus DNS zabezpečuje, že je možné efektívne nájsť IP adresu priradenú k danému doménovému názvu.

Spätné mapovanie adries na doménové mená: Okrem rozlíšenia doménových mien na IP adresy je dôležité aj spätné mapovanie IP adries na doménové mená. Tento proces produkuje záznamy, ktoré sú ľahko čitateľné pre ľudí a často sa používajú v logovacích súboroch a autentizačných kontrolách. DNS využíva doménu in-addr.arpa na štruktúrovane

a správu týchto záznamov. Táto doména je štruktúrovaná tak, aby odzrkadľovala hierarchickú povahu IP adries a umožňovala efektívne vyhľadávanie doménových mien na základe adries. Záznamy v doméne in-addr.arpa sú indexované podľa klasického formátu IP adries a umožňujú rýchle a spoľahlivé vyhľadávanie. Dôležitým mechanizmom, ktorý zvyšuje efektivitu DNS, je caching. DNS servery ukladajú údaje získané počas rozlíšenia do vyrovnávacej pamäte, čo umožňuje rýchlejšie odpovede na opakované dotazy. Caching znižuje zaťaženie DNS infraštruktúry a zabezpečuje rýchlejšiu odozvu pre používateľov. TTL je kľúčovým aspektom cachingu, ktorý určuje, ako dlho môžu byť údaje v cache uložené pred ich odstránením. Krátke TTL zabezpečujú aktuálnosť údajov, zatiaľ čo dlhé TTL zlepšujú výkon, ale môžu viesť k nekonzistencii údajov. Správne nastavená hodnota premennej TTL je dôležitá pre optimálnu funkčnosť DNS dotazov [10].

Mechanizmy DNS, ako je rozlíšenie doménových mien, spätné mapovanie adries, doména in-addr.arpa, caching a TTL, tvoria základné piliere DNS a zabezpečujú spoľahlivú správu doménových mien na internete. Porozumenie týmto mechanizmom je nevyhnutné pre úspešné nasadenie a správu DNS infraštruktúry. Komplexná znalosť týchto mechanizmov umožňuje efektívne riešenie problémov s DNS a optimalizáciu výkonu siete.

1.3.1 DNS over HTTPS

DNS over HTTPS (DoH) je mechanizmus, ktorý umožňuje šifrovanú a autentizovanú komunikáciu DNS dotazov pomocou HTTPS protokolu. Tento mechanizmus poskytuje vyššiu úroveň bezpečnosti a súkromia pre DNS komunikáciu v porovnaní s tradičným nešifrovaným DNS, ktorý využíva UDP alebo TCP. DNS nad HTTPS funguje tak, že DNS dotazy sú zapuzdrené do HTTPS dátových paketov a prenášané cez HTTPS spojenie. To zabezpečuje, že dáta sú šifrované pomocou SSL/TLS, čo zabraňuje neoprávnenému odposluchu a manipulácii s DNS premávkou. Rozdiely medzi DoH a tradičným DNS zahŕňajú:

Tradičný DNS používa špecifický port (napr. 53 pre UDP a TCP), kým DoH využíva HTTPS na bežnom porte 443. Toto umožňuje maskovanie DNS premávky medzi inými HTTPS dátovými tokmi a zvyšuje ochranu pred neoprávnenými zásahmi. DoH môže využívať funkcie HTTP, ako sú cookies a hlavičkové polia, na identifikáciu a sledovanie [11].

1.3.2 DNS over Transport Layer Security

Protokol DNS over Transport Layer Security (TLS) je spôsobom zabezpečenia DNS komunikácie. V porovnaní s tradičným DNS umožňuje šifrovanie spojení a autentifikáciu serverov, čo zvyšuje súkromie a bezpečnosť DNS prevádzky. DNS nad TLS funguje na princípe šifrovaného spojenia medzi DNS klientmi a servermi pomocou protokolu TLS. To zabezpečuje dôvernosť a integritu DNS dotazov a odpovedí. Rozdiely medzi DNS nad TLS a tradičným DNS zahŕňajú:

- DNS over TLS bežne využíva špecifický port (napr. 853), ktorý je určený pre šifrovanú DNS komunikáciu.
- DNS over TLS umožňuje autentifikáciu DNS serverov pomocou certifikátov, čo zvyšuje dôveru v komunikáciu s DNS resolvermi.
- Obe technológie, DoH a DNS nad TLS, poskytujú vyššiu úroveň bezpečnosti a súkromia v porovnaní s tradičným nezabezpečeným DNS [12].

1.4 Firewall

Firewall je počítačový systém navrhnutý na zabezpečenie siete a má za úlohu obmedziť prístup nežiaducich dátových tokov do alebo zo siete. Tento softvér alebo počítačový systém funguje na základe selektívneho povolenia alebo blokovania dátových paketov. Vo väčšine prípadov slúži na ochranu pred škodlivou činnosťou zo strany potenciálnych útočníkov.

Firewall môžeme prirovnať k hranici alebo bráne, ktorá riadi prenos povolených alebo zakázaných webových aktivít v sieti. Termín "firewall" pochádza z konceptu fyzickej steny, ktorá, v prípade požiaru, spomaľuje šírenie.

Firewally pracujú na základe filtrovania, čím rozhodujú, ktorý sieťový tok má byť povolený a ktorý sa má považovať za potenciálne nebezpečný. Tieto rozhodnutia sú zvyčajne založené na nastaveniach pravidiel, ktoré definujú, ktoré dáta majú byť povolené a ktoré majú byť zablokované. Pravidlá môžu obsahovať rôzne parametre, ako sú zdrojová a cieľová adresa, porty, alebo používané protokoly.

1.4.1 Typy firewallov

Firewally sú kritickým prvkom zabezpečenia sietí, ktoré zohrávajú kľúčovú úlohu pri ochrane dôverných informácií a zariadení pred neoprávneným prístupom a potenciálnymi útokmi. Existuje niekoľko hlavných typov firewallov, pričom každý z nich ponúka rôzne prístupy k filtrovaniu a zabezpečeniu siete. Autori knihy DNS and Bind, Albitz a Liu popisujú nasledujúce rozdelenie firewallov [13]:

- Statické filtrovanie paketov je jedným z najzákladnejších typov firewallu. Tento systém rozhoduje o priepustnosti dátových paketov na základe ich údajov, ako sú zdrojová a cieľová IP adresa a porty. Tento prístup je založený na preddefinovaných pravidlách a pracuje na úrovni siete.
- Firewally na úrovni obvodu fungujú na úrovni spojenia a sledujú stav sieťových spojení. Tento typ firewallu umožňuje lepšiu kontrolu nad sieťovým tokom a rozhoduje na základe informácií o stave spojenia.
- Firewally so stavovou inšpekciou sú schopné dôkladnejšej kontroly nad komunikáciou v sieti, keďže sledujú stav každého sieťového spojenia a rozhodujú na základe kontextu, nie len na základe jednotlivých paketov. Tento prístup poskytuje pokročilú detekciu a ochranu pred hrozbami v sieti.
- Proxy firewally pracujú na úrovni aplikačnej vrstvy a majú schopnosť filtrovať dáta na základe aplikácií alebo služieb. Tieto firewally môžu vykonávať hĺbkovú inšpekciu paketov a sledovať obsah komunikácie, čo zvyšuje ich schopnosť identifikovať a blokovať škodlivý obsah.
- Next-Generation Firewall (NGFW) kombinuje vlastnosti tradičného firewallu s funkcionalitou systémov pre prevenciu prieniku do siete (IPS). Poskytuje pokročilú detekciu a ochranu pred hrozbami, ako sú malvéry a útoky na sieť.

Výhody použitia firewallov zahŕňajú ochranu pred neoprávneným prístupom a škodlivým obsahom, kontrolu a monitorovanie sieťového toku, prispôsobiteľnosť a konfigurovateľnosť pravidiel a prevenciu pred rôznymi typmi útokov. Napriek svojim výhodám majú firewally aj niekoľko nevýhod, vrátane možných obmedzení vo filtrovaní paketov, zvýšenej komplexity konfigurácie, možných problémov s kompatibilitou a nákladov na implementáciu a údržbu [13].

Správna implementácia a konfigurácia firewallov je nevyhnutná pre zvýšenie bezpečnosti sietí a ochranu pred rôznymi hrozbami, čím zabezpečuje bezpečnú a spoľahlivú komunikáciu v sieti [14].

1.4.2 Iptables

Iptables je nástrojom pre konfiguráciu sieťových firewallov v prostredí Linuxu a Unixu. Svojou schopnosťou filtrovať, prepisovať a presmerovať sieťovú komunikáciu na základe definovaných pravidiel poskytuje robustné možnosti zabezpečenia siete. V tejto časti práce sme vysvetlili základné pojmy, funkcie a syntax príkazov iptables.

- **Základné pojmy**
  - Pravidlá: Pravidlá určujú, ako sa majú spracovať jednotlivé sieťové pakety na základe ich vlastností.
  - Tabuľky: Tabuľky sú kontajnery pre pravidlá. Existujú štyri hlavné tabuľky: filter, nat, mangle a raw.
  - Reťazce: Reťazce sú zoznamy pravidiel v rámci jednej tabuľky. Existujú preddefinované reťazce ako INPUT, OUTPUT, FORWARD, PREROUTING a POSTROUTING.
- Hlavné akcie
  - ACCEPT: Povoliť prechod paketu.
  - DROP: Zahodiť paket, neodpovedá naň.
  - REJECT: Zamietnuť paket a poslať o tom informáciu odosielateľovi.
- **Praktické príklady použitia**
  - Vytvorenie firewallu na zabezpečenie siete.
  - Presmerovanie portov a správa sieťového toku.
  - NAT (Network Address Translation) pre zdieľanie internetu a ochranu siete.

Iptables poskytuje efektívne nástroje na zabezpečenie a správu sietí vo firemných aj domácich prostrediach. Jeho znalosť a správne použitie je kľúčom k efektívnemu riadeniu sieťovej komunikácie a ochrane sietí pred neoprávneným prístupom [15].

2 Cieľ, metodika práce a metódy skúmania

Naším hlavným cieľom bakalárskej práce bolo demonštrovať využitie mikropočítača Raspberry Pi ako základného bezpečnostného prvku v malej počítačovej sieti. Konkrétne sme sa sústredili na testovanie a porovnanie rôznych open-source riešení pre sieťovú správu, aby sme identifikovali najvhodnejšie softvérové vybavenie pre zabezpečenie a efektívnosť siete. Po analýze sme vyberali a implementovali optimálne riešenie, pričom náš výber bol založený na kritériách ako sú výkon, cena, bezpečnosť, používateľská prívetivosť a podpora komunity.

Cieľom práce je nielen demonštrovať schopnosť Raspberry Pi slúžiť ako bezpečnostný prvok, ale tiež poskytnúť praktický návod a odporúčania pre malé organizácie alebo jednotlivcov, ktorí hľadajú cenovo efektívne riešenia na zvýšenie bezpečnosti svojich počítačových sietí.

Na začiatku bolo nevyhnutné vybrať vhodné zariadenie a operačný systém, ktoré by splnili požiadavky projektu na flexibilitu, dostupnosť a podporu komunity. Rozhodli sme sa pre Raspberry Pi 4 kvôli jeho možnostiam prispôsobenia a silnej užívateľskej komunite. Pre operačný systém bol vybraný OpenWRT, pretože poskytuje rozsiahle možnosti konfigurácie sieťových služieb a bezpečnosti.

V procese konfigurácie sme nainštalovali operačný systém OpenWRT na SD kartu, ktorú sme následne vložili do Raspberry Pi. Detailne sme nastavili sieťové parametre vrátane IP adries, masky podsiete, a konfigurácie DHCP. Na zabezpečenie siete sme implementovali špecifické firewall pravidlá.

Na začiatku projektu sme určili, že pre automatizáciu rutinných úloh použijeme skripty v jazyku Bash, ktorý je štandardne dostupný na Linuxových systémoch a je ideálny pre správu systémových a sieťových operácií.

Bash Skripty: Tieto skripty boli navrhnuté na automatizáciu základných úloh ako aktualizácie softvéru, zálohovanie konfigurácii a monitorovanie stavu zariadenia.

Po úspešnom testovaní a revízii nástrojov a scriptov sme ich nasadili na produkčné zariadenie. Tento proces zahŕňal konfiguráciu spúšťacích skriptov, nastavenie príslušných práv pre spustenie a integráciu s existujúcimi systémovými službami na Raspberry Pi 4 pod kontrolou OpenWRT.

