Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Systém jednotné správy hrozeb pro malé a střední podniky založený na Raspberry Pi

Ladislav Topoľský

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Ladislav Topoľský

Informatika

Název práce

Systém jednotné správy hrozeb pro malé a střední podniky založený na Raspberry Pi

Název anglicky

Raspberry Pi-Based Unified Threat Management System for Small to Medium-sized Enterprises

---

Cíle práce

Cílem této práce je navrhnout, implementovat a vyhodnotit systém jednotné správy hrozeb využívající počítač Raspberry Pi, který integruje různé bezpečnostní funkce, včetně detekce narušení, prevence narušení, VPN, firewallu a DNS sinkhole. Systém bude přizpůsoben požadavkům a omezením malých a středních podniků a nabídne flexibilní a cenově dostupné bezpečnostní řešení.

Dílčí cíle:
- Definice systémů jednotné správy hrozeb(UTM) a jeho význam a principy systému v zabezpečení sítě.
- Průzkum a představení stávajících technologií a řešení systémů jednotné správy hrozeb.
- Návrh architektury systému výběrem konkrétní hardwarové a softwarové komponenty pro systém.
- Instalace softwarové časti a konfigurace jednotlivých častí bezpečnostní vrstvy systému
- Provést komplexní testování systému a prezentovaní a vyhodnocení výsledku

Metodika

V teoretické fázi bude představen základní koncept jednotné správy hrozeb (UTM) a její význam pro bezpečnost sítě. Budou probrány různé technologie běžně používané v systémech UTM, jako je detekce narušení, prevence narušení, VPN, firewall a DNS sinkhole. Budou určeny konkrétní typy technologií vybrané pro praktické experimenty, které tvoří jádro praktické fáze.

V praktické fázi této práce bude komplexně zdokumentováno nasazení a provoz systému UTM na bázi počítače Raspberry Pi. Půjde o použití vybraných technologií, včetně Suricata, Snortu, OpenVPN, iptables a Pi-hole, se zaměřením na jejich konfiguraci a nastavení.

Součástí práce budou navíc konfigurace a kód vytvořené během praktické fáze. Tato dokumentace bude navržena tak, aby byla přístupná a referenční a sloužila jako zdroj pro pochopení a reprodukci výsledků dosažených během experimentu.

Doporučený rozsah práce

50-60 stran

Klíčová slova

Jednodeskové počítače, Linux, DNS Sinkhole, Zabezpečení sítě, Detekce narušení sítě, Prevence narušení sítě, Firewall, Systém jednotné správy hrozeb

---

Doporučené zdroje informací

Bace, R. (1999). Intrusion Detection 1st Edition. Carmel: Sams Publishing. ISBN 1578701856.

Karen Scarfone, P. M. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology Special Publication 800-94.

Ruixi Yuan, W. T. (2001). Virtual Private Networks: Technologies and Solutions 1st Edition. Addison-Wesley Professional. ISBN 0201702096.

Szor, P. (2005). The Art of Computer Virus Research and Defense. Boston: Addison-Wesley Professional. ISBN 9780321304544.

Tittel, E. (2016). Unified Threat Management For Dummies®, 2nd Fortinet Special Edition. Hoboken, New Jersey: John Wiley & Sons, Inc. ISBN 978-1-119-30299-5

Vacca, J. (2004). Firewalls: Jumpstart for Network and Systems Administrators 1st Edition. ISBN 1555582974

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 2. 4. 2024

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 4. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 03. 04. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Systém jednotné správy hrozeb pro malé a střední podniky založený na Raspberry Pi" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 5.4.2024 _____

Poděkování

Rád(a) bych touto cestou poděkoval panu doktorovi Píckovi za vedení diplomové práce.

Systém jednotné správy hrozeb pro malé a střední podniky založený na Raspberry Pi

Abstrakt

Tato práce se zabývá problematikou zabezpečení sítě v prostředí malých a středních firem prostřednictvím systému jednotné správy hrozeb na platformě jednodeskových počítačů. Jako hardwarové zařízení bylo zvoleno Raspberry Pi 4 B 8 GB. Jako základ softvérového řešení byl zvolen operační systém Ubuntu Server 22.04 LTS. Architektura komponent systému jednotné správy hrozeb zahrnovala DNS Sinkhole – Pi-Hole, virtuální privátní sít (VPN) – Pi-VPN, systém pro rozšířenou detekci a reakci (XDR) a správu bezpečnostních informací a událostí (SIEM) – Wazuh a firewall – UFW. Práce dále zahrnovala testování dílčích celků systému a následné vyhodnocení výsledků.

Klíčová slova: Jednodeskové počítače, Linux, DNS Sinkhole, Zabezpečení sítě, Detekce narušení sítě, Prevence narušení sítě, Firewall, Systém jednotné správy hrozeb, VPN

Raspberry Pi-Based Unified Threat Management System for Small to Medium-sized Enterprises

Abstract

This thesis examines the challenges of network security in a small and medium-sized business environments through a unified threat management system on a single board computer platform. Raspberry Pi 4 B 8 GB was chosen as the hardware device. The Ubuntu Server 22.04 LTS operating system was chosen as the basis of the software solution. The architecture of the Unified Threat Management System components included a DNS Sinkhole - Pi-Hole, a Virtual Private Network (VPN) - Pi-VPN, an Enhanced Detection and Response (XDR) and Security Information and Event Management (SIEM) system - Wazuh, and a firewall - UFW. The work also included testing of the system sub-assemblies and subsequent evaluation of the results.

Keywords: Single-board computers, Linux, DNS Sinkhole, Network Security, Network Intrusion Detection, Network Intrusion Prevention, Firewall, Unified Threat Management System, VPN

Obsah

1 Úvod

V současném digitálním věku je zabezpečení síťových systémů prvořadé, zejména pro malé a střední podniky, které často nemají prostředky na sofistikovanou bezpečnostní infrastrukturu. Šíření kybernetických hrozeb vyžaduje robustní a komplexní bezpečnostní řešení, která dokáží ochránit síťové systémy před nesčetnými zranitelnostmi. Systémy jednotné správy hrozeb se v této souvislosti jeví jako klíčové řešení, které nabízí integrovanou bezpečnostní infrastrukturu schopnou řešit více bezpečnostních potřeb současně. Složitost a cena tradičních systémů UTM je však často činí nedostupnými pro malé a střední podniky. Cílem této práce je překlenout tuto mezeru návrhem, implementací a vyhodnocením nákladově efektivního a flexibilního systému UTM malých a středních podniků s využitím kompaktního, ale výkonného počítače Raspberry Pi. Práce využívá praktický přístup a zaměřuje se na praktickou implementaci a hodnocení navrhovaného systému UTM. Budou zkoumány klíčové technologie běžně používané v systémech UTM, jako je detekce/prevence narušení, VPN, firewall a DNS sinkhole. V praktické fázi bude zdokumentováno nasazení a provoz systému UTM založeného na Raspberry Pi. V této fázi budou hrát zásadní roli technologie jako systému pro rozšířenou detekci a reakci (XDR) a správu bezpečnostních informací a událostí (SIEM), Pi-VPN, UFW a Pi-hole, přičemž důraz bude kladen na jejich konfiguraci, nastavení a integraci tak, aby tvořily ucelený a efektivní systém UTM.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je navrhnout, implementovat a zhodnotit systém jednotné správy hrozeb s využitím počítače Raspberry Pi jako základního hardwaru. Tento systém by měl zahrnovat komplexní sadu bezpečnostních funkcí, včetně detekce a prevence narušení, VPN, firewallu a funkcí DNS sinkhole v prostředí malých a středních podniků. Cílem je poskytnout těmto subjektům bezpečnostní řešení, které je nejen flexibilní a robustní, ale také nákladově efektivní, a řešit tak běžný problém omezených zdrojů a technických znalostí, s nímž se malé a střední podniky v oblasti kybernetické bezpečnosti často potýkají.

2.2 Metodika

Metodika této práce je rozdělena na dva základní segmenty: teoretický výklad a praktickou implementaci. Toto rozdělení zajišťuje komplexní přístup, který kombinuje hluboké pochopení teoretických základů s praktickými empirickými poznatky.

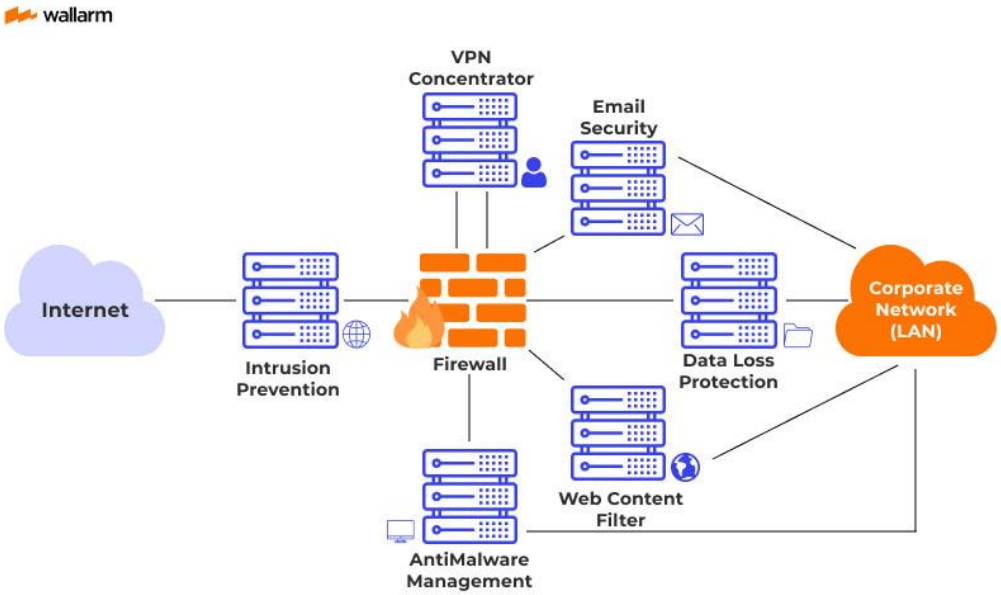
Teoretický základ této práce je vytvořen na základě přehledu literatury, jehož cílem je objasnit základní principy a současný stav systémů jednotné správy hrozeb. To zahrnuje analýzu odborných článků a případových studií s cílem rozebrat funkčnost, význam a problémy integrace komponent UTM, konkrétně v kontextu malých a středních podniků. Přehled literatury zkoumá nejen dynamiku technologií detekce a prevence narušení, VPN, firewallu a DNS sinkhole, ale zabývá se také pochopením jedinečných výzev spojených s využitím jednodeskových počítačů v oblasti IT infrastruktury, se zvláštním důrazem na model Raspberry Pi.

V praktické fázi práce přechází od teorie k aplikaci a zaměřuje se na návrh, konfiguraci a vyhodnocení systému UTM založeného na Raspberry Pi. Proces začíná pečlivým výběrem a integrací hardwarových a softwarových komponent, přičemž je zajištěna kompatibilita a optimalizace výkonu. Následně je použita postupná konfigurace a režim testování, aby bylo zajištěno, že každá komponenta – od systémů detekce narušení, až po funkce firewallu a DNS sinkhole fungují.

3 Teoretická východiska

3.1 Jednotná správa hrozeb (UTM)

Jednotná správa hrozeb (UTM) představuje zásadní posun ve vývoji technologií a zařízení pro zabezpečení sítě, neboť zahrnuje širokou škálu důležitých funkcí zabezpečení sítě, přístupu a připojení do jediného centrálně spravovaného zařízení. Řešení UTM spojují základní bezpečnostní funkce, jako jsou síťové firewally provádějící stavovou kontrolu paketů, systémy prevence narušení (IPS) detekující a zabraňující narušení a některým útokům, kontrola aplikací pro přehled a regulaci chování a obsahu aplikací, VPN pro bezpečný vzdálený přístup k síti a filtrování webu pro blokování přístupu ke škodlivému, nevhodnému nebo pochybnému online obsahu. Usnadňují také podporu protokolu IPv6 ve všech funkcích zabezpečení sítě, zabezpečují sítě při přechodu z protokolu IPv4 na IPv6 a podporují virtualizovaná prostředí včetně virtuálních domén i virtuálních zařízení.



Obrázek 1Diagram UTM (1)

Řešení UTM navíc rozšiřují své bezpečnostní a síťové technologie o prevenci ztráty dat, antimalwarovou/antispamovou ochranu, kontrolu koncových bodů, technologii sandboxing, integrovaný řadič bezdrátových sítí LAN (WLAN), integrované porty kabelových přepínačů a integrovanou optimalizaci rozsáhlých sítí WAN. Tyto funkce společně zabraňují náhodné nebo úmyslné ztrátě citlivých dat, blokují průnik škodlivých dat nebo nežádoucích zpráv do sítě, vynucují firemní bezpečnostní zásady u vzdálených uživatelů a zařízení, nabízejí další vrstvu ochrany proti malwaru spouštěním podezřelých

souborů ve virtuálním prostředí a zjednodušují vytváření a vynucování zásad při současném snížení složitosti sítě.

UTM se vyznačuje flexibilitou, připraveností na budoucnost a výkonem. Poskytuje univerzální řešení přizpůsobitelné jedinečným a měnícím se požadavkům moderních organizací a vyvíjejícímu se prostředí hrozeb. Zařízení UTM jsou navržena tak, aby zůstala relevantní a výkonná i do budoucna, což zajišťuje, že se mohou přizpůsobovat změnám funkcí a síťového prostředí, aniž by se stala úzkým hrdlem sítě. Tato přizpůsobivost spolu se zvýšeným povědomím a kontrolou nad bezpečnostními otázkami a potenciálními problémy souvisejícími se síťovým provozem, chováním uživatelů a obsahem aplikací staví UTM do pozice robustní a nedílné součásti moderních strategií zabezpečení sítě. (2)

3.2 Komponenty UTM

3.2.1 Firewall

Firewall je systém zabezpečení sítě, který řídí tok příchozího a odchozího síťového provozu na základě použité sady pravidel. Vytváří bariéru mezi důvěryhodnou, zabezpečenou vnitřní sítí a jinou vnější sítí, například internetem, u které se předpokládá, že není bezpečná nebo důvěryhodná. Firewally mohou být implementovány jak hardwarově, tak softwarově nebo kombinací obojího a často se používají k zabránění přístupu neoprávněných uživatelů internetu do soukromých sítí připojených k internetu, zejména intranetu. Hlavním cílem brány firewall je filtrovat provoz a blokovat škodlivou komunikaci a datové pakety a zároveň umožnit průchod legitimnímu provozu. (3)

Brána firewall kontroluje každý datový paket, který prochází do sítě a ze sítě. Datový paket ve struktuře pro internetovou komunikaci se skládá z:

- Obsah datového toku (vlastní obsah zprávy).
- Záhlaví (podrobnosti o datech, včetně informací o odesílateli a příjemci).

Firewall provádí důkladnou analýzu těchto paketů na základě předem definovaných kritérií a rozlišuje bezpečný provoz od škodlivého. Tato kritéria zahrnují pokyny, které brána firewall vyhodnocuje:

- IP adresy odesílatele a příjemce.
- Obsah v užitečném zatížení.
- typ použitých protokolů paketů (například použití protokolu TCP/IP).
- specifické aplikační protokoly (například HTTP, Telnet, FTP, DNS, SSH a další).

- Specifické datové vzory, které naznačují kybernetické hrozby.

Po kontrole brána firewall prosazuje přísné zásady, blokuje všechny pakety, které neodpovídají stanoveným pravidlům, a povolené pakety bezpečně směruje k jejich cíli. Při setkání s provozem, který porušuje pravidla, má brána firewall dvě možnosti reakce:

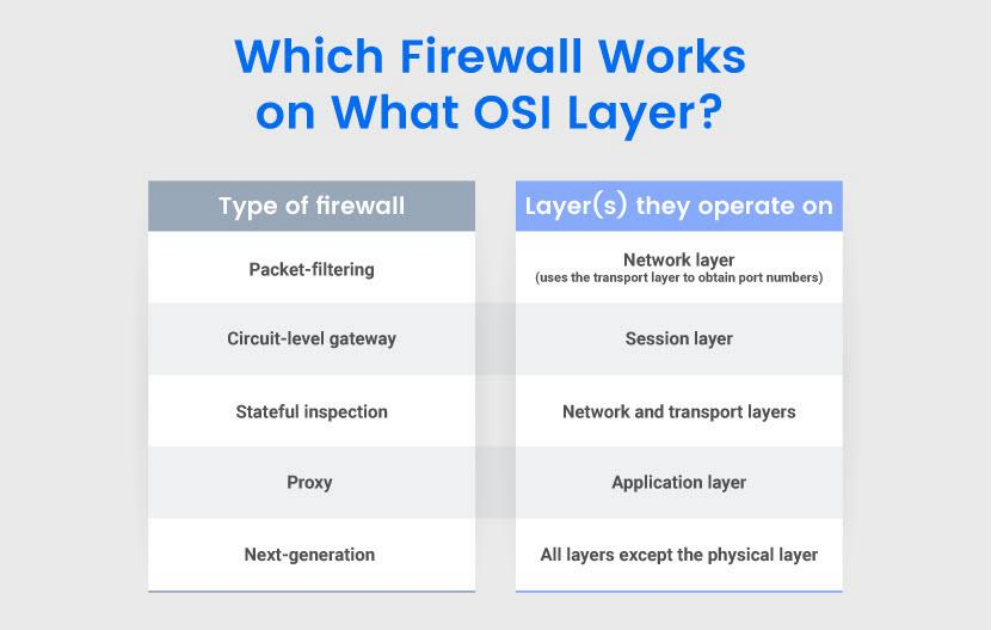
- Požadavek v tichosti zamítne.
- Odesílateli zašlete chybovou odpověď.

3.2.1.1 Typy firewallů podle způsobu doručení

- **Softwarové brány firewall** jsou nainstalovány na jednotlivých zařízeních, nabízejí podrobnou kontrolu, ale spotřebovávají systémové prostředky. Poskytují vynikající ochranu pro jednotlivé počítače, ale vyžadují rozsáhlou konfiguraci a údržbu.
- **Hardwarové brány firewall** jako samostatná zařízení chrání více systémů, aniž by zatěžovaly jejich zdroje, což je ideální pro větší sítě. Nabízejí robustní ochranu perimetru, ale jsou nákladnější a vyžadují kvalifikovanou správu.
- **Cloudové brány firewall**, poskytované jako služba, poskytují škálovatelnou a flexibilní ochranu spravovanou poskytovateli služeb, vhodnou pro distribuované společnosti. Eliminují potřebu hardwaru, ale vyvolávají obavy ohledně latence, transparentnosti a dlouhodobých nákladů.

3.2.1.2 Typy firewallů podle způsobu činnosti

Na obrázku 2 jsou firewally podle své funkce a vrstvy OSI, na které pracují. Každý z nich můžete nasadit jako hardware, software nebo v cloudu.