Zariadenie sme testovali začínajúc funkcionálnym testovaním jednotlivých komponentov, cez integračné testovanie celého systému až po stresové testy, ktoré simulovali reálne používanie v prostredí so sieťovou záťažou. Použili sme nástroje ako Wireshark pre sledovanie sieťovej komunikácie a custom skripty pre automatizované testovanie rôznych sieťových scenárov.

Údaje pre sme získali z rôznych zdrojov vrátane akademických prác z iných univerzít, oficiálnych dokumentácií nástrojov a knižných zdrojov, čo poskytlo komplexný prehľad o existujúcich riešeniach a teoretických základoch. Okrem toho, dôležitú časť údajov tvoria vlastné logy získané priamo z implementovaného bezpečnostného systému na Raspberry Pi, ktoré umožnia presné vyhodnotenie funkčnosti a efektivity navrhnutého riešenia.

3 Výsledky práce

V tejto časti práce sa venujeme prezentácii a diskusii výsledkov získaných počas realizácie projektu zabezpečenia malej počítačovej siete prostredníctvom Raspberry Pi. Praktické aplikácie teoretických konceptov a metodík, ktoré boli opísané v predchádzajúcich častiach, sú tu demonštrované na konkrétnych príkladoch a experimentoch.

Hlavným cieľom bolo ukázať, ako môže byť Raspberry Pi s operačným systémom OpenWRT použité ako efektívny nástroj na správu a zabezpečenie siete. Porovnali sme viaceré open-source ale aj komerčné riešenia a na základe analýzy sme vybrali najvhodnejšie riešenie podľa našich kritérií výkonnosti, ceny, bezpečnosti, prívetivosti pre používateľa a podpory komunity.

3.1 Konfigurácia OpenWRT

OpenWRT je vysoko prispôsobiteľnou distribúciou GNU/Linuxu navrhnutou špeciálne pre embedded zariadenia, ako sú bezdrôtové routery. Svojou flexibilitou a rozšíriteľnosťou poskytuje užívateľom úplnú kontrolu nad ich sieťami. OpenWRT umožňuje detailné nastavenie sieťových parametrov vrátane IP adresácie, VLAN, bridgingu a trunkingu, čo je ideálne pre pokročilých užívateľov, ktorí si želajú široké možnosti konfigurácie. S implementáciou VPN klienta a servera a nástrojmi na riadenie prenosu dát, ako je QoS a Smart Queue Management, OpenWRT poskytuje aj pokročilé funkcie pre optimalizáciu výkonu siete. Jeho ďalšie schopnosti zahŕňajú konfiguráciu DNS a DHCP serverov, riadenie prístupu, rozšírenú správu siete a monitorovanie a správu sieťových pripojení [16].

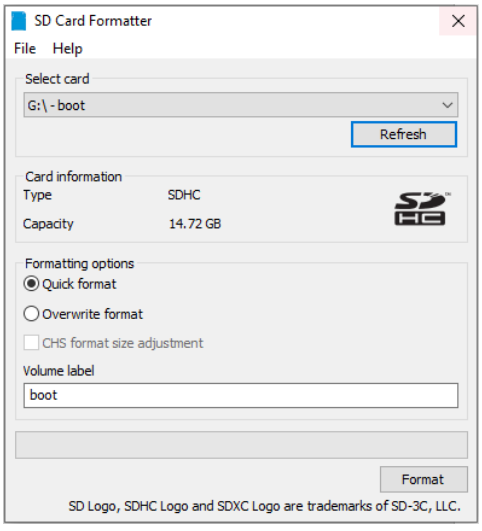
OpenWRT ponúka modulárnu štruktúru, ktorá umožňuje inštaláciu rôznych softvérových balíkov a rozšírení, čo poskytuje širokú škálu možností prispôsobenia siete podľa konkrétnych požiadaviek. S OpenWRT sme mali úplnú kontrolu nad každým aspektom našej siete, čo nám umožnilo vytvoriť robustné a bezpečné riešenie.

Namiesto snahy vytvoriť jednotný, statický firmvér poskytuje OpenWrt plne zapisovateľný súborový systém s voliteľným správcom balíkov. Táto voľba oslobodzuje od obmedzení výberu aplikácií a konfigurácie poskytovaných výrobcom a umožňuje používať balíky na prispôsobenie embedded zariadenia pre akúkoľvek aplikáciu.

Úspech každého informačného systému závisí od jeho správnej konfigurácie. V tejto podkapitole práce sa zameriavame na detailné nastavenie Raspberry Pi s operačným systémom OpenWRT, ktoré slúži ako základ pre naše bezpečnostné riešenie. Presné a premyslené nastavenia nielenže zvyšujú bezpečnosť a výkonnosť siete, ale zároveň definujú, ako efektívne môžeme využívať dostupné sieťové zdroje. V nasledujúcich podkapitolách prejdeme krok za krokom procesom konfigurácie od základného nastavenia hardvéru, cez inštaláciu a nastavenie operačného systému, až po špecifické nastavenia sieťových služieb, ako sú DHCP, DNS, a firewall. Každý z týchto krokov je kritický pre zabezpečenie a správnu funkčnosť našej počítačovej siete a vyžaduje si dôslednú pozornosť k detailom. Dôkladná konfigurácia nám umožňuje nielen zabezpečiť súlad s najlepšími praxami v oblasti IT bezpečnosti, ale tiež poskytuje príležitosť pre praktické aplikovanie teoretických znalostí z predchádzajúcich kapitol.

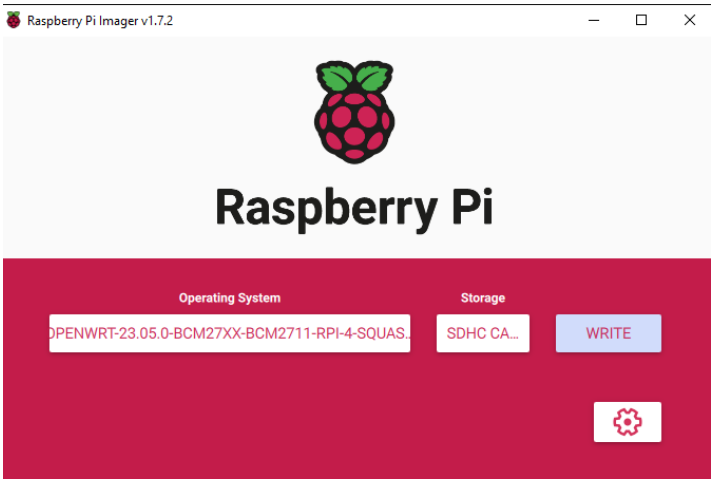
Pred zahájením inštalácie sme zhromaždili všetky potrebné komponenty a súbory, čo zabezpečilo hladký a efektívny priebeh inštalácie. Navštívili sme oficiálnu stránku OpenWRT, odkiaľ sme stiahli najnovší obraz systému určený pre Raspberry Pi 4 Model B a uložili ho na našu pracovnú stanicu.

Použili sme kvalitnú SD kartu s kapacitou 18 GB a zabezpečili sme čítačku kariet pre pohodlný prenos dát. Následne sme vykonali hĺbkové formátovanie SD karty pomocou nástroja SD Card Formatter, čím sme kartu pripravili na nahratie nového obrazu.



Obrázok 1 – Predstavenie nástroja SD Card Formatter, zdroj: Vlastné spracovanie

Použitím nástroja Raspberry Pi Imager sme nahrali obraz OpenWRT na SD kartu, pričom tento softvér zabezpečil správne zaznamenanie obrazu. V procese nahrávania obrazu bolo nutné zvoliť inštalačný súbor pre Openwrt a taktiež SD kartu.



Obrázok 2 – Predstavenie nástroja Raspberry Pi, zdroj: Vlastné spracovanie

Po úspešnom zápise sme SD kartu vložili do slotu na Raspberry Pi 4, ktoré bolo následne pripravené na spustenie a konfiguráciu. Po zapojení a spustení Raspberry Pi sa počas prvého bootovania vykonali inicializačné procesy, vrátane nastavení siete a služieb.

Nastavenie jazyku a časovej zóny a konfigurácie sieťových parametrov ako protokolu pre prideľovanie IP adries, DNS a pripojenia k internetu sme vykonali, aby zariadenie správne komunikovalo v sieti. Nastavenia z obrázku č. 3 sme nakonfigurovali prostredníctvom Rasppberry Pi a OpenWrt terminálu. Použili sme príkaz: *vi /etc/config/network*, ktorý nám umožnil prepísať konfiguračný súbor.

```
config interface 'lan'
        option proto 'dhcp'
        option device 'eth1'
config interface 'wan'
        option proto 'dhcp'
        option device 'eth0'
```

Obrázok 3 – Ukážka časti konfiguračného súboru pre sietové nastavenia, zdroj: Vlastné spracovanie

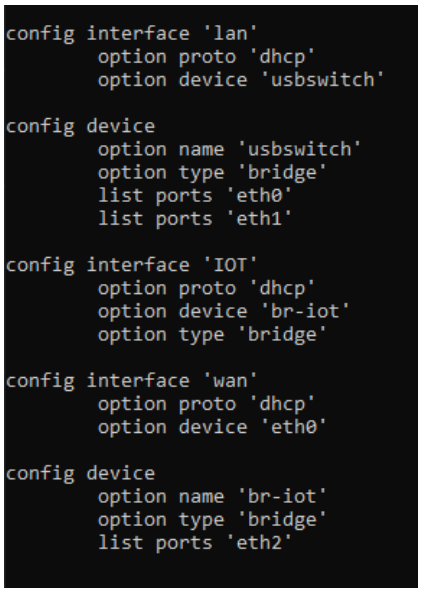
V nasledujúcej podkapitole podrobne popíšeme konfiguráciu LAN, WAN a ďalších sieťových rozhraní, vrátane vytvárania *bridgu* medzi rôznymi segmentmi siete, čo umožní efektívnejšie riadenie a izoláciu sieťového toku. Zabezpečíme automatické prideľovanie IP adries klientom v sieti a správne smerovanie DNS dotazov s použitím šifrovania a DNSSEC šifrovania pre zvýšenie bezpečnosti a dôveryhodnosti DNS služieb. Definujeme a prispôsobíme pravidlá pre firewall, aby sme zabezpečili ochranu siete pred nežiaducimi prístupmi a útokmi, pričom zachováme správne fungovanie komunikácie medzi jednotlivými zónami siete.

Týmto komplexným prístupom k inštalácii a konfigurácii OpenWRT sme zabezpečili nielen správne fungovanie siete, ale aj zvýšenú bezpečnosť a účinnosť využitia dostupných sieťových zdrojov. Poďme sa pustiť do detailnej analýzy a nastavenia jednotlivých aspektov siete pre dosiahnutie optimálneho výsledku.

3.1.1 Konfigurácia rozhraní a zariadení

Súbory nachádzajúce sa v */etc/config/network* sme upravili pre nastavenie sieťových rozhraní a definovanie *bridgov* medzi LAN a WAN segmentmi. To zahŕňalo pridanie alebo úpravu konfiguračných blokov pre každé rozhranie, kde sme špecifikovali protokoly, typ a názov zariadenia alebo IP adresy, masky podsiete a iné relevantné parametre pre správnu funkčnosť siete.

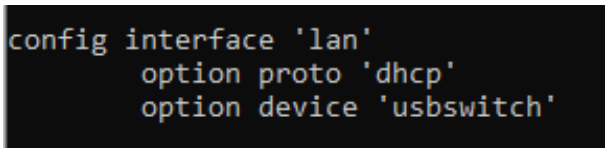
Pre detailnejšiu analýzu konfigurácie siete, ktorá je založená na uvedených nastaveniach v OpenWrt alebo podobnom systéme, poskytneme komplexné vysvetlenie každej časti konfigurácie, vrátane možných dôsledkov pre sieťovú bezpečnosť a funkčnosť:



Obrázok 4 – Ukážka časti konfiguračného súboru pre sietové nastavenia, zdroj: Vlastné spracovanie

Konfigurácia LAN rozhrania

Rozhranie *lan* je nastavené na získavanie IP adries dynamicky cez DHCP. Rozhranie je pripojené cez zariadenie *usbswitch*, ktoré je definované ako *bridge* a zahŕňa viaceré porty. Použitie DHCP na LAN rozhraní zjednodušuje správu IP adries pre zariadenia v sieti. *Bridge* spojuje fyzické porty do jedného logického rozhrania, umožňujúc efektívnejšie riadenie a rozširovanie lokálnej siete.