Obrázek 2 Rozdělení firewallu podle způsobu činnosti (1)

- **Firewally s filtrováním paketů:** Pracují na síťové vrstvě a posuzují hlavičky paketů podle předem definovaných pravidel, přičemž se zaměřují na IP adresy, typy paketů a protokoly. Jsou ideální pro základní zabezpečení, jsou cenově výhodné, ale postrádají kontrolu datového obsahu a jsou zranitelné vůči sofistikovaným útokům.
- **Brány na úrovni okruhu:** Tyto brány, které fungují na relační vrstvě, ověřují handshake protokolu TCP a efektivně řídí provoz bez kontroly obsahu paketů. Jsou jednoduché a nenáročné na zdroje, poskytují základní zabezpečení, ale postrádají funkce filtrování obsahu a nemohou být samostatným řešením.
- **Firewally se stavovou kontrolou:** spravují příchozí i odchozí pakety na síťové a transportní vrstvě. Udržují databázovou tabulku sledující stavy připojení a ukládají důležité informace o paketech, jako jsou zdrojové/cílové IP adresy a porty. To jim umožňuje rychle rozpoznávat a zpracovávat známé pakety a zároveň důsledně kontrolovat nový nebo neznámý datový přenos, což výrazně zvyšuje zabezpečení sítě. Nabízejí vyšší zabezpečení díky zohlednění předchozího provozu, ale vzhledem ke své složitosti mohou ovlivnit výkon sítě.
- **Proxy brány firewall:** Proxy firewally pracují na aplikační vrstvě a nabízejí hloubkovou kontrolu paketů, přičemž analyzují jak hlavičky, tak užitečné datové obsahy. Přidávají další vrstvu zabezpečení maskováním klientských požadavků, což

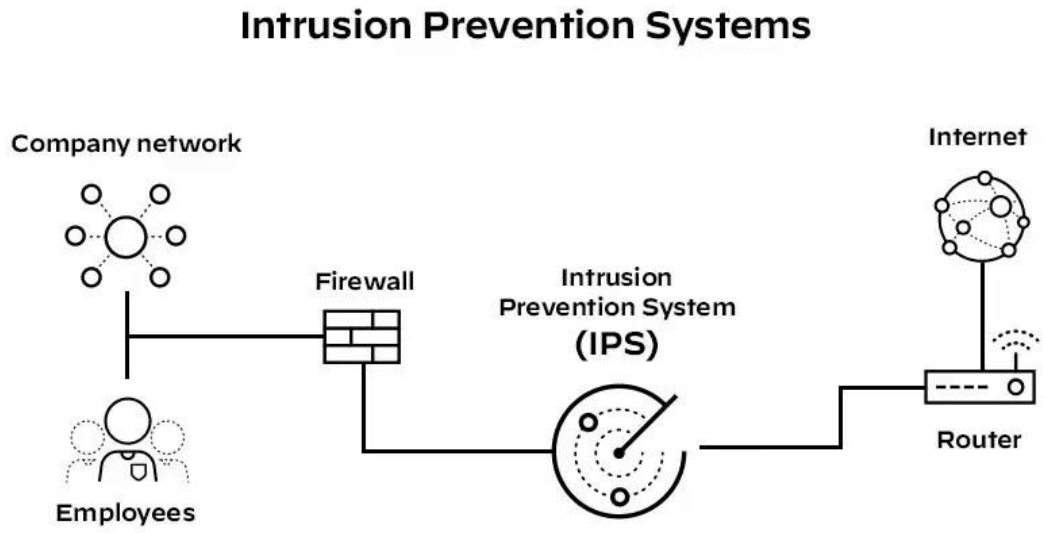
je ideální pro ochranu webových aplikací a zajištění anonymity sítě, ale může to zvýšit latenci.

- **Firewally nové generace:** NGFW integrují funkce tradičních firewallů s pokročilými bezpečnostními funkcemi a kontrolují provoz na více vrstvách OSI. Poskytují komplexní ochranu s dalšími funkcemi, jako je IDS/IPS a filtrování malwaru, ale jsou složitější a nákladnější. (4) (5)

3.2.2 Systém detekce narušení a systém prevence narušení (IDS/IDPS)

Systém detekce narušení a systém prevence narušení (IDS/IPS) je bezpečnostní řešení, které monitoruje síťové a systémové aktivity a hledá škodlivé aktivity nebo porušení pravidel. Jakákoli zjištěná aktivita nebo porušení jsou obvykle hlášeny buď správci, nebo shromažďovány centrálně pomocí systému správy bezpečnostních informací a událostí (SIEM). IPS má schopnost nejen odhalit potenciálně škodlivou činnost, ale také přijmout preventivní opatření k zastavení činnosti nebo zmírnění jejího dopadu.

IPS a IDS jsou nedílnými součástmi zabezpečení sítě a obě se zaměřují na detekci hrozeb prostřednictvím analýzy síťového provozu. Jejich společným rysem je detekce hrozeb pomocí známých signatur útoků nebo neobvyklého chování a zaznamenávání aktivit pro analýzu. Jejich provozní role a dopad na síť se však liší. IPS aktivně filtruje a spravuje síťový provoz na základě stanovených pravidel, je umístěn přímo v komunikačním toku sítě a okamžitě řeší nebo zmírňuje hrozby. Tento proaktivní postoj může přinést zpoždění při zpracování, což může mít vliv na propustnost sítě. Naproti tomu IDS slouží jako monitorovací systém, který kontroluje síťový provoz, aniž by jej upravoval. Funguje tak, že upozorňuje bezpečnostní týmy na potenciální hrozby a umožňuje jim přijmout následná opatření. Protože je IDS pasivním pozorovatelem, nezpůsobuje v síti zpoždění výkonu. Zpočátku mohou organizace nasadit IDS, aby pochopily a zaznamenaly chování systému. Jakmile je systém dobře nakonfigurován tak, aby přesně identifikoval skutečné hrozby, přechod na IPS nebo jeho integrace zajistí robustnější, aktivní obranný mechanismus. (6)



Obrázek 3 Schéma umístnění IPS na síti (7)

K identifikaci potenciálních bezpečnostních hrozeb se používají tři základní metody detekce:

- **Detekce na základě signatur:** Tato metoda se opírá o komplexní databázi známých signatur hrozeb. Kontroluje síťový provoz podle těchto signatur a identifikuje známé škodlivé aktivity. Detekce je dvojího typu:
    - **Signatury zaměřené na zneužití:** Ty se zaměřují na konkrétní pokusy o zneužití tím, že porovnávají síťovou aktivitu s jedinečným vzorem známého zneužití.
    - **Signatury zaměřené na zranitelnost:** Tyto signatury jsou širší a zaměřují se na zranitelnosti, které mohou zneužití využít, a nabízejí ochranu před řadou neidentifikovaných hrozeb, ale potenciálně zvyšují míru falešně pozitivních výsledků.
- **Detekce založená na anomáliích:** Tato technika zahrnuje stanovení základní úrovně normálního chování sítě a následné sledování síťového provozu z hlediska odchylek od této normy. Jakákoli významná odchylka spustí systém k akci, což umožňuje odhalit dosud neznámé nebo vznikající hrozby.
- **Detekce založená na směrnicích:** Tato metoda vyžaduje, aby správci definovali bezpečnostní zásady přizpůsobené síťové infrastruktuře organizace. Systém nepřetržitě monitoruje síťové aktivity a jakákoli akce porušující tyto předem

definované bezpečnostní zásady spustí výstrahu, která správcům umožní problém okamžitě řešit. (7)

Typy útoků, kterým systémy prevence narušení zabraňují

Systémy prevence narušení jsou určeny k odhalování různých typů útoků na bezpečnost sítě a k jejich prevenci. Mezi běžné útoky, kterým IPS pomáhají předcházet, patří:

- **Útoky hrubou silou:** Tyto útoky spočívají v tom, že se útočník pokouší získat neoprávněný přístup do systému vyzkoušením několika kombinací uživatelských jmen a hesel.
- **Útoky typu DDoS:** Útoky DDoS zahrnují více zdrojových dat, která zahlcují cílový systém provozem, což ztěžuje zmírnění útoku.
- **Zneužití zranitelností:** IPS dokáže odhalit a zabránit útokům, které využívají známé zranitelnosti softwarových systémů k získání kontroly nad systémem.
- **Červi:** Červi jsou samoreplikující se škodlivý software, který se může šířit po síti a způsobovat škody a narušení. IPS může pomoci odhalit a zablokovat šíření červů.
- **Viry:** IPS může také pomoci odhalit a zabránit šíření virů, což jsou škodlivé programy, které mohou infikovat a poškodit systémy.
- **Nezabezpečené protokoly:** IPS může prosazovat bezpečné protokoly a odmítat používání nezabezpečených protokolů, jako jsou starší verze protokolu SSL nebo protokoly používající slabé šifry.
- **Odstraňování škodlivého obsahu:** IPS může po útoku pomoci odstranit nebo nahradit veškerý zbývající škodlivý obsah v síti, například opětovným zabalením užitečných souborů, odstraněním informací z hlaviček a odstraněním infikovaných příloh ze souborových nebo e-mailových serverů.
- **Zneužití zero-day:** Zero-day exploity se zaměřují na zranitelnosti, které ještě nejsou známé nebo pro které nebyla vydána záplata. I když IPS nemusí být schopen odhalit a zabránit všem zero-day exploitům, může poskytnout další vrstvu ochrany blokováním provozu, který vykazuje podezřelé chování nebo odpovídá známým vzorcům útoků. (6)

Řešení IDPS se dělí na různé typy podle metody detekce, kterou používají:

- **Síťové (NIDS/NIPS):** Sleduje celou síť a analyzuje podezřelý provoz pomocí aktivity protokolů.

- **Hostitelské (HIDS/HIPS):** Instaluje se na jednotlivé hostitele a monitoruje pouze příchozí a odchozí pakety ze zařízení, čímž nabízí podrobnější přehled o aktivitách daného hostitele.
- **Detekce založená na signaturách:** Používá konkrétně známé vzory neoprávněného chování k předvídání a detekci následných podobných pokusů.
- **Detekce založená na anomáliích:** Používá strojové učení k definování základní linie běžných činností a poté sleduje odchylky od této základní linie.
- **Detekce založená na chování:** Vyhledává odchylky v chování, jako je neobvyklá doba přihlášení nebo nadměrné čtení databáze, které mohou naznačovat škodlivou činnost.

Mezi hlavní funkce IDPS patří monitorování, detekce a reakce na hrozby. To zahrnuje zaznamenávání informací týkajících se pozorovaných událostí, upozorňování správců zabezpečení na důležité pozorované události a vytváření zpráv. Mnoho IDPS je také schopno reagovat na zjištěnou hrozbu tím, že se jí pokusí zabránit v úspěchu. Používají různé techniky reakce, které zahrnují zastavení samotného útoku, změnu bezpečnostního prostředí (např. rekonfiguraci brány firewall) nebo změnu obsahu útoku. (8) (9)

3.2.3 Virtuální privátní síť (VPN)

Virtuální privátní síť je služba, která vytváří zabezpečené šifrované připojení přes méně zabezpečenou síť, například veřejný internet. Hlavním účelem sítě VPN je zajistit soukromí a bezpečnost datového provozu vytvořením chráněného síťového připojení při používání veřejných sítí. Sítě VPN maskují adresu internetového protokolu (IP), takže online akce jsou prakticky nevystopovatelné. Vytvořením zabezpečeného tunelu pro přenos dat zajišťují sítě VPN bezpečný přenos citlivých dat, zabraňují odposlouchávání provozu neoprávněnými osobami a umožňují uživateli vykonávat práci na dálku. Technologie VPN se hojně využívá ve firemním prostředí.

Virtuální privátní síť (VPN) funguje v podstatě jako kanál mezi zařízením uživatele a širším internetem a zajišťuje bezpečný a soukromý přístup. Mezi hlavní součásti fungování VPN patří servery VPN, šifrování dat, tunelování VPN a používání různých protokolů VPN.

- **Servery VPN:** Tyto servery fungují jako zabezpečené brány a směrují internetový provoz uživatele chráněnou trasou. Po připojení k serveru VPN je veškerý provoz

uživatele (příchozí i odchozí) veden přes šifrovaný tunel, který účinně chrání data před vnějšími hrozbami. Každý server je spojen s jedinečnou IP adresou, často v jiné zeměpisné poloze, což uživatelům umožňuje maskovat jejich skutečné IP adresy a tvářit se, jako by přistupovali k internetu z místa, kde se nachází server.

- **Šifrování dat:** VPN využívají robustní techniky šifrování, které převádějí obyčejná data do nečitelného formátu (šifrový text) pomocí digitálních klíčů a složitých algoritmů. K tomuto šifrování dochází v okamžiku, kdy data vstupují do tunelu VPN, a zůstává v platnosti, dokud nedorazí na server VPN, kde jsou dešifrována. Tento proces zajišťuje, že jakákoli zachycená data jsou pro neoprávněné subjekty nerozluštitelná.
- **Tunelování VPN:** Tento proces spočívá ve vytvoření bezpečného šifrovaného průchodu pro data mezi zařízením uživatele a serverem VPN. Je základem funkcí zabezpečení a ochrany soukromí sítě VPN a zajišťuje, že data zůstanou během přenosu důvěrná a nedotknutelná.
- **Protokoly sítě VPN:** Protokoly jsou pravidla a metody, které definují specifika přenosu dat prostřednictvím tunelu VPN. Různé protokoly splňují různé potřeby týkající se rychlosti, zabezpečení a kompatibility. Mezi běžné protokoly patří OpenVPN, IPSec, SSTP, L2TP a WireGuard. Každý z nich má své výhody a nevýhody, takže si uživatelé mohou vybrat podle svých specifických požadavků na rychlost, úroveň zabezpečení nebo kompatibilitu zařízení.

Služby VPN lze rozdělit do tří hlavních typů, z nichž každý je přizpůsoben konkrétním síťovým potřebám:

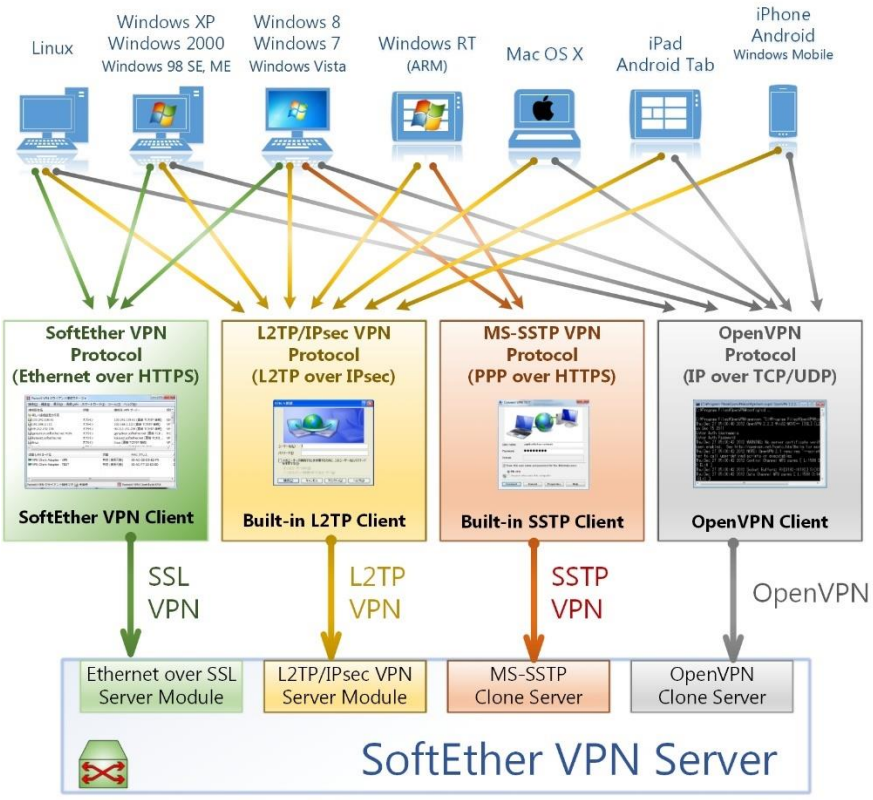
- **Vzdálený přístup:** Tento typ VPN je ideální pro jednotlivé uživatele nebo dálkové pracovníky, kteří se potřebují bezpečně připojit k síti své organizace ze vzdáleného místa. V podstatě vytváří zabezpečený tunel ze zařízení uživatele do podnikové sítě, který umožňuje přístup k interním zdrojům, jako by byly na místě, a zajišťuje důvěrnost a integritu dat při práci na dálku.
- **Site-to-Site VPN:** Sítě VPN typu site-to-site, které často využívají organizace s více kancelářemi, vytvářejí bezpečné a šifrované spojení mezi oddělenými sítěmi v různých zeměpisných oblastech. Toto nastavení usnadňuje bezpečnou a bezproblémovou komunikaci mezi kancelářemi a zajišťuje, že data přenášená napříč

sítěmi zůstanou soukromá a nepřístupná cizím osobám, a efektivně propojuje vzdálené pobočky, jako by byly ve stejné místní síti.

- **Privátní VPN:** Soukromé sítě VPN jsou určeny pro individuální použití a zaměřují se na zvýšení soukromí a bezpečnosti na internetu. Uživatelé obvykle používají tyto sítě VPN k ochraně svých internetových aktivit před sledováním, k přístupu k obsahu s geografickým omezením nebo k zajištění anonymity online. (10)

  Existuje několik funkcí sítí VPN:

  - **Vzdálený přístup:** VPN umožňují uživatelům vzdálené připojení k firemní síti, což z nich činí důležitou technologii pro vzdálené pracovníky a vzdálené kanceláře.
  - **Anonymita:** VPN pomáhají skrývat IP adresu uživatele a zachovávají tak jeho anonymitu online, což třetím stranám ztěžuje sledování online aktivit nebo krádeže dat.
  - **Obcházení geografických omezení:** VPN lze použít k obcházení zeměpisných omezení webových stránek a streamovacích služeb.

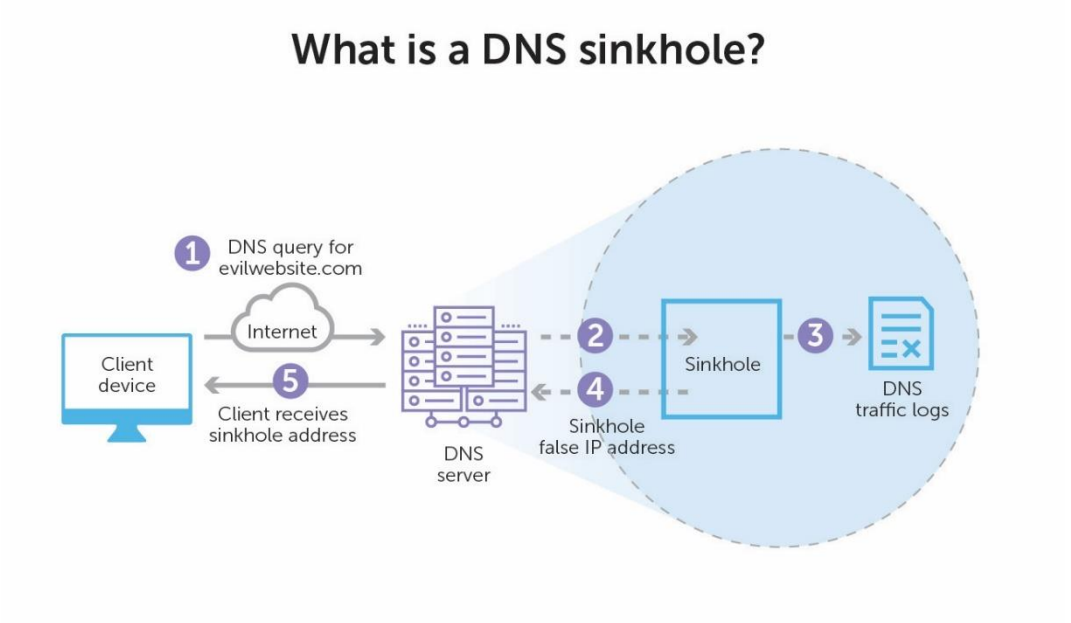


Obrázek 4 Schéma připojení zabezpečených protokolů sítě VPN (11)

Mezi zabezpečené protokoly VPN patří mimo jiné protokol IPsec (Internet Protocol Security), protokol SSL/TLS (Transport Layer Security) a protokol SSTP (Microsoft Secure Socket Tunneling Protocol), které jsou navrženy tak, aby splňovaly bezpečnostní cíle dostupnosti, integrity a důvěrnosti. Jsou široce používány v osobním i obchodním kontextu k ochraně citlivých informací a zajištění bezpečné komunikace přes potenciálně nezabezpečené sítě. (12) (11)

3.2.4 DNS Sinkhole (Filtrování webu)

DNS sinkhole, známý také jako sinkhole server nebo blackhole DNS, je mechanismus zabezpečení sítě, který slouží k zabránění připojení zařízení v síti ke škodlivým nebo nežádoucím doménám. Funguje tak, že poskytuje nesprávné informace DNS pro zadaná doménová jména a účinně přesměrovává provoz od potenciálních hrozeb na bezpečnou IP adresu, často na server kontrolovaný správci sítě nebo odborníky na zabezpečení.



Obrázek 5 Diagram fungování systému DNS sinkhole (13)

Hlavní funkcí technologie DNS sinkhole je ochrana sítí zachycením provozu určeného pro škodlivé weby a jeho přesměrováním na server, který není škodlivý, čímž se zabrání šíření malwaru, phishingovým útokům nebo jiným kybernetickým hrozbám. To je obzvláště účinné proti botnetům nebo serverům C2 (command-and-control), protože může narušit komunikační kanály, na kterých tyto hrozby závisí.

Kromě ochrany proti hrozbám lze propady DNS využít také k prosazování síťových zásad blokováním přístupu k obsahu, který není v souladu se směrnicemi organizace,

například k platformám sociálních médií nebo jiným stránkám nesouvisejícím s prací. Správci sítě mohou sledováním pokusů o přístup k těmto přesměrovaným adresám identifikovat infikované hostitele ve své síti a získat tak cenné informace pro další bezpečnostní opatření. (14) (13)

3.2.5 Anti-virus a Anti-malware

Antivirový a antimalwarový software jsou bezpečnostní programy určené k detekci, prevenci a odstranění škodlivého softwaru, tzv. malwaru, z počítačových systémů. Antivirový software se primárně zaměřuje na prevenci, detekci a odstraňování virů, červů a trojských koní, zatímco antimalwarový software nabízí širší škálu ochrany proti širšímu spektru typů škodlivého softwaru, včetně spywaru, adwaru, ransomwaru a dalších. Tato bezpečnostní řešení fungují na základě databáze známých signatur malwaru a metod heuristické analýzy, které identifikují podezřelé chování nebo vzory souborů a poskytují ochranu v reálném čase před novými hrozbami. (15)

3.2.6 Ochrana před ztrátou dat (DLP)

Ochrana před ztrátou dat (DLP) je soubor nástrojů a postupů, který je součástí celkové bezpečnostní strategie společnosti a zaměřuje se na odhalování a prevenci ztráty, úniku nebo zneužití dat v důsledku narušení, exfiltrace přenosů a neoprávněného použití. Existují tři typy DLP.

3.2.6.1 Síťový DLP

Síťový DLP se zaměřuje na monitorování a analýzu síťové aktivity organizace, a to jak v tradičních sítích, tak v cloudu. Bedlivě sleduje e-maily, zprávy a přenosy souborů a aktivně vyhledává případy, kdy jsou citlivá nebo důvěrná data přenášena v rozporu se zásadami zabezpečení informací organizace. Síťový DLP vytváří komplexní databázi, která zaznamenává nejen to, kdo přistupuje k citlivým datům, ale také sleduje, kam se tato data v síti přesouvají. Tento typ DLP poskytuje týmu zabezpečení informací úplný přehled o všech datech, ať už jsou v provozu, v pohybu nebo v klidu.

3.2.6.2 DLP koncových bodů

Při DLP koncových bodů jde o zabezpečení všech možných koncových bodů, kde se data nacházejí nebo jsou využívána. To zahrnuje servery, cloudová úložiště, počítače, notebooky,

mobilní telefony a jakákoli další zařízení. Hlavním cílem je zabránit úniku, ztrátě nebo zneužití dat. Technologie DLP pro koncové body pomáhá klasifikovat typy dat, čímž pomáhá zjednodušit vykazování a požadavky na dodržování předpisů. Neomezuje se pouze na zařízení připojená k síti, protože sleduje data na koncových bodech v síti i mimo ni, čímž zajišťuje ochranu citlivých informací bez ohledu na to, kde se nacházejí.

3.2.6.3 Cloudový DLP

Cloudový DLP je přizpůsoben organizacím, které se při ukládání dat spoléhají na cloudová úložiště. Tento typ řešení DLP skenuje a kontroluje data v cloudu a automaticky detekuje a šifruje citlivé informace před jejich uložením v cloudovém prostředí. Cloudový DLP udržuje seznam autorizovaných cloudových aplikací a uživatelů a při zjištění porušení zásad nebo anomálních aktivit vydává varování. Uchovává také protokol všech přístupů k důvěrným datům v cloudu, čímž vytváří komplexní přehled o datech uložených v cloudu a poskytuje robustní bezpečnostní opatření pro organizace závislé na cloudu. (16)

3.2.7 Systém pro rozšířenou detekci a reakci (XDR) a správu bezpečnostních informací a událostí (SIEM)

Rozšířená detekce a reakce (XDR) je komplexní řešení kybernetické bezpečnosti, které kombinuje více bezpečnostních technologií a zdrojů dat a poskytuje rozšířené možnosti detekce hrozeb, reakce na ně a nápravy. XDR jde nad rámec tradičních řešení detekce a reakce na koncové body (EDR) a zahrnuje další bezpečnostní telemetrická data z různých zdrojů, jako je síťový provoz, cloudová prostředí a další koncové body.

Správa bezpečnostních informací a událostí (SIEM) je řešení kybernetické bezpečnosti, které pomáhá organizacím shromažďovat, analyzovat a korelovat data o bezpečnostních událostech z různých zdrojů napříč IT infrastrukturou. Systémy SIEM poskytují funkce monitorování v reálném čase, detekce hrozeb, reakce na incidenty a monitorování dodržování předpisů. (17)

Wazuh je komplexní open source bezpečnostní platforma, která integruje funkce XDR i SIEM. Tím, že nabízí jednotné řešení pro detekci hrozeb, reakci na incidenty, hlášení o dodržování předpisů a monitorování v reálném čase, řeší Wazuh problémy se složitostí a škálovatelností, kterým čelí moderní frameworky kybernetické bezpečnosti. (18)

3.2.7.1 Architektura systému Wazuh

Wazuh využívá víceúrovňovou architekturu navrženou tak, aby poskytovala efektivní analýzu dat v reálném čase z různých zdrojů, včetně koncových bodů, cloudových služeb a sítí. Jádro architektury Wazuh tvoří tři základní součásti: agenta Wazuh, server Wazuh a řídicí panel Wazuh.

- **Agent Wazuh:** Tito agenti jsou nasazeni na koncových bodech a jsou zodpovědní za sběr dat, včetně systémových protokolů, konfiguračních souborů a síťových metadat. Hrají klíčovou roli při monitorování integrity, odhalování narušení a identifikaci anomálií.
- **Wazuh Server:** Serverová komponenta provádí analýzu dat shromážděných agenty. Používá logiku založenou na pravidlech k identifikaci potenciálních hrozeb a generuje výstrahy pro další vyšetřování. Server také slouží jako centrální úložiště pro ukládání dat, což usnadňuje komplexní analýzu hrozeb a incidentů.
- **Wazuh Dashboard:** Dashboard Wazuh nabízí pro vizualizaci a správu uživatelsky přívětivé rozhraní, které poskytuje přehled o stavu zabezpečení organizace v reálném čase. Umožňuje správcům zobrazovat výstrahy, spravovat nastavení konfigurace a provádět podrobné analýzy bezpečnostních incidentů. (19)

3.2.7.2 Součásti a funkce systému Wazuh

Wazuh zahrnuje širokou škálu funkcí zaměřených na posílení bezpečnostního rámce organizace. Tyto funkce lze rozdělit do 4 hlavních skupin:

- **Detekce a řešení hrozeb:** Pomocí pokročilé analýzy a mechanismů detekce založených na signaturách Wazuh účinně identifikuje známé i nově vznikající hrozby. Jeho schopnosti reakce jsou navrženy tak, aby automaticky reagovaly na hrozby na základě předem definovaných pravidel a minimalizovaly tak příležitost pro útočníky.
- **Monitorování souladu s předpisy:** Wazuh pomáhá organizacím dodržovat různé regulační požadavky tím, že nepřetržitě monitoruje konfigurace a změny systému a podává o nich zprávy, čímž zajišťuje soulad se standardy, jako jsou PCI DSS, GDPR a HIPAA.
- **Posuzování rizik:** Díky průběžnému vyhodnocování zranitelností a zranitelných míst poskytuje Wazuh cenné informace o bezpečnostních rizikách přítomných v

digitální infrastruktuře organizace. Tento proaktivní přístup umožňuje včasné úsilí o nápravu a zvyšuje celkovou odolnost zabezpečení.

- **Správa protokolů a analýza dat:** Robustní funkce platformy pro správu protokolů umožňují agregaci, analýzu a ukládání velkých objemů dat protokolů. To nejen podporuje úsilí o zabezpečení a dodržování předpisů, ale také poskytuje základ pro pokročilou analýzu dat a forenzní analýzu. (18)

3.3 Výhody UTM

Mezi výhody systému jednotné správy hrozeb patří:

- **Jednoduchost ovládání:** UTM zjednodušuje správu zabezpečení IT tím, že poskytuje řešení "vše v jednom" od jediného dodavatele. Odpadá tak složité řešení s více softwary a dodavateli, což usnadňuje sledování a efektivní správu bezpečnostních rizik. Jeho centralizovaná povaha zjednodušuje úkol zajistit komplexní zabezpečení sítě.
- **Cenově výhodné:** Malé a střední podniky s omezeným rozpočtem považují UTM za nákladově efektivní bezpečnostní řešení. Zefektivňuje správu zabezpečení, čímž snižuje potřebu různých produktů a dodavatelů. Tato konsolidace minimalizuje výdaje, protože není nutné kupovat různá bezpečnostní řešení, což vede k dlouhodobým úsporám nákladů.
- **Rychlá reakční doba:** Systémy UTM umožňují organizacím rychle reagovat na narušení bezpečnosti. Provozování jediného, všezahrnujícího systému je jednodušší ve srovnání s oddělenou správou více systémů. Tato agilita umožňuje správcům IT pohotově zmírnit škody způsobené bezpečnostními incidenty, což zvyšuje bezpečnost sítě a dobu odezvy.
- **Snadné škálování:** UTM konsoliduje různá bezpečnostní řešení pod jednu střechu. V případě potřeby aktualizací nebo upgradů je lze snadno implementovat, aniž by bylo ohroženo bezpečnostní pokrytí. Toto snadné škálování zajišťuje, že se organizace může efektivně přizpůsobovat vyvíjejícím se bezpečnostním potřebám, což může být u jednotlivých bezpečnostních řešení náročné.
- **Nízké náklady na údržbu:** Systémy UTM jsou známé svými nízkými náklady na zavedení a nižšími režijními náklady na zdroje. Ve srovnání se samostatnou správou více bezpečnostních systémů spotřebovávají méně prostředků na straně klienta i

serveru. To se časem projeví ve významných úsporách nákladů, protože není třeba často investovat do dalšího hardwaru nebo vyměňovat zařízení. Díky této nákladové efektivitě je UTM atraktivní volbou pro malé podniky s omezenými zdroji, protože poskytuje konsolidovaná a účinná bezpečnostní řešení. (20)

3.4 Nevýhody UTM

Mezi nevýhody systému jednotné správy hrozeb patří:

- **Jediný bod selhání:** V některých ohledech může být použití jediného zařízení pro všechny bezpečnostní potřeby výhodné, ale je to také jedna z největších slabin UTM. Funguje jako jediný bod selhání. Každý, kdo chce zničit vaši síť, se musí zaměřit pouze na UTM.
- **Výkonnostní problémy:** Pokud musí zařízení UTM zpracovávat velké množství aplikací nebo klientů, může to vést ke snížení výkonu vaší sítě.
- **Závislost na jediném poskytovateli:** Mnoho organizací nepovažuje používání UTM za nejlepší přístup k zabezpečení sítě, protože se můžete stát závislými na jediném dodavateli. Nejlepším přístupem je používat bezpečnostní nástroje od více dodavatelů, takže i když koncové body produktu jednoho dodavatele nedokážou detekovat bezpečnostní hrozbu, druhý produkt tak může učinit. (21)

3.5 Frameworky a modely ke klasifikaci a pochopení hrozeb

V systémech jednotné správy hrozeb (UTM) je kategorizace internetových bezpečnostních hrozeb klíčová pro efektivní identifikaci, správu a zmírňování hrozeb. Pro systematickou klasifikaci a pochopení těchto hrozeb se používá několik frameworků a modelů. Zde jsou uvedeny některé z významných rámců používaných pro kategorizaci internetových bezpečnostních hrozeb v systémech UTM.

3.5.1 Cyber Kill Chain (Kybernetický řetězec zabíjení)

Kybernetický řetězec zabíjení je řada kroků, které sledují fáze kybernetického útoku od počátečních fází průzkumu až po exfiltraci dat. Tento řetězec nám pomáhá porozumět ransomwaru, narušení bezpečnosti a pokročilým trvalým útokům (APT) a bojovat proti nim. Společnost Lockheed Martin odvodila framework kill chain z vojenského modelu – původně byl vytvořen pro identifikaci, přípravu na útok, napadení a zničení cíle. Od svého vzniku se

kill chain vyvinul tak, aby lépe předvídal a rozpoznával vnitřní hrozby, sociální inženýrství, pokročilý ransomware a inovativní útoky.

Každá fáze souvisí s určitým typem činnosti při kybernetickém útoku, bez ohledu na to, zda se jedná o interní nebo externí útok:

1. **Průzkum:** Fáze pozorování: útočníci obvykle hodnotí situaci zvenčí dovnitř, aby určili cíle i taktiku útoku.
2. **Vniknutí:** Na základě toho, co útočníci zjistili ve fázi průzkumu, se dostanou do vašich systémů: často využívají malware nebo bezpečnostní zranitelnosti.
3. **Využití:** Akt zneužití zranitelností a dodání škodlivého kódu do systému s cílem získat lepší pozici.
4. **Zvýšení oprávnění:** Útočníci často potřebují větší oprávnění v systému, aby získali přístup k více datům a oprávněním: k tomu potřebují eskalovat svá oprávnění často na úroveň správce.
5. **Boční pohyb:** Jakmile se útočníci dostanou do systému, mohou se bočně přesunout do jiných systémů a účtů, aby získali větší vliv: ať už jde o vyšší oprávnění, více dat nebo větší přístup k systémům.
6. **Obfuskace / antiforenzní ochrana:** Aby mohli útočníci úspěšně provést kybernetický útok, potřebují zamést stopy a v této fázi často kladou falešné stopy, kompromitují data a vymazávají protokoly, aby zmátli a/nebo zpomalili případný forenzní tým.
7. **Odmítnutí služby:** Narušení běžného přístupu uživatelů a systémů, aby útok nemohl být monitorován, sledován nebo blokován.
8. **Exfiltrace:** Fáze extrakce: získání dat z napadeného systému. (22)

3.5.2 MITRE ATT&CK

Framework MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) poskytuje komplexní model pro pochopení a kategorizaci chování kybernetických protivníků. Nastiňuje životní cyklus útoku protivníka a podrobně popisuje konkrétní používané taktiky, techniky a postupy. Cílem rámce, který byl vyvinut na základě experimentu Fort Meade Experiment (FMX) společností MITRE v roce 2013, je zlepšit detekci hrozeb po kompromitaci prostřednictvím telemetrického snímání a analýzy chování. Framework je postaven na třech základních složkách:

- **Taktika:** Ty představují krátkodobé cíle protivníka během útoku.
- **Techniky:** Ty podrobně popisují metody, které útočníci používají k dosažení svých taktických cílů.
- **Zdokumentované použití útočníka:** Jedná se o dokumentaci způsobu, jakým protivníci využívají techniky, a další relevantní metadata.

Tento framework je celosvětovým standardem používaným v různých oborech kybernetické bezpečnosti, jako je detekce narušení, vyhledávání hrozeb, bezpečnostní inženýrství a řízení rizik. Matice MITRE ATT&CK, která je součástí rámce, uvádí techniky používané protivníky zařazené do konkrétních taktik. Tyto taktiky uvádí lineárně od průzkumu až po konečný cíl, kterým může být exfiltrace dat nebo dopad na systém. Taktiky zahrnují:

- **Průzkum:** Shromažďování informací o cíli.
- **Rozvoj zdrojů:** Rozvoj zdrojů: Vytvoření zdrojů na podporu operací.
- **Počáteční přístup:** Získání vstupu do sítě.
- **Provedení:** Spuštění škodlivého kódu.
- **Trvalost:** Udržení přítomnosti v síti.
- **Zvýšení oprávnění:** Získání oprávnění vyšší úrovně.
- **Vyhýbání se obraně:** Vyhýbání se detekci.
- **Přístup k pověření:** Krádež uživatelských jmen a hesel.
- **Odhalení:** Pochopení prostředí.
- **Boční pohyb:** Pohyb v prostředí.
- **Shromažďování:** Shromažďování relevantních údajů.
- **Velení a řízení:** Ovládání ohrožených systémů.
- **Exfiltrace:** Krádež dat.
- **Dopad:** Manipulace, přerušení nebo zničení systémů a dat.