Obrázok 5 – Ukážka časti konfiguračného súboru pre lan rozhranie, zdroj: Vlastné spracovanie

Konfigurácia IOT rozhrania

Rozhranie IOT, určené pre zariadenia Internetu vecí (IoT), je zásadné pre spojenie a správu rôznych typov zariadení, ktoré sú bežne používané v domácnostiach, obchodných priestoroch alebo priemyselných aplikáciách.

- Opption proto *'dhcp':* Toto nastavenie určuje, že rozhranie IOT získava svoju IP adresu dynamicky pomocou DHCP. Tento spôsob pridelenia IP adresy

zjednodušuje správu siete IoT zariadení, keďže sa IP adresy nemusia nastavovať manuálne.

- option device *'br-iot'*: Toto rozhranie je pripojené cez *bridge* s názvom *br-iot*. Bridge umožňuje spojiť viacero fyzických alebo logických rozhraní do jedného segmentu siete, čo poskytuje lepšiu kontrolu a izoláciu sieťového toku medzi IoT zariadeniami.
- option type *'bridge*': Určuje, že br-iot funguje ako „most“, čo znamená, že všetky zariadenia pripojené k tomuto *bridge* môžu vzájomne komunikovať ako keby boli na rovnakej fyzickej sieti.

Konfigurácia WAN Rozhrania

Rozhranie *wan* umožňuje zariadeniu pripojiť sa na širšiu sieť alebo internet, získavajúc IP adresu prostredníctvom DHCP priamo od poskytovateľa internetových služieb. Dynamické pridelenie IP adresy zjednodušuje konfiguráciu a pripojenie na internet. Vhodné je starostlivé zabezpečenie tohto rozhrania, pretože predstavuje vstupný bod pre vonkajšie sieťové hrozby.

```
config interface 'wan'
        option proto 'dhcp'
        option device 'eth0'
```

Obrázok 6 – Ukážka časti konfiguračného súboru pre wan rozhranie, zdroj:Vlastné spracovanie

Konfigurácia zariadenia (bridge – usbswitch)

Definuje *bridge* s názvom *usbswitch*, ktorý logicky spojí porty *eth0* a *eth1*. Umožňuje zdieľanie siete a komunikáciu medzi portami zahrnutými v *bridge*. Zabezpečuje, že všetky zariadenia pripojené cez tieto porty môžu komunikovať medzi sebou ako jedna súčasť siete. Toto zariadenie môže predstavovať potencionálne bezpečnostné riziko, ak nie sú správne nastavené pravidlá pre prístup a ochranu dát.

```
config device
        option name 'usbswitch'
        option type 'bridge'
        list ports 'eth0'
        list ports 'eth1'
```

Obrázok 7 – Ukážka časti konfiguračného súboru pre usbswitch zariadenie, zdroj:Vlastné spracovanie

Konfigurácia zariadenia (bridge – br-iot)

Tento *bridge*, nazvaný *br-iot*, môže byť použitý na izoláciu IoT zariadení od zvyšku siete, pokiaľ je k nemu priradené osobitné rozhranie. Umožňuje lepšiu kontrolu a segregáciu IoT zariadení, čím zvyšuje bezpečnosť týchto zariadení a znižuje riziko narušenia siete.

```
config device
        option name 'br-iot'
        option type 'bridge'
        list ports 'eth2'
```

Obrázok 8 – Ukážka časti konfiguračného súboru pre pre zariadenie br-iot, zdroj:Vlastné spracovanie

3.1.2 Nastavenie DHCP a DNS

V súbore */etc/config/dhcp* sme v predchádzajúcej inštalácií nakonfigurovali DHCP server pre automatické prideľovanie IP adries klientom v našej sieti. Rovnako sme nastavili DNS forwardovanie, čo zabezpečuje, že všetky DNS požiadavky z našej siete sú správne spracované a smerované. Pre nakonfigurovanie DNS over TLS sme sa rozhodli pre voľbu resolvera Unbound

Pre inštaláciu a prípravu potrebných balíčkov sme na zariadení, s OpenWRT, pomocou package managera opkg nainštalovali Unbound a odhcpd. Dnsmasq sme odinštalovali, pretože jeho funkcionalitu prevezme Unbound.V súbore */etc/unbound/unbound_ext.conf* sme nastavili Unbound, aby používal Cloudflare DNS servery s TLS:

```
##############################################################
forward-zone:
  name: "."
  forward-addr: 1.1.1.1@853
  forward-addr: 1.0.0.1@853
  forward-addr: 2606:4700:4700::1111@853
  forward-addr: 2606:4700:4700::1001@853
  forward-ssl-upstream: yes
```

Obrázok 9 – Konfiguračný súbor pre unbound DNS, č.1, zdroj:Vlastné spracovanie

Aby bol Unbound správne nakonfigurovaný a integroval s odhcpd, vykonali sme úpravu súboru */etc/config/unbound* a */etc/config/dhcp* tak, aby podporovala naša konfigurácia dynamické DNS aktualizácie

```
config unbound
  option add_local_fqdn '1'
  option add_wan_fqdn '1'
  option dhcp_link 'odhcpd'
  option dhcp4_slaac6 '1'
  option domain 'lan'
  option domain_type 'static'
  option listen_port '53'
  option rebind_protection '1'
  option unbound_control '1'
```

Obrázok 10 – Konfiguračný súbor pre unbound DNS, č.2, zdroj:Vlastné spracovanie

```
config dhcp 'lan'
        option interface 'lan'
        option start '100'
        option limit '150'
        option leasetime '12h'
        option dhcpv4 'server'
        option dhcpv6 'hybrid'
        option ra 'hybrid'
        list ra_flags 'managed-config'
        list ra_flags 'other-config'

config odhcpd 'odhcpd'
        option maindhcp '1'
        option leasefile '/var/lib/odhcpd/dhcp.leases'
        option leasetrigger '/usr/lib/unbound/odhcpd.sh'

config dhcp 'wan'
        option interface 'wan'
```

Obrázok 11 – Konfiguračný súbor pre unbound DNS, č.3, zdroj:Vlastné spracovanie

Pre zabezpečenie, že DNSSEC je aktívne a správne nastavené v Unbound, sme skontrolovali a aktualizovali niekoľko konfiguračných nastavení v konfiguračnom súbore */etc/unbound/unbound.conf.*

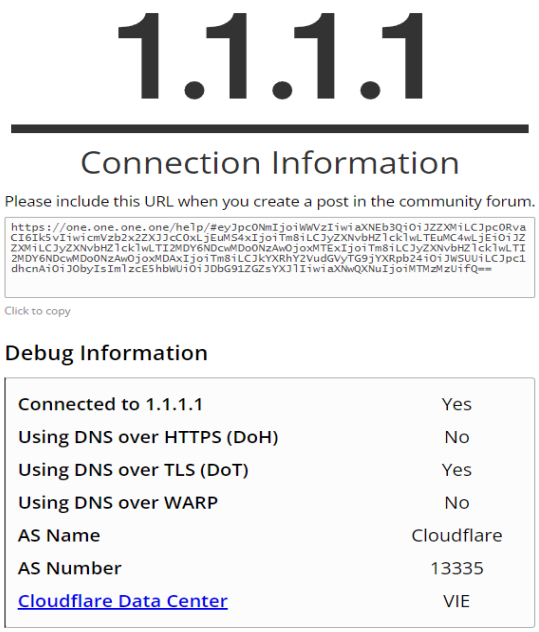
```
# The pid file is created before privleges drop so no concern
pidfile: "/var/run/unbound.pid"
auto-trust-anchor-file: "/var/lib/unbound/root.key
val-permissive-mode: no
val-log-level: 2
# no threads and no memory slabs for threads
num-threads: 1
msg-cache-slabs: 1
```

Obrázok 12 – Ukážka časti konfiguračného súboru pre DNSSEC, zdroj:Vlastné spracovanie

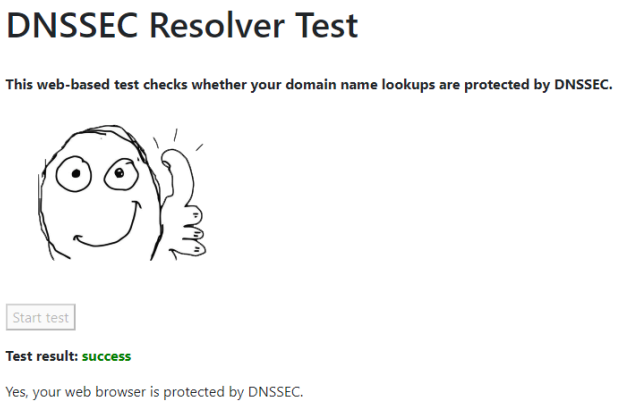
- auto-trust-anchor-file: Tento súbor obsahuje koreňové DNSSEC kľúče, ktoré sú potrebné pre validáciu podpisov. Unbound obvykle spravuje tento súbor automaticky.
- val-permissive-mode: Ak je nastavený na "no", Unbound odmietne odpovede, ktoré neprejdú DNSSEC validáciou. Ak je nastavený na "yes", odpovede, ktoré zlyhajú na DNSSEC validácii, budú akceptované.
- val-log-level: Táto hodnota umožňuje nastaviť úroveň logovania pre DNSSEC operácie, kde vyššie čísla poskytujú viac detailov o validácii.

Pre aktiváciu unbound sme vykonali aktiváciu služby prostredníctvom príkazu *service unbound enable* a následne zapli resolver Unbound - *service unbound start.*

Použitím nástroja Wireshark a webových služieb one.one.one.one sme overili, že DNS dotazy sú naozaj šifrované, spracovávané serverom spoločnosti Cloudflare a zároveň zabezpečené prostredníctvom DNSSEC. DNSSEC overuje, že DNS údaje neboli počas tranzitu manipulované, a zabezpečuje ich integritu a autentickosť.



Obrázok 13 – Webový nástroj pre overenie DNS konigurácie, zdroj: Vlastné spracovanie



Obrázok 14 – Webový nástroj pre overenie DNSSEC konigurácie, zdroj: Vlastné spracovanie

3.1.3 *Konfigurácia firewallu*

V konfiguračnom súbore */etc/config/firewall* sme definovali a upravili pravidlá pre firewall. Tieto pravidlá zahŕňajú definície zón, politík medzi zónami a špecifické pravidlá pre aplikácie a služby, ktoré zabezpečujú ochranu našej siete pred nežiaducimi prístupmi a potenciálnymi útokmi. Základné pravidlá sú nastavené tak, aby predvolene zamietali prichádzajúce spojenia, akceptovali odchádzajúce a zamietali smerovanie, čo zvyšuje bezpečnosť. Premenná *synflood_protect* je nastavená na hodnotu 1, pre ochranu pred SYN flood útokmi.

```
config defaults
        option input 'REJECT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option synflood_protect '1'
```

Obrázok 15 – Ukážka časti konfiguračného súboru pre konfiguráciu firewallu , zdroj: Vlastné spracovanie,

Zóny firewallu

- LAN zóna povoľuje všetky druhy sieťovej komunikácie medzi zariadeniami v LAN.
- WAN zóna prijíma prichádzajúce spojenia (čo môže byť potrebné pre konkrétne prípady), povoľuje odchádzajúce a zamietne presmerovanie, s maskovaním NAT pre odchádzajúce spojenia.

```
config zone
        option name 'lan'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'ACCEPT'
        list network 'lan'

config zone
        option name 'wan'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option masq '1'
        option mtu_fix '1'
        list network 'wan6'
```

Obrázok 16 – Ukážka časti konfiguračného súboru pre konfiguráciu firewallu - zóny , zdroj: Vlastné spracovanie

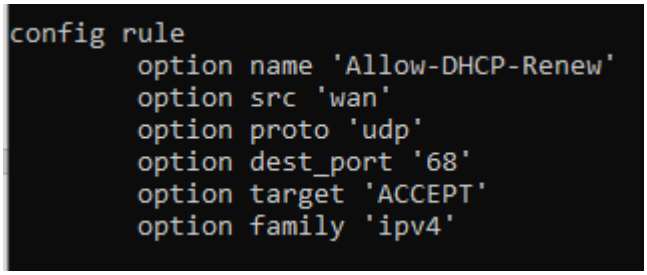
Pravidlá pre smerovanie a špecifické pravidlá

- Pravidlá umožňujú zariadeniam v LAN a hostovskej sieti prístup na internet cez WAN.
- Config forwarding umožňuje zariadeniam v LAN a hostovskej sieti prístup na internet cez WAN.

```
config forwarding
        option src 'lan'
        option dest 'wan'

config forwarding
        option src 'guest'
        option dest 'wan'
```

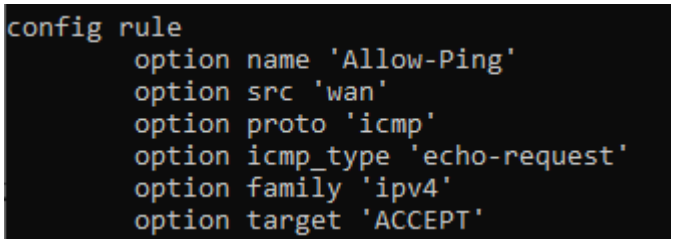
Obrázok 17 – Ukážka časti konfiguračného súboru pre konfiguráciu firewallu - smerovanie , zdroj: Vlastné spracovanie

- Allow-DHCP-Renew: Povoluje obnovu DHCP pre zariadenia vo WAN.