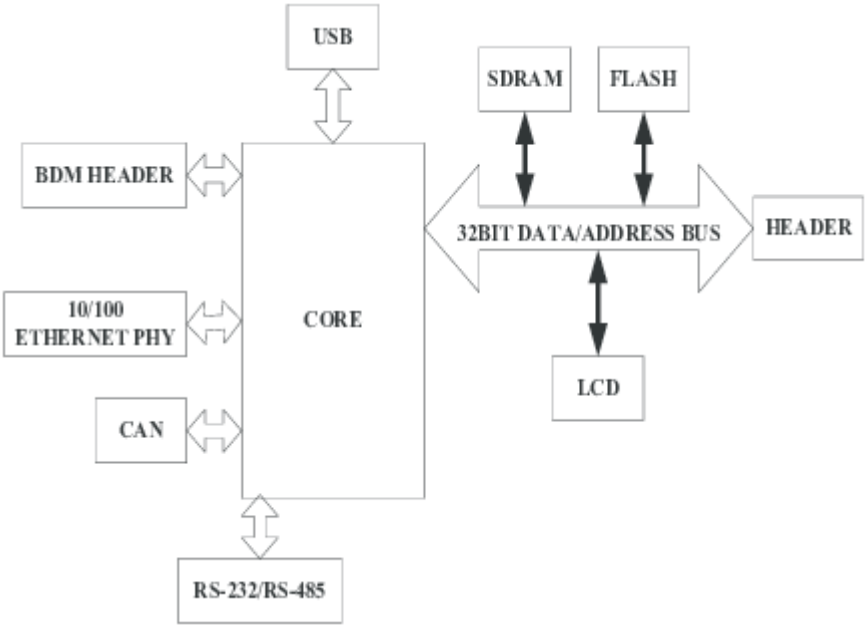
3.5.3 STRIDE Model

STRIDE vyvinuli koncem 90. let dva inženýři pracující ve společnosti Microsoft, Koren Kohnfelder se zabývali novými bezpečnostními hrozbami pro systémy způsobenými vývojem technologií a zjistili, že je třeba najít způsob, jak zmapovat umístění potenciálních hrozeb. Model hrozeb STRIDE počítá se šesti různými kategoriemi hrozeb, včetně:

1. **Zfalšování identity uživatele:** Vydávání se za legitimní uživatele za účelem získání neoprávněného přístupu do systémů.
2. **Manipulace s daty:** Neoprávněná změna dat, ať už uložených nebo přenášených.
3. **Odmítnutí:** Pachatelé popírají své činy beze stopy, což ztěžuje prokázání protiprávního jednání.
4. **Zveřejnění informací (narušení soukromí):** Neoprávněný přístup k důvěrným informacím.
5. **Odmítnutí služby (Denial of Service, D.o.S.):** Narušení služeb s cílem dočasně znepřístupnit nebo znemožnit používání systémů.
6. **Zvýšení oprávnění:** Neoprávnění uživatelé získají zvýšený přístup, který může ohrozit celý systém. (23)

3.6 Jednodeskové počítače (SBC)

Jednodeskové počítače (SBC) jsou kompaktní, plně funkční počítačové systémy postavené na jediné desce s plošnými spoji. Tyto počítače integrují všechny nezbytné součásti kompletního počítače, včetně procesoru (CPU), paměti (RAM), vstupně-výstupních (I/O) rozhraní a dalších funkcí potřebných pro funkční počítač. SBC jsou navrženy tak, aby byly levné, energeticky úsporné a snadno nastavitelné pro různé aplikace, od vzdělávacích účelů až po průmyslové a komerční aplikace. Architektura SBC je často založena na architektuře ARM (Advanced RISC Machine) nebo x86, což jim umožňuje provozovat různé operační systémy a softwarové aplikace. SBC, jako je Raspberry Pi, si získaly obrovskou popularitu díky své cenové dostupnosti, všestrannosti a rostoucímu zájmu o počítačové projekty typu "udělej si sám" a hnutí tvůrců. (24)



Obrázek 6 Architektura jednodeskových počítačů (25)

3.7 Historie jednodeskových počítačů

Historie jednodeskových počítačů (Single Board Computers, SBC) představuje významný vývoj počítačové technologie, který byl způsoben pokrokem v oblasti integrovaných obvodů a posunem směrem ke kompaktnějším a efektivnějším výpočetním řešením. Původně koncepce SBC vycházela z myšlenky integrovat všechny základní počítačové komponenty (procesor, paměť, vstupy a výstupy) na jednu desku s plošnými spoji. Tato konstrukce se lišila od tradičních počítačových architektur s více deskami, kde komponenty jako video, audio a síťové karty tvořily samostatné jednotky.

Příchod platformy Arduino v Itálii zhruba před deseti lety znamenal významný bod v historii SBC. Znamenal nástup cenově dostupných vývojových sad založených na mikrořadičích, které zpřístupnily moderní mikrořadiče pro různé projekty a významně přispěly k růstu trhu SBC. Pokles cen mikroprocesorů v důsledku úspěchu integrovaných komerčních procesorových platforem byl katalyzátorem tohoto trendu. V roce 2010 zaznamenala oblast SBC rychlý růst, který výrazně podpořil počítač Raspberry Pi, jenž byl původně vyvinut jako vzdělávací nástroj, ale rychle si získal oblibu mezi hobbyisty pro nesčetné projekty, jako je domácí automatizace a streamování médií. Kompaktní tvar SBC spolu s jejich schopností efektivně provádět složité úlohy vedly k jejich širokému rozšíření jak ve vzdělávacím prostředí, tak v různých průmyslových odvětvích.

V současné době lze SBC rozdělit především na open-source a proprietární typy. Open-source SBC nabízejí uživatelům transparentnost a kontrolu nad hardwarem i softwarem, takže jsou ideální pro učení a přizpůsobení. Proprietární SBC jsou však obvykle více propracované a procházejí přísným testováním, což je přizpůsobuje požadavkům koncových aplikací v průmyslovém prostředí. Současná nabídka SBC zahrnuje širokou škálu typů procesorů a rozsáhlou softwarovou podporu, převážně distribucí založených na Linuxu. Zásadní roli v úspěchu open-source SBC sehrává model podpory řízený komunitou, který zajišťuje průběžné aktualizace softwaru a prostřednictvím různých projektů prezentuje možnosti desek. Při pohledu do budoucnosti trend naznačuje, že výkon a všestrannost desek SBC bude i nadále růst a dále překlenovat mezeru mezi tradičními osobními počítači a kompaktními a výkonnými výpočetními zařízeními. Integrace výkonnějších procesorů a rozšíření přídavných desek a příslušenství pravděpodobně otevře nové možnosti pro profesionální i kutilské projekty. Kromě toho se očekává, že se bude zvyšovat podíl SBC v nízkoobjemových koncových produktech, což bude dáno neustálou zpětnou vazbou a zlepšováním, které umožňuje celosvětová komunita open-source a vysoce kvalitní konstrukční a výrobní procesy. (26) (27) (28)

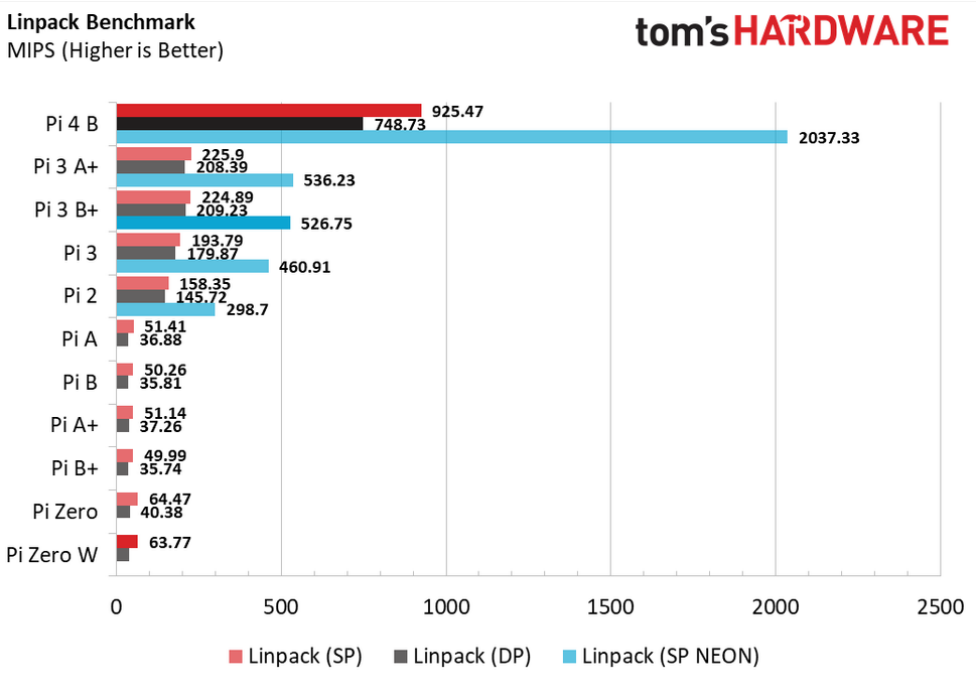
3.8 Raspberry Pi

Raspberry Pi, vyvinutý britskou nadací Raspberry Pi Foundation, je jednodeskový počítač navržený tak, aby byl cenově dostupný, zejména pro vzdělávací účely. Běží na systému Linux a jako hlavní programovací jazyk používá Python. Projekt, který v roce 2006 inicioval Eben Upton se svým týmem na univerzitě v Cambridge. Název "Raspberry Pi" kombinuje trend pojmenovávání počítačů podle ovoce a programovacího jazyka Python. Nadace se zaměřuje na charitativní a vzdělávací cíle a reinvestuje zisk do vzdělávacích programů a zdrojů. Od svého prvního vydání v roce 2012 se počítač Raspberry Pi vyvinul do několika modelů: (29)

3.8.1 Raspberry Pi 4 (2019)

Raspberry Pi 4B 8 GB představuje významný krok vpřed v řadě Raspberry Pi, sadu vylepšení, která zvyšují jeho výkon a použitelnost. Procesor Broadcom BCM2711B0 s frekvencí 1,5 GHz, který využívá efektivnější architekturu Cortex-A72, spolu s výkonným grafickým procesorem umožňují znatelné zvýšení výpočetního výkonu, což se projevilo

nárůstem o 413 % v testu Linpack benchmark s jednou přesností ve srovnání s Raspberry Pi 3B+.



Obrázek 7 Linpack Benchmark (30)

Mezi klíčová vylepšení patří také zvýšená kapacita a rychlost paměti RAM, zavedení portů USB 3 pro vyšší rychlost přenosu dat a dva porty micro HDMI podporující výstup 4K. Tyto funkce v kombinaci s gigabitovým ethernetovým připojením a rychlejším slotem pro karty microSD výrazně rozšiřují možnosti Raspberry Pi 4B 8GB jako všestranné výpočetní platformy. Raspberry Pi 4B 8GB má nyní napájecí konektor USB typu C, který vyžaduje robustnější napájení, ale nabízí pohodlí oboustranného konektoru. Čtečka microSD Pi 4B jako primární úložiště má teoretickou maximální přenosovou rychlost 50 MB/s, což je dvojnásobek oproti předchůdci 3B+. Reálné testy s kartou microSD Samsung EVO Plus však ukázaly nižší rychlosti, a to 45,7 MB/s při čtení a 27,7 MB/s při zápisu. Zavedení portů USB 3 v počítači Pi 4B, které je u řady Raspberry Pi první, umožňuje používat externí disky SSD, což výrazně zvyšuje výkon úložiště. Testy s SSD diskem Western Digital Blue ukázaly přenosové rychlosti výrazně převyšující rychlost karty microSD, což zlepšilo časy spouštění aplikací. Aktualizace firmwaru navíc umožnila spouštět počítač Raspberry Pi 4 přímo z externího USB SSD nebo flash disku, čímž odpadá nutnost používat kartu microSD. (30)

4 Vlastní práce

V této části prozkoumáme topologii malé podnikové sítě a popíšeme začlenění jednodeskového počítače do síťové infrastruktury za účelem posílení zabezpečení prostřednictvím systému jednotné správy hrozeb (UTM). Tento přístup zahrnuje výběr vhodného hardwaru a softwaru, integraci klíčových součástí UTM, testování a vyhodnocování, které zajistí optimální výkon a zabezpečení. Zde je přehled jednotlivých aspektů:

Topologie sítě malého podniku

Topologie sítě malého podniku je navržena s ohledem na efektivitu, škálovatelnost a zabezpečení. Ústředním prvkem tohoto nastavení je směrovač, který řídí tok provozu mezi interními zařízeními a vnějším internetem. Zařízení v síti se připojují buď prostřednictvím kabelového Ethernetu pro stabilitu a rychlost, nebo bezdrátově pro flexibilitu a mobilitu, a vytvářejí tak hybridní síť, která vyhovuje různým provozním požadavkům.

Návrh softvérových komponent systému jednotné správy hrozeb

Klíčovým úkolem je navrhnout softvérové komponenty pro systém jednotné správy hrozeb. Tento návrh zahrnuje systém pro detekci a reakci, VPN, filtraci obsahu pomoci DNS sinkhole a firewallu, přičemž klade důraz na integraci těchto komponent do koherentního a snadno spravovatelného celku.

Výběr jednodeskového počítače

Klíčovým prvkem této konfigurace je jednodeskový počítač (SBC), který byl vybrán pro svou kompaktnost, cenovou výhodnost a všestrannost. Bude popsán konkrétní model SBC a jeho specifikace, přičemž bude zdůrazněno, proč je ideální volbou pro zvládnutí požadavků systému UTM v prostředí malého podniku.

Instalace softwaru

SBC bude vybaven pečlivě vybraným operačním systémem a dalšími softwarovými komponentami nezbytnými pro funkčnost UTM. Bude popsán proces instalace, včetně nastavení operačního systému, instalace potřebných knihoven a balíčků a úvodních konfiguračních kroků, které připraví SBC na jeho roli v síti.

Integrace komponent UTM

Systém UTM implementovaný na SBC bude zahrnovat několik klíčových komponent, z nichž každá řeší různé aspekty zabezpečení sítě:

- Systému pro rozšířenou detekci a reakci (XDR) a správu bezpečnostních informací a událostí (SIEM).
- Brána firewall: Firewall: slouží k prosazování zásad zabezpečení sítě a řízení příchozího a odchozího provozu.
- VPN (virtuální privátní síť): K zajištění bezpečného vzdáleného přístupu.
- DNS Sinkhole: Slouží k zajištění bezpečného připojení k internetu: K zamezení přístupu ke známým škodlivým doménám.

Testování a hodnocení

Bude provedeno důkladné testování, aby bylo zajištěno, že každá součást systému funguje, jak má, a v rámci sítě bezproblémově spolupracuje:

- Funkční testování: Ověření správné funkce jednotlivých součástí a zajištění, že splňují stanovené požadavky.
- Testování zabezpečení: Vyhodnocení účinnosti systému při identifikaci a zmírňování různých bezpečnostních hrozeb.

4.1 Topologie sítě malého podniku

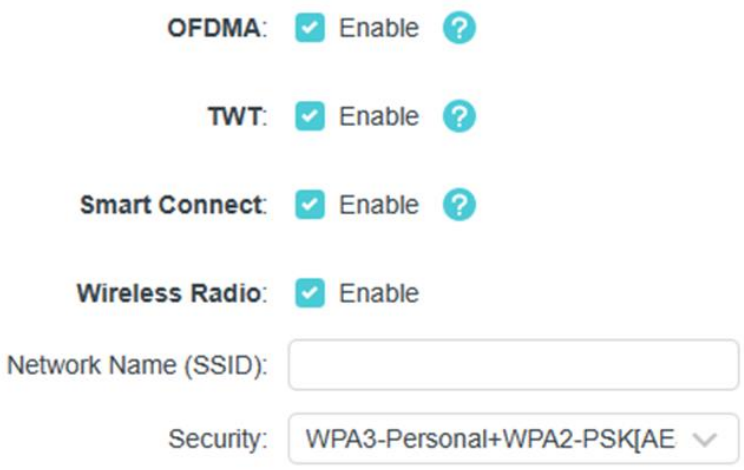
Síťová infrastruktura pro nasazení systému jednotné správy hrozeb je soustředěna do hvězdicové topologie, přičemž router TP-Link AX73 funguje jako hlavní uzel. Tento router podporuje technologii WiFi 6, která nejen usnadňuje vysokorychlostní bezdrátové připojení v celém prostředí malé kanceláře, ale slouží také jako klíčový bod pro správu sítě a implementaci zabezpečení. V této topologii se různá zařízení, včetně pracovních stanic, tiskáren a zařízení IoT, připojují primárně prostřednictvím WiFi. Centralizace, která je charakteristická pro hvězdicovou topologii, představuje specifické bezpečnostní výhody a problémy. Na jedné straně ústřední bod řízení umožňuje zjednodušené uplatňování bezpečnostních zásad a monitorování veškeré komunikace prostřednictvím systému UTM. Na druhou stranu závislost topologie na centrálním uzlu přináší kritický bod, riziko selhání jediného bodu. Pro zmírnění tohoto rizika jsou nezbytné mechanismy redundance, které zajistí, že selhání centrálního uzlu neohrozí funkčnost nebo bezpečnost sítě. V této práci se nezaměříme na dosažení lepší redundance, ale budeme se soustředit na dosazení optimální bezpečnosti routeru.

4.1.1 Optimalizace konfigurace zabezpečení routeru

V době psaní této práce nebyly známy žádné zranitelnosti, které by ovlivňovaly router AX73. Vždy je však vhodné aktualizovat firmware routeru na nejnovější verzi. Protože to přináší výhody v oblasti výkonu a zabezpečení. Pro aktualizaci směrovače byl použit webový prohlížeč. IP adresa směrovače byla 192.168.0.1. Po připojení ke směrovači a po zadání přihlašovacích údajů byl v sekci nastavení a sekci aktualizace systému a firmwaru vykonán update. Aktuální verze firmwaru routeru byla 1.2.1 Build 20230626 rel.36899(455). K dispozici byla novější verze 1.2.4 Build 20240125 rel.39949.

Obrázek 8 Archer AX73 Firmware update

Bezpečnost routeru byla zvýšena přechodem z WPA2-PSK[AES]+WPA-PSK[TKIP] na kombinaci WPA3-Personal a WPA2-PSK[AES]. Tato aktualizace využívá pokročilé šifrování WPA3, které nabízí vyšší zabezpečení proti útokům brute-force, a zároveň zachovává kompatibilitu s WPA2 pro zařízení nepodporující WPA3. Dále byly aktivovány funkce OFDMA a TWT. Technologie Orthogonal frequency-division multiple access (OFDMA) zvyšuje účinnost přenosu dat, což je výhodné pro obsluhu více zařízení současně, aniž by byla ohrožena bezpečnost. Technologie Target Wake Time (TWT) optimalizuje spotřebu energie zařízení a snižuje přetížení sítě, čímž nepřímo zlepšuje bezpečnost sítě tím, že umožňuje předvídatelnější správu a sledování časových úseků.



Obrázek 9 Archer AX73 WiFi nastavení

4.2 Návrh softvérových komponent systému jednotné správy hrozeb

Výběr konkrétních technologií při vytváření systému jednotné správy hrozeb byl veden snahou o robustní zabezpečení, stabilitu systému a efektivní správu sítě. Základní operační systém, nástroje pro filtrování sítě, technologie VPN, řešení pro správu zabezpečení a incidentů a rozhraní pro správu firewallu byly oblasti, které vyžadovaly pečlivé zvážení. Po vyhodnocení obecných technologií dostupných v každé kategorii byla vybrána konkrétní řešení na základě jejich výkonu, bezpečnostních funkcí, kompatibility a podpory komunity. Níže je vysvětlen proces výběru pro každou kategorii a zdůrazněno, proč byly upřednostněny konkrétní technologie.

- **Operační systém –** Stabilní a bezpečný operační systém je základem každého systému UTM. Slouží jako základ, na kterém fungují všechny ostatní bezpečnostní komponenty, což vyžaduje spolehlivost, podporu a bezpečnost. Ubuntu Server 22.04 LTS byl vybrán pro svou dlouhodobou podporu (LTS), která zajišťuje průběžné aktualizace zabezpečení a stabilitu systému. Díky jeho širokému rozšíření a rozsáhlé dokumentaci je spolehlivým základem.
- **Nástroje pro filtrování sítě** – Nástroje pro filtrování sítě jsou nezbytné pro blokování nežádoucího nebo škodlivého obsahu. Tyto nástroje pracují na různých síťových vrstvách a zlepšují zabezpečení i výkon. Pi-Hole byla vybrána pro svou schopnost blokovat reklamy a škodlivé domény na úrovni DNS. Toto nenáročné řešení účinně snižuje síťový provoz a zvyšuje zabezpečení bez výrazného zatížení zdrojů.

- **Technologie VPN** – Zabezpečené technologie VPN mají zásadní význam pro ochranu vzdálených připojení. VPN šifruje provoz mezi sítí a vzdálenými uživateli a chrání data před zachycením nebo neoprávněným přístupem. Pi-VPN s technologií WireGuard byla upřednostněna pro svůj moderní přístup k připojení VPN. WireGuard nabízí ve srovnání s tradičními řešeními VPN vynikající výkon a snadnou konfiguraci, takže je ideální pro zabezpečení vzdáleného přístupu s minimem správcovské zátěže.
- **Bezpečnostní a incidentní systémy** – Pro odhalování hrozeb a správu bezpečnostních incidentů jsou zapotřebí komplexní řešení, která dokáží analyzovat bezpečnostní události a reagovat na ně v reálném čase. Volbou byl open source systém Wazuh, integrovaný s Elastic Stackem, pro jeho škálovatelnost a rozsáhlé možnosti zabezpečení. Tato kombinace umožňuje efektivní monitorování bezpečnostních událostí, správu shody a analýzu protokolů a poskytuje výkonnou sbírku nástrojů pro získávání informací o zabezpečení v reálném čase.
- **Technologie firewall** – Správa pravidel síťového provozu a ochrana před neoprávněným přístupem jsou funkce, které plní rozhraní pro správu firewallu. Tyto nástroje zjednodušují konfiguraci a správu řízení přístupu k síti. Technologie Uncomplicated Firewall (UFW) byla vybrána pro svou jednoduchost a účinnost. UFW poskytuje uživatelsky přívětivý způsob správy iptables a umožňuje snadné nastavení robustních pravidel firewall bez nutnosti hluboké znalosti syntaxe příkazového řádku.

Souhrnně lze říci, že výběr konkrétních technologií Ubuntu Server 22.04 LTS, Pi-Hole, Pi-VPN s WireGuard, Wazuh s Elastic Stack a UFW byl výsledkem promyšleného procesu s cílem vyvážit výkon, zabezpečení a spravovatelnost systému. Každá vybraná technologie vyniká svou spolehlivostí, bezpečnostními funkcemi a vhodností pro vytvoření efektivního a bezpečného síťového prostředí.

4.2.1 Analýza systémových požadavků systému UTM

Níže je uvedena tabulka s minimálními systémovými požadavky na jednotlivé softwarové komponenty systému jednotné správy hrozeb. Tato tabulka má pomoci při posuzování základních hardwarových potřeb pro efektivní nasazení jednotlivých komponent.

Tabulka 1 Minimální požadavky komponent UTM

Komponenta	CPU	RAM	Úložiště
Ubuntu Server	1 GHz (64-bit)	1 GB	2.5 GB
Pi-Hole	Single-core 1 GHz	512 MB	1 GB
Pi-VPN	1 GHz (64-bit)	256 MB	Nespecifikováno
Wazuh	Quad-core 2 GHz	8 GB	50 GB
UFW	Nespecifikováno	Nespecifikováno	Nespecifikováno

Výše uvedená tabulka ukazuje, že je možné zkonstruovat vysoce efektivní systém jednotné správy hrozeb pomocí jednodeskového počítače. Nejnáročnější komponenta z hlediska zdrojů, Wazuh s Elastic Stack, vyžaduje čtyřjádrový procesor s frekvencí 2 GHz, 8 GB paměti RAM a 50 GB úložiště. Tyto požadavky jsou v rámci možností několika špičkových počítačů SBC, které jsou v současné době dostupné na trhu. Ostatní komponenty Ubuntu Server 22.04 LTS, Pi-Hole a Pi-VPN s WireGuard mají navíc výrazně nižší systémové požadavky a mohou pohodlně běžet vedle systému Wazuh na vhodně vybaveném počítači. Minimální požadavky UFW nepřidávají významnou režii, což zajišťuje, že systém zůstává úsporný a efektivní. Konvergence těchto komponent na jediné platformě SBC podtrhuje technologický pokrok v možnostech SBC a umožňuje nasazení komplexních řešení zabezpečení sítě za zlomek nákladů, spotřeby energie a fyzické plochy spojené s tradičními serverovými sestavami. Tento přístup nejen ukazuje životaschopnost SBC pro sofistikované úlohy správy a zabezpečení sítě, ale také zdůrazňuje potenciál malých a středních podniků implementovat robustní systém UTM bez nadměrných nákladů.

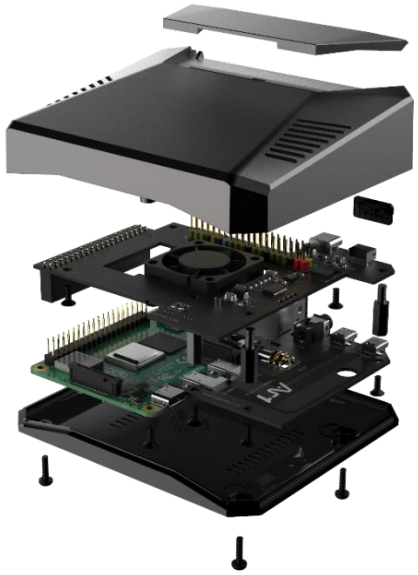
4.3 Výběr jednodeskového počítače

Po vyhodnocení několika počítačů SBC, které splňovaly minimální požadavky na systém, se jako nejvhodnější volba pro nasazení systému UTM ukázal počítač Raspberry Pi 4 Model B 8 GB. Toto rozhodnutí bylo ovlivněno několika klíčovými faktory:

- **Dostupnost na trhu:** Raspberry Pi 4 je široce dostupný na světových trzích. Jeho popularita a zavedený dodavatelský řetězec zajišťují snadné pořízení a potenciální škálovatelnost systému.

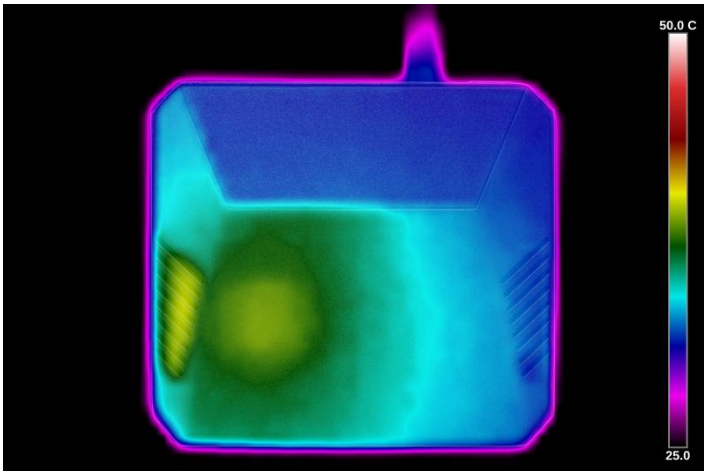
- **Výkon a kompatibilita:** Tento model díky čtyřjádrovému procesoru Cortex-A72 a 8 GB paměti RAM nejen splňuje požadavky systému UTM. Zajišťuje bezproblémový provoz Ubuntu Server 22.04 LTS a Wazuh s Elastic Stackem a poskytuje spolehlivý výkon i při zátěži.
- **Podpora a komunita:** Raspberry Pi se těší rozsáhlé a aktivní komunitě a rozsáhlé dokumentaci. Tato robustní síť podpory je při řešení problémů a optimalizaci systému velkou výhodou.
- **Cenová výhodnost:** Cenová dostupnost má zásadní význam při dokazování, že vybudování vysoce výkonného řešení UTM na platformě SBC je nejen proveditelné, ale také finančně únosné, a to i pro malé a střední podniky.
- **Energetická účinnost a rozměry:** Díky kompaktním rozměrům a nízké spotřebě energie je Raspberry Pi významnou výhodou, takže je ideální pro nepřetržitý provoz bez vysokých nákladů na energii.

Pro umístění počítače Raspberry Pi 4 byla vybrána skříň Argon ONE V2 pro svou robustní konstrukci, integrovaný chladicí ventilátor. Pouzdro obsahuje tlačítko napájení pro spouštění a vypínání systému a také standartní porty HDMI. Integrované řešení chlazení je klíčové pro udržení optimálních provozních teplot, zejména při velkém zatížení systému nebo při přetaktování za účelem zvýšení výkonu. Vysoká tepelná vodivost hliníku efektivně odvádí teplo po celé ploše povrchu a funguje jako pasivní chladicí prvek.



Obrázek 10 Argon ONE V2 (31)

V praktických testech prokázala skříň Argon ONE V2 při vysokém zatížení během 10 minut při vypnutém ventilátoru výborný výkon. Snímky z termokamery pořízené po testu ukázaly, že teplota se pohybovala kolem 37 stupňů Celsia.



Obrázek 11 Výsledky temperování systému Argon ONE V2 (32)

Výběr karty Samsung MicroSDXC 256 GB EVO Plus jako primárního úložného média byl podmíněn posouzením spolehlivosti, výkonu, snadné integrace a cenové efektivity ve srovnání s alternativními úložnými řešeními, jako jsou USB klíčenky, SSD nebo HDD. Tato karta MicroSD se vyznačuje robustní odolností a spolehlivou integritou dat, která je pro nepřetržitý provoz systému UTM klíčová, a nabízí dostatečně vysoké rychlosti čtení/zápisu nezbytné pro efektivní zpracování a vyhledávání dat bez dodatečných nároků na napájení a fyzický prostor v případě disků SSD nebo bez rizika mechanického selhání spojeného s disky HDD. Jeho přímá integrace do počítače Raspberry Pi navíc minimalizuje riziko odpojení a fyzického poškození, což zvyšuje přenositelnost a stabilitu systému.

4.3.1 Kalkulace nákladů spotřeby elektřiny

Na základě hardwarových specifikací modelu Raspberry Pi 4 8 GB s průměrnou spotřebou energie v nečinnosti 2,7 W a maximální spotřebou energie v zátěži 6,4 W byla vypočtena průměrná spotřeba energie v typických scénářích použití na 4,55 W. Tento odhad předpokládá vyváženou kombinaci nečinnosti a aktivních období v průběhu provozu. (33)

Vzhledem k této průměrné spotřebě energie lze denní a roční spotřebu energie vypočítat následovně: Denní spotřeba energie je 109,2 watthodin (Wh), což je odvozeno od 4,55 wattů zprůměrovaných za 24 hodin. Roční spotřeba energie činí 39 858 watthodin (Wh), tj. přibližně 39,86 kilowatthodin (kWh), pokud vezmeme v úvahu, že zařízení pracuje

nepřetržitě po celý rok. Při předpokládané ceně elektřiny 4,5 Kč za kilowatthodinu (kWh) lze náklady na provoz modelu Raspberry Pi 4 8 GB odhadnout takto:

Denní náklady: Přibližně **0,4914 Kč**

Roční náklady: Přibližně **179,37 Kč**

4.4 Instalace operačního systému

Instalace operačního systému na kartu SD byla provedena pomocí notebooku vybaveného adaptérem pro microSD karty. Poté byl spuštěn software Raspberry Pi Imager, který nabízí jednoduché rozhraní pro výběr požadovaného operačního systému. Ze seznamu dostupných možností byl vybrán Ubuntu Server 22.04 LTS, který je speciálně optimalizován pro nasazení na Raspberry Pi 4. Tato verze byla vybrána pro svou kompatibilitu s hardwarem a požadavky systému UTM, včetně podpory Wazuh s Elastic Stack a dalších bezpečnostních komponent. Po dokončení instalace operačního systému byla do počítače Raspberry Pi 4 vložena microSD karta a zařízení bylo připojeno k monitoru pomocí kabelu HDMI. Toto přímé připojení umožnilo počáteční nastavení a konfiguraci operačního systému. Následná instalace a konfigurace softwarových komponent UTM probíhala vzdálené za pomoci protokolu SSH.

4.5 Instalace firewall

Při návrhu a implementaci systému jednotné správy hrozeb bylo klíčové rozhodnutí o výběru firewallu. Toto rozhodnutí zahrnovalo vyhodnocení komplexity a granularity kontroly, kterou nabízejí různá řešení brány firewall, od nižších úrovní iptables a netfilteru až po vyšší abstrakci, kterou poskytuje Uncomplicated Firewall (UFW). Hlavním cílem bylo najít nástroj, který by vyvážil snadnou konfiguraci s požadovanou úrovní ochrany a kontroly sítě. Nástroj iptables jako všestranný a výkonný nástroj nabízí podrobnou kontrolu nad síťovým provozem tím, že umožňuje specifikaci složitých sad pravidel. Netfilter, základní framework využívaný nástrojem iptables, pracuje na úrovni jádra a nabízí ještě hlubší kontrolu nad zpracováním paketů. Ačkoli tyto nástroje poskytují rozsáhlé možnosti přizpůsobení řízení síťového provozu, vyžadují pro efektivní konfiguraci a správu značnou míru technických znalostí. Složitost iptables a netfilteru, zejména v souvislosti s vytvářením a údržbou komplexních pravidel firewallu, představuje problém z hlediska režie konfigurace a možnosti chybné konfigurace.

4.5.1 Volba firewallu

K rozhodnutí použít UFW vedla filozofie jeho návrhu, která upřednostňuje jednoduchost a snadnost použití bez obětování funkčnosti. UFW slouží jako frontend k iptables a abstrahuje složitost syntaxe jeho sady pravidel do jednodušších příkazů a konfigurací. Díky této vyšší úrovni abstrakce je UFW ideální volbou, zejména s ohledem na následující faktory:

- **Snadná konfigurace:** UFW zjednodušuje proces správy brány firewall a zpřístupňuje jej správcům s různou úrovní odborných znalostí. Tato snadná konfigurace snižuje pravděpodobnost chyb, které by mohly ohrozit zabezpečení systému.
- **Dostatečná kontrola:** UFW poskytuje i přes své zjednodušené rozhraní dostatečnou kontrolu nad příchozím a odchozím provozem, což umožňuje efektivní implementaci bezpečnostních zásad systému UTM. Podporuje specifikaci pravidel založených na aplikacích, což usnadňuje povolování nebo blokování provozu pro konkrétní služby.

4.5.2 Počáteční nastavení

Na Ubuntu Server 22.04 LTS je UFW nainstalován ve výchozím nastavení a poskytuje okamžitý přístup k možnostem konfigurace brány firewall. Následující kroky popisují proces konfigurace UFW, který zajistil ochranu sítě systému před neoprávněným přístupem. Pro účinné zabezpečení sítě jsou stanoveny výchozí zásady pro příchozí a odchozí komunikace. Tímto přístupem se přijímá bezpečné nastavení, které omezuje potenciální neoprávněný přístup. První příkaz nastaví UFW tak, aby blokoval veškerý příchozí provoz, aby byla přípustná pouze výslovně povolená připojení. Druhý příkaz naopak povoluje veškerý odchozí provoz ze systému, čímž usnadňuje potřebnou komunikaci s externími službami a internetem.

```
$ sudo ufw default deny incoming
$ sudo ufw default allow outgoing
```

Syntaxe pro správu nastavení portů v systému je přímočará. Pro povolení nebo odepření komunikace na portu musí být příkaz v této struktuře sudo ufw allow / deny číslo portu. Následně bylo provedeno povolení připojení SSH přes firewall a po nastavení výchozích zásad byla posledním krokem aktivace UFW.

```
$ sudo ufw allow 22
$ sudo ufw enable
```

4.6 Instalace DNS Sinkhole

V této části byla provedena instalace Pi-hole. Statická IP adresa je nezbytná pro zajištění stabilního a stálého referenčního bodu v síti, což je předpokladem pro fungování služeb DNS. Spuštění instalace Pi-hole probíhá pomocí zjednodušeného automatizovaného skriptu. Skript prochází fázemi instalace s důrazem na konfiguraci síťových nastavení.

Obrázek 12 Instalační příkaz Pi-Hole

4.6.1 Výběr Upstream DNS poskytovatele

Upstream DNS poskytovatel zvolený během konfigurace Pi-hole je klíčový, protože určuje službu, které Pi-hole předává dotazy DNS, které nejsou místně blokovány. Uživatelé mají možnost vybrat si z poskytovatelů DNS, jako je Google, OpenDNS, nebo zadat vlastního poskytovatele. Rozhodnutí je často ovlivněno různými faktory, včetně zásad ochrany osobních údajů poskytovatele, účinnosti jeho funkcí filtrování a rychlosti řešení dotazů. Jako poskytovatel DNS byl zvolen poskytovatel **Quad9 (filtered, ESC, DNSSEC).**

4.6.1.1 Filtrovaný systém DNS

Služba filtrovaného DNS společnosti Quad9 blokuje přístup ke známým škodlivým doménám. Toho je dosaženo využitím informací o hrozbách z různých zdrojů k sestavení rozsáhlé databáze škodlivých webových stránek spojených s phishingem, malwarem a exploit kity. Tím zabraňuje zařízením v síti v připojení k těmto nebezpečným webům.

4.6.1.2 Klientská podsíť EDNS (ECS)

Klientská podsíť EDNS (ECS) je rozšíření protokolu DNS, které umožňuje zahrnout do dotazů DNS částečné informace o IP adresách. Tyto informace se používají k poskytování geograficky lokalizovaných odpovědí, což zvyšuje rychlost a relevanci doručování webového obsahu.

4.6.1.2.1 DNSSEC

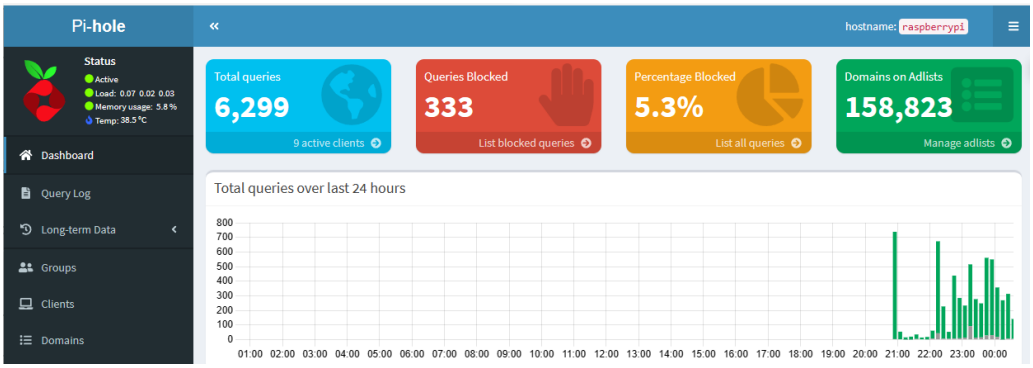
Rozšíření zabezpečení DNS (DNSSEC) přidává do procesu vyhledávání DNS další vrstvu zabezpečení tím, že umožňuje digitálně podepisovat odpovědi DNS. Tyto podpisy lze ověřit, aby bylo zajištěno, že s daty DNS nebylo manipulováno, což poskytuje ochranu proti určitým typům kybernetických útoků, jako je například cache poisoning a man-in-the-middle útoky.

4.6.2 Určení blocklistů

Blocklisty, které jsou nedílnou součástí fungování služby Pi-hole, se skládají z domén, které byly rozpoznány jako hostitelské pro reklamy, trackery nebo malware, což účinně brání přístupu ze sítě. Pi-hole nabízí výchozí sadu blocklistů a uživatelé mají možnost přizpůsobit tyto seznamy svým jedinečným požadavkům. Toto přizpůsobení může zahrnovat přidání dalších seznamů pro komplexnější ochranu nebo odstranění konkrétních seznamů, aby se minimalizoval výskyt falešných pozitivních výsledků. Byl zvolen výchozí blocklist **StevenBlack's Unified Hosts List.** Tenhle seznam obsahuje přes 150 tisíc záznamu DNS.

4.6.3 Instalace správcovského webového rozhraní a webového serveru

Pi-hole obsahuje volitelné webové rozhraní, které poskytuje vizuální zobrazení dotazů, statistik a nastavení, což usnadňuje efektivní monitorování a správu systému. Webový server je nezbytnou součástí, pokud je nainstalováno webové rozhraní Pi-hole. Zajišťuje provoz rozhraní a zpřístupňuje jej uživatelům. Pi-hole dokáže samostatně nainstalovat a nakonfigurovat Lighttpd jako možnost jednoduchého webového serveru a jednoduché databáze SQLite.