Obrázok 18 – Ukážka časti konfiguračného súboru firewall – pravidlo č. 1 , zdroj: Vlastné spracovanie

- Allow-Ping: Umožňuje ICMP echo request (ping) z WAN, čo môže pomôcť pri diagnostike.



Obrázok 19 – Ukážka časti konfiguračného súboru pre firewall – pravidlo č. 2 , zdroj: Vlastné spracovanie

3.1.4 Pravidelné údržby a aktualizácie

Aby sme zabezpečili najvyššiu úroveň bezpečnosti a výkonu, pravidelne sme aktualizovali náš systém pomocou príkazov opkg update (aktualizácia zoznamu dostupných balíčkov) a opkg upgrade (aktualizácia inštalovaných balíčkov). Tieto príkazy zabezpečujú, že všetky komponenty systému sú na najnovšej verzii a chránené proti známym zraniteľnostiam.

Úlohu pravidelného aktualizovania softvérových balíkov a bezpečnostných záplat na systéme sme nakonfigurovali prostredníctvom CRON úlohy (command run on notice), tieto úlohy sú určené pre vykonávanie predefinovaných úkonov na základe konkrétnej časovej frekvencie. Úloha pomáha udržiavať systém bezpečný a stabilný tým, že pravidelne inštaluje najnovšie dostupné opravy a aktualizácie.

*0 3 * * * /usr/bin/opkg update && /usr/bin/opkg upgrade*

Príkaz sa spustí každý deň o 3:00 ráno. Proces začína aktualizáciou zoznamu dostupných balíkov pomocou opkg update a pokračuje aktualizáciou nainštalovaných balíkov na ich

najnovšie verzie pomocou opkg upgrade. Zabezpečuje najnovšiu ochranu pred bezpečnostnými hrozbami. Znižuje riziko systémových chýb vďaka najnovším opravám. Minimalizuje potrebu ručnej údržby systému. Konfigurácia pre manažér balíkov opkg sa obvykle nachádza v */etc/opkg.conf*.

Úloha pre zálohovanie konfiguračných súbor pravidelne vytvára zálohy dôležitých konfiguračných súborov siete, čo zabezpečuje ochranu pred stratou dát a umožňuje rýchle obnovenie v prípade potreby. V systéme sme ju nakonfigurovali takto:

*02***/bin/tar -czf /var/backups/network_configs_$(date +\%Y\%m\%d).tar.gz /etc/config/*

Spustí sa každý deň o 2:00 ráno a vytvorí komprimovaný archív s názvom *network_configs_YYYYMMDD.tar.gz*, obsahujúci konfiguračné súbory zo zložky */etc/config/*. Zaisťuje dostupnosť záloh v prípade poruchy alebo chyby. Umožňuje rýchle obnovenie konfigurácií do ich posledného funkčného stavu. Pomáha v auditovaní zmien v konfigurácii. Zálohy sa ukladajú v */var/backups/* a zdrojové konfiguračné súbory sa nachádzajú v */etc/config/*.

Úloha pre účely testovania pripojenia k internetu pravidelne testuje dostupnosť internetového pripojenia a zaznamenáva výsledky do logovacieho súboru, čo umožňuje monitorovanie a rýchlu reakciu na prípadné problémy s pripojením.

**/15 * * * * /bin/ping -c 4 8.8.8.8 >> /var/log/internet_connection.log*

Vykonáva sa každých 15 minút a spustí štyri ICMP ping žiadosti na adresu 8.8.8.8, pričom výsledky sa zapisujú do internet_connection.log. Poskytuje nepretržité sledovanie dostupnosti siete. Umožňuje identifikovať a diagnostikovať problémy siete v reálnom čase. Zaznamenáva historické údaje o stabilite pripojenia. Výsledky sa ukladajú do logovacieho súboru v */var/log/internet_connection.log*.

Ďaľšou z nastavených automatických Cron úloh je určená pre pravidelné spúšťanie skenovania sieťových portov na identifikáciu otvorených portov a potenciálnych bezpečnostných zraniteľností.

*01***/usr/bin/nmap -p 1-65535 -T4 -A -v 192.168.1.0/24> /var/log/security_scan.log*

Spustí sa každý deň o 1:00 ráno, používa nástroj nmap na skenovanie všetkých portov v rozsahu IP adries 192.168.1.0/24 a výsledky ukladá do security_scan.log. Zisťuje potenciálne

zraniteľnosti a otvorené porty. Umožňuje proaktívne riešenie bezpečnostných hrozieb. Zlepšuje celkovú bezpečnosť siete. Výsledky skenovania sa ukladajú do */var/log/security_scan.log*.

V prípade potreby by taktiež bolo možné tieto CRON úlohy kombinovať vytvorením bash scriptu a následným pridaním scriptu medzi CRON úlohy. Príklad takéhoto scriptu

```
#!/bin/bash

# Logovací súbor
LOGFILE="/var/log/cron_task.log"

# Funkcia na logovanie
log() {
    echo "$(date '+%Y-%m-%d %H:%M:%S') - $1" >> $LOGFILE
}

# Aktualizácia systému
log "Spúšťam aktualizáciu systému..."
/usr/bin/opkg update && /usr/bin/opkg upgrade
if [ $? -eq 0 ]; then
    log "Aktualizácia systému bola úspešná."
else
    log "Chyba pri aktualizácii systému!"
fi

# Zálohovanie konfiguračných súborov
log "Spúšťam zálohovanie konfiguračných súborov..."
tar -czf "/var/backups/network_configs_$(date +'%Y%m%d').tar.gz" /etc/config/
if [ $? -eq 0 ]; then
    log "Zálohovanie konfiguračných súborov bolo úspešné."
else
    log "Chyba pri zálohovaní konfiguračných súborov!"
fi

# Testovanie pripojenia k internetu
log "Testovanie pripojenia k internetu..."
ping -c 4 8.8.8.8 > /dev/null
if [ $? -eq 0 ]; then
    log "Internetové pripojenie je funkčné."
else
    log "Internetové pripojenie nie je dostupné!"
fi
```

Obrázok 20 – Vzorový bash script , zdroj: Vlastné spracovanie

3.1.5 Inštalácia IPS Snort

IPS (Intrusion Prevention System) je systém, ktorý nielen detekuje potenciálne hrozby, ale aktívne zasahuje proti hrozbám tým, že blokuje alebo zastavuje škodlivú aktivitu predtým, než môže spôsobiť škodu. IPS je obvykle integrovaný do firewallu alebo siete tak, že dokáže prijímať preventívne opatrenia.

Inštaláciu balíku *snort* sme vykonali zadaním príkazu:

opkg install snort

Po inštalácii sme použili konfiguračný nástroj uci na povolenie a základné nastavenie Snortu. Tieto príkazy nastavia Snort tak, aby bol systém aktívny a automaticky nakonfigurovaný na počúvanie na WAN rozhraní:

uci set snort.snort.enabled=1

uci set snort.snort.manual=0

uci set snort.snort.home_net="any"

uci set snort.snort.interface="$(uci get network.wan.device)"

uci commit

Po základnej inštalácii a konfigurácii sme pristúpili k pridaniu komunitných pravidiel. Komunitné pravidlá poskytujú základnú ochranu pred bežnými hrozbami a sú dostupné zdarma na oficiálnej stránke Snortu - https://snort.org/downloads/#rule-downloads. Navštívili sme stránku s pravidlami Snortu a stiahli najnovšiu verziu komunitných pravidiel.

Na OpenWRT sme vytvorili príslušné adresáre a umiestnili stiahnuté pravidlá. Ako je vidieť na obrázku č. 17, práca s adresárovou štruktúrou a súbormi vyzerá takto:

```
root@OpenWrt:/etc/snort/builtin_rules# cd /etc/snort/
root@OpenWrt:/etc/snort# vi  snort_defaults.lua
root@OpenWrt:/etc/snort# vi  snort_defaults.lua
root@OpenWrt:/etc/snort# cd /etc/snort/rules/
root@OpenWrt:/etc/snort/rules# touch community.rules
root@OpenWrt:/etc/snort/rules# ll
drwxr-xr-x    2 root     root          1024 May  4 16:32 ./
drwxr-xr-x    6 root     root          1024 May  4 15:58 ../
-rw-r--r--    1 root     root             0 May  4 16:32 community.rules
root@OpenWrt:/etc/snort/rules# vi community.rules
root@OpenWrt:/etc/snort/rules# /etc/init.d/snort status
running
root@OpenWrt:/etc/snort/rules# /etc/init.d/snort restart
root@OpenWrt:/etc/snort/rules# /etc/init.d/snort status
running
```

Obrázok 21 – Práca so súborovou štruktúrou, zdroj: Vlastné spracovanie

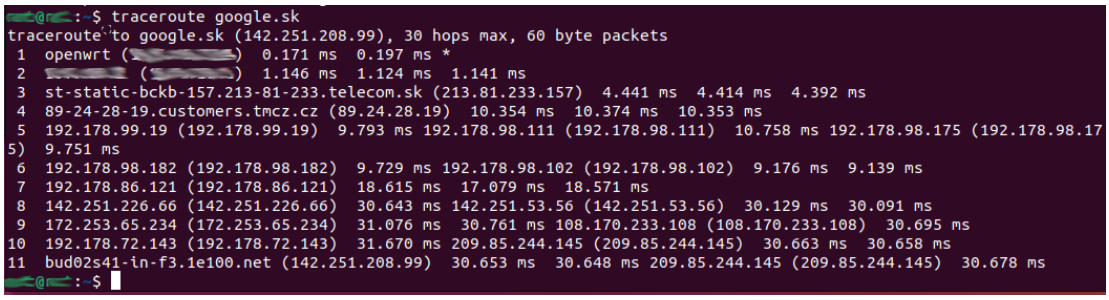
V tomto súbore *(etc/snort/builtin_rules/snort_defaults.lua)* sme upravili cesty tak, aby odkazovali na miesto, kde sme umiestnili komunitné pravidlá. Pravidlá sme nakopírovali cez SSH na zariadenie, umiestnili sme ich do predtým vytvoreného súboru a aktualizovali konfiguráciu, aby boli tieto pravidlá načítané pri štarte Snortu. Pri používaní komunitných pravidiel sme postupovali v súlade s licenčnými podmienkami Cisco Systems, Inc., ktoré sa

týkajú pravidiel Snort (Snort Subscriber Rules License Agreement, verzia 3.1). Toto zahŕňa dodržiavanie pravidiel na používanie, šírenie a úpravy pravidiel. Po umiestnení pravidiel do konfiguračného súboru sme vykonali reštart služby Snort a následnú kontrolu, či je služba správne spustená.

3.2 Analýza konfigurácie

Nástroj Traceroute je diagnostickým nástrojom určeným na sledovanie cesty paketov od zdroja k cieľu cez internetovú sieť. Po zadaní príkazu *traceroute google.sk*, bol zobrazený detailný zoznam sieťových uzlov a smerovačov, ktoré pakety prechádzali. Každý uzol predstavuje hop (skok), kde sa paket posunul bližšie k svojmu cieľu. Tento proces nejenže potvrdzuje funkčnosť smerovania v našej sieti, ale tiež identifikuje potenciálne úzke miesta, kde môže dôjsť k zbytočnému oneskoreniu alebo stratám paketov. Tieto informácie sú zásadné pre optimalizáciu výkonnosti siete a pre identifikáciu potreby zlepšení najmä väčších infraštruktúr.