Obrázek 13 Logovací rozhraní Pi-Hole

4.6.4 Konfigurace úrovní logování a ochrany osobních údajů

Pi-hole provádí logování dotazů pro zvýšení výkonu a usnadnění řešení problémů. Rozsah logování a uchovávání logovaných informací však může být předmětem úvah z důvodu ochrany soukromí nebo omezení úložiště. Pi-hole se přizpůsobuje různým preferencím tím, že poskytuje možnosti nastavení granularity zaznamenávaných podrobností. Uživatelé se mohou rozhodnout, že logování zcela zakážou, zda se rozhodnou pro anonymizaci logů, nebo zda upraví objem logovaných dat tak, aby odpovídal jejich preferencím v oblasti ochrany soukromí a ukládání. Byla vybrána možnost úplné transparence **Show everything.** Nezbytnou součástí pro zabezpečení přístupu k webovému rozhraní z jiných zařízení je povolení příchozí komunikace na portu 80 jako výchozího portu HTTP. Byl otevřen port 53, který je důležitý pro zpracování dotazů DNS. Kromě toho byl povolen port 67, využívaný pro protokoly TCP i UDP, aby podporoval funkci serveru DHCP systému Pi-Hole, která dynamicky přiděluje síťovým zařízením adresy IP. K povolení byli použitý příkazy:

```
$ sudo ufw allow 80
$ sudo ufw allow 67
$ sudo ufw allow 53
```

4.6.5 Konfigurace statické IP adresy a výchozí DNS adresy

V závěrečné fázi konfigurace Pi-Hole byla serveru Pi-Hole přidělena statická IP adresa a tato adresa byla nastavena jako výchozí server DNS prostřednictvím webového uživatelského rozhraní routeru TP-Link Archer AX73. Prostřednictvím nastavení DHCP byla serveru Pi-Hole přidělena statická IP adresa. Tato akce zabraňuje konfliktům IP tím, že udržuje konzistentní adresu pro Pi-Hole. Nastavení DNS routeru bylo upraveno tak, aby stávající adresy DNS byly nahrazeny statickou IP adresou serveru Pi-Hole a všechny síťové požadavky DNS byly směrovány na server Pi-Hole. Těmito kroky bylo zajištěno nepřetržité filtrování DNS, což přispělo k bezpečnosti a efektivitě sítě centralizací správy DNS prostřednictvím Pi-Hole.

4.7 Instalace virtuální privátní sítě

V této části byla provedena instalace Pi-VPN tak, aby poskytovala bezpečný, šifrovaný tunel pro internetový provoz. Proces instalace zahrnuje řadu metodických kroků, které zajistí optimální integraci služby VPN do stávající síťové infrastruktury. Jako základní protokol pro službu VPN byl zvolen WireGuard, který je známý svou jednoduchostí, vysokým výkonem a moderními kryptografickými protokoly. Protokol WireGuard využívá moderní kryptografické standardy, jako jsou Curve25519, ChaCha20 a Poly1305, které zajišťují robustní zabezpečení a minimální rizika zranitelnosti. Jeho kompaktní kódová struktura, zhruba 4 000 řádků, nejen zjednodušuje audity, ale také zvyšuje spolehlivost a efektivitu systému. Pro spuštění instalačního skriptu Pi-VPN byl použit následující příkaz:

Obrázek 14 Instalační příkaz Pi-VPN

Pro správní fungování služby VPN je třeba, aby poskytovatel internetového připojení poskytl veřejnou IP adresu nebo je potřeba zajistit dynamický DNS. Pokud poskytovatelé internetových služeb používají CGNAT, stává se efektivní využívání dynamického DNS (DDNS) problematickým pro služby, které vyžadují přímý přístup k internetu, jako jsou například sítě VPN. CGNAT totiž přiděluje stejnou veřejnou IP adresu více zákazníkům, což brání tomu, aby DDNS dokázal přesně nasměrovat externí provoz na konkrétní zařízení. Kromě toho typické zamezení příchozích připojení CGNAT, které je nezbytné pro fungování VPN, znamená, že DDNS nemůže navázat spolehlivé připojení k vaší síti. Situaci zhoršují konflikty mapování portů vyplývající z prostředí sdílené IP, kdy pokusy více uživatelů o použití stejného portu mohou vést k nesrovnalostem ve směrování. Časté změny IP spojené s CGNAT mohou navíc způsobit problémy systému DDNS, což může vést k výpadkům, protože se snaží udržet záznamy DNS aktualizované. Strukturální omezení CGNAT tak zásadně omezují účinnost DDNS při poskytování přímého přístupu k internetu, který vyžadují některé služby. Proto je jedinou možnou volbou veřejná IP adresa. Pro získání veřejné IP adresy je třeba vyplnit žádost u poskytovatele připojení k internetu. Pro ověření, zda je adresa IP veřejně přístupná, byl použit příkaz ping.

```
$ ping 83.2XX.2XX.XX
Pinging 83.2XX.2XX.XX with 32 bytes of data:
Reply from 83.2XX.2XX.XX bytes=32 time=3ms TTL=127
Reply from 83.2XX.2XX.XX: bytes=32 time=3ms TTL=127
Reply from 83.2XX.2XX.XX: bytes=32 time=5ms TTL=127
Reply from 83.2XX.2XX.XX: bytes=32 time=3ms TTL=127
```

Wireguard také nastaví veškerou komunikaci přes port 51820 pomocí protokolu UDP. Protokol UDP nevyžaduje navázání spojení před přenosem dat a neprovádí opravu chyb, která může způsobit zpoždění. Díky tomu je protokol UDP vhodnější pro požadavky přenosu v reálném čase v sítích VPN, kde je nejdůležitější rychlost a efektivita. Pokud je služba VPN umístěna za routerem v síti, aby se provoz dostal na port bylo nastavené pravidlo pro přesměrování portů. Přesměrování portů v kontextu nastavení sítě WireGuard VPN usnadňuje přístup k serveru z internetu a pomáhá při obcházení NAT. Konfigurací routeru tak, aby předával provoz z určitého externího portu na odpovídající port na místní IP adrese serveru, se zajistí, že příchozí připojení VPN mohou úspěšně dosáhnout serveru WireGuard. To je obzvláště důležité v sítích využívajících NAT, kde je více privátních IP adres mapováno na jednu veřejnou IP adresu. Díky přesměrování portů jsou pakety přicházející na veřejnou IP adresu routeru na určeném portu přesně přesměrovány na server WireGuard, čímž je zachována nepřerušená služba VPN a konektivita. Nezbytnou součástí je povolení příchozí komunikace na portu 51820. K povolení byl použitý příkaz:

```
$ sudo ufw allow 51820
```

Přidání zařízení do sítě VPN bylo vykonáno za pomoci příkazu „**pivpn -a**“. Tento příkaz se pak zeptá na název zařízení. Pro připojení k síti VPN pak existují dvě možnosti. První možností je použít příkaz „**pivpn -qr**“, který vygeneruje QR kód ke skenování. Druhá možnost je připojit se pomocí konfiguračního souboru. Pro kontrolu připojených zařízení k VPN slouží příkaz „**pivpn -c**“, který zobrazí všechna zařízení.

```
ltopolsky@ltopolsky-utm:~$ pivpn -a
Enter a Name for the Client: ltopolsky-win10-pc
::: Client Keys generated
::: Client config generated
::: Updated server config
::: Updated hosts file for Pi-hole
::: WireGuard reloaded
================================================================
::: Done! ltopolsky-win10-pc.conf successfully created!
::: ltopolsky-win10-pc.conf was copied to /home/ltopolsky/configs for easytransfer.
::: Please use this profile only on one device and create additional
::: profiles for other devices. You can also use pivpn -qr
::: to generate a QR Code you can scan with the mobile app.
================================================================
```

```
ltopolsky@ltopolsky-utm:~$ pivpn -c
::: Connected Clients List :::
Name                  Remote IP              Virtual IP                                  Bytes Received  Bytes Sent
     Last Seen
ltopolsky-mobil       78.80.108.61:36285     10.10.48.2,fd11:5ee:bad:c0de::2/128         151KiB          244KiB
     bře 23 2024 - 14:57:17
aklimcikova-mobil     37.48.16.136:21680     10.10.48.3,fd11:5ee:bad:c0de::3/128         119KiB          62KiB
     bře 23 2024 - 14:57:42
ltopolsky-win10-pc    (none)                 10.10.48.4,fd11:5ee:bad:c0de::4/128         0B              0B
     (not yet)
::: Disabled clients :::
```

4.8 Instalace systému pro rozšířenou detekci a reakci (XDR) a správu bezpečnostních informací a událostí (SIEM)

Integrace Wazuh, systému pro rozšířenou detekci a reakci (XDR) a správu bezpečnostních informací a událostí (SIEM), do systému jednotné správy hrozeb významně zvyšuje kybernetickou bezpečnost organizace. Pokročilé funkce systému Wazuh pro detekci hrozeb, reakci na incidenty, monitorování shody a hodnocení rizik jsou v souladu s cíli systému UTM, který poskytuje komplexní bezpečnostní opatření proti široké škále kybernetických hrozeb. Jeho open-source povaha a modulární architektura nabízejí flexibilní a škálovatelné řešení, které lze přizpůsobit konkrétním potřebám organizace.

4.8.1 Instalace systému Wazuh

Pro instalaci systému Wazuh na Raspberry Pi se systémem Ubuntu Server byl použitý jejich průvodce nasazením vše v jednom s použitím komponent Elastic stack.

1. **Příprava serveru Ubuntu:** Pro zajištění aktuálnosti serveru Ubuntu je třeba spustit příkazy update a upgrade pomocí apt-get. Tento krok je zásadní pro bezpečnost a výkon systému, protože zajišťuje, že veškerý software na serveru je aktuální před instalací nových balíčků. K instalaci jsou potřeba některé další balíčky, například curl nebo unzip, které byli použity v dalších krocích.

```
$ apt-get install apt-transport-https zip unzip lsb-release curl gnupg
```

2. **Instalace Elasticsearch:** Elasticsearch jako základní součást balíku Elastic Stack slouží jako vyhledávací a analytický engine. Instalaci Elasticsearch provede přidáním zdroje balíčků Elastic do seznamu repozitáře a následnou instalací samotného balíčku Elasticsearch. Tento proces zahrnuje import klíče GPG pro úložiště Elastic a následnou instalaci Elasticsearch pomocí apt-get. Po instalaci je nutné povolit a spustit službu Elasticsearch a zajistit její spuštění při startu systému. Pro vygenerování pověření pro všechny předpřipravené role a uživatele Elastic Stack byl proveden tenhle příkaz.

```
# /usr/share/elasticsearch/bin/elasticsearch-setup-passwords
  auto

# Changed password for user apm_system
# PASSWORD apm_system = lLPZhZkB6oUOzzCrkLSF
# Changed password for user kibana_system
# PASSWORD kibana_system = TaLqVOnSoqKTYLIU0vDn
# Changed password for user kibana
# PASSWORD kibana = TaLqVOvXoqKTYLIU0vDn
# Changed password for user logstash_system
# PASSWORD logstash_system = UtuDv2tWkXGYL83v9kWA
# Changed password for user beats_system
# PASSWORD beats_system = qZcbvCslafMpoEOrE9Ob
# Changed password for user remote_monitoring_user
# PASSWORD remote_monitoring_user = LzJpQiSylncmCU2GLBTS
# Changed password for user elastic
# PASSWORD elastic = AN4UeQGA7HGl5iHpMla7
```

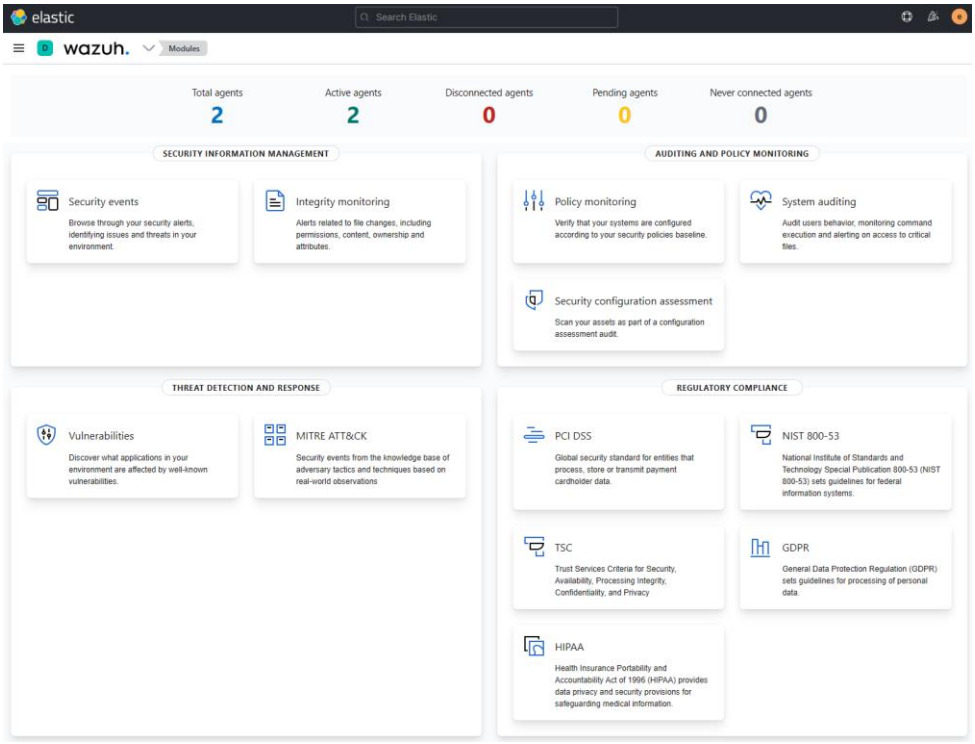
3. **Instalace Wazuh server:** Pro instalaci serveru Wazuh byl přidán do systému repozitář Wazuh a nainstalujeme balíček Wazuh manager. Tato komponenta je zodpovědná za správu agentů Wazuh, včetně analýzy dat a detekce na základě pravidel.
4. **Instalace systému Filebeat:** Služba Filebeat, je zodpovědná za předávání a centralizaci dat logů. Filebeat je součástí Elastic Stack a hraje klíčovou roli při sběru a odesílání dat protokolu. Instalace probíhá přidáním zdroje balíčků Elastic a instalací Filebeat pomocí apt-get. Po instalaci je Filebeat nakonfigurován tak, aby shromažďoval protokoly a metriky a předával je do Elasticsearch k indexování. Je důležité stáhnout a použít modul Wazuh pro Filebeat, který

obsahuje předdefinovaná pravidla, dekodéry a šablony pro interpretaci a vizualizaci bezpečnostních dat generovaných agenty Wazuh.

5. **Instalace nástroje Kibana:** Kibana poskytuje vizualizační vrstvu pro data uložená v Elasticsearch a je nezbytná pro vytváření ovládacích panelů pro vizualizaci výstrah a přehledů Wazuh. Proces instalace je stejný jako u Elasticsearch, zahrnuje přidání úložiště, import klíče GPG a instalaci Kibany pomocí apt-get. Po instalaci nakonfigurujte Kibanu tak, aby se připojila k instanci Elasticsearch.

Nyní je dashboard Wazuh přístupný přes prohlížeč na IP adrese Raspberry Pi. Dashboard je přístupný přes port HTTPS 443 ve srovnání s dashboardem z Pi-Hole, který je přístupný přes port HTTP 80. Uživatelské jméno je elastic a heslo je to, které bylo vygenerováno dříve.

Pro úspěšný provoz systému Wazuh v rámci našeho systému jednotné správy hrozeb je třeba nakonfigurovat konkrétní porty, které umožní komunikaci mezi serverem Wazuh, agenty, indexerem a dashboardem. Konfigurace byla provedena pomocí příkazů UFW, které povolují následující porty. Pro server Wazuh, který je centrální pro správu agentů a zpracování dat, byly povoleny porty 1514/TCP (výchozí pro připojení agentů), 1515/TCP (pro službu registrace agentů), 1516/TCP (pro daemon clusteru Wazuh) a 55000/TCP (pro rozhraní RESTful API). Indexer Wazuh, který je zodpovědný za indexování a ukládání dat, vyžadoval povolení portu 9200/TCP pro své rozhraní RESTful API a portů 9300-9400/TCP pro komunikaci clusteru, čímž se zajistila efektivní manipulace s daty a jejich načítání v rámci infrastruktury Wazuh. Pro dashboard Wazuh, který poskytuje webové uživatelské rozhraní pro monitorování a správu systému, byl povolen port 443/TCP, který usnadňuje bezpečný přístup k rozsáhlým bezpečnostním přehledům a analýzám Wazuh.



Obrázek 15 Wazuh dashboard

4.8.2 Instalace agentu Wazuh

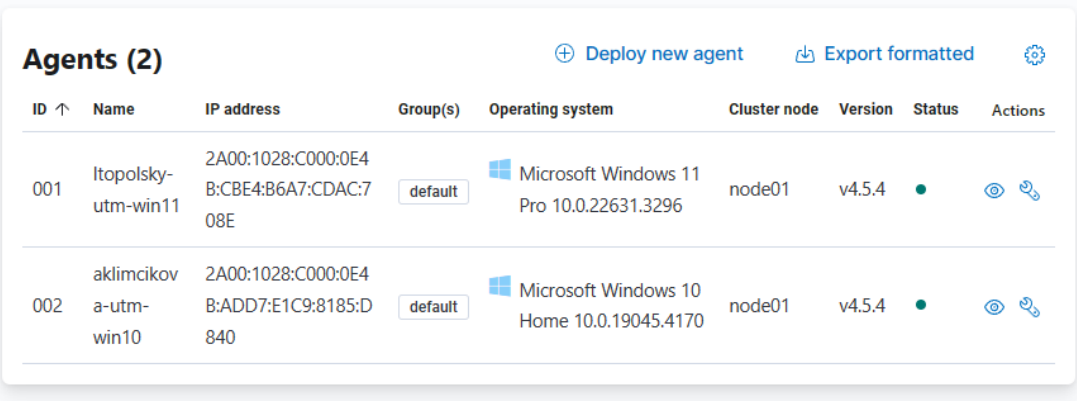
Nasazení agentů Wazuh je důležitým krokem při vytváření komplexní infrastruktury pro monitorování zabezpečení. Tito agenti jsou zodpovědní za sběr dat, včetně protokolů, systémových a aplikačních dat, která jsou následně odesílána na server Wazuh k analýze. Proces instalace se liší v závislosti na operačním systému koncových bodů. Níže jsou podrobně popsány postupy instalace pro koncové body se systémy Windows a Ubuntu.

4.8.2.1 Pro koncové body systému Windows

Pro instalaci agenta Wazuh na koncový bod systému Windows si z oficiálních webových stránek Wazuh nejprve stáhneme příslušný instalační program agenta Wazuh. Tento instalační program je speciálně přizpůsoben pro prostředí Windows a je dodáván ve formě spustitelného souboru. Instalační program spustíme jako správce, bychom zahájili proces instalace. Instalace vyžaduje zadání IP adresy správce Wazuh, čímž se zajistí, že agent bude moci komunikovat se serverem. Podle pokynů na obrazovce dokončíme instalaci, která automaticky nastaví spuštění agenta při startu systému. Po instalaci ověříme připojení agenta k serveru Wazuh prostřednictvím dashboardu Wazuh.

4.8.2.2 Pro koncové body Ubuntu

Instalace agenta Wazuh na koncových bodech Ubuntu začíná přidáním repozitáře Wazuh do systému. To lze provést importem klíče GPG repozitáře a přidáním repozitáře do správce balíčků systému. Po přidání repositáře je třeba aktualizovat informace o balíčcích a zajistit, aby systém o novém repositáři věděl. Agenta Wazuh nainstalujeme provedením příslušného příkazu apt-get. Během instalace je třeba nakonfigurovat agenta tak, aby se připojil ke správci Wazuh, a to zadáním jeho IP adresy. Tím se vytvoří komunikační kanál mezi agentem a serverem. Po dokončení instalace a konfigurace spustíme službu agenta Wazuh a povolíme její spuštění při startu systému. Stejně jako v případě instalace na systému Windows ověříme připojení k serveru Wazuh, aby agent fungoval a odesílal data podle očekávání.