[1]



Obrázok 22 – Práca s nástrojom tracerout, zdroj: Vlastné spracovanie

Pre overenie správnosti DNS konfigurácie a zabezpečenia sme využili nástroj dig s rozšírenými DNSSEC parametrami. Príkaz smeroval na adresu google.sk, pričom sme použili DNS server 1.1.1.1, známy svojou podporou DNSSEC. Výstup z tohto testu poskytol viacero kľúčových informácií:

- Status: NOERROR - Tento status potvrdzuje, že dotaz na DNS server bol úspešne spracovaný bez akýchkoľvek chýb.
- Query time: 7 ms - Rýchlosť odpovede bola mimoriadne nízka, čo ukazuje na efektivitu a rýchlu reakciu DNS servera.

[1] IP adresy sme zacenzurovali z dôvodu ochrany súkromia.

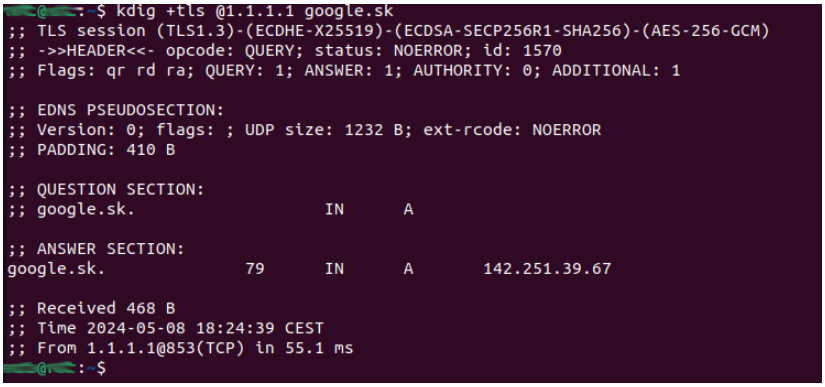
- Answer Section: Táto sekcia poskytla konkrétnu IP adresu spojenú s doménou, čo je kritické pre správne usmerňovanie internetovej komunikácie.

Aby sme zabezpečili, že DNSSEC je aktívne a správne konfigurované, funkčnosť sme preverili aj pomocou príkazu *dig +dnssec +multi @1.1.1.1*, hľadali sme špecifické bezpečnostné záznamy v odpovedi, ako sú RRSIG. Prítomnosť týchto záznamov potvrdila, že DNS dotazy a odpovede sú správne overené a chránené pred útokmi zneužívajúcimi slabiny v DNS protokole.

```
[redacted]: $ dig +dnssec +multi @1.1.1.1

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec +multi @1.1.1.1
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50219
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;.                      IN NS

;; ANSWER SECTION:
.                       517929 IN NS a.root-servers.net.
.                       517929 IN NS b.root-servers.net.
.                       517929 IN NS c.root-servers.net.
.                       517929 IN NS d.root-servers.net.
.                       517929 IN NS e.root-servers.net.
.                       517929 IN NS f.root-servers.net.
.                       517929 IN NS g.root-servers.net.
.                       517929 IN NS h.root-servers.net.
.                       517929 IN NS i.root-servers.net.
.                       517929 IN NS j.root-servers.net.
.                       517929 IN NS k.root-servers.net.
.                       517929 IN NS l.root-servers.net.
.                       517929 IN NS m.root-servers.net.
.                       517929 IN RRSIG NS 8 0 518400 (
                                20240521050000 20240508040000 5613 .
                                UgT0oq4mPBLAtCLWnNbVXTy8RCHWoXUt9mDwigiCa659
                                sr2Sy6ksHKYtI/T4wyrD4JfiZOvp/5fTnoTYfyAPOfsW
                                [redacted]3t6S27QYAQ+lMHX
                                j08Y55VTgk54fJVoFqx94Sf7/SZLPaeRRRqzhHw88pFA
                                bLnYdx/36eAWPo/vnBYA2pUeq9izeznjFW01nwFblHDV
                                +o8nMkHaUqR515okpwhwJ5RxBu+q2+dC2ButPsdDV8Uw
                                UFh94WbW6UpsXXrhkPpehEgk7RWimBH3Xpr/gM93lvJD
                                gfAJeODPqJPZawkTedM8EP4PWmWn328fgW== )

;; Query time: 8 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Wed May 08 18:47:20 CEST 2024
;; MSG SIZE  rcvd: 525
```

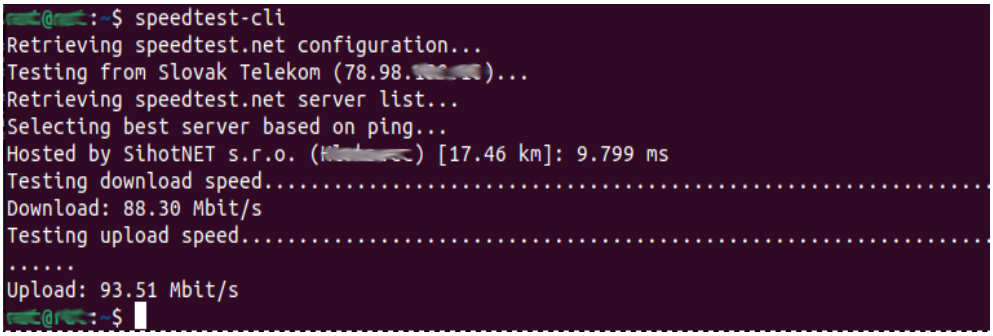
Obrázok 23 – Práca s nástrojom dig, zdroj: Vlastné spracovanie

DNS over TLS (DoT) je bezpečnostná vrstva, ktorá zaisťuje šifrovanie DNS dotazov a odpovedí, čím značne zvyšuje súkromie a bezpečnosť používateľov. Pomocou príkazu *kdig +tls @1.1.1.1 google.sk* sme overili, že náš DNS resolver *(1.1.1.1*) podporuje a správne implementuje TLS. Výsledky testu potvrdili, že komunikácia prebiehala cez šifrovaný kanál, čo je nevyhnutné pre ochranu pred potenciálnymi útočníkmi, ktorí by mohli odpočúvať alebo manipulovať s DNS dotazmi.



Obrázok 24 – Práca s nástrojom kdig, zdroj: Vlastné spracovanie

Dôležitým parametrom v oblasti sietí je aj testy rýchlosti internetového pripojenia, test sme vykonali pomocou nástroja *speedtest-cli*, ktorý poskytol kvantitatívne údaje o rýchlostiach uploadu a downloadu. Vysoké rýchlosti, sme konzistentne merali v rôznych časoch, ukazujú na stabilitu a spoľahlivosť poskytovaného internetového pripojenia. Tieto informácie sú neoceniteľné pre hodnotenie súčasného poskytovateľa internetových služieb a pre rozhodovanie o potenciálnych zlepšeniach sieťovej infraštruktúry.



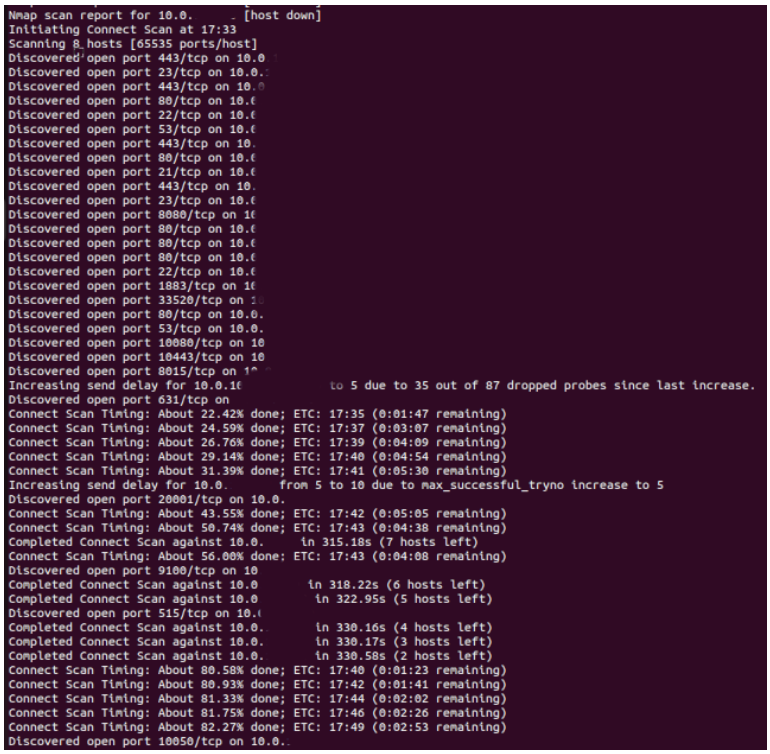
Obrázok 25 – Práca s nástrojom speedtest-cli, zdroj: Vlastné spracovanie

Detailné skenovanie IP adresy 127.0.0.111 pomocou nmap odhalilo niekoľko otvorených portov, ktoré sú esenciálne pre základné sieťové a internetové služby. Každý z týchto portov je dôležitý pre určité aplikácie a služby:

- Port 22/tcp (SSH): Základná služba pre bezpečný vzdialený prístup, vyžaduje prísne bezpečnostné protokoly a silné autentifikačné metódy.
- Port 53/tcp (DNS): Kritický pre spracovanie DNS dotazov, optimalizovaný pre rýchlu a bezpečnú odpoveď.

- Port 80/tcp (HTTP) a 443/tcp (HTTPS): Základné porty pre webové služby, pričom HTTPS zaručuje šifrovanie webového obsahu.
- Port 10050/tcp: Špecifický port používaný pre monitorovanie alebo špeciálne aplikácie, vyžaduje zvýšenú pozornosť z hľadiska bezpečnosti a prístupových práv.

Každý z týchto portov má kritický význam pre bezpečné a efektívne fungovanie siete, a preto je nevyhnutné ich pravidelne kontrolovať, napríklad prostredníctvom skenovania otvorených portov a zabezpečiť proti neoprávnenému prístupu alebo zneužitiu.



Obrázok 26 – Práca s nástrojom nmap, zdroj: Vlastné spracovanie

Následne sme pre otestovanie, či bude zariadenie správne pracovať v prípade systémovej záťaže vykonali aj kompletný sken rozsahu siete, kde sa nachádza naša LAN sieť.

Pre účely overenia funkčnosti CRON úloh, sme uskutočnili kontrolu zaznamenaných logov, konkrétne *security_scan.log*, aby sme zistili, či úlohy prebiehajú podľa očakávaní. Logy z nmap poskytujú detailné informácie o otvorených portoch a službách bežiacich na sieťových zariadeniach, čo je nevyhnutné pre identifikáciu potenciálnych bezpečnostných rizík.

Výsledky z logu *security_scan.log* ukázali, že skenovanie bolo úspešne vykonané a zaznamenané, čo dokazuje, že CRON úloha je správne nastavená a funguje podľa plánu. Na overenie a validáciu týchto výsledkov odporúčame pravidelné preskúmanie logových súborov a aktualizáciu bezpečnostných pravidiel v reakcii na zistené hrozby, ako sú neoprávnené otvorené porty alebo podozrivé sieťové aktivity.

Tento prístup zabezpečuje, že systémy a sieť sú neustále monitorované a chránené pred potenciálnymi útokmi, čo je zásadné pre zachovanie bezpečnosti a dôveryhodnosti infraštruktúry.

3.3 Porovnanie nástrojov a zariadení

V tejto kapitole porovnáme dostupné softvérové balíky s otvoreným a zatvoreným zdrojovým kódom. Naším cieľom je analyzovať ich flexibilitu a možnosti prispôsobitelnosti. Jedným z kľúčových aspektov vykonanej analýzy bolo zváženie výhod a nevýhod softvérov s otvoreným a zatvoreným zdrojovým kódom. V našom porovnaní sme taktiež zohľadnili dostupnosť technickej podpory a aktualizácií.

3.3.1 Pi-hole

Pi-hole je nástrojom určenným pre blokovanie reklám na webových stránkach, čo vedie k rýchlejšiemu načítaniu stránok a zlepšeniu užívateľského zážitku. Okrem toho, že zabraňuje nežiaducim reklamám, zabezpečuje aj súkromie užívateľov tým, že obmedzuje sledovacie cookies a prvky tretích strán, čo znižuje množstvo zhromažďovaných údajov. Pi-hole tiež poskytuje bezpečnostné funkcie, ako je blokovanie prístupu k známym škodlivým doménam, čo zvyšuje celkovú bezpečnosť siete. S funkciami ako nastavenie firewallu, VPN klienta a servera, správa DNS a DHCP serveru, riadenie prístupu a monitorovanie a správa siete, Pi-hole sa stáva kompletným nástrojom na správu a ochranu domácej siete[17].

Tento nástroj sme sa rozhodli následne otestovať, pri výbere distribúcie Linuxu sme sa rozhodli pre Ubuntu kvôli jeho širokej podpore a rozsiahlej používateľskej komunite. Ubuntu ponúka stabilný a intuitívny užívateľský zážitok, ideálny pre nasadenie v podnikových aj osobných prostrediach.

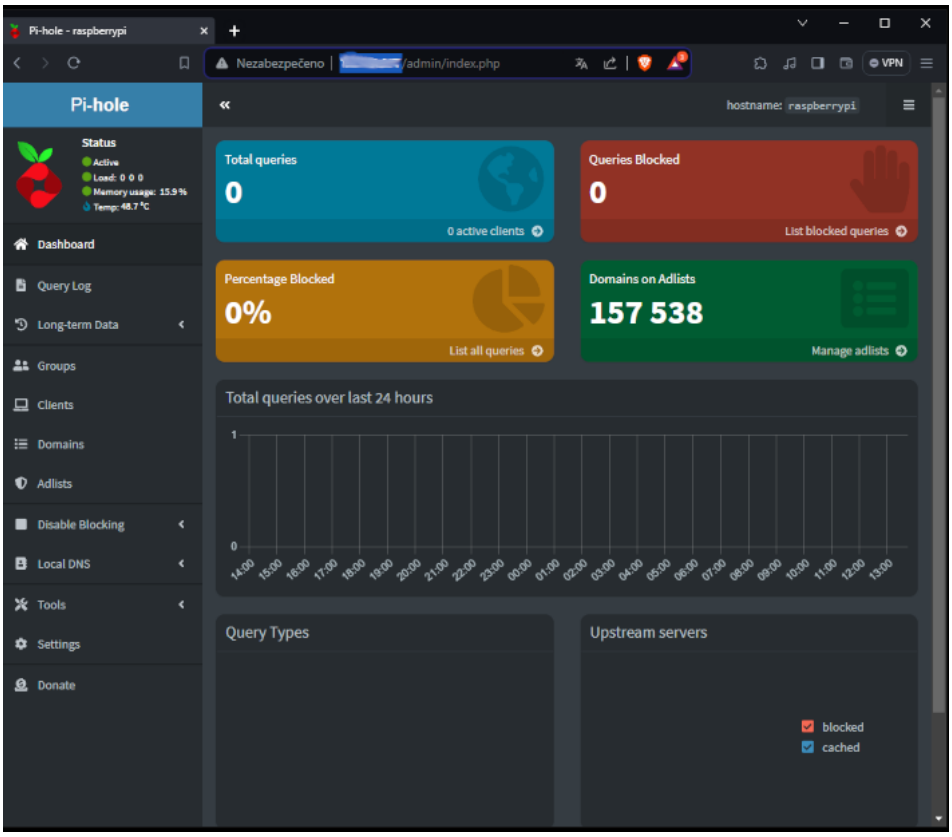
ISO súbor pre desktopovú verziu Ubuntu sme stiahli z oficiálnej webovej stránky. Tento súbor je digitálny obraz inštalačného média obsahujúci všetky potrebné súbory na inštaláciu operačného systému.

Na vytvorenie bootovateľnej USB jednotky sme využili nástroj Rufus, ktorý umožňuje jednoduché a rýchle vytvorenie inštalačného média z ISO súboru. Tento krok umožňuje inštaláciu operačného systému na cieľovom zariadení. Po vytvorení bootovateľnej USB jednotky sme USB vložili do cieľového zariadenia a reštartovali sme ho. Následne sme nastavili zariadenie tak, aby bootovanie prebiehalo z USB Počas inštalácie sme vykonali všetky potrebné nastavenia vrátane výberu jazyka, časovej zóny, diskových oddielov a ďalších relevantných konfigurácií.

Po úspešnom dokončení inštalácie sme reštartovali zariadenie, čím sme aktivovali novoinštalovaný operačný systém Ubuntu. Prvotná konfigurácia systému zahŕňala nastavenie používateľského účtu, prihlasovacieho hesla a sieťových parametrov.

Priamo v termináli sme stiahli inštalačný skript Pi-hole pomocou príkazu *curl -sSL https://install.pi-hole.net | bash*, čo nám umožnilo získať najnovšiu verziu softvéru. Inštalačný skript sme spustili pomocou príkazu *sudo bash basic-install.sh*, ktorý zahájil automatizovaný proces inštalácie vrátane počiatočného nastavenia a konfigurácie softvéru.

Počas inštalácie sme boli vyzvaní k základným nastaveniam, vrátane výberu jazyka a časovej zóny, ako aj k súhlasu s licenčnými podmienkami. Vybrali sme preferované DNS servery, ktoré Pi-hole používa na blokovanie reklám. Po dokončení všetkých nastavení inštalačný skript úspešne nainštaloval Pi-hole na naše zariadenie s Ubuntu. Tento proces nielenže zabezpečil funkčnosť systému, ale tiež optimalizoval naše prostredie pre zlepšenie bezpečnosti a výkonu siete.



Obrázok 27 – Rozhranie Pi-hole, zdroj: Vlastné spracovanie

3.3.2 pfSense

pfSense je operačný systém založený na FreeBSD, ktorý je zameraný na firewallové a routerové aplikácie. Poskytuje komplexné možnosti konfigurácie siete s dôrazom na bezpečnosť a výkonnosť. S podporou pre VLAN, bridging a trunking, pfSense umožňuje užívateľom vytvárať robustné a bezpečné siete. Implementácia VPN klienta a servera poskytuje bezpečné pripojenia k sieti cez internet. Pokročilé funkcie pre riadenie prenosu dát, ako sú QoS a Smart Queue Management, prispievajú k optimalizácii výkonu siete. Ďalšie schopnosti pfSense zahŕňajú konfiguráciu DNS a DHCP serverov, riadenie prístupu, podporu rozšírených sieťových techník ako združovanie WAN pre vyváženie zaťaženia a monitorovanie a správu sieťovej prevádzky, zariadení a zabezpečenia [18].

pfSense sme sa rozhodli vylúčiť z dôvodu jeho nedostupnosti pre zariadenia s ARM procesormi. Táto limitácia by nám znemožnila využiť Raspberry Pi 4. Nástroj pfSense spĺňa inak všetky požiadavky pre potrebnú konfiguráciu siete a je vhodný pre pokročilú konfiguráciu firewallov.

3.3.3 Komerčné riešenia

V tejto podkapitole sa zameriame na komerčné riešenia na správu sietí, ktoré ponúkajú pokročilé funkcie a spoľahlivé bezpečnostné možnosti pre podnikové prostredia.

Cisco Systems, je jedna z popredných spoločností v oblasti sieťovej infraštruktúry a bezpečnosti. Ponúka produkty ako Cisco ASA Firewall, ktorý integruje viaceré bezpečnostné funkcie vrátane stateful firewall, VPN, antivírusových nástrojov, antispamových riešení a Intrusion Prevention System (IPS). Cisco DNA Center je platforma pre centralizovanú správu siete, ktorá umožňuje automatizáciu, analýzu a zabezpečené pripojenie, čo zjednodušuje správu rozsiahlych sietí. Cisco je známe svojou vysokou spoľahlivosťou, silným zabezpečením a rozsiahlou zákazníckou podporou, čo ho robí ideálnym riešením pre komplexné podnikové prostredia.. Cisco Meraki poskytuje centralizovanú správu všetkých sieťových zariadení vrátane bezdrôtových prístupových bodov, prepínačov a bezpečnostných zariadení cez jednotné grafické rozhranie. Tento prístup významne znižuje komplexnosť správy a zabezpečuje konzistentnú politiku bezpečnosti naprieč celou organizáciou [19].

Palo Alto Networks sa vyznačuje poskytovaním komplexných bezpečnostných riešení, vrátane svojich Next-Generation Firewall, ktoré umožňujú podrobné sledovanie a kontrolu aplikácií, užívateľov a sieťového obsahu. Taktiež ponúka Endpoint Detection and Response (EDR), nástroj na detekciu a reakciu na bezpečnostné incidenty na koncových bodoch. Produkty od Palo Alto Networks sú vyhľadávané pre ich pokročilé analytické schopnosti a efektívnu prevenciu a manažment hrozieb, čo zabezpečuje vysokú úroveň ochrany dát a identifikáciu hrozieb [20].

Fortinet je ďalším významným poskytovateľom bezpečnostných riešení, ktorého produkty ako FortiGate poskytujú integrované bezpečnostné zariadenie s funkciami ako firewall, VPN, antivírus, IPS a web filtering. FortiManager umožňuje centralizovanú správu bezpečnostných politík a zjednodušuje administráciu viacerých zariadení FortiGate. Produkty Fortinet sú známe svojou vysokou škálovateľnosťou a prispôsobivosťou, čo ich robí vhodnými pre rôzne sieťové prostredia [21].

Juniper Networks ponúka širokú škálu sieťových zariadení, vrátane Juniper SRX Series, ktoré poskytujú komplexné bezpečnostné služby vrátane firewallu, VPN, IPS a ochrany proti hrozbám. Junos OS, robustný operačný systém, je základom pre všetky produkty Juniper a

ponúka pokročilé funkcie smerovania, bezpečnosti a správy siete. Výkonnosť a stabilita produktov Juniper ich robí vhodnými pre veľké podnikové a telekomunikačné siete [21].

Pri rozhodovaní o implementácii komerčných riešení je kľúčové zvážiť ich kompatibilitu s existujúcou sieťovou infraštruktúrou, náklady na počiatočnú investíciu a dlhodobú údržbu, ako aj špecifické bezpečnostné a výkonnostné požiadavky organizácie. Komerčné platformy často poskytujú rozsiahlu podporu a aktualizácie, ktoré môžu zlepšiť celkovú efektivitu a bezpečnosť sieťových operácií.

3.3.4 *Výsledok porovnania*

Po dôkladnom preskúmaní dostupných nástrojov a zariadení na správu siete, vrátane OpenWRT, Pi-hole a komerčných riešení od lídrov ako Cisco Systems, Palo Alto Networks, Fortinet a Juniper Networks, ako aj nízkonákladových alternatív, sme vyhodnotili rôzne aspekty ich výkonu, ceny, prispôsobiteľnosti a bezpečnosti. Pre ilustráciu porovnania sme vytvorili aj tabuľku, tvoriacu celkový prehľad.

Názov produktu	Zdrojový kód	Funkcie	Cena	Typické použitie
Pi-hole	Otvorený	Ad Blocking, DNS, Privacy Protection	Nízka	Domáce siete
pfSense	Otvorený	Firewall, VPN, DNS, DHCP, Advanced Routing	Nízka	Podnikové siete
OpenWRT	Otvorený	DNS, DHCP, Firewall, VPN, Advanced Routing	Nízka	Široké využitie
Cisco Systems	Zatvorený	VPN, Firewall, Intrusion Prevention, Advanced Routing	Vysoká	Podnikové siete
Palo Alto Networks	Zatvorený	Next-Gen Firewall, VPN, Threat Protection	Vysoká	Podnikové siete
Fortinet	Zatvorený	Firewall, VPN, Antivirus, Web Filtering	Vysoká	Podnikové a SME siete
Juniper Networks	Zatvorený	Firewall, VPN, Advanced Routing, Threat Protection	Vysoká	Veľké podnikové siete
MikroTik	Zatvorený	Firewall, VPN, Routing, QoS	Stredná	Malé a stredné podniky
Ubiquiti	Zatvorený	Firewall, VPN, Wireless AP Management	Stredná	Malé a stredné podniky
Zariadenia od poskytovateľov	Zatvorený	Basic Routing, Firewall, Parental Controls	Nízka	Domáce siete, malé firmy

Obrázok 28 – Porovnanie zariadení, zdroj: Vlastné spracovanie

OpenWRT nám ponúka vysokú mieru prispôsobiteľnosti a ovládateľnosti, umožňuje detailné nastavenie siete a prispôsobenie prostredníctvom modulárnej štruktúry a širokej škály softvérových balíčkov. Vďaka svojej otvorenej komunite a širokému základu podporovaných

zariadení, OpenWRT poskytuje veľmi nákladovo efektívne riešenie, ktoré je ideálne pre široké využitie, od malých domácich sietí až po pokročilé podnikové aplikácie.

V porovnaní s komerčnými riešeniami, ako zariadenia od Cisco a Palo Alto, ktoré sú známe svojou robustnosťou, rozsiahlymi bezpečnostnými funkciami a vysokou spoľahlivosťou, si OpenWRT vyžaduje viac technickej zručnosti pre správu a optimalizáciu. Komerčné produkty často prichádzajú s komplexnými analytickými nástrojmi a podporou, ktoré sú užitočné pre veľké organizácie, kde môže byť manažment bezpečnosti a sieťovej prevádzky oveľa náročnejší. Komerčné pokročilé riešenia od popredných poskytovateľov sieťovej infraštruktúry a bezpečnosti prinášajú významné výhody v oblasti efektivity, škálovateľnosti a bezpečnosti. Rozhodnutie o výbere konkrétneho produktu by malo vždy zohľadňovať špecifické potreby a požiadavky organizácie, ako aj kompatibilitu s existujúcimi systémami a zariadeniami.

Za zmienku stoja aj nízko nákladové komerčné riešenia, ako sú napríklad tie od spoločností ako MikroTik a Ubiquiti. Tieto produkty ponúkajú pomerne dobrý kompromis medzi cenou a výkonom, poskytujú základné funkcie správy siete a bezpečnosti vhodné pre malé a stredne veľké podniky. Ich konfiguračné rozhrania sú zvyčajne jednoduchšie na používanie ako OpenWRT a môžu ponúknuť stabilnejšie prostredie s menšou potrebou technickej údržby.

Poskytovatelia telekomunikačných služieb, ako sú Orange a telekomunikačné spoločnosti, obvykle ponúkajú riešenia, ktoré sú integrované s ich širšou ponukou produktov a služieb, vrátane internetového pripojenia, televízneho vysielania a mobilných služieb. Tieto riešenia sú zamerané predovšetkým na zabezpečenie stabilného, spoľahlivého pripojenia s minimálnou potrebou zásahu užívateľa. Sú ideálne pre bežných spotrebiteľov alebo malé firmy, ktoré hľadajú 'plug-and-play' riešenie bez nutnosti zložitejšej konfigurácie alebo technickej podpory.

Nízko nákladové riešenia môžu zahŕňať rôzne druhy bezpečnostných funkcií, ako sú firewally, rodičovská kontrola, čo ich robí vhodnými pre domáce prostredia. Avšak, v porovnaní s OpenWRT alebo dokonca nízko nákladovými komerčnými produktami ako MikroTik alebo Ubiquiti, často ponúkajú menej možností pre pokročilé nastavenie siete alebo špecifické bezpečnostné politiky.

Tieto riešenia sú efektívne pre štandardné použitie, môžu byť limitované v prípade potreby špeciálnych sieťových konfigurácií alebo pokročilejšej sieťovej správy, ktoré sú bežné v podnikových prostrediach. Pre organizácie s vysokými požiadavkami na sieťovú infraštruktúru a bezpečnosť, komerčné produkty od spoločností ako Cisco alebo Palo Alto alebo vysoko prispôsobiteľné riešenia ako OpenWRT môžu byť lepšou voľbou.

Ak porovnáme OpenWRT a Pi-hole, jedná sa o populárne nástroje používané na správu sieťových služieb, ale slúžia na mierne odlišné účely. Pi-hole je primárne softvér na blokovanie reklám na úrovni siete, ktorý funguje ako DNS sinkhole. Hoci je účinný pri blokovaní reklám, je menej flexibilný, pokiaľ ide o iné sieťové úlohy. OpenWRT je úplný Linuxový operačný systém pre embedded zariadenia, ako sú smerovače a firewally. Ponúka výrazne väčšiu flexibilitu a škálovateľnosť pre rôzne sieťové úlohy, vrátane, ale nielen, blokovania reklám, správy firewallu, VPN a pokročilého smerovania.

- Väčšia kontrola a prispôsobiteľnosť: OpenWRT nám poskytlo prístup k širšej škále sieťových nástrojov a konfiguračných možností, čo nám umožnilo prispôsobiť naše siete presne podľa našich potrieb.
- Pokročilé sieťové funkcie: Ako plný operačný systém podporuje OpenWRT pokročilé sieťové funkcie, ako sú Quality of Service (), dynamické smerovanie, pokročilé firewall pravidlá a podpora viacerých VPN protokolov.
- Široká podpora hardvéru a softvéru: OpenWRT je podporovaný na širokej škále hardvérových zariadení a ponúka bohatú zbierku balíčkov a nástrojov, ktoré je možné do systému ľahko integrovať.

Hoci Pi-hole je efektívnym nástrojom na blokovanie reklám a sledovacích prvkov v sieti, zistili sme, že OpenWRT ponúka rovnaké funkcionality s väčšou flexibilitou a možnosťami prispôsobenia. Pi-hole je primárne určený na blokovanie reklám a sledovacích prvkov prostredníctvom DNS záznamov, zatiaľ čo OpenWRT poskytuje komplexnejšie riešenie, ktoré zahŕňa aj funkcie ako firewall, VPN a ďalšie.

Pri porovnávaní prispôsobiteľnosti, OpenWRT jasne dominuje vďaka svojej otvorenej architektúre, ktorá umožňuje užívateľom upraviť takmer každý aspekt systému. Naopak, komerčné riešenia a nízko nákladové alternatívy obvykle ponúkajú menej možností prispôsobenia, zamerané viac na plug-and-play riešenia, ktoré zjednodušujú nasadenie a správu.

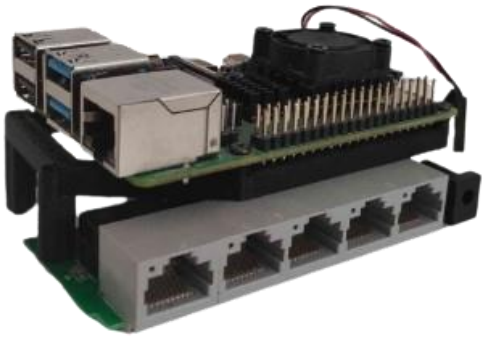
Z hľadiska nákladovej efektívnosti, OpenWRT a nízko nákladové riešenia sú atraktívne pre rozpočtovo obmedzené projekty, zatiaľ čo komerčné riešenia môžu predstavovať významné počiatočné investície a pravidelné náklady na licencie a podporu.

Po analýze a porovnaní všetkých uvažovaných možností sme sa rozhodli pokračovať s OpenWRT pre našu sieťovú infraštruktúru. Tento výber je motivovaný potrebou vysokého stupňa prispôsobiteľnosti a ovládateľnosti, ktoré OpenWRT poskytuje, ako aj jeho schopnosťou efektívne pracovať s existujúcim hardvérom, čo nám umožňuje optimalizovať naše náklady zároveň dosiahnuť požadovanú úroveň výkonu a bezpečnosti.

Vytvorené zariadenie

V rámci bakalárskej práce sme sa zamerali na integráciu a konfiguráciu viacerých hardvérových komponentov s cieľom vytvorenia efektívneho a multifunkčného zariadenia. Naším hlavným cieľom bolo spojiť Raspberry Pi 4 s sieťovým switchom TP-Link TL-SG1005D a USB adaptérom TP-Link UE-300, čím sme vytvorili kompaktný, ale výkonný systém.

Prvým krokom bolo fyzické spojenie Raspberry Pi 4 s TP-Link TL-SG1005D. Táto kombinácia nám umožnila rozšíriť sieťové možnosti Raspberry Pi, ktoré sú obmedzené na jediný Ethernetový port. Pripojením piatich gigabitových portov switcha sme získali možnosť pripojenia viacerých zariadení alebo rozšírenia sieťovej infraštruktúry.



Obrázok 29 – Tvorba zariadenia, zdroj: Vlastné spracovani

Následne sme pridali USB adaptér TP-Link UE-300, ktorý Raspberry Pi 4 poskytol drôtovú konektivitu. Adaptér sa osvedčil ako spoľahlivé riešenie pre stabilné pripojenie, čo je kritické pre naše aplikácie zahŕňajúce prenos dát a riadenie sieťových operácií.

Zariadenie sme umiestnili do púzdra, vytlačeného prostredníctvom 3D tlače, ktoré nielenže chráni elektroniku, ale tiež zabezpečuje estetický vzhľad a praktickosť v každodennom používaní. Puzdro poskytuje dostatočné vetranie pre chladenie komponentov a umožňuje ľahký prístup k portom pre rýchlu a efektívnu údržbu.

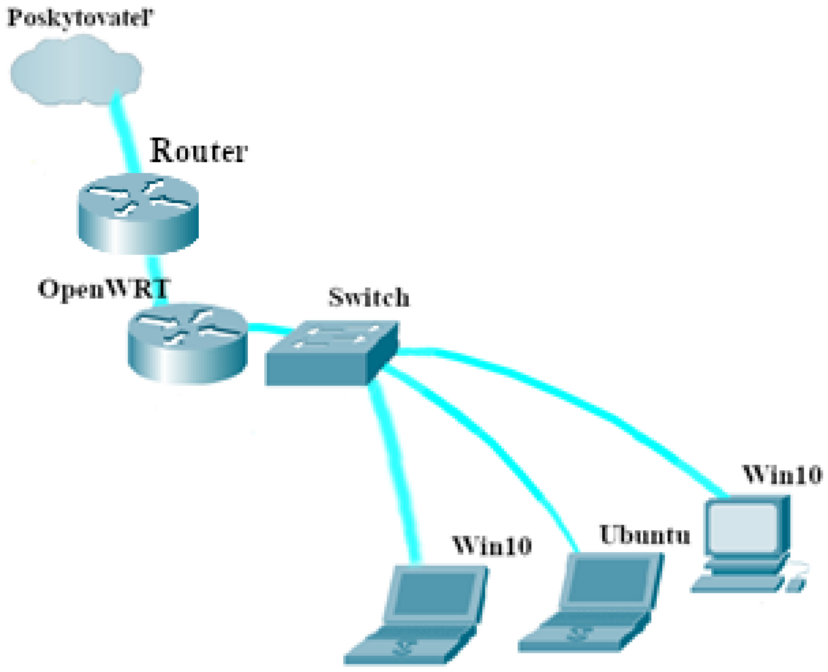
- Raspberry Pi 4 - Cena: 122,90 €. Pre komerčné zariadenie by bolo možné využiť aj menej výkonný mikropočítač, napríklad Raspberry Pi 3 za 42,90 €, keďže systém aj pri záťaži využíval maximálne 20% RAM a CPU záťaž sa tiež pohybovala v nízkych hodnotách.
- TP-Link UE300 - USB adaptér, ktorý poskytuje drôtovú konektivitu pre Raspberry Pi 4 - Cena: 16,90 €.
- TP-Link SG1005D - Sieťový switch s piatimi gigabitovými portami, ktorý rozširuje sieťové možnosti Raspberry Pi 4 - Cena: 15,90 €.
- Patch kábel - AlzaPower Patch CAT5E UTP 0,25 m - Cena: 2,39 €.

Obrázok 30 – Vytvorené zariadenie, zdroj: Vlastné spracovanie

Celková cena za zariadenie je 158,09 €. V prípade produkčného zariadenia by bolo možné sumu minimalizovať, napríklad presunutím výroby do inej krajiny, kde by vplyv na cenu mohol byť výrazný vďaka nižším výrobným nákladom a množstevným zľavám na komponenty. Pri výrobe aspoň 100 kusov zariadení a použitia Raspberry Pi3 by sa mohla cena pohybovať

v sume 53,41€. [2] Zariadenie sme navrhli ako fanless (bez ventilátora), čo je v súčasnosti veľmi populárne a žiadané kvôli jeho tichému chodu a nižším energetickým nárokom.

Na obrázku je zobrazené sieťové riešenie, ktoré sme vytvorili v rámci našej bakalárskej práce. Toto riešenie zahŕňa konfiguráciu OpenWRT smerovača, ktorý je pripojený k poskytovateľovi internetových služieb. Smerovač je ďalej pripojený k sieťovému switchu, čím sa rozširuje sieťová kapacita a umožňuje pripojenie viacerých koncových zariadení. Celkové riešenie je navrhnuté tak, aby poskytovalo stabilné a efektívne sieťové pripojenie pre všetky zariadenia, pričom zároveň demonštruje flexibilitu OpenWRT smerovača v prispôsobení na rozličné sieťové požiadavky. Táto schéma teda predstavuje vytvorené sieťové riešenie.



Obrázok 31 – Diagram siete, zdroj: Vlastné spracovanie

[2] Suma odhadnutá na základe cien zahraničných obchodov.

4 Diskusia

V prípade potreby komplexnejšej konfigurácie by bolo možné porovnávané technológie kombinovať, napríklad pomocou Dockeru, čo by nám poskytlo väčšiu flexibilitu a možnosť integrovať rôzne funkcionality do našej infraštruktúry, čo je obzvlášť vhodné pre väčšie a komplexnejšie siete, kde je potrebná granulárna kontrola a široká paleta funkcií na správu a zabezpečenie siete. Granulárna kontrola v prípade sietí znamená, že máme schopnosť presne definovať a nastaviť rôzne parametre a pravidlá pre jednotlivé časti sietí alebo pre jednotlivé používateľské zariadenia. Využitie Dockeru môže efektívne posilniť možnosti konfigurácie, pretože každý kontajner môže hostiť špecifickú službu alebo aplikáciu, pričom všetky môžu byť spravované centrálnym nástrojom ako Kubernetes. Táto platforma by umožnila dynamickú rekonfiguráciu siete a aplikácií podľa aktuálnych potrieb a záťaže, čím by sa zvýšila celková efektívnosť a pružnosť siete.

Možné inovácie, ktoré práca predstavuje, zahŕňajú vývoj vlastných nástrojov na správu a monitorovanie sieťových systémov, ktoré efektívne integrujú rôzne technológie do jednotného, ľahko spravovateľného riešenia. Zariadenie by mohlo byť tiež zlepšené použitím manažovaného switchu, ktorý by umožnil rozdelenie fyzických portov eth0 a eth1, a implementáciou DHCP lease alebo statických IP adries pre efektívnejšie pridelenie sieťových zdrojov a lepšiu kontrolu nad sieťovým prevádzkom.

Manažované switche ponúkajú pokročilé funkcie ako VLAN (Virtual Local Area Network), QoS (Quality of Service) a port mirroring, ktoré by nám umožnili detailnejšiu kontrolu a segmentáciu siete. Implementáciou VLAN môžeme efektívne oddeliť rôzne typy sieťovej prevádzky, čo zabezpečí vyššiu bezpečnosť a lepšiu výkonnosť siete. QoS zase zaisťuje prioritizáciu dátových tokov, čím sa zabezpečí, že kritické aplikácie majú dostatočné zdroje aj v čase vysokej sieťovej záťaže.

Implementáciou DHCP lease managementu alebo statických IP adries cez manažovaný switch alebo softvérové definície môžeme zlepšiť efektívnosť pridelenia IP adries a zároveň zabezpečiť vyššiu kontrolu nad sieťovými zariadeniami. Toto by umožnilo nielen lepšie sledovanie a reportovanie o využívaní siete, ale aj rýchlejšie odhaľovanie a riešenie problémov v sieti.

Záver

Sieťová infraštruktúra predstavuje základný kameň informačných systémov vo všetkých typoch organizácií a jej správna konfigurácia a správa sú kritické pre bezpečné a efektívne fungovanie celého IT prostredia. V oblasti sieťovej infraštruktúry sa v súčasnosti uplatňujú dva hlavné prístupy: použitie otvoreného zdrojového softvéru, ako je OpenWRT a komerčných produktov, ako sú riešenia od spoločností Cisco, Juniper Networks, a Fortinet FortiGate. Otvorené zdroje poskytujú vysokú flexibilitu a nízke náklady, ale môžu trpieť obmedzenou podporou a nižšou spoľahlivosťou v kritických aplikáciách. Komerčné produkty na druhej strane ponúkajú rozsiahle podporné služby, záruky a sú často certifikované pre použitie v regulovaných prostrediach, čo zabezpečuje vyššiu spoľahlivosť a bezpečnosť, ale za vyššiu cenu a menšiu flexibilitu.

V porovnaní s týmito štandardnými prístupmi, naše zariadenie pristupuje k problému s dôrazom na hybridné využitie obidvoch typov riešení, čím sa snažíme kombinovať flexibilitu a nízke náklady otvorených zdrojov s bezpečnosťou a spoľahlivosťou komerčných produktov. Tento prístup ponúka možnosť využiť výhody otvorených zdrojov pre menej kritické časti infraštruktúry pri súčasnom zabezpečení kľúčových funkcií prostredníctvom komerčných riešení a zníženie celkových nákladov na vlastníctvo pri zachovaní vysokého štandardu bezpečnosti, dostupnosti softvéru a podpory.

Medzi výzvy, s ktorými sme sa pri písaní bakalárskej práce stretli, patrí integrácia rôznych technológií a zabezpečenie, že všetky systémy spolupracujú bez problémov. Taktiež sa zaoberáme potenciálnymi bezpečnostnými rizikami, ktoré môžu vzniknúť pri kombinácii otvorených a komerčných riešení.

V porovnaní, otvorené zdrojové riešenia môžu vyžadovať viac vlastného vývoja pre dosiahnutie podobnej funkcionality, avšak ponúkajú vyššiu mieru prispôsobenia a môžu byť efektívnejšie z hľadiska nákladov v menej kritických aplikáciách. Vývoj vlastných nástrojov na správu hybridných systémov môže teda poskytnúť podobnú úroveň kontroly a efektivity ako komerčné produkty, ale s väčšou flexibilitou a potenciálne nižšími celkovými nákladmi. Vzhľadom na tieto faktory je kľúčové dôkladne zvážiť, kedy a kde aplikovať komerčné riešenia

a kedy sú vhodnejšie otvorené zdroje, a vytvoriť správne rozhodnutia na základe špecifických potrieb a bezpečnostných požiadaviek organizácie.

Vo vývoji a správe sieťových systémov je rovnako dôležité zohľadniť ľudský faktor. Správna implementácia technológií a nástrojov je jeden z faktorov ale bez adekvátnej úrovne odbornosti a tréningu zamestnancov, ktorí tieto systémy spravujú, sa môže zvýšiť riziko chýb a bezpečnostných incidentov.

Otvorené zdrojové riešenia často vyžadujú vyššiu technickú zručnosť a hlbšie porozumenie fungovania sieťových komponentov, pretože sú menej "užívateľsky priateľské" v porovnaní s komerčnými produktami, ktoré sú navrhnuté s dôrazom na intuitívnosť a ľahkú integráciu do existujúcich systémov. Komerčné riešenia zase často poskytujú rozsiahlejšie školenia a podporné služby, čo pomáha zabezpečiť, že zamestnanci sú dobre pripravení na riešenie bežných i výnimočných situácií.

Implementácia sieťových konfigurácií v skutočnom prostredí vyžaduje nielen technické schopnosti, ale aj schopnosť rýchlo reagovať na zmeny v sieťovom prostredí a efektívne riadiť bezpečnostné protokoly. Vývoj vlastných nástrojov na správu sieťových systémov by preto mal zahŕňať nielen technické aspekty, ale aj plán školenia a rozvoja kompetencií pracovníkov.

Takto integrovaný prístup, ktorý spája technologické a ľudské zdroje, maximalizuje výkonnosť a bezpečnosť sieťových systémov a zabezpečuje, že organizácia môže plne využívať svoje investície do infraštruktúry s minimalizovaným rizikom a optimalizovanými nákladmi.

V tejto bakalárskej práci sme demonštrovali schopnosť prístupu kombinovať flexibilitu otvoreného softvéru s robustnosťou komerčných riešení na zabezpečenie malej počítačovej siete. Stanovený cieľ bol dosiahnutý implementáciou Raspberry Pi s OpenWRT, čo nám umožnilo vytvoriť efektívne a nízko nákladové riešenie, ktoré bolo porovnateľné s komerčnými produktami v oblasti bezpečnosti a spoľahlivosti.

Zoznam použitej literatúry

[1] RASPBERRY, F. Buy A raspberry pi – raspberry pi. In *Raspberry Pi computers and microcontrollers* [online]. 2023. [cit. 2024-05-04]. Dostupné na internete: <https://www.raspberrypi.com/products/>.

[2] RASPBERRY, F. Operating system images – raspberry pi. In *Raspberry Pi OS* [online]. 2020. [cit. 2024-05-04]. Dostupné na internete: <https://www.raspberrypi.com/software/operating-systems/>.

[3] RASPBERRY, R. Buy A raspberry pi 4 model B – raspberry pi. In *Raspberry Pi 4* [online]. 2020. [cit. 2024-05-04]. Dostupné na internete: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/>.

[4] ALANI, M.M. OSI Model. In *Guide to OSI and TCP/IP Models* [online]. 1. vyd.[s.l.]: Springer Chams. 5–17. [cit. 2024-03-04]. Dostupné na internete: <https://link.springer.com/book/10.1007/978-3-319-05152-9>.

[5] CLOUDFLARE What is the OSI model? | cloudflare. In *What is the OSI Model?* [online]. 2023. [cit. 2024-05-04]. Dostupné na internete: <https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>.

[6] ALANI, M.M. TCP/IP Model. In *Guide to OSI and TCP/IP Models* [online]. 1. vyd.[s.l.]: Springer Cham, 2014. s. 19–50. [cit. 2024-03-04]. Dostupné na internete: <https://link.springer.com/book/10.1007/978-3-319-05152-9>.

[7] CLOUDFLARE What is SSH? | secure shell (SSH) protocol. In *What is the Secure Shell (SSH) protocol?* [online]. 2022. [cit. 2024-03-11]. Dostupné na internete: <https://www.cloudflare.com/learning/access-management/what-is-ssh>.

[8] VARMARKEN, J. - LE, H. - SHUBA, A. - MARKOPOULOU, A. - SHAFIQ, Z. The TV is smart and full of trackers: Measuring Smart TV advertising and tracking. In *Proceedings on Privacy Enhancing Technologies* . 2020. Vol. 2020, no. 2, s. 129–154. .

[9] SANDERS, C. Packet analysis and network basics. In *Practical packet analysis* . 2. vyd.San Francisco, USA: No starch press, 2011. s. 1–16. .

[10] ALBITZ, P. - LIU, C. How Does DNS Work? In *DNS and BIND* . 4. vyd.[s.l.]: O'Reilly Media, Inc, 2001. s. 11–34. .

[11] HOFFMAN, P. - MCMANUS, P. DNS queries over HTTPS (DOH). In *DNS Queries over HTTPS (DoH)* . 2018. s. 3–20. .

[12] DICKINSON, S.S. - GILLMOR, D.A. - REDDY, T.M. Usage profiles for DNS over TLS and DNS over DTLS. In *Usage Profiles for DNS over TLS and DNS over DTLS* . 2018. s. 4–21. .

[13] ALBITZ, P. - LIU, C. DNS and Internet Firewalls. In *DNS and BIND* . 5. vyd.[s.l.]: O'Reilly Media, Inc, 2001. s. 300–319. .

[14] SCARFONE, K.A. - HOFFMAN, P. Guidelines on firewalls and firewall policy. In *Recommendations of the National Institute of Standards and Technology* . 2009. no. Special Publication 800-41, s. 2–12. .

[15] OPENWRT - 532910 Firewall configuration /etc/config/firewal. In *[OpenWrt Wiki]* [online]. 2023. [cit. 2024-04-05]. Dostupné na internete: <https://openwrt.org/docs/guide-user/firewall/firewall_configuration>.

[16] OPENWRT - FLYGARN12 Network configuration. In *[OpenWrt Wiki]* [online]. 2024. [cit. 2024-05-01]. Dostupné na internete: <https://openwrt.org/docs/guide-user/network/network_configuration>.

[17] PI-HOLE Pi-hole documentation. In *Overview* [online]. 2022. [cit. 2024-03-04]. Dostupné na internete: <https://docs.pi-hole.net/>.

[18] PFSENSE Configuration. In *Configuration | pfSense Documentation* [online]. 2023. [cit. 2024-05-04]. Dostupné na internete: <https://docs.netgate.com/pfsense/en/latest/config/>.

[19] Products, solutions, and services. In *Cisco* [online]. 2024. [cit. 2024-05-04]. Dostupné na internete: <https://www.cisco.com/c/en_my/products/index.html#~services>.

[20] AI-Powered Next Generation Hardware Firewall. In Palo Alto Networks [online]. 2024. [cit. 2024-05-08]. Dostupné na internete: <https://www.paloaltonetworks.com/network-security/hardware-firewall-innovations>.

[21] SEGEC, P. - MORAVCIK, M. - KONTSEK, M. - PAPAN, J. - URAMOVA, J. - YEREMENKO, O. Network virtualization tools – analysis and application in Higher Education. In *2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA)* . 2019. .