Obrázek 16 Agenti Wazuh

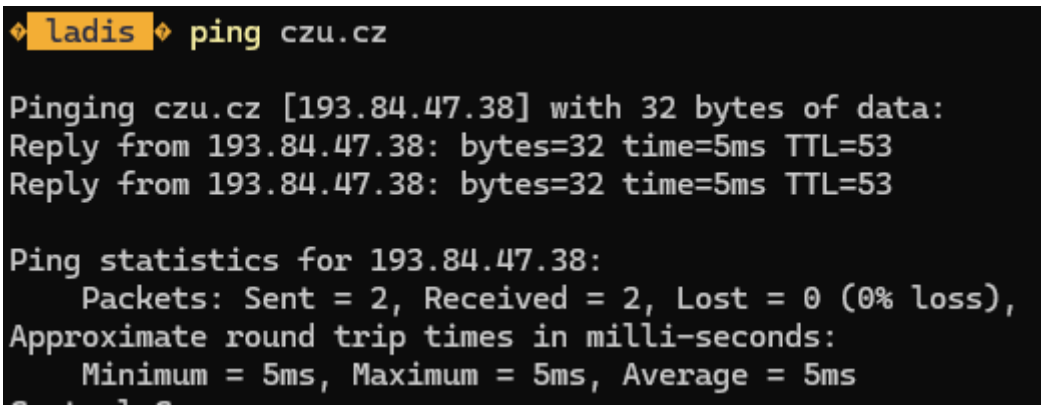
4.9 Testování funkčních celků systému

Jednotlivé části systému jednotné správy hrozeb byli otestovány, aby byla zajištěna účinnost a spolehlivost systému DNS sinkhole, VPN, služby Wazuh a brány firewall UFW. U systému DNS sinkhole se testování zaměřilo na jeho schopnost blokovat přístup k doménám na černé listině a k ověření funkčnosti se použilo cílené blokování domén a testy ping. Testy prvku VPN hodnotily konektivitu, šifrování a řízení přístupu a zajišťovaly bezpečné a stabilní připojení. U komponenty Wazuh byly testovány její schopnosti výstrah a analýzy protokolů, přičemž k ověření její účinnosti detekce a reakce byly použity simulované bezpečnostní události. A firewall UFW prošel kontrolou vynucování pravidel a posouzením dopadu na výkon, čímž se potvrdil účinnost při regulaci provozu bez omezení výkonu systému. Tento metodický přístup k testování nejen potvrdil provozní integritu

jednotlivých komponent, ale také ověřil jejich společný přínos k celkovému zabezpečení systému UTM.

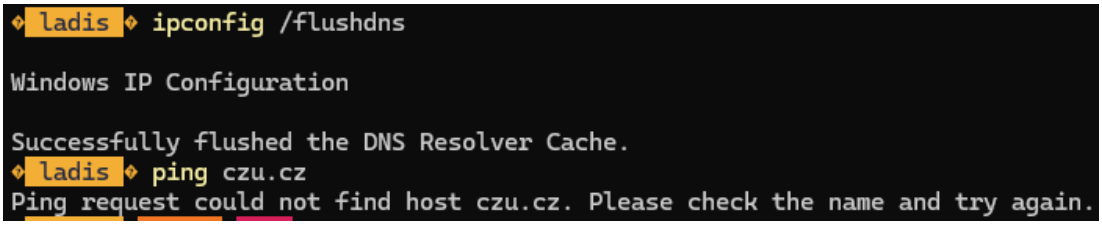
4.9.1 Test DNS Sinkhole (Pi-Hole)

Abychom ověřili účinnost mechanismu DNS sinkhole, provedli jsme cílený test zahrnující doménu czu.cz. Tato doména byla vybrána speciálně pro účely testování a přidána na černou listinu konfigurace DNS sinkhole. Metodika použitá pro testování funkčnosti DNS sinkhole byla jednoduchá, ale účinná. Pomocí nástroje ping v systému Windows jsme se pokusili zahájit požadavek ping na doménu czu.cz před a po jejím zařazení na černou listinu DNS sinkhole. Důvodem pro použití příkazu ping byla jeho závislost na rozlišení DNS pro získání IP adresy spojené s názvem domény, což z něj činí ideálního kandidáta pro tento test. Před zařazením na černou listinu příkaz ping úspěšně přeložil doménu czu.cz na její IP adresu a následné požadavky protokolu ICMP echo byly odeslány a přijaty, což svědčí o nerušeném připojení. Tento počáteční test sloužil jako kontrolní, který potvrdil, že síťová cesta k doméně je volná a že překlad DNS funguje normálně.



Obrázek 17 DNS Test 1

Po přidání domény czu.cz na černou listinu se očekávalo, že DNS sinkhole zachytí všechny dotazy DNS na tuto doménu a zabrání jejich přeložení na skutečnou IP adresu. Po opětovném provedení příkazu ping na adresu czu.cz se dostavil očekávaný výsledek; doménu nebylo možné přeložit, a proto nástroj ping nemohl zahájit echo požadavky na tuto doménu. Tento výsledek svědčil o úspěšném zachycení a zablokování dotazů DNS pro domény na černé listině ze strany DNS sinkhole, čímž byl znemožněn přístup k czu.cz ze sítě.

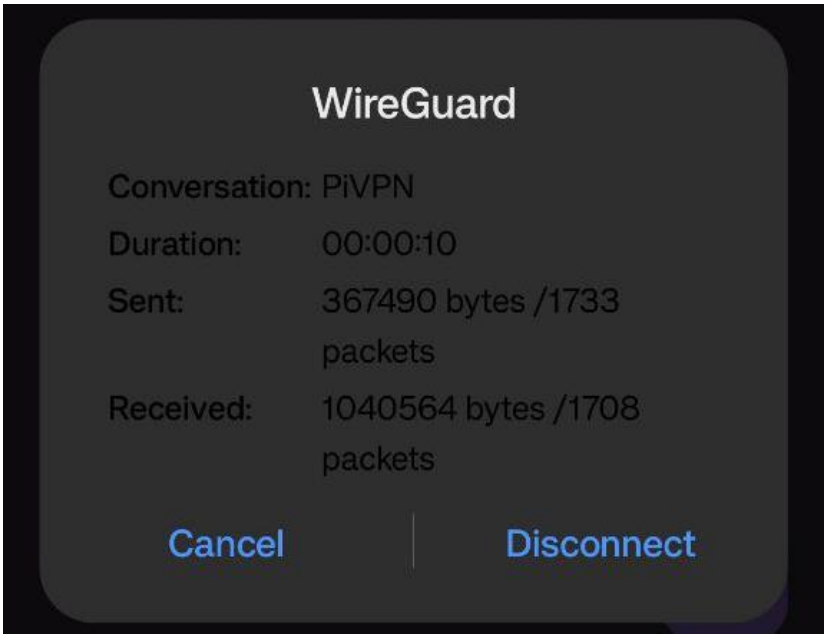


Obrázek 18 DNS Test 2

Úspěch tohoto testu podtrhuje klíčovou roli DNS sinkhole v systému UTM jako preventivního bezpečnostního opatření. Tím, že účinně ruší pokusy o přístup ke známým škodlivým nebo nežádoucím doménám, zvyšuje DNS sinkhole celkové zabezpečení sítě. Jednoduchost a účinnost metodiky testování navíc posilují spolehlivost systému DNS sinkhole jako klíčové součásti arzenálu systému UTM proti kybernetickým hrozbám.

4.9.2 Test VPN (Pi-VPN)

Při ověřování účinnosti a funkčnosti nastavení VPN v rámci našeho systému jednotné správy hrozeb byl proveden kritický test s použitím mobilního telefonu s aplikací WireGuard pro navázání připojení k Pi-VPN. Cílem tohoto testu bylo prokázat nejen snadnost připojení a konfigurace mezi mobilními zařízeními a sítí VPN, ale také bezproblémovou integraci sítě Pi-VPN s dalšími součástmi systému, zejména s Pi-Hole.



Obrázek 19 Tabulka dat mobilního připojeni Pi-VPN

Po konfiguraci aplikace WireGuard v mobilním zařízení s potřebnými přístupovými údaji a podrobnostmi o připojení pro Pi-VPN bylo připojení úspěšně navázáno. Tento

okamžik testování byl významný z několika důvodů. Zaprvé ukázal kompatibilitu a efektivitu WireGuard jako protokolu VPN pro mobilní zařízení, který nabízí jednoduchý a bezpečný způsob připojení k síti VPN. Zadruhé, možnost přístupu k ovládacímu panelu Pi-Hole z mobilního zařízení při připojení k Pi-VPN zdůraznila funkční integraci v rámci systému UTM a zajistila rozšíření funkcí filtrování DNS a blokování reklamy na zařízení připojená prostřednictvím sítě VPN. Dalšího ověření připojení VPN bylo dosaženo provedením příkazu pivpn -c na serveru Pi-VPN. Tento příkaz, který zobrazuje seznam aktuálně aktivních připojení VPN, zobrazil mobilní zařízení jako připojené.

```
ltopolsky@ltopolsky-utm:~$ pivpn -c
[sudo] password for ltopolsky:
::: Connected Clients List :::
Name                  Remote IP              Virtual IP                          Bytes Received      Bytes Sent
    Last Seen
ltopolsky-mobil       78.80.108.61:36309     10.10.48.2,fd11:5ee:bad:c0de::2/128 1,4MiB              5,3MiB
    bře 23 2024 - 22:44:44
```

Obrázek 20 Připojená zařízení Pi-VPN

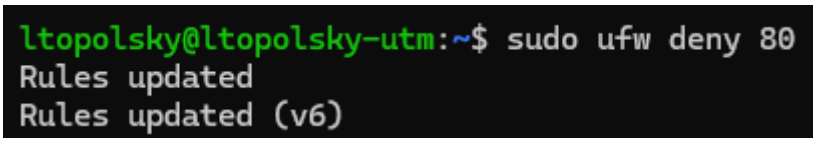
Tento testovací scénář podtrhl účinnost Pi-VPN ve spojení s WireGuard pro zajištění bezpečného vzdáleného přístupu. Ukázal také bezproblémové fungování Pi-Hole přes VPN, které zajišťuje, že výhody blokování reklam a filtrování DNS na úrovni sítě jsou dostupné i vzdáleným uživatelům.

4.9.3 Test firewall (UFW)

V komplexním nastavení zabezpečení systému jednotné správy hrozeb, který je centralizován na počítači Raspberry Pi, je pro ochranu sítě zásadní použití pravidel firewall prostřednictvím UFW. Na počítači Raspberry Pi jsou umístěny kritické součásti systému UTM včetně Pi-Hole, který zajišťuje filtrování DNS prostřednictvím webového uživatelského rozhraní umístěného na webovém serveru Apache. Vzhledem ke klíčové povaze těchto služeb je zajištění jejich zabezpečení proti neoprávněnému přístupu prvořadé. Důležitým aspektem této bezpečnostní strategie bylo zavedení pravidla ufw pro blokování přístupu na port 80, výchozí port používaný serverem Apache pro obsluhu webového obsahu, včetně webového uživatelského rozhraní Pi-Hole.

Pro empirické posouzení účinnosti tohoto pravidla brány firewall byl navržen specifický test. Po použití pravidla UFW pro blokování příchozího provozu na portu 80 byl proveden pokus o přístup k webovému serveru Apache hostujícímu webové rozhraní Pi-Hole z jiného prostředí, konkrétně z instance subsystému Windows pro Linux (WSL2) se systémem Ubuntu. Tento scénář byl zvolen za účelem simulace pokusu o přístup k webové službě zvenčí, což napodobuje potenciální snahu o neoprávněnou interakci s rozhraním Pi-

Hole. Nejprve bylo nastaveno pravidlo UFW pro blokování portu 80. Pomocí příkazu jsme zablokovali povolenou aktivitu na tomhle portu.



Obrázek 21 UFW pravidlo pro blokovaní portu 80

Poté testovací proces zahrnoval spuštění příkazu curl z instance Ubuntu na WSL2, směřujícího na IP adresu Raspberry Pi s úmyslem přistoupit k webové službě na blokovaném portu. Příkaz curl byl vybrán pro svou jednoduchost a účinnost při získávání webového obsahu, což z něj činí ideální nástroj pro tento ověřovací test. Po provedení tohoto příkazu po použití pravidla UFW se dostavil očekávaný výsledek; z webového serveru počítače Raspberry Pi nepřišla žádná odpověď. Tento výsledek potvrdil úspěšné vynucení pravidla firewallu, které účinně blokuje pokusy o neoprávněný přístup na port 80.

Obrázek 22 cURL REST GET request

4.9.4 Test systému XDR a SIEM (Wazuh)

Další zkoumanou složkou byl systém Wazuh, zejména jeho schopnost reagovat v reálném čase na bezpečnostní hrozby. Integrace systému Wazuh do architektury systému UTM zajišťuje komplexní monitorování a detekci hrozeb napříč koncovými body sítě. Klíčovou vlastností systému Wazuh, která umožňuje automatické reakce systému na zjištěné hrozby. Tato schopnost je významně rozšířena použitím seznamů CDB (Centralized Configuration Block) a mechanismů aktivní reakce společnosti Wazuh. Pro empirické vyhodnocení účinnosti systému Wazuh při zmírňování hrozeb byl navržen test zaměřený na jeho schopnost blokovat škodlivého aktéra, který se zaměřil na koncové zařízení systému Windows.

Server Wazuh byl nakonfigurován tak, aby integroval služby externího vyhodnocování hrozeb, konkrétně se zaměřil na posílení bezpečnostních opatření pro koncový bod systému Windows. Tento proces začal aktualizacemi systému a instalací nástroje wget, který je nezbytný pro stahování potřebných komponent. Pomocí nástroje wget byla načtena databáze reputace IP adres Alienvault, která slouží jako základní vrstva služby. Pro tuto integraci bylo klíčové zahrnutí konkrétní IP adresy útočníka do databáze, čímž se

služby externího vyhodnocování hrozeb přizpůsobilo jedinečnému bezpečnostnímu kontextu systému.

```
$ sudo yum update && sudo yum install -y wget
$ sudo wget https://raw.githubusercontent.com/firehol/blocklist-
ipsets/master/alienvault_reputation.ipset -O
/var/ossec/etc/lists/alienvault_reputation.ipset
$ sudo echo "192.168.0.245" >>
/var/ossec/etc/lists/alienvault_reputation.ipset
$ sudo wget https://wazuh.com/resources/iplist-to-cdblist.py -O
/tmp/iplist-to-cdblist.py
$ sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-to-
cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset
/var/ossec/etc/lists/blacklist-alienvault
$ sudo chown wazuh:wazuh /var/ossec/etc/lists/blacklist-alienvault
```

Poté byla aktualizována konfigurace mechanismu aktivní odezvy Wazuh. Tato aktualizace zahrnovala začlenění nově vytvořeného seznamu do konfigurace systému Wazuh, což systému umožnilo využívat tento soubor dat k určení škodlivých IP adres. Následně bylo v souboru local_rules.xml definováno vlastní pravidlo, které má iniciovat aktivní reakci, kdykoli se IP adresa z černé listiny pokusí o interakci se sítí. Tato příprava se rozšířila na konfiguraci specifických protokolů aktivní odezvy pro různé operační systémy v síti. Na koncových bodech Ubuntu byl použit příkaz firewall-drop, který instruoval iptables, aby zablokoval příchozí spojení z těchto škodlivých IP adres, zatímco na koncových bodech Windows byl strategicky použit příkaz netsh, který za chodu upravil pravidla firewallu a účinně zabránil přístupu z IP adresy útočníka.

```
<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlienVault reputation database.</description>
  </rule>
</group>
```

Obrázek 23 local_rules.xml

```
<ossec_config>
  <active-response>
    <command>netsh</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>
</ossec_config>
```

Obrázek 24 Skript aktivní odezvy koncového bodu systému Windows

Počítač se systémem Windows, na kterém byla umístěna služba Apache, představoval kritické síťové aktivum a potenciální cíl pokusů o neoprávněný přístup. Pro účely tohoto testu byla služba Apache nakonfigurována tak, aby běžela na standardním portu HTTP, takže byla přístupná přes síť. Z odděleného prostředí ve stejné síti, konkrétně z instance WSL2, byl spuštěn příkaz curl, který simuloval pokus o přístup ke službě Apache. Toto nastavení mělo napodobit vzor přístupu neškodného uživatele ke službě.

```
lacinecko@Lacinkov-Kompik:~$ curl --connect-timeout 10 http://192.168.0.245
<html><body><h1>It works!</h1></body></html>
lacinecko@Lacinkov-Kompik:~$ curl --connect-timeout 10 http://192.168.0.245
curl: (28) Connection timeout after 10001 ms
```

Obrázek 25 cURL požadavek na Apache web server

Následně se simulace vystupňovala tak, aby napodobovala pokusy o škodlivý přístup, které byly navrženy tak, aby spustily detekční mechanismy systému Wazuh. Po detekci těchto simulovaných hrozeb byl systém aktivní odezvy Wazuh nakonfigurován tak, aby automaticky provedl příkaz netsh a zablokoval na dobu 60 sekund IP adresu aktéra pokoušejícího se o neoprávněný přístup, čímž efektivně využil firewall hostitele k odmítnutí další komunikace. Po odhalení těchto aktivit sehrála klíčovou roli v celkovém zabezpečení systému Wazuh komponenta SIEM. Generovala výstrahu na ovládacím panelu a informovala správce o zjištěném pokusu o přístup a následné aktivaci mechanismu aktivní reakce. Toto upozornění sloužilo nejen jako upozornění na potenciální narušení bezpečnosti v reálném čase, ale také jako záznam o úspěšném úsilí systému o identifikaci a zmírnění, což dokládá účinnost integrované obranné strategie.

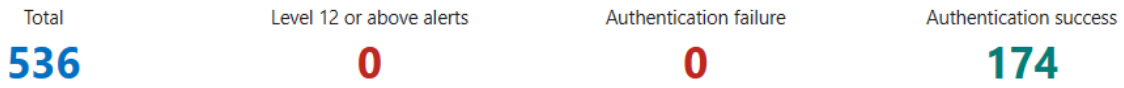
Time	agent.name	rule.description	rule.level	rule.id
Mar 24, 2024 @ 00:33:14.504	ltopolsky-utm-win11	Active response: active-response/bin/netsh.exe - delete	3	657
Mar 24, 2024 @ 00:32:14.243	ltopolsky-utm-win11	Active response: active-response/bin/netsh.exe - add	3	657
Mar 24, 2024 @ 00:32:12.228	ltopolsky-utm-win11	IP address found in AlienVault reputation database.	10	100100

Obrázek 26 SIEM výpis operací

5 Výsledky

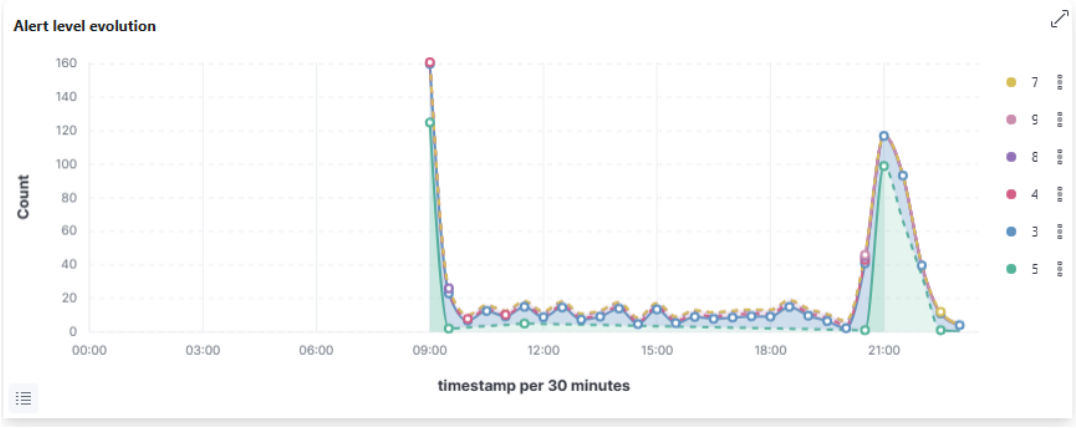
Tato práce o nasazení systému jednotné správy hrozeb na platformě Raspberry Pi 4 přinesla několik klíčových zjištění týkajících se návrhu, funkčnosti a výkonu systému. Integrace systémů Pi-Hole, Pi-VPN, UFW a Wazuh jako hlavních součástí systému UTM prokázala komplexní přístup k zabezpečení sítě, který zahrnuje filtrování DNS, bezpečný vzdálený přístup, správu firewallu a pokročilé funkce detekce hrozeb a reakce na ně.

Fáze testování odhalila, že každá ze součástí významně přispívá k celkové účinnosti systému zabezpečení. Pi-Hole účinně snížil provoz na škodlivé a nežádoucí stránky, čímž zvýšil bezpečnost sítě. Pi-VPN poskytoval robustní a bezpečný vzdálený přístup s využitím silných metod šifrování a ověřování. Úloha UFW jako firewallu zajistila přísné filtrování vstupů a výstupů, čímž se minimalizovaly potenciální vektory útoku. A co je nejdůležitější, nasazení systému Wazuh jako systému XDR a SIEM poskytlo hluboký přehled o činnostech systému a sítě, což usnadnilo včasné odhalení a zmírnění hrozeb. Navzdory omezeným hardwarovým prostředkům počítače Raspberry Pi 4 si systém udržel odpovídající úroveň výkonu. Intenzivní operace, zejména ty, které zahrnovaly komplexní úlohy zpracování a analýzy dat systému Wazuh, však zdůraznily omezení, která jsou vlastní jednodeskovým počítačům při zpracování velkého objemu bezpečnostních dat s vysokou rychlostí. Bezproblémová interakce mezi komponentami byla důkazem dobře navrženého systému.



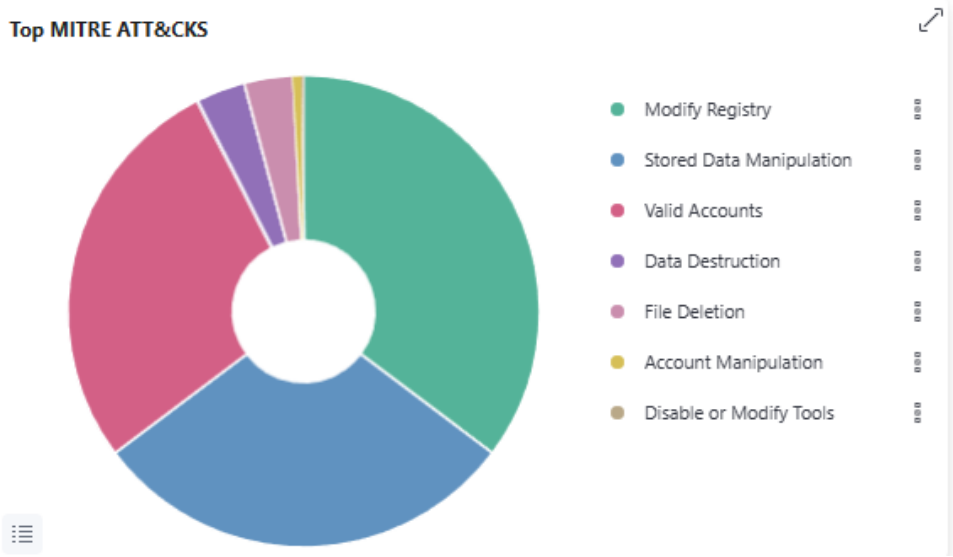
Obrázek 27 Wazuh Dashboard přehled

Zpráva na dashboardu Wazuh poskytuje komplexní analýzu bezpečnostních upozornění generovaných jedním konkrétním agentem za posledních 24 hodin. Během tohoto období bylo zaznamenáno celkem 536 upozornění, která nabízejí přehled o bezpečnostním prostředí, s nímž se agent setkal. Žádný z upozornění zaznamenaných v tomto časovém rámci nepřekročil úroveň závažnosti 12, což naznačuje, že ačkoli objem upozornění byl značný, zjištěné upozornění byly nanejvýš středně závažné. Toto rozložení naznačuje prostředí s převažujícími, ale nikoli kriticky závažnými hrozbami.

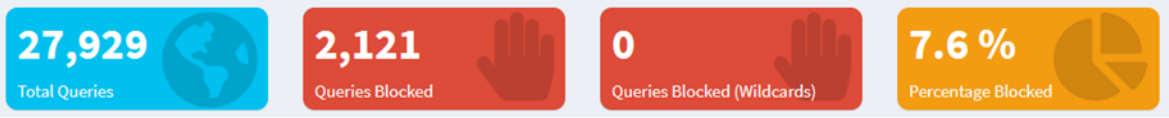


Obrázek 28 Graf četnosti výstrah

Analýza četnosti výstrah odhalila špičku v generování výstrah v 9 hodin ráno a poté 9 hodin večer, což naznačuje časovou koncentraci zjištěných činností nebo hrozeb. Identifikované špičky by mohli naznačovat nějaký vzorec nebo konkrétní událost, která vyvolala nárůst výstrah, což by si zasloužilo další zkoumání. Z údajů vizualizovaných v kruhovém grafu je patrné, že víc jak 90 % tvořili 3 typy z celkových 7 typů výstrah. Nejvíce výstrah, které tvořily 35.25 % celkového počtu, se týkala změn v registru, poté 29.51 % tvořily manipulace s uloženými daty a jako třetí s 27.75 % tvořily výstrahy typu „platný účty“. Naopak výstrahy týkající se zastavení nebo modifikace služby tvořily nejmenší část, pouhých 0,16 %, což naznačuje, že tyto události byly ve sledovaném období zřídkavé.

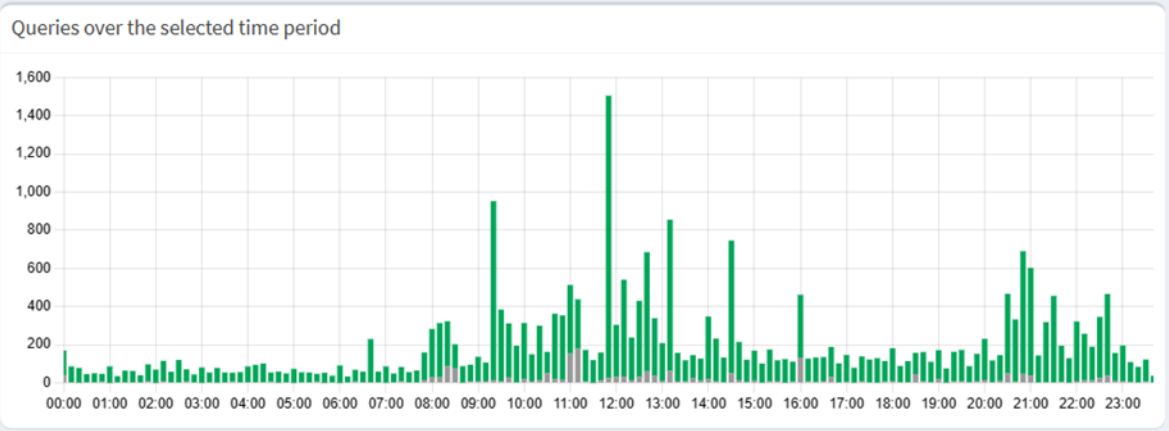


Obrázek 29 Graf zaznamenaných útoků



Obrázek 30 Pi-Hole Dashboard přehled

Zpráva z dashboardu Pi-Hole nabízí podrobné zkoumání aktivit síťových dotazů za období 24 hodin a poskytuje zásadní přehled o filtrování internetového provozu prováděném systémem Pi-Hole v celé síti. Během tohoto sledovaného období bylo v síti zaznamenáno celkem 27 929 dotazů. Z toho bylo úspěšně zablokováno 2 121 dotazů, což představuje míru blokování 7,6 %.



Obrázek 31 Graf četnosti dotazů

Rozložení dotazů, vizualizované v předloženém grafu s granularitou 10 minut, odhaluje dynamiku využívání sítě a filtrační aktivity systému Pi-Hole. Graf rozlišuje mezi povolenými dotazy, zobrazenými zelenými sloupci, a blokovanými dotazy, reprezentovanými šedými sloupci. Analýza grafu poukazuje na špičku v objemu dotazů v období 11:50 - 12:00, kdy bylo zaznamenáno celkem 1 506 dotazů. Z nich bylo povoleno 1 478 a blokováno bylo pouze 26 dotazů. Toto vrcholné období naznačuje okamžik zvýšené aktivity sítě, pravděpodobně v důsledku specifických provozních vzorců nebo vzorců chování uživatelů v prostředí sítě.

```
$ cat /sys/class/thermal/thermal_zone0/temp | awk '{print $1/1000}' | xargs
printf "%.1f°C\n"
```

Pro zjištění teploty procesoru byl použitý hoře vypsaný linuxový příkaz, kterým získáme aktuální teplotu procesoru přímo logů systému, kde je uvedena v milistupních Celsia. Pro účely čitelnosti a praktického sledování byla provedena konverze na stupně Celsia. Výsledkem byla provozní teplota 45,8 stupňů.

Celkově lze říci, že nasazení systému UTM na počítači Raspberry Pi 4 znamenalo výrazné zlepšení obranyschopnosti sítě. Vícevrstvý přístup k zabezpečení, který kombinuje preventivní kontroly se schopnostmi detekce a reakce, nabídl komplexní ochranu proti široké škále kybernetických hrozeb. Systém sice prokazuje robustní bezpečnostní schopnosti a nabízí nákladově efektivní řešení pro malé sítě nebo domácí použití, ale vybízí k dalšímu zkoumání řešení škálovatelnosti, automatizace úkolů údržby a zdokonalených technik integrace.

6 Závěr

Tato diplomová práce se zabývala zkoumáním, implementací a nasazením systému jednotné správy hrozeb na platformě Raspberry Pi 4, podtrhuje potenciál využití kompaktních a cenově výhodných jednodeskových počítačů pro robustní aplikace síťového zabezpečení. Konkrétně se zaměřuje na jedinečné požadavky prostředí malých kanceláří. Integrací systémů Pi-Hole, Pi-VPN, UFW a Wazuh do jediného soudržného systému. Tato práce ukazuje proveditelný návrh pro dosažení komplexní ochrany kybernetické bezpečnosti, která řeší hrozby DNS, zabezpečuje vzdálený přístup, spravuje zásady firewallu a usnadňuje pokročilou detekci hrozeb a reakci na ně, a to vše v rámci omezení malých kanceláří.

Přestože nasazený systém UTM byl slibný, úvahy o projektu naznačují několik možností pro zdokonalení a zlepšení. Zaprvé by se mohl přehodnotit výběr hardwaru, aby se vyřešila výkonnostní omezení, zejména u datově náročných úloh spravovaných systémem Wazuh. Použití výkonnějšího jednodeskového počítače nebo clusteru Raspberry Pi by mohlo tato omezení zmírnit, zvýšit škálovatelnost systému a jeho schopnost zpracovávat a analyzovat bezpečnostní data v reálném čase. Základ položený touto prací nabízí možností dalšího rozvoje. Integrace dalších bezpečnostních vrstev nebo hlubší analýza síťového provozu, by mohla rozšířit možnosti systému UTM. Jako kritická oblast pro rozšíření se jeví automatizace, zejména pokud jde o zefektivnění aktualizací, správu konfigurací a organizování reakcí na zjištěné hrozby, čímž se sníží provozní zátěž a zvýší přizpůsobivost systému novým hrozbám. Přínos této práce pro oblast kybernetické bezpečnosti na jednodeskových počítačích poskytuje rámec pro návrh, implementaci a testování integrovaných bezpečnostních systémů v prostředích s omezenými zdroji. Tato práce navíc obohacuje diskusi o použitelnosti systémů UTM v prostředí malých sítí a nabízí pohled na kompromisy mezi náklady, výkonem a účinností zabezpečení. Práce otevírá několik směrů budoucího výzkumu, včetně zkoumání algoritmů strojového učení pro prediktivní detekci hrozeb anebo vývoje vlastních modulů pro rozšířené bezpečnostní funkce.

Závěrem lze říci, že tato práce nejen rozšiřuje technické znalosti týkající se nasazení systémů jednotné správy hrozeb na jednodeskových počítačích, ale také zdůrazňuje význam inovací a integrace v boji proti kybernetickým hrozbám. Úspěšná implementace a testování systému osvětlují potenciál pro vývoj vysoce účinných a levných bezpečnostních řešení, což

představuje významný krok vpřed při zpřístupňování pokročilých opatření kybernetické bezpečnosti a jejich přizpůsobení širšímu okruhu aplikací a uživatelů.

7 Seznam použitých zdrojů

1. **wallarm.** Unified Threat Management. *wallarm.* [Online] 21. 1 2024. https://www.wallarm.com/what/unified-threat-management.
2. **Tittel, Ed.** *Unified Threat Management For Dummies®, 2nd Fortinet Special Edition.* Hoboken, New Jersey : John Wiley & Sons, Inc., 2016.
3. **Vacca, John.** *Firewalls: Jumpstart for Network and Systems Administrators 1st Edition.* 2004.
4. **Velimirovic, Andreja.** The 8 Types of Firewalls. *phoenixNAP.* [Online] 2. 2 2024. https://phoenixnap.com/blog/types-of-firewalls.
5. **wallarm.** What Is A Firewall And How Does It Work? *wallarm.* [Online] 2. 2 2024. https://www.wallarm.com/what/the-concept-of-a-firewall.
6. **Proofpoint.** What Is an Intrusion Prevention System (IPS)? *Proofpoint.* [Online] 2. 2 2024. https://www.proofpoint.com/us/threat-reference/intrusion-prevention-system-ips.
7. **Smartdataweek.** What is an Intrusion Prevention System? (2024) . *Smartdataweek.* [Online] 2. 2 2024. https://smartdataweek-com.custommapposter.com/article/what-is-an-intrusion-prevention-system.
8. **Bace, Rebecca.** *Intrusion Detection 1st Edition.* Carmel : Sams Publishing, 1999.
9. **Karen Scarfone, Peter Mell.** *Guide to Intrusion Detection and Prevention Systems (IDPS).* s.l. : National Institute of Standards and Technology Special Publication 800-94, 2007.
10. **Incogni.** What is a VPN & how does it work? *Incogni.* [Online] 2. 2 2024. https://blog.incogni.com/what-is-vpn/.
11. **Tsukuba, University of.** Ultimate Powerful VPN Connectivity. *SoftEther VPN.* [Online] 21. 1 2024. https://www.softether.org/1-features/1._Ultimate_Powerful_VPN_Connectivity#SoftEther_VPN's_Solution:_Using_HTTPS_Protocol_to_Establish_VPN_Tunnels.
12. **Ruixi Yuan, W. Timothy Strayer.** *Virtual Private Networks: Technologies and Solutions 1st Edition.* s.l. : Addison-Wesley Professional, 2001.
13. **Taylor, Rebekah.** DNS sinkhole: A tool to help thwart cyberattacks. *Bluecat.* [Online] 21. 1 2024. https://bluecatnetworks.com/blog/dns-sinkhole-a-tool-to-help-thwart-cyberattacks/.
14. **InfoPay.** What Is a DNS Sinkhole? *ID Strong.* [Online] 21. 1 2024. https://www.idstrong.com/sentinel/what-is-a-dns-sinkhole/.
15. **Szor, Peter.** *The Art of Computer Virus Research and Defense.* Boston : Addison-Wesley Professional, 2005.
16. **Boehm, Amber.** WHAT IS DATA LOSS PREVENTION (DLP)? *CROWDSTRIKE.* [Online] 21. 1 2024. https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/.
17. **Palo Alto Networks.** Palo Alto Networks. *What is the Difference Between XDR vs. SIEM?* [Online] 29. 3 2024. https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem.
18. **Wazuh.** Wazuh. *Active XDR protection from modern threats.* [Online] 29. 3 2024. https://wazuh.com/platform/xdr.
19. —. Wazuh. *Components.* [Online] 29. 3 2024. https://documentation.wazuh.com/current/getting-started/components/index.html.
20. **Xcitium.** Benefits of Unified Threat Management System for SMEs. *Xcitium.* [Online] 21. 1 2024. https://www.xcitium.com/unified-threat-management/.

21. **Firewall, NGFW vs UTM.** NGFW vs UTM Firewall. *Zenzamor.* [Online] 21. 1 2024. https://www.zenarmor.com/docs/network-security-tutorials/ngfw-vs-utm-firewall.
22. **Buckbee, Michael.** What is The Cyber Kill Chain and How to Use it Effectively. *Varonis.* [Online] 2. 2 2024. https://www.varonis.com/blog/cyber-kill-chain.
23. **Hewko, Alex.** STRIDE THREAT MODELING: WHAT YOU NEED TO KNOW. *Software Secured.* [Online] 2. 2 2024. https://www.softwaresecured.com/post/stride-threat-modeling.
24. **Eben Upton, Gareth Halfacree.** *Raspberry Pi User Guide 2nd Edition.* Hoboken : Wiley, 2013.
25. *Applications of the Single Board Computers in the Software Defined Radio Systems.* **Jovanovic, Predrag & Mileusnic, Mladen & Pavic, Branislav & Miskovic, Boris.** 2014, SINTEZA.
26. **Bowers, Nat.** Then and now: a brief history of single board computers. *Electronic Specifier.* [Online] 1. 2 2024. https://www.electronicspecifier.com/products/communications/then-and-now-a-brief-history-of-single-board-computers.
27. **Swift, Malia.** History Of Single Board Computers. *The World Beast.* [Online] 1. 2 2024. https://www.theworldbeast.com/history-of-single-board-computers.html.
28. **ExplainingComputers.com.** Single Board Computers. *Explaining Computers.* [Online] 1. 2 2024. https://www.explainingcomputers.com/sbc.html.
29. **Team, DevicePlus Editorial.** The History of Raspberry Pi. *Device Plus.* [Online] 2. 2 2024. https://www.deviceplus.com/raspberry-pi/the-history-of-raspberry-pi/.
30. **Piltch, Avram.** Tom's Hardware. *Raspberry Pi 4: Review, Buying Guide and How to Use.* [Online] 29. 3 2024. https://www.tomshardware.com/reviews/raspberry-pi-4.
31. **RPishop.cz.** RPishop.cz. *Argon ONE V2.* [Online] 29. 3 2024. https://rpishop.cz/raspberry-pi-4/2067-argon-one-case-s-vetrackem-a-vypinacem-pro-raspberry-pi-4b-hlinik.html.
32. **Halfacree, Gareth.** TheMagPi. *Group test: Best Raspberry Pi 4 thermal cases tested and ranked.* [Online] 29. 3 2024. https://magpi.raspberrypi.com/articles/group-test-best-raspberry-pi-4-thermal-cases-tested-and-ranked.
33. **Geerling, Jeff.** Raspberry Pi Dramble. *Power Consumption Benchmarks.* [Online] 29. 3 2024. https://www.pidramble.com/wiki/benchmarks/power-consumption.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek