Universitatea „Ştefan cel Mare” - Suceava
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor

TEZĂ DE DOCTORAT

- REZUMAT-

Contribuții la Securizarea Transportului de Date în Sistemele IoT

Doctorand:
ing. Daniel-Florin Hrițcan

Conducător de doctorat:
prof. univ. dr. ing. Adrian Graur

Mulțumiri

Adresez mulțumirile mele Prof. univ. dr. ing. **Adrian GRAUR**. Îndrumarea dumneavoastră mi-a servit drept busolă înțelepciunea, răbdarea și încurajările dumneavoastră au transformat provocările în succese. Vă mulțumesc că ați crezut în mine încă de la început.

Adresez multumirile mele comisiei de îndrumare, Prof. dr. ing. **Alin-Dan POTORAC,** Ș.l. dr. ing. **Doru- Gabriel BĂLAN,** prof.univ. dr. ing. **Constantin FILOTE,** care prin perspectivele lor riguroase și reacțiile constructive și perinente au condus la perfecționarea muncii depuse și m-au ajutat să tind spre a excela în unele din cercetările mele. Expertiza dumnealor stă la baza acestei finalizări de etapă, iar eu sunt profund onorat de timpul și încrederea de care am beneficiat în acești ani.

Țin să multumesc membrilor comisiei de evaluare, respectiv **Prof.univ.dr.ing. Răzvan-Victor RUGHINIȘ**, **Conf.univ.dr.ing. Ciprian-Pavel OPRIȘA**, **Prof.univ.dr.ing. Alin-Dan POTORAC**, **Prof.univ.dr.ing. Corneliu-Octavian TURCU**, care au binevoit să analizeze și să facă observațiile necesare pentru susținerea publică a tezei, cu mulțumiri pentru timpul acordat, părerile și contribuțiile aduse, pentru deplasarea la Suceava în vederea susținerii tezei.

Aduc mulțumiri **părinților mei,** cuvintele nefiind suficiente pentru a exprima sacrificiile pe care le-au făcut, dragostea pe care mi-au oferit-o și încrederea de care am beneficiat, pentru nopțile târzii sau în momente de îndoială. Sunteți cea mai mare forță a mea și Vă mulțumesc pentru tot.

Nu în ultimul rând, aduc mulțumiri Centrului integrat de cercetare, dezvoltare şi inovare pentru Materiale Avansate, Nanotehnologii şi Sisteme Distribuite de fabricaţie şi control (MANSiD, 671/09.04.2015) al Universităţii *Ştefan cel Mare* din Suceava în perioada 2021 – 2025, pentru facilitarea obținerii rezultatelor experimentale într-un procent semnificativ.

Cuprins

Lista de figuri

Lista de tabele

Lista de abrevieri

ABE - Attribute-Based Encryption
AI – Artificial Inteligence
AMQP - Advanced Message Queuing Protocol
AODV - Ad Hoc On-Demand Distance Vector
ARP - Address Resolution Protocol
CapEx - Capital Expenditure
CGNAT - Carrier-Grade Network Address Translation
CoAP - Constrained Application Protocol
DDoS - Distributed Denial of Service
DNS - Domain Name System
DoS - Denial of Service
DTLS - Datagram Transport Layer Security
ESX - Elastic Sky X
GSM - Global System for Mobile Communications
GUI - Graphical User Interface
HTTP – Hypertext Transfer Protocol
HTTPS - HyperText Transfer Protocol Secure
IDS - Intrusion Detection System
IoT - Internet of Things
IP - Internet Protocol
iSCSI - Internet Small Computer System Interface
LAN - Local Area Network
LTE - Long Term Evolution
MAC – Media Access Control Address
MITM - Man-in-the-Middle
MQTT - MQ Telemetry Transport
NAS - Network-Attached Storage
NAT - Network Address Translation
OpEx - Operating Expense
RAID - Redundant Array of Independent Disk
RAM - Random-Access Memory
RRD - Round Robin Database
RREP - Route Reply
RREQ - Route Request
SDN - Software-Defined Networking
SSL - Secure Sockets Layer
SSO - Single Sign-On
TCP - Transmission Control Protocol
TLS - Transport Layer Security
UDP - User Datagram Protocol
VLAN - Virtual Local Area Network
VPN - Virtual Private Network
VPS - Virtual Private Server
WAN - Wide Area Network
Wi-Fi - Wireless Fidelity
WPA - Wi-Fi Protected Access
WSN - Wireless Sensor Network
XMPP - Extensible Messaging and Presence Protocol

Glosar de termeni

ACME = este un protocol care automatizează obținerea și reînnoirea certificatelor TLS. Acesta permite unui server să comunice direct cu o autoritate (precum Let's Encrypt) pentru a dovedi proprietatea domeniului și a instala securitatea HTTPS fără intervenție manuală.

API = (*Application Programming Interface* – Interfață de Programare a Aplicațiilor) este un ansamblu de definiții și protocoale care permite unui *software* să comunice și să schimbe date cu un altul în mod automat.

ARP (*Address Resolution Protocol*) este un protocol de rețea care asociază adresele IPv4 cu adresele MAC în rețelele locale prin intermediul cererilor și răspunsurilor de difuzare, permițând transmiterea cadrelor *Ethernet*; este vulnerabil la atacuri ARP *spoofing/poisoning*, în care atacatorii trimit răspunsuri false pentru a corupe *cache*-urile ARP.

Bare-metal într-un system de calcul aplicațiile rulează direct pe hardware, fără suprasarcina generată de sistemul de operare sau de hipervizor, maximizând performanța, predictibilitatea și securitatea fiind ideal pentru dispozitivele IoT *edge* care funcționează în timp real (de exemplu, *gateway*-uri Zigbee, senzori LoRaWAN) sau pentru sistemele încorporate care necesită o latență redusă, spre deosebire de mediile virtualizate; este utilizat în *firmware*-ul critic, unde vulnerabilitățile sistemului de operare sunt inacceptabile.

Bitrate sau rata de transfer este numărul de biți transmiși pe secundă (bps, kbps, Mbps) pe un canal de comunicație, determinând capacitatea de transfer a datelor.

Blockchain este un registru distribuit, descentralizat și imuabil, care conține blocuri de tranzacții legate criptografic prin consens, permițând partajarea de date într-un mod protejat împotriva falsificării,

Bluetooth Low Energy (BLE) este un protocol wireless cu consum redus de energie (Bluetooth 4.0+) destinat conexiunilor IoT pe distanțe scurte (~10-50 m), ideal pentru dispozitive purtabile, balize și senzori, cu viteze de transfer de date de până la 2 Mbps și un consum extrem de redus de energie, care permite funcționarea timp de ani de zile cu baterii tip pastilă, spre deosebire de tehnologia Zigbee, orientată către rețele *mesh* de dimensiuni mai mari.

Brute-force = este un atac care încearcă toate parolele sau cheile posibile până când este găsită cea corectă, bazându-se pe calcul și timp. Acesta este contracarat prin parole puternice, limitarea vitezei și autentificarea cu mai mulți factori.

Bufferbloat apare atunci când routerele/*switch*-urile utilizează memorii tampon excesiv de mari, care se umplu în timpul congestiei, provocând vârfuri de latență ridicate (sute de milisecunde), jitter și pierderi de lățime de bandă ceea ce afectează aplicațiile IoT în timp real, precum fluxurile video Zigbee sau comunicațiile VoIP prin *gateway*-uri WiFi.

CRYSTALS-Kyber = *Cryptographic Suite for Algebraic Lattices – Kyber* este un mecanism de încapsulare a cheilor bazat pe latici, conceput pentru a rezista atacurilor cibernetice lansate de viitoarele calculatoare cuantice. Acesta face parte din proiectul de criptografie post-cuantică (*Post-Quantum Cryptography - PQC*) și a fost selectat de către NIST (*National Institute of*

Standards and Technology – Institutul Național de Standarde și Tehnologie) ca standard principal pentru securizarea schimbului de chei pe internet.

DNS (*Domain Name System*) = este un sistem care traduce numele de domenii în adrese IP, permițând calculatoarelor să găsească servicii pe internet.

Edge computing = dispositive ce procesează datele în apropierea sursei lor, cum ar fi dispozitivele IoT sau serverele locale, în locul centrelor cloud îndepărtate. Acest lucru reduce latența, economisește lățime de bandă și sporește performanța în timp real pentru aplicații precum fabricile inteligente și vehiculele autonome.

ETSI oneM2M = reprezintă un standard global de interoperabilitate dezvoltat de (Institutul European pentru Standarde în Telecomunicații, în colaborare cu alți parteneri internaționali, pentru a crea o arhitectură comună în domeniul *Machine-to-Machine*. Acesta funcționează ca un strat intermediar de servicii (*middleware*) care permite dispozitivelor și aplicațiilor din ecosistemul Internetul Lucrurilor să comunice unitar, indiferent de producător sau de tehnologia de rețea utilizată. Prin acest cadru, oneM2M simplifică gestionarea datelor și securitatea, eliminând barierele dintre platformele *software* izolate și facilitând dezvoltarea sistemelor inteligente la scară largă.

Firewall = un dispozitiv sau un program de securitate a rețelei care monitorizează și controlează traficul de intrare și de ieșire pe baza unor reguli de securitate prestabilite.

Firmware = este „*software*-ul *hardware*-ului”, adică setul de instrucțiuni de bază stocat permanent pe un dispozitiv pentru a-i permite să pornească și să funcționeze corect. Acesta acționează ca un intermediar vital între componentele fizice și restul sistemului, fiind prezent în aproape orice, de la telecomenzi la routere.

Gateway = în domeniul rețelelor, este un dispozitiv sau un program care conectează rețele care utilizează protocoale diferite, traducând și dirijând traficul între acestea ca un traducător între sisteme diferite.

Hash = o funcție criptografică unidirecțională care transformă date de intrare arbitrare într-un rezultat de dimensiune fixă (valoare *hash/digest*), permițând verificarea integrității datelor, stocarea parolelor (*hash*-uri cu salt) și semnăturile digitale fiind rezistent la coliziuni (este dificil să se găsească două intrări care să genereze același rezultat), precum SHA-256; este utilizat în tehnologia blockchain (arbori Merkle) și în securitatea IoT (verificări de *firmware*), spre deosebire de criptarea reversibilă.

Hotspot = este o locație fizică sau un dispozitiv care oferă acces la internet fără fir prin Wi-Fi, permițând dispozitivelor din apropiere, precum telefoanele și laptopurile, să se conecteze la internet prin intermediul unui abonament de date mobile sau al unei conexiuni prin cablu.

Hypervizor = un program, un *firmware* sau un component *hardware* care creează și gestionează mașini virtuale (VM) prin abstractizarea și partajarea resurselor hardware fizice, precum procesorul, memoria și spațiul de stocare, între mai multe sisteme de operare oaspete.

Intrusion detection system (IDS) = este un instrument de securitate care monitorizează activitățile din rețea sau din sistem pentru a depista acțiuni rău intenționate sau încălcări ale politicilor, avertizând administratorii cu privire la potențialele amenințări.

Load balancer = este un dispozitiv sau un program de rețea care distribuie uniform traficul primit între mai multe servere pentru a optimiza utilizarea resurselor, a preveni supraîncărcarea și a asigura o disponibilitate ridicată. Poate fi folosit și ca punct de intrare într-o rețea prin intermediul TLS.

LoRaWAN = este un protocol de rețea de mare acoperire cu consum redus de energie (LPWAN) destinat dispozitivelor IoT cu rază lungă de acțiune (~2-15 km), care utilizează o topologie în stea cu *gateway*-uri pentru transmisii sporadice de date de dimensiuni reduse (până la 50 kbps) de la senzori alimentați cu baterii din agricultură, orașe inteligente și monitorizare spre deosebire de rețeaua mesh a Zigbee pentru locuințe cu rază scurtă de acțiune sau de rețeaua în stea a BLE pentru dispozitive purtabile cu consum energetic extrem de redus.

Man-in-the-Middle = este un atac ce interceptează și retransmite comunicațiile dintre două părți (de exemplu, între un dispozitiv și o poartă de acces în rețelele Zigbee sau LoRaWAN) pentru a intercepta, modifica datele sau a se da drept dispozitive finale fără a fi detectat acest lucru fiind posibil prin falsificarea adreselor ARP sau criptarea slabă; atacul poate fi prevenit prin utilizarea TLS/HTTPS, fixarea certificatelor, rețelele VPN sau autentificarea reciprocă.

Mesh = este un tip de rețea cu o topologie descentralizată în care fiecare nod (dispozitiv) se conectează direct la mai multe alte noduri, retransmitând datele prin intermediul unor căi de difuzare sau de rutare cu capacitate de auto-reparare (rerutare automată în cazul unor defecțiuni) pentru a asigura o acoperire fiabilă utilizată în Zigbee pentru casele IoT, spre deosebire de topologiile în stea din BLE/LoRaWAN.

Modelul OSI = un cadru teoretic utilizat pentru a înțelege și a standardiza modul în care computerele comunică într-o rețea. Acesta împarte întregul proces de transmitere a datelor în șapte straturi distincte, fiecare având o funcție specifică și comunicând cu straturile adiacente (cel de deasupra și cel de dedesubt).

OWASP CRS = un set de reguli *open-source* pentru *firewall*-uri *web* care detectează și blochează automat atacurile cibernetice generice, precum SQL *Injection* sau XSS, înainte ca acestea să ajungă la aplicație.

Passthrough = în domeniul informatic această tehnologie oferă unei mașini virtuale acces direct la hardware (de exemplu, GPU, USB, NIC) prin intermediul IOMMU (VT-d/AMD-Vi), ocolind suprasarcina hipervizorului pentru a obține o performanță aproape de cea nativă — soluție ideală pentru *gateway*-urile IoT care rulează stive Zigbee/LoRaWAN sau procesează date în timp real la marginea rețelei, beneficiind în același timp de eficiența unui sistem „bare-metal”, spre deosebire de I/O-ul emulat sau paravirtualizat.

Phishing = este un atac cibernetic în care atacatorii se dau drept entități de încredere prin e-mail, mesaje text sau site-uri web false pentru a-i determina pe utilizatori să dezvăluie date sensibile, precum parole, numere de carduri de credit sau date de autentificare.

Port forwarding = este o tehnică de configurare a router-ului care direcționează traficul de intrare pe un anumit port către un dispozitiv și un port specific din cadrul unei rețele private, permițând accesul extern la serviciile interne.

Reverse proxy = funcționează ca *server*-ul expus publicului: acesta gestionează întregul proces de stabilire a conexiunii TLS, încheie criptarea folosind propriul certificat și

redirecționează traficul HTTP necriptat (sau recriptat) către serviciile interne. Acest lucru ascunde detaliile *server*-ului din spate, permite stocarea în *cache* și compresia și facilitează rescrierea adreselor URL sau autentificarea printr-un singur punct de acces.

Router = dispozitiv de rețea care transmite pachete de date între rețelele de calculatoare, facilitând comunicarea între dispozitive precum modemul de acasă și internetul.

SDK = (*Software Development Kit* – Set de Dezvoltare *Software*) este o colecție de instrumente, biblioteci de cod, documentație și procese de testare puse la dispoziția programatorilor pentru a crea aplicații destinate unei platforme specifice sau unui anumit sistem de operare.

Side-channel acest tip de atac exploatează scurgeri fizice neintenționate, precum sincronizarea, consumul de energie, radiațiile electromagnetice sau sunetele emise de *hardware/software* în timpul operațiunilor de criptare, pentru a recupera informații confidențiale (de exemplu, chei), spre deosebire de bruiajul activ; măsurile de atenuare includ codul cu timp constant, mascarea, injectarea de zgomot și ecranarea *hardware*.

Spoofing = este un atac cibernetic în care un atacator se dă drept un utilizator, un dispozitiv sau o sursă legitimă, falsificând date de identitate precum adresele IP, anteturile de e-mail sau ID-ul apelantului, pentru a obține acces neautorizat sau pentru a induce în eroare sistemele/utilizatorii.

Sweep sau bruierea prin baleiaj este un tip de atac de bruiere în care dispozitivul de bruiere baleiază rapid un semnal pe o bandă de frecvență (de exemplu, 2,4 GHz pentru Zigbee/BLE sau 868 MHz pentru LoRaWAN), perturbând comunicațiile prin suprapunerea temporară a semnalelor legitime pe măsură ce trece; această metodă este eficientă împotriva protocoalelor IoT cu canal fix, dar poate fi contracarată prin tehnici de salt de frecvență sau de spectru împrăștiat.

Sybil = este un atac ce are loc atunci când o entitate rău intenționată creează mai multe identități false (noduri/conturi) pentru a obține o influență disproporționată în rețelele *peer-to-peer*, precum *blockchain*, rețelele de senzori fără fir (WSN) sau rețelele IoT *mesh* (de exemplu, Zigbee), ceea ce permite manipularea voturilor, epuizarea resurselor sau perturbarea rutării aceste atacuri fiind prevenite prin validarea identității (PKI, PoW), testarea resurselor (PoS) sau autorități de încredere.

Wormhole (atacul "gaură de vierme") = este un atac ce presupune colaborarea unor noduri rău intenționate care redirecționează pachetele între puncte de rețea îndepărtate printr-o legătură cu latență redusă (de exemplu, prin cablu sau *wireless* de lungă distanță), creând o falsă proximitate pentru a scurta rutele în rețelele *mesh*/*ad-hoc* precum Zigbee perturbând rutarea, facilitând atacurile DoS sau analiza traficului; este detectat/contracarat prin tehnici precum „*packet leashes*", măsurarea timpului de dus-întors sau verificarea vecinilor.

Zigbee = este un protocol wireless de mică putere și rază scurtă de acțiune (IEEE 802.15.4) destinat Internetului obiectelor (IoT) și caselor inteligente, care utilizează rețele *mesh* pentru o comunicare eficientă și sigură între dispozitive pe o distanță de 10-100 m, cu un consum energetic minim.

1. Introducere

Internetul obiectelor a transformat fundamental paradigmele de achiziție și transmitere a datelor în domenii precum automatizarea industrială, monitorizarea sănătății și infrastructura orașelor inteligente. Constrângerile de resurse inerente dispozitivelor IoT necesită compromisuri între capacitățile de calcul și mecanismele de securitate, ducând adesea la slăbirea pozițiilor defensive față de sistemele tradiționale. Mediile IoT se confruntă cu vectori de atac din ce în ce mai sofisticați, vizând fiecare strat al modelului OSI, necesitând strategii de apărare cuprinzătoare [1].

Proliferarea masivă a dispozitivelor conectate introduce provocări profunde de securitate, diferite de paradigmele tradiționale. Natura eterogenă a sistemelor IoT combinând dispozitive de la mai mulți producători cu capacități, implementări de securitate și protocoale de comunicare diferite creează o complexitate fără precedent în realizarea unei posturi de securitate cuprinzătoare [2]. Soluțiile tradiționale de securitate, concepute pentru stații de lucru puternice, se dovedesc inadecvate pentru dispozitivele IoT cu putere de procesare, memorie și bugete energetice minime [3].

Natura wireless a majorității comunicațiilor IoT expune transportul de date la atacuri de interceptare, bruiaj, manipulare a semnalelor și atacuri la nivel fizic. Dispozitivele alimentate cu baterii trebuie să mențină o durată de funcționare de luni sau ani, limitând complexitatea mecanismelor de securitate care pot fi implementate fără a epuiza rapid energia disponibilă [4]. Securitatea eficientă necesită implementări integrate pe mai multe niveluri, recunoscând că niciun control de securitate nu este impenetrabil. Vulnerabilitățile de securitate se extind pe toate straturile stivei de rețea, creând suprafețe de atac multilaterale pe care adversarii le pot exploata sistematic [5].

1.1 Motivație și rolul cercetării

Un factor critic pentru cercetarea intensivă în domeniul securității transportului de date IoT este asimetria dintre ceea ce pot face apărătorii și ceea ce pot face atacatorii. Apărătorii acționează în condiții restrictive: trebuie să mențină compatibilitatea cu dispozitivele existente, să echilibreze securitatea cu costurile și consumul de energie și să implementeze soluții care funcționează în medii eterogene. Atacatorii nu se confruntă cu astfel de constrângeri. Ei pot viza cea mai slabă implementare dintre miliarde de dispozitive. Pot aștepta momentul perfect în care un dispozitiv este vulnerabil.

Pot utiliza tehnici sofisticate de la analiza canalelor laterale la manipularea lanțului de aprovizionare care necesită resurse și expertiză care depășesc ceea ce majoritatea organizațiilor pot implementa. Această asimetrie se adâncește, în loc să se reducă. Pe măsură ce implementările IoT se extind și devin mai critice pentru infrastructură, stimulentele financiare pentru atacarea sistemelor IoT cresc. Statele naționale vizează acum în mod activ dispozitivele IoT ca parte a operațiunilor strategice. Organizațiile criminale exploatează compromiterile IoT pentru fraudă, *ransomware* și furt de date. Actorii individuali experimentează noi tehnici de atac și le împărtășesc prin forumuri subterane. Între timp, multe organizații care implementează dispozitive IoT nu dispun nici măcar de practici de securitate de bază, creând medii în care atacatorii se confruntă cu o rezistență minimă.

Comunitatea de cercetare a rămas în mare măsură în urmă în ceea ce privește dezvoltarea unor măsuri de apărare adecvate acestui peisaj advers. Majoritatea cercetărilor în domeniul securității IoT se concentrează pe probleme izolate – securizarea unui singur protocol, apărarea unui anumit tip de dispozitiv sau implementarea unui mecanism criptografic specific – în loc

să abordeze vulnerabilitățile sistemice care afectează întregul ecosistem. Ceea ce este necesar este fundamental diferit: cercetări care abordează securitatea transportului de date IoT ca o problemă de sistem care necesită soluții coordonate la nivel fizic, de rețea, de transport și de aplicații.

Pentru a înțelege de ce securitatea transportului datelor IoT necesită cercetări intensive, luați în considerare consecințele în cascadă atunci când securitatea transportului eșuează. Sistemele de monitorizare IoT ale unui spital ar putea fi compromise, ducând la alarme false sau alerte ratate cu privire la starea pacienților, amenințând direct viețile. Rețeaua de senzori a unei instalații industriale ar putea fi atacată, ducând la decizii incorecte de control al proceselor care deteriorează echipamentele sau creează pericole pentru siguranță. Infrastructura de comunicații a unei rețele inteligente ar putea fi perturbată, ducând la întreruperi de curent care afectează sute de mii de oameni.

Telemetria unui vehicul conectat ar putea fi interceptată, dezvăluind locația și modelele de comportament care pun în pericol ocupanții sau permit atacuri fizice. Acestea nu sunt scenarii teoretice. Fiecare dintre ele a fost documentat ca fiind real. Ceea ce le face deosebit de îngrijorătoare este faptul că ele se datorează adesea unor defecțiuni fundamentale în securitatea transportului de date: canale de comunicare care nu dispun de criptare adecvată, autentificare care nu este implementată sau este implementată incorect, controale de autorizare care nu împiedică accesul neautorizat sau sisteme de monitorizare care nu detectează compromiterea canalelor de comunicare.

Motivația pentru cercetarea intensivă în domeniul securizării transportului de date în sistemele IoT are la bază convergența mai multor factori critici. În primul rând, implementarea IoT se accelerează dramatic, cu miliarde de dispozitive conectate în prezent și altele care se conectează în fiecare zi. În al doilea rând, securitatea acestor implementări rămâne fundamental inadecvată, multe dispozitive funcționând fără o protecție semnificativă. În al treilea rând, consecințele eșecurilor de securitate ale IoT sunt din ce în ce mai grave, variind de la încălcări ale confidențialității la incidente de siguranță și întreruperi ale infrastructurii. În al patrulea rând, soluțiile de securitate existente, concepute pentru contexte diferite, nu funcționează eficient în mediul IoT. Și, în al cincilea rând, comunitatea de cercetare abia a început să abordeze această problemă în mod cuprinzător.

Provocarea cercetării nu este doar tehnică, ci și profund practică: cum putem crea soluții de securitate suficient de robuste pentru a împiedica atacatorii hotărâți să reușească, dar suficient de simple încât dispozitivele cu resurse limitate să le poată implementa? Cum implementăm aceste soluții pe miliarde de dispozitive existente care nu au fost proiectate având în vedere acest nivel de securitate? Cum menținem securitatea chiar și pe măsură ce peisajul tehnologic continuă să evolueze? Cum echilibrăm nevoia de protecție puternică cu realitățile economice care limitează investițiile companiilor în securitate?

1.2 Structura tezei

Teza este structurată în șapte capitole. Capitolul 1 stabilește bazele cercetării, identificând problema centrală: arhitecturile de securitate existente nu au reușit să țină pasul cu proliferarea IoT. Capitolul 2 prezintă o taxonomie sistematică a vulnerabilităților IoT, analizate per strat OSI. Capitolul 3 descrie cadrul metodologic și platforma de testare experimentală. Capitolul 4 introduce cadrele de securitate originale propuse, combinând arhitecturi de rețea îmbunătățite, mecanisme adaptive și protocoale de comunicare sigure. Capitolul 5 prezintă concluziile și direcțiile viitoare de cercetare, inclusiv paradigme de învățare federată, criptografie post-cuantică și integrarea cu arhitecturi 6G emergente.

2. Analiza stadiului actual al vulnerabilităților IoT

2.1 Introducere și obiectivele analizei

Pentru a propune soluții eficiente de securizare a sistemelor IoT este esențial să se cunoască tipologia vulnerabilităților existente, amploarea lor statistică și soluțiile propuse în literatura de specialitate. Prezentul capitol reprezintă o sinteză critică și sistematică a stadiului tehnicii, structurată pe trei dimensiuni: clasificarea conceptuală a vulnerabilităților, analiza per strat OSI și evaluarea paradigmelor emergente de securitate.

Conform raportului ENISA Threat Landscape 2024 [106], în intervalul iulie 2023 – iunie 2024 au fost identificate peste 19.754 de vulnerabilități, dintre care 9,3% critice și 21,8% cu risc înalt. Atacurile DDoS au depășit *ransomware*-ul ca cel mai frecvent tip de incident. Dispozitivele IoT constituie un vector major, continuând tendința documentată din 2016, odată cu emergența *botnet*-ului Mirai [56]. Obiectivele analizei sunt: identificarea și clasificarea vulnerabilităților IoT; analiza pe straturile modelului OSI; evaluarea tehnologiilor emergente; identificarea lacunelor care motivează contribuțiile din Capitolul 4.

2.2 Elemente de clasificare a vulnerabilităților IoT

Vulnerabilitățile hardware includ atacuri de *side-channel* (analiza consumului de putere, emisii electromagnetice, variații de temporizare), capturarea fizică a dispozitivelor și extragerea *firmware*-ului prin interfețe de depanare expuse (JTAG, UART). Mecanismele de actualizare nesigure permit atacuri *rollback* sau injecție de *firmware* malițios [57]. Practicile deficitare de gestionare a cheilor criptografice codificarea cheilor direct în *firmware*, reutilizarea cheilor, stocarea în memorie neprotejată transformă criptarea dintr-o protecție robustă într-un fals sentiment de securitate [58].

Protocoalele concepute pentru eficiență în medii cu resurse limitate (CoAP, MQTT, 6LoWPAN) introduc compromisuri de securitate. MQTT, originar din rețele private industriale, nu includea mecanisme native de criptare sau autentificare puternică [46]. CoAP, bazat pe UDP, este vulnerabil la *spoofing* IP și atacuri de amplificare [50]. Cea mai prevalentă categorie operațională rămâne utilizarea credențialelor implicite: *botnet*-ul Mirai (2016) a exploatat 62 de perechi implicite username/parolă, infectând peste 600.000 de dispozitive. Descendentul Aisuru (august 2024) a acumulat peste 300.000 de dispozitive compromise și a generat atacuri record de 5,6 Tbps [107].

TABEL I. CLSIFICAREA TRANSVERSALĂ A VULNERABILITĂȚILOR IOT DUPĂ NATURA LOR [SURSA: AUTORUL]

Categorie	**Exemple reprezentative**	**Frecvență exploatare (ENISA)** [106]	**Impact potențial**
Hardware & Firmware	Side-channel, capturare fizică, biblioteci terțe vulnerabile, rollback firmware	Moderat – țintit	Compromitere completă a dispozitivului, exfiltrare chei
Protocol & Transport	MQTT fără TLS, CoAP UDP spoofing,	Ridicat - automatizat	Interceptare date, DoS, MITM

	RPL rank manipulation, replay attacks		
Configurare & Operare	Credențiale implicite, ACL permisive, absența segmentării rețelei	Foarte ridicat - botnet	Compromitere în masă, DDoS record

2.3 Nivelul fizic

Nivelul fizic cuprinde componentele hardware, mediile de transmisie, caracteristicile semnalului și schemele de modulație care stau la baza tuturor comunicațiilor în rețea [6]. În sistemele IoT, tehnologiile wireless predomină: LoRaWAN, ZigBee, Bluetooth Low Energy (BLE) și protocoalele celulare servesc fiecare scenarii de implementare distincte [7]. LoRaWAN este utilizat pe scară largă pentru aplicații IoT cu rază lungă de acțiune și consum redus de energie, permițând transmiterea datelor pe distanțe considerabile cu funcționare a bateriei de ani de zile. Atacurile la nivelul fizic includ detectarea pasivă a semnalelor, atacuri de inferență, bruiaj activ și manipularea semnalelor fără detecție [8].

TABEL II. VULNERABILITĂȚI NIVEL FIZIC: SEVERITATE, SOLUȚII ȘI OVERHEAD ESTIMAT [SURSA: AUTORUL]

Vulnerabilitate	Severitate	Soluție principală	Overhead estimat
Interceptare semnal (eavesdropping) [11]	ÎNALT	Spectru împrăștiat + criptare strat superior [15]	Moderat (+15% BW)
Bruiaj (jamming) [12]	ÎNALT	Diversitate frecvență/antenă, salt de frecvență [18]	Redus (+5% latență)
Atac side-channel [13]	CRITIC	Calcul cu timp constant, mascarea puterii [17]	Ridicat (+20–30% cicli)
Capturare dispozitiv [14]	CRITIC	Boot securizat, stocare hardware chei (TPM/SE) [57]	Neglijabil runtime
Gateway fals (rogue gateway) [9]	ÎNALT	RFFI autentificare hardware, certificate X.509 [16]	Moderat

2.4 Nivelul de legătură de date

Nivelul de legătură de date organizează semnalele fizice brute în cadre structurate, gestionând adresarea dispozitivelor prin adrese MAC și coordonând accesul la mijloace de transmisie wireless [19]. În mediile IoT, standardul IEEE 802.15.4 constituie baza pentru ZigBee și 6LoWPAN, stabilind formate de cadre consistente și mecanisme de control al accesului [20]. Atacurile de *spoofing* al adreselor MAC manipulează informațiile de adresare

pentru a se da drept dispozitive legitime, permițând redirecționarea traficului sau accesul neautorizat la rețea. Când rutarea se bazează exclusiv pe adrese MAC fără autentificare suplimentară, atacatorii pot falsifica cu ușurință adresele sursă sau destinație, redirecționând traficul prin sisteme controlate de ei [23].

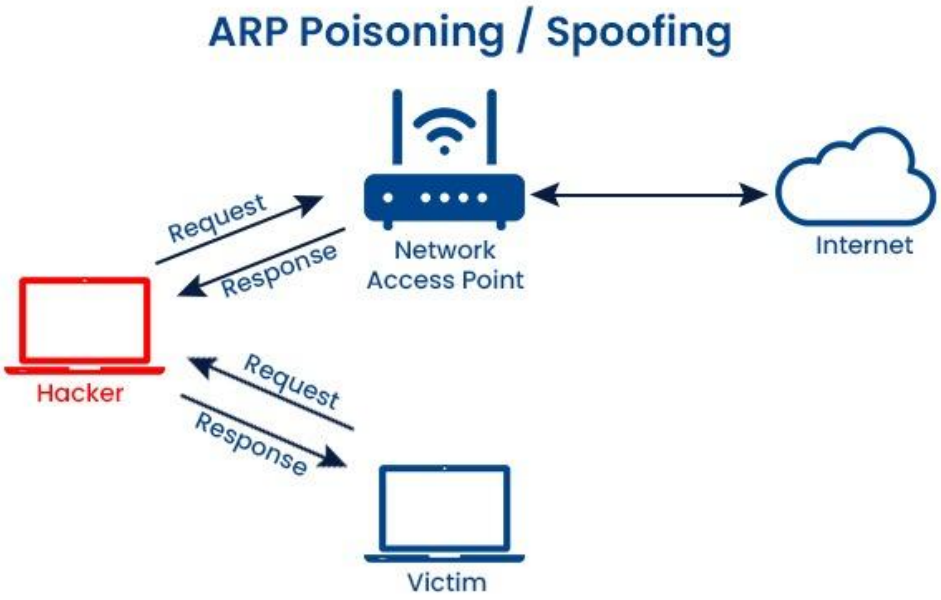

Figura 1. Ilustrarea atacului ARP Poisoning [Sursa: https://www.pynetlabs.com/what-is-arp-poisoning]

TABEL III. ATACURI NIVELUL DE LEGĂTURĂ DE DATE, MECANISME ȘI CONTRAMĂSURI [SURSA: AUTORUL]

Atac	Protocol afectat	Mecanism	Contramasură	Overhead RAM estimat
ARP Poisoning / MITM [24]	Ethernet / Wi-Fi	Mesaje ARP false → corupere cache	Inspecție dinamică ARP, VLAN [29]	Neglijabil (tabele switch)
MAC Spoofing [23]	IEEE 802.11/802.15.4	Modificare câmp sursă în cadre	Autentificare MAC Criptografică [28]	< 1 KB per intrare
ZigBee Replay Attack [25]	ZigBee (IEEE 802.15.4)	Retrimitere mesaje Capturate	Numere de secvență + timestamp [27]	~512 B fereastră replay
BLE Pairing MITM [26]	Bluetooth LE	Intercept schimb chei în asociere	Numeric Comparison / Passkey [26]	< 2 KB stare sesiune
Sybil (identități false) [40]	ZigBee mesh / RPL	Noduri multiple controlate de un actor	PKI per dispozitiv, PoW [40]	~4 KB cert. X.509 ECC

2.5 Nivelul de rețea

Nivelul de rețea gestionează rutarea informațiilor între segmente de rețea utilizând adrese logice. IPv6 și 6LoWPAN sunt deosebit de importante pentru dispozitivele IoT cu resurse limitate [31]. RPL (*Routing Protocol for Low-Power and Lossy Networks*) este protocolul standardizat pentru rețele IoT *mesh*, stabilind topologii bazate pe arbori cu retransmitere prin noduri intermediare [32].

TABEL IV. ATACURI LA NIVELUL DE REȚEA RPL ȘI METODE DE DETECTARE [SURSA: AUTORUL]

Atac RPL	Mecanism	Impact	Metodă detectare	Precizie raportată
Rank Attack [35]	Anunțare rang fals Scăzut → atragere trafic	Interceptare, MITM	Monitorizare topologie + IDS ML [41]	~94% [studii 2023]
Wormhole [36]	Tunel out-of-band → false adiacențe	Interceptare volum mare	Packet leashes, RTT Măsurare [32]	~89% detectare
Blackhole [37]	Eliminare selectivă pachete	DoS nedectabil	IDS bazat pe Reputație [29]	~91%
Selective Forwarding [38]	Drop mesaje critice (auth, routing)	Compromitere parțială ascunsă	Analiza flow-urilor + Anomalii [42]	~87%
Sybil [40]	Identități virtuale multiple	Control rutare, epuizare resurse	PKI per dispozitiv, PoW [30]	Preventiv (nu reactiv)

2.6 Nivelul de transport

Stratul de transport este responsabil pentru comunicarea end-to-end între gazde, concentrând securitatea pe protejarea datelor în tranzit și asigurând confidențialitatea, integritatea și autenticitatea mesajelor schimbate [31]. DTLS (Datagram Transport Layer Security) oferă criptarea orientată către datagrame potrivită pentru comunicarea bazată pe UDP [43]. OSCORE (Object Security for Constrained RESTful Environments) aplică securitatea la nivel de obiect înainte ca datele să ajungă la stratul de transport, criptând încărcăturile utile cu protecție criptografică ce persistă prin intermediari și proxy-uri [44].

TABEL V. COMPARAȚIE PROTOCOALE DE SECURITATE TRANSPORT IOT: OVERHEAD ȘI LATENȚĂ [SURSA: AUTORUL]

Protocol	Transport	Criptare	Auth.	Overhead RAM	Latență handshake	Potrivit IoT limitat
TLS 1.3 (profil IoT) [53][54]	TCP	AES-128-GCM	Certificate /PSK	~10–20 KB	1-RTT (~50 ms LAN)	Moderat (SBC)

DTLS 1.3 [43]	UDP	AES-128-GCM /ChaCha20	Certificate /PSK	~6–12 KB	1.5-RTT	Bun (MCU mediu)
OSCORE + EDHOC [44][45]	UDP/TCP	AES-CCM (COSE)	Chei simetrice / ECC	~3–5 KB	3 mesaje (~30 ms)	Excelent (MCU mic)
MQTT + TLS [46][47]	TCP	TLS extern	User/Parolă + cert.	~15–25 KB	2-RTT + MQTT conn.	Acceptabil (SBC)
CoAP + DTLS [50][51]	UDP	DTLS extern	PSK / Certificate	~6–10 KB	DTLS + CoAP req.	Bun
MQTT fără TLS [47]	TCP	Niciuna	Parolă în clar	~5 KB	Minim	NESECURIZAT

2.7 Nivelurile de sesiune, prezentare și de aplicație

Stratul de aplicație reprezintă cele mai înalte niveluri ale modelului OSI, unde aplicațiile destinate utilizatorilor interacționează cu serviciile de rețea. Securitatea la acest strat se concentrează pe protejarea funcționalității aplicațiilor, integritatea datelor, autentificarea și autorizarea utilizatorilor. Spre deosebire de securitatea stratului de transport, securitatea stratului de aplicație abordează vulnerabilitățile din software-ul în sine, firmware-ul care rulează pe dispozitive, gestionarea cheilor criptografice și politicile de control al accesului [55]. Implementarea riguroasă a acestor măsuri se aliniază cu principiile zero-trust predominante în securitatea rețelelor moderne.

TABEL VI. VULNERABILITĂȚI STRAT APLICAȚIE: SEVERITATE, ATACURI ȘI CONTRAMĂSURI [SURSA: AUTORUL]

Vulnerabilitate	Severitate	Mecanism de atac	Contramasură
Credențiale implicite	CRITIC	Brute-force dicționar (Mirai)	Parole unice la fabricație, forțare schimbare la prima utilizare [56]
Injecție cod/comenzi	CRITIC	Input nevalidat → exec. OS/DB	Validare input, WAF (OWASP CRS) [56]
Firmware vulnerabil (lib terțe) [14]	ÎNALT	Exploatare CVE în dependențe	SBOM, patch management, actualizare semnată criptografic [57]
Gestiunea cheilor Deficitară [58]	ÎNALT	Extragere chei hardcodate din firmware	HSM/SE, rotație periodică a cheilor, PKI [59][60]
Autorizare permisivă (MQTT ACL) [48]	ÎNALT	Abonare la subiecte wildcard nerestricționate	ACL principiu privilegiu

			minim, audit regulat [29]
Actualizare firmware nesigură	ÎNALT	MITM → injectare firmware malițios	Semnătură criptografică + transport TLS + anti-rollback [57]
Escaladare privilegii [29]	MEDIU	Exploatare permisiuni eronate	RBAC/ABAC, separare roluri, audit access [56]

2.8 Tehnologii emergente în securitatea IoT

Dincolo de soluțiile per nivel OSI, literatura recentă propune paradigme arhitecturale transversale care abordează securitatea IoT în mod holistic. Această secțiune le analizează prin prisma fezabilității pe hardware cu resurse limitate (SBC ARM Cortex, Raspberry Pi, NanoPi R5C).

Blockchain permite modele de încredere descentralizate prin registre distribuite imuabile, eliminând punctele unice de eșec și permițând sisteme tolerante la erori bizantine [62]. Aplicațiile includ urmărirea lanțului de aprovizionare, autentificarea dispozitivelor și înregistrarea tranzacțiilor. Cu toate acestea, mecanismele de consens necesită resurse computaționale substanțiale, făcând implementarea pe dispozitive cu resurse limitate impracticabilă [63]. Implementările ușoare reduc costurile prin algoritmi de consens simplificați, dimensiuni reduse ale blocurilor și registre fragmentate [64].

Criptografia post-cuantică abordează amenințarea că computerele cuantice ar putea sparge algoritmii cu cheie publică actuali prin algoritmul lui Shor [65][108]. NIST standardizează algoritmi rezistenți la atacuri cuantice, inclusiv criptografia bazată pe rețea cea mai promițătoare pentru implementare practică datorită dimensiunilor rezonabile ale cheilor și timpilor de calcul [66]. Abordările hibride (algoritmi clasici + post-cuantici) permit tranziția graduală, menținând compatibilitatea cu infrastructura existentă [67][109].

Învățarea automată permite detectarea automată a anomaliilor, sistemele învățând modele de comportament normal și identificând abaterile care indică atacuri, fără specificarea manuală a semnăturilor. Abordările supervizate ating o precizie ridicată pe date etichetate [68], cele nesupravizate detectează tipuri noi de atacuri fără antrenament etichetat [69]. Totuși, atacurile adversariale pot determina sistemele să clasifice eronat atacurile. Apărarea include antrenarea adversarială și apărări certificate cu garanții matematice de robustețe [70]. Învățarea federată permite antrenarea distribuită fără centralizarea datelor sensibile, cu confidențialitate diferențială pentru protejarea informațiilor individuale [78].

Securitatea zero-trust verifică fiecare cerere de acces, eliminând încrederea implicită bazată pe locația în rețea [71]. Arhitecturile zero-trust pentru IoT necesită autentificarea continuă, controlul accesului detaliat și microsegmentarea rețelei [72]. Soluțiile VPN evaluate în Capitolul 4 (TailScale, ZeroTier, WireGuard) implementează aceste principii prin tuneluri criptate *peer-to-peer* cu autentificare mutuală, fără dependență de un perimetru fix.

Edge computing procesează datele la marginea rețelei, reducând latența, consumul de lățime de bandă și energia [74]. Gateway-urile SBC evaluate în Capitolul 4 (Raspberry Pi 3B+, NanoPi R5C) reprezintă noduri edge care implementează securizarea transportului de date prin tunelare VPN pentru dispozitivele IoT din subrețea. *Fog computing* extinde conceptul prin straturi ierarhice de la dispozitive *edge*, prin noduri intermediare, până la sisteme cloud necesitând autentificare între niveluri și criptare a datelor în tranzit [76]. Securitatea IoT

cuprinzătoare necesită strategii de apărare în profunzime, prin mecanisme multiple la diferite niveluri OSI ce funcționează sinergic [80][81].

3. Tehnologiile folosite în cadrul cercetării

În scopul securizării transportului de date în sistemele IoT s-au folosit tehnologii ce facilitează transmisia datelor colectate de rețelele de senzori în mod sigur, criptat și pe bază de autorizație. Securizarea a vizat anonimizarea adresei publice de IP pentru minimizarea atacurilor DDoS, iar accesul în rețeaua locală a fost controlat la nivelul firewall-ului.

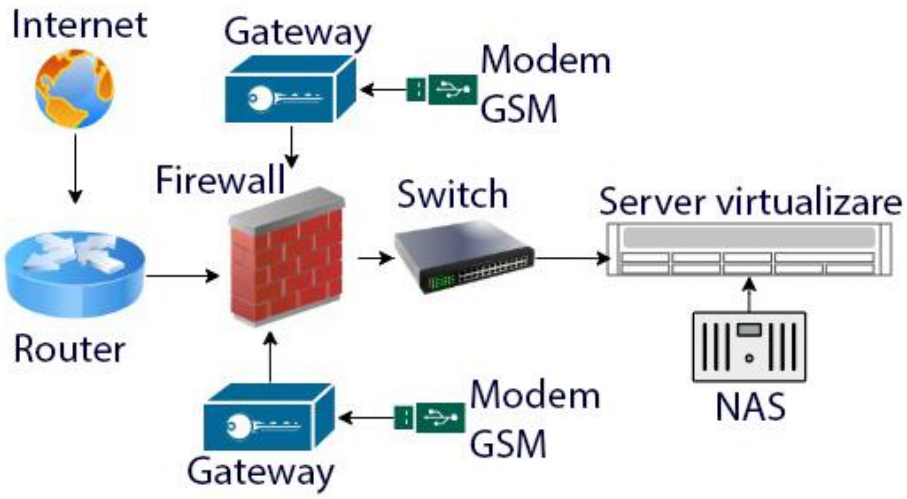

Figura 2. Diagrama infrastructurii hardware din laborator [Sursa: Autorul]

3.1 Infrastructura hardware și platforme de procesare la margine edge

Nivelul fizic cuprinde sisteme de calcul, aparate de rețea și plăci SBC consolidate într-un dulap rack cu mecanism blocabil — primul strat de apărare în profunzime conform ISO/IEC 27001.

Figura 3. Infrastructura Hardware din laborator [Sursa: Autorul]

Sistemul industrial Beckhoff (arhitectură x86, suport AES-NI) a fost ales ca platformă de firewall datorită transparenței complete față de soluțiile blackbox costisitoare (Cisco ASA, Fortinet), disponibil second-hand la cost redus.

Figura 4. Sistemul de calcul pentru firewall [Sursa: https://www.beckhoff.com]

Serverul HP ProLiant DL360 G7 asigură virtualizarea (VMware ESXi) — două unități în paralel permit segmentarea serviciilor IoT de securitate față de platformele de colectare date, reducând suprafața de atac prin izolare arhitecturală.

Figura 5. Server HP pentru virtualizare [Sursa: https://www.hpe.com/us]

ReadyNAS 3200 în configurație RAID 5, conectat prin iSCSI cu autentificare CHAP, asigură redundanță pentru log-urile de securitate și capturile de trafic IoT fără risc de pierdere a datelor la defectarea unui disc.

Figura 6. Sistemul NAS pentru extinderea spațiului de stocare [Sursa: https://www.netgear.com]

3.1.1 Componente de comunicație radio și module de extensie pentru redundanță

Modem-ul Huawei E3372 oferă conectivitate WAN LTE independentă de infrastructura fixă, cu *firmware* HiLink ce expune un API HTTP pentru monitorizarea semnalului (RSSI, RSRP) și gestionarea automată a conexiunii esențial în zone rurale izolate.

Figura 7. Modem portabil cu conectivitate GSM [Sursa: https://lowcostmobile.com]

3.1.2 Analiza comparativă a unităților de procesare de mică putere SBC pentru gateway IoT

Raspberry Pi 3B+: cea mai largă comunitate SBC, consum sub 5 W, compatibil cu alimentare fotovoltaică miniaturală democratizează accesul la *gateway*-uri IoT securizate fără investiții semnificative.

Figura 8. Placa de dezvoltare Raspberry Pi 3B+ [Sursa: https://www.raspberrypi-spy.co.uk]

NanoPi R5C (procesor RK3568): alternativă superioară tehnic cu performanțe VPN/IDS mai bune la același consum energetic și suport nativ WPA3, eliminând vulnerabilitățile WPA2 fără reproiectarea infrastructurii existente.

Figura 9. Placa de dezvoltare NanoPi R5C [Sursa: https:// youyeetoo.com/]

3.2 Ecosistemul software și sisteme de operare specializate

Tehnologiile software au fost instalate atât la nivelul hardware (sistem de operare specializat, hipervizor) cât și la nivel de mașini virtuale.

3.2.1 Sisteme de operare consolidate pentru securizarea rețelelor

pfSense (FreeBSD): firewall *enterprise* cu *stateful packet inspection*, VPN multi-protocol, IDS/IPS Snort și VLAN 802.1Q la cost zero comparabil cu Cisco ASA sau Fortinet. VLAN-urile izolează traficul IoT prevenind mișcarea laterală post-compromitere.

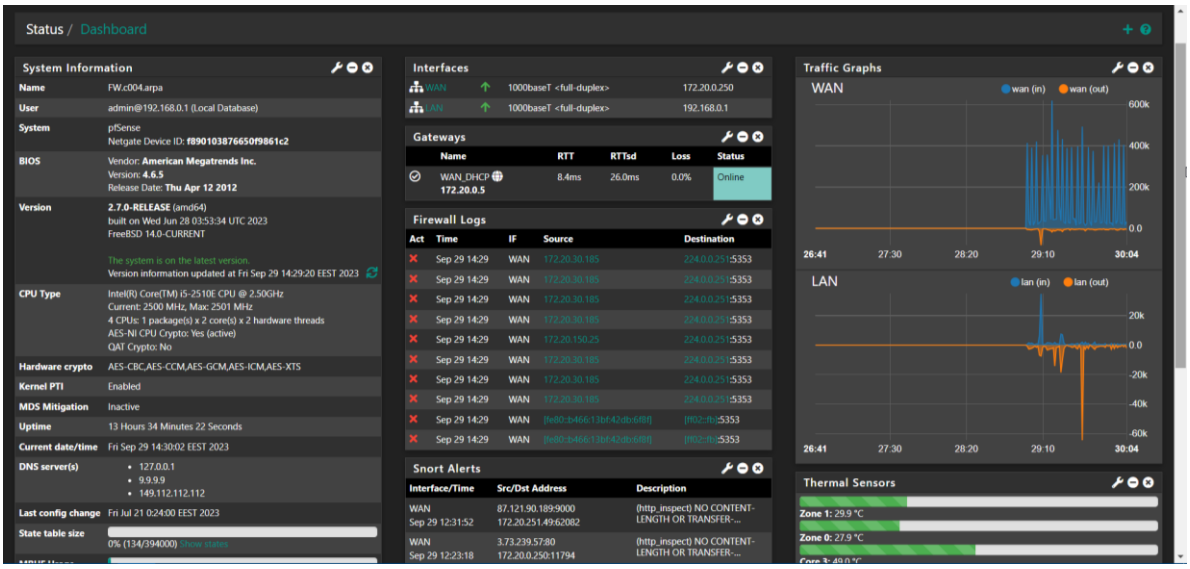

Figura 10. Interfața web pentru Pfsense firewall [Sursa: Autorul]

OPNsense: alternativă cu actualizări săptămânale de securitate și baza HardenedBSD (ASLR, SafeStack, Retpoline, 2FA nativ) fereastră de expunere la vulnerabilități semnificativ mai mică față de pfSense, critic în medii IoT.

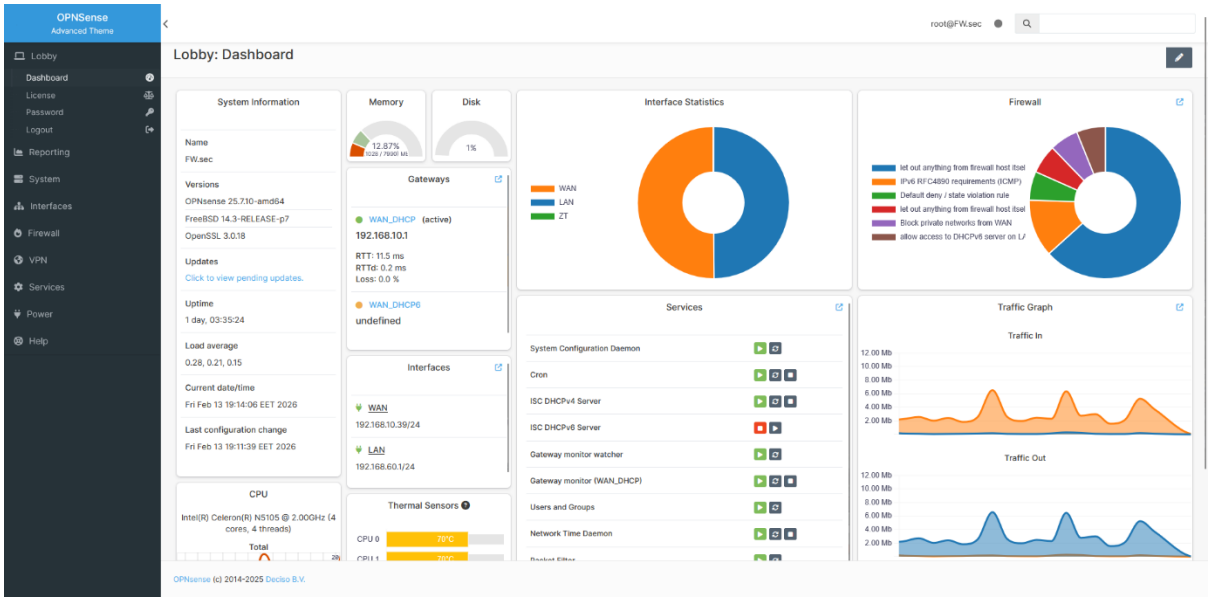

Figura 11. Interfața web pentru OPNSense firewall [Sursa: Autorul]

OpenWRT: transformă SBC-uri și routere vechi în gateway-uri IoT programabile (VPN WireGuard/OpenVPN, firewall nftables) cu cerințe minime — 8 MB flash, 64 MB RAM, suport oficial pentru peste 1.500 de dispozitive.

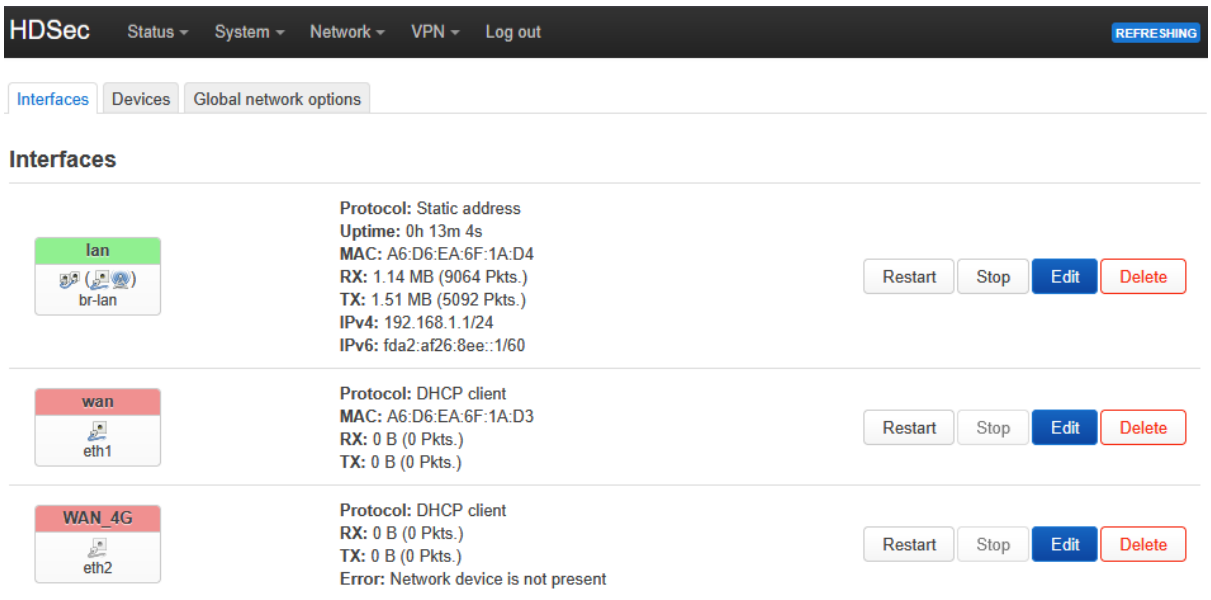

Figura 12. Interfața web pentru OpenWRT [Sursa: Autorul]

3.2.2 Platforme de virtualizare și izolare a serviciilor de management

VMware ESXi 7.0: hipervizor *bare-metal* cu funcție vTPM pentru atestare criptografică la pornire, NIOC/SIOC pentru prioritizarea traficului IoT și vMotion pentru migrare fără *downtime*. Disponibil gratuit pentru uz personal și cercetare.

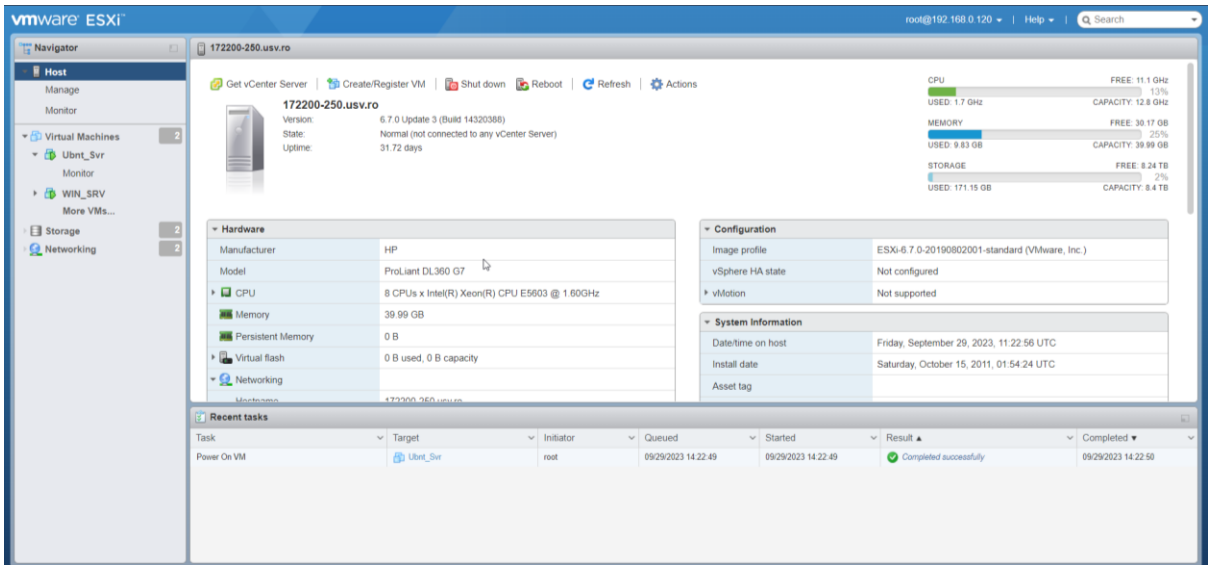

Figura 13. Interfața web pentru Vmware ESXI virtualizare [Sursa: Autorul]

3.2.3 Servicii proxy și mecanisme de echilibrare a sarcinii la nivel aplicație

Kemp LoadMaster: mitigare DDoS L7 (Slowloris, flood conexiuni) cu inspecție IPS Snort versiune gratuită până la 20 Mbps, suficientă pentru implementări IoT mici și medii.

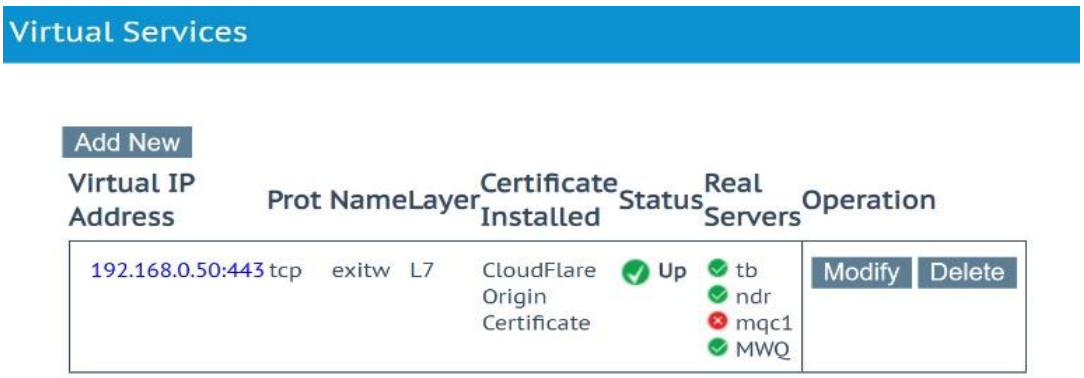

Figura 14. Interfața web pentru Kemp loadbalancer [Sursa: Autorul]

Nginx Proxy Manager (MIT): configurare proxy invers cu certificate TLS Let's Encrypt auto-reînnoite în sub 2 minute, fără cunoștințe Nginx, superior alternativelor comerciale (Kemp, Citrix) ca accesibilitate.

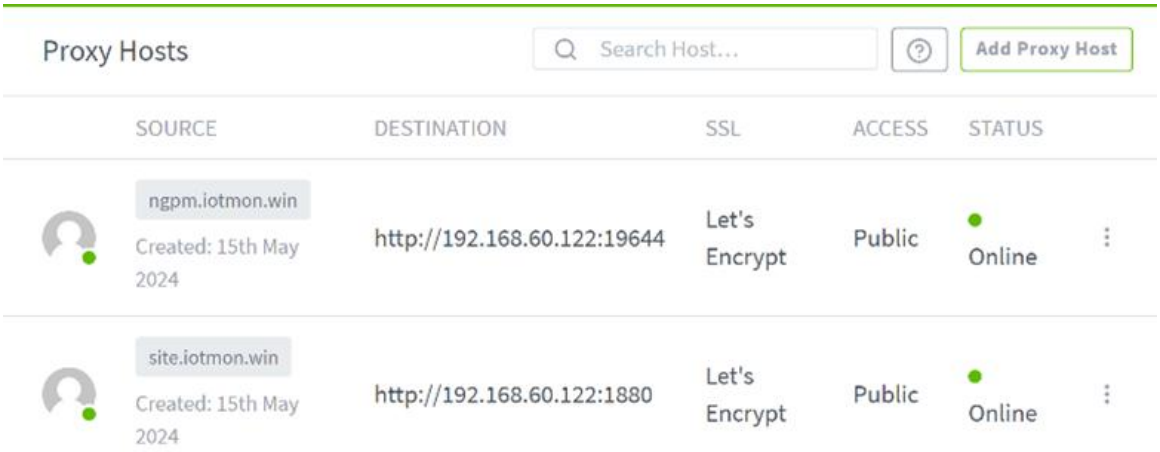

Figura 15. Interfața web pentru Nginx Proxy Manager load balancer [Sursa: Autorul]

3.2.4 Protocoale de comunicare și tehnologii de tunelare securizată

ZeroTier: rețea Ethernet virtuală *peer-to-peer* cu criptare AES-256-GCM *end-to-end*, funcționând transparent prin NAT fără porturi deschise gratuit pentru 25 dispozitive, cu opțiune *self-hosted* pentru confidențialitate maximă.

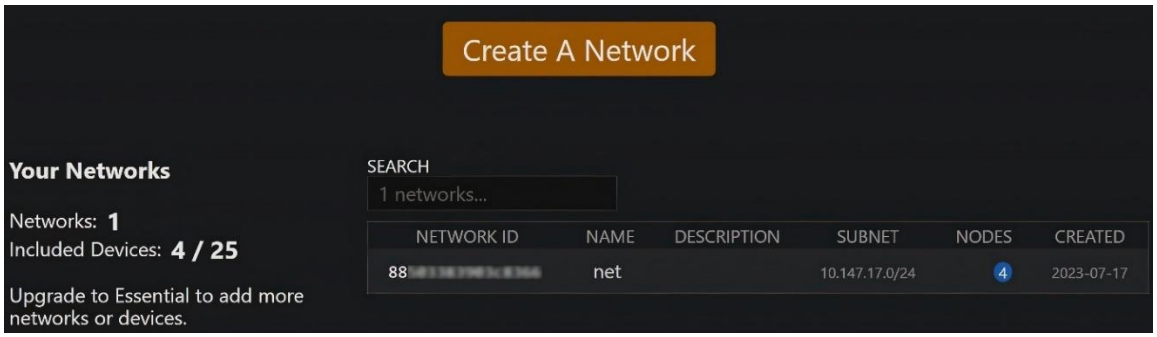

Figura 16. Interfața web pentru ZeroTier [Sursa: Autorul]

Tailscale (bazat pe WireGuard): latențe sub 5 ms, model Zero-Trust cu autentificare prin furnizori existenți (Google, Microsoft, GitHub), gratuit pentru 100 dispozitive. WireGuard: bază de cod ~4.000 linii, integrat nativ în *kernel* Linux 5.6+, *throughput* de 3–20× superior OpenVPN. OpenVPN: operează pe TCP 443 mascând traficul VPN drept HTTPS, cu autentificare multistrat (PKI, LDAP/RADIUS, 2FA-OTP) și revocare instantanee a accesului.

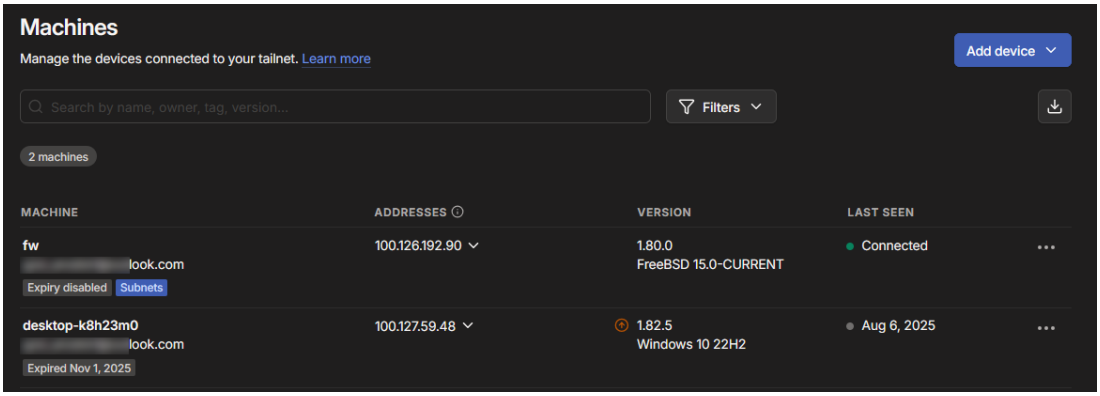

Figura 17. Interfața web pentru TailScale [Sursa: Autorul]

4. Soluțiile propuse pentru securizarea transportului de date

Soluțiile propuse sunt structurate conform modelului OSI, clasificate pe niveluri, pentru a facilita înțelegerea lor atât de către specialiști, cât și de către persoanele mai puțin familiarizate cu jargonul tehnic specific.

4.1 Soluții de securizare la nivelul fizic

Pe măsură ce dispozitivele IoT devin tot mai răspândite, securizarea acestora împotriva amenințărilor cibernetice capătă o importanță crescută. *Firewall*-urile, împreună cu *gateway*-urile bazate pe platforme Single Board Computer (SBC) precum Raspberry Pi 3B+ și NanoPi R5C, constituie prima linie de apărare la nivelul fizic, oferind control al traficului, izolare a rețelei și conectivitate securizată pentru senzori IoT la cost redus și consum energetic scăzut.

4.1.1 Firewall fizic și gateway-uri bazate pe platforme SBC

Pentru protejarea serverelor IoT este recomandată utilizarea unui firewall dedicat sau a unui router cu funcționalități firewall, folosind soluții software precum PfSense sau OPNsense (ambele bazate pe FreeBSD). Gateway-ul dintre senzori și firewall se poate baza pe plăci SBC, alimentate la 5V, opțional cu panouri solare și modem USB LTE pentru conectivitate în locații greu accesibile.

Raspberry Pi 3B+ rulând Kali Linux cu desktop XFCE asigură partajarea conexiunii prin NetworkManager, suportând WPA2 ca standard maxim de securitate wireless. Consumul maxim de ≈2,5 A îl face compatibil cu panouri solare de 5V/10W și controllere MPPT. Pinii GPIO permit interfațarea senzorilor (I2C/SPI/1-Wire), iar systemd-networkd configurează etichetarea VLAN pentru traficul IoT segmentat.

Figura 18. Gateway-ul bazat pe Raspberry Pi 3B+ [Sursa: Autorul]

Sistemul de operare instalat pe Raspberry Pi este Kali linux cu mediul *desktop* XFCE, iar partea de partajare a conexiunii se face din instrumentul intern de gestionare a conexiunilor de internet al sistemului de operare. Partajarea se va face desigur după instalarea și conectarea clientului TailScale la rețeaua privată *mesh* și ZeroTier la rețeaua privată SDN.

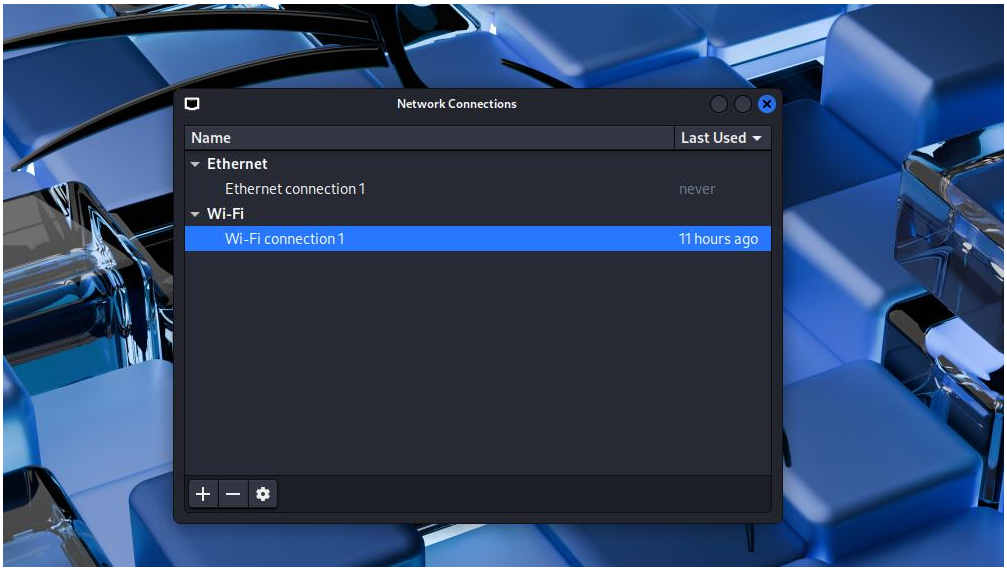

Figura 19. Instrumentul de gestiune al conexiunilor de internet în Kali [Sursa: Autorul]

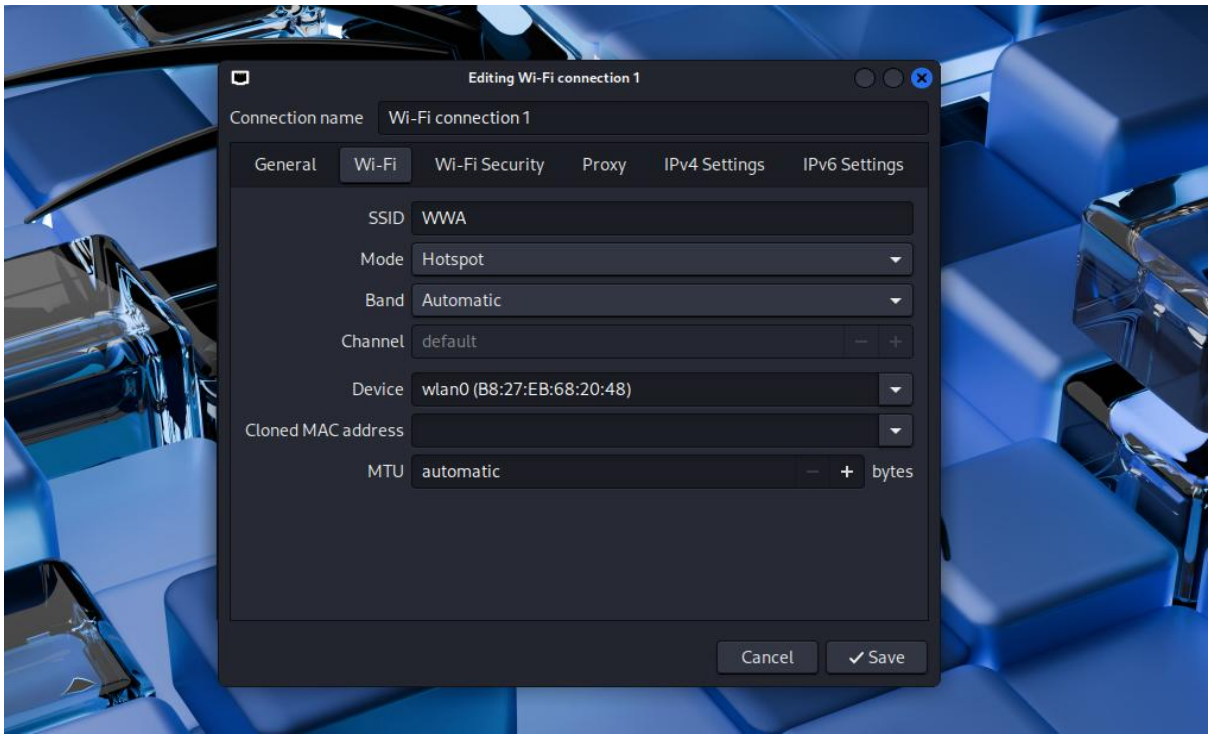

Figura 20. Partajarea conexiunii prin interfața wireless [Sursa: Autorul]

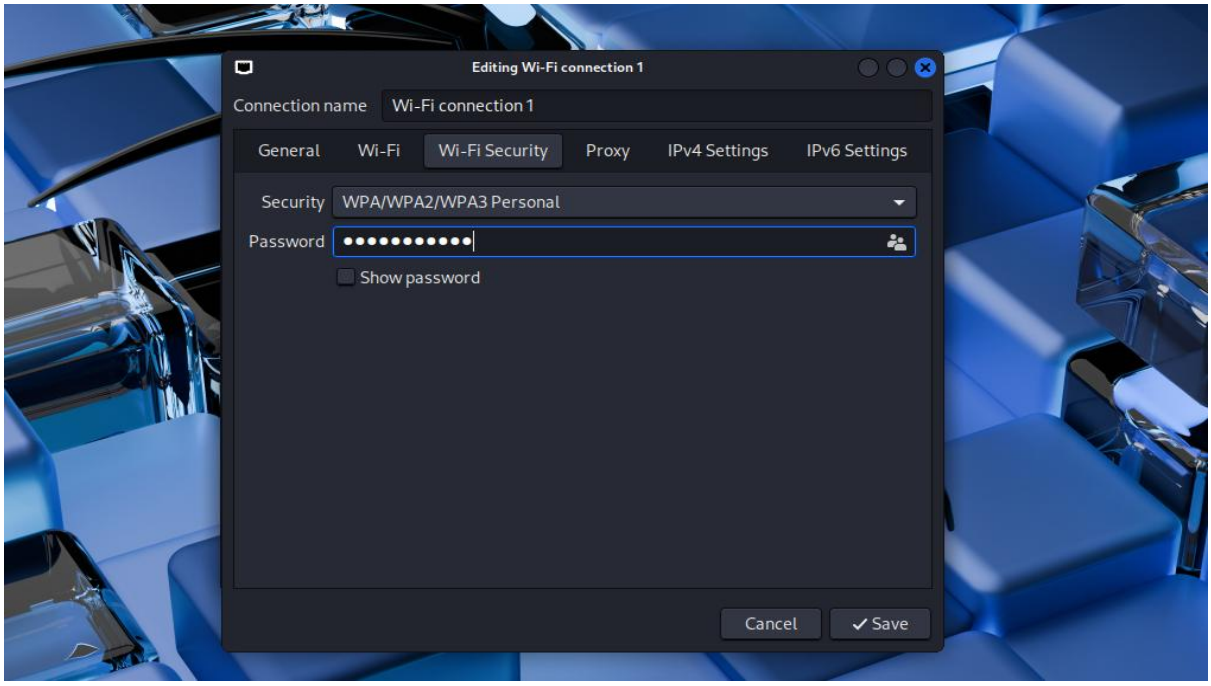

Figura 21. Selectarea standardului de securizare și parola pentru hotspot [Sursa: Autorul]

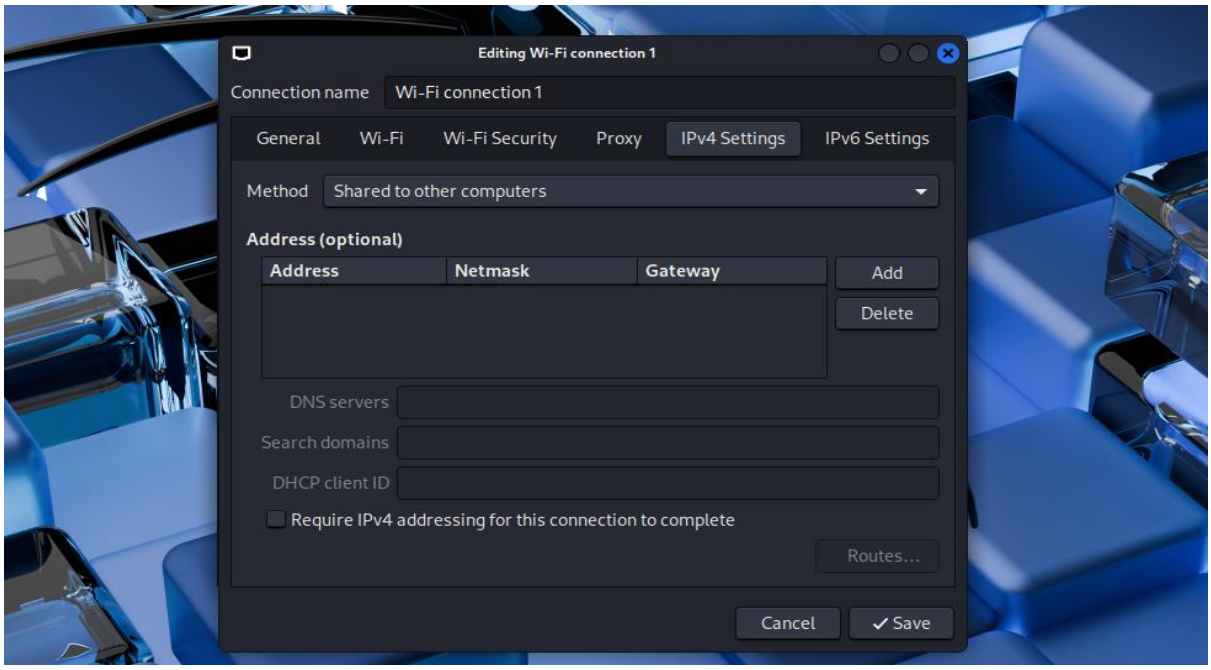

Figura 22. Partajarea conexiunii locale cu rețeaua hotspot creată [Sursa: Autorul]

NanoPi R5C, alimentat de Rockchip RK3399 (dual Cortex-A72 @1,8 GHz + quad A53) cu 4 GB RAM LPDDR4, oferă performanțe de aproximativ două ori mai mari față de Raspberry Pi 4 și suportă WPA3-SAE prin slotul PCIe/M.2 cu plăci WiFi 6 (802.11ax). Rulând OpenWRT 24.10.0, permite instalarea clientului ZeroTier și a driverelor pentru *modem*-ul GSM USB direct din managerul de pachete integrat.

WPA3 introduce autentificarea simultană a egalilor (SAE) care înlocuiește vulnerabilitățile PSK ale WPA2, atenuând atacuri precum KRACK și atacurile offline de tip dicționar sau *brute-force* asupra *handshake*-ului.

Figura 23. Gateway-ul bazat pe NanoPi R5C [Sursa: Autorul]

Sistemul de operare folosit pentru a transforma NanoPi R5C într-un *router* cu funcționalități avansate se numește OpenWRT versiunea 24.10.0. OpenWRT are compatibilitatea cu ZeroTier după cum se observă în figura 22, clientul instalat este la versiunea 1.14.1. Pentru a avea conexiune la internet trebuie instalate driverele pentru *modem*-ul GSM usb, toate aceste drivere se găsesc la secțiunea „*Software*” și se instalează prin apăsarea butonului „Install”.

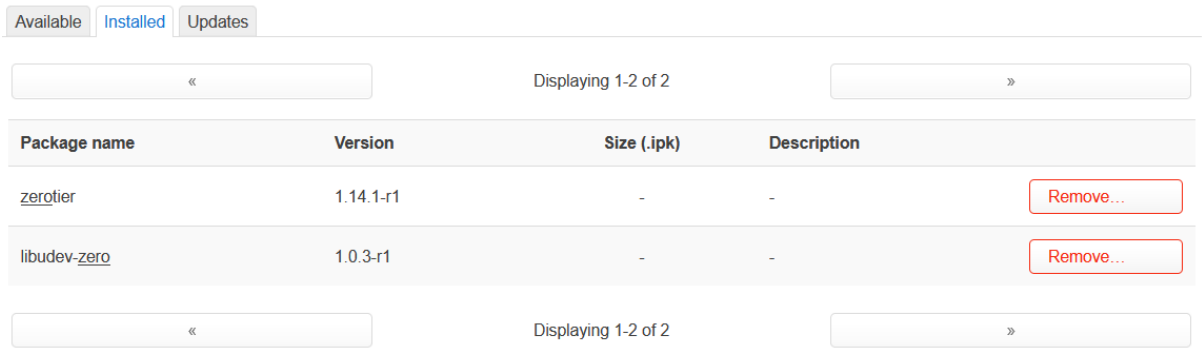

Figura 24. Managerul de aplicații și drivere în OpenWRT [Sursa: Autorul]

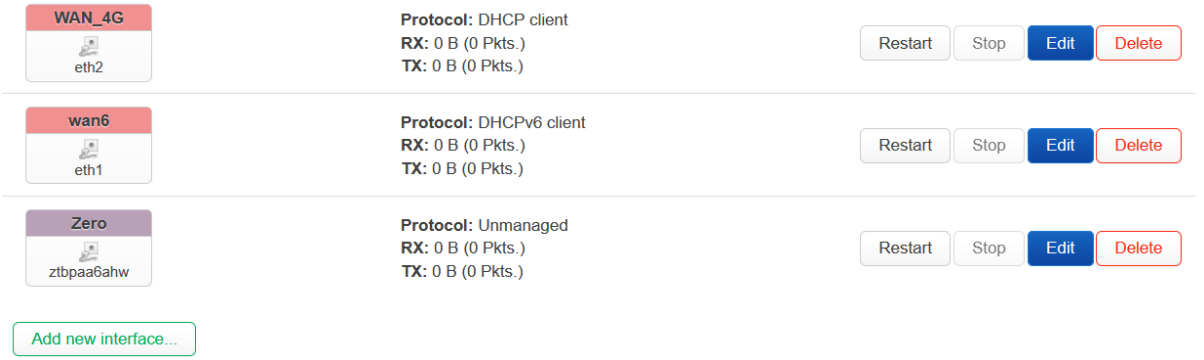

Figura 25. Secțiunea de management al interfețelor în OpenWRT [Sursa: Autorul]

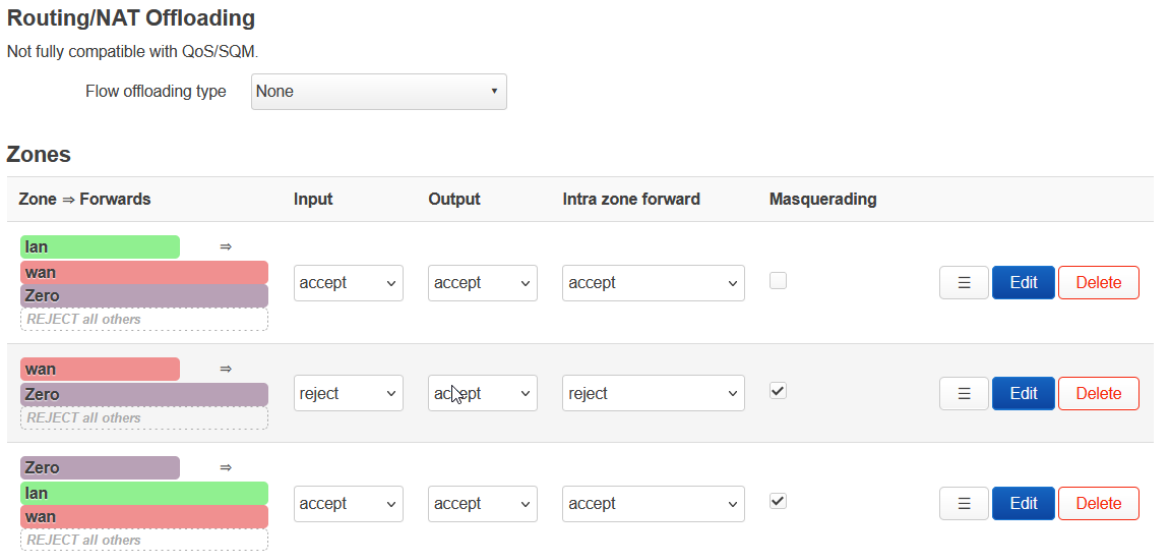

Figura 26. Secțiunea rutare și regulile fierewall în OpenWRT [Sursa: Autorul]

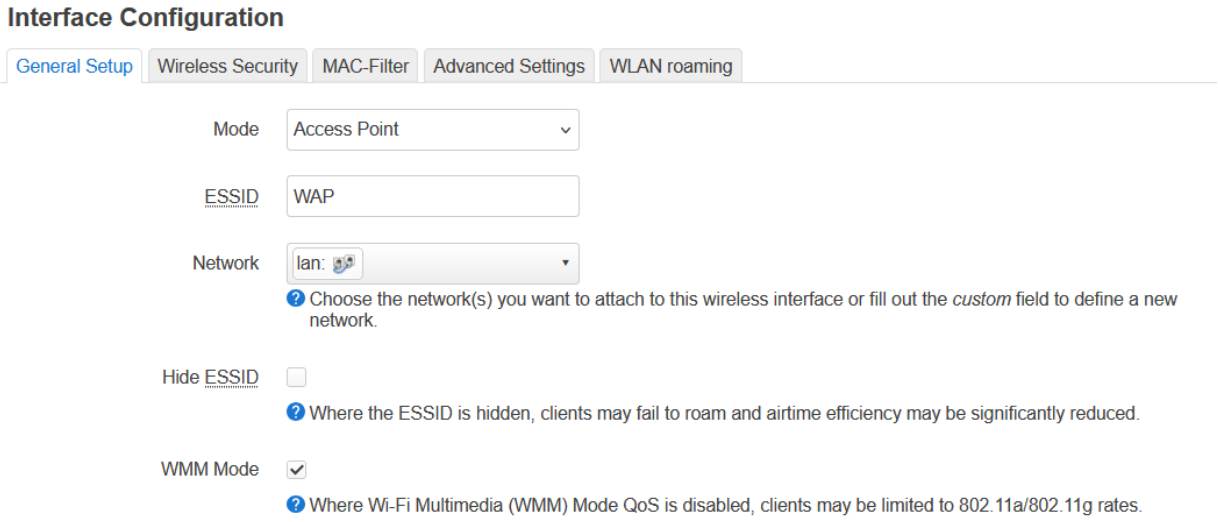

Figura 27. Secțiunea interfeței wireless în OpenWRT [Sursa: Autorul]

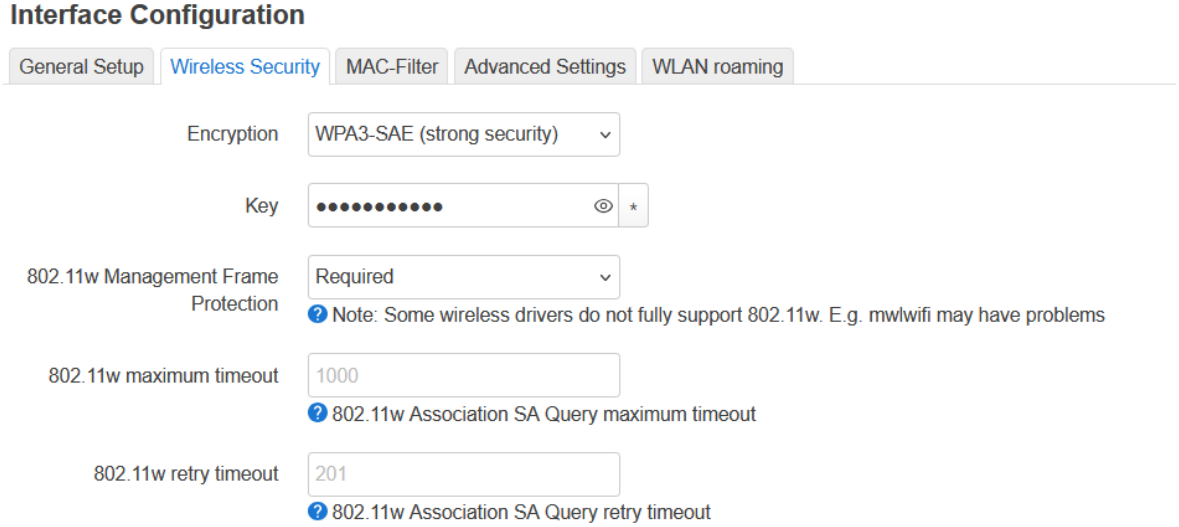

Figura 28. Securizarea interfeței wireless în OpenWRT [Sursa: Autorul]

4.2 Soluții de securizare la nivelul rețea

Izolarea dispozitivelor IoT într-o rețea locală separată cu o gamă IP distinctă reduce riscul ca acestea să fie folosite ca puncte de intrare spre rețeaua principală. La nivelul rețea se pot utiliza sisteme IDS (Intrusion Detection System) care monitorizează traficul IP pentru a detecta spoofing, scanări și acces neautorizat prin analiza antetelor pachetelor și a informațiilor de rutare.

4.2.1 Sistem de detecție a intruziunii Pfsense

PfSense utilizează Snort și Suricata ca sisteme IDS/IPS *open-source*, capabile de inspecție profundă a pachetelor și analiză a traficului în timp real la nivelurile 3 și 4 OSI. Snort necesită crearea unei interfețe interne asociate interfețelor rețelei (WAN și LAN), cu seturi de reguli descărcabile (VRT, Emerging Threats) ce acoperă amenințări IoT: *malware*, *botnet*-uri și liste de IP-uri dăunătoare.

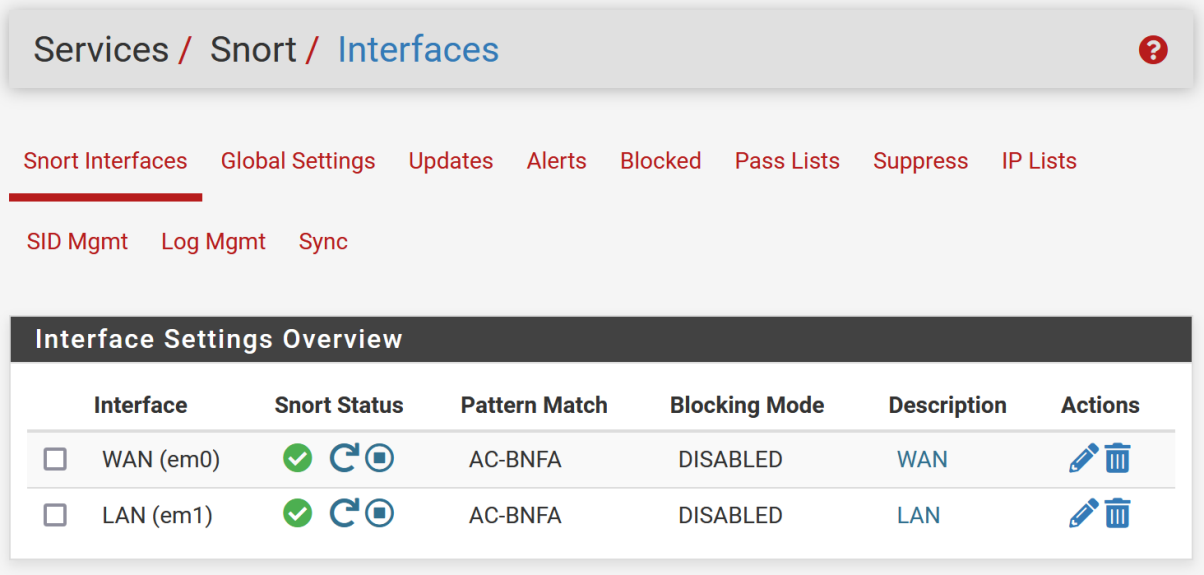

Figura 29. Panoul de configurare Snort Pfsense [Sursa: Autorul]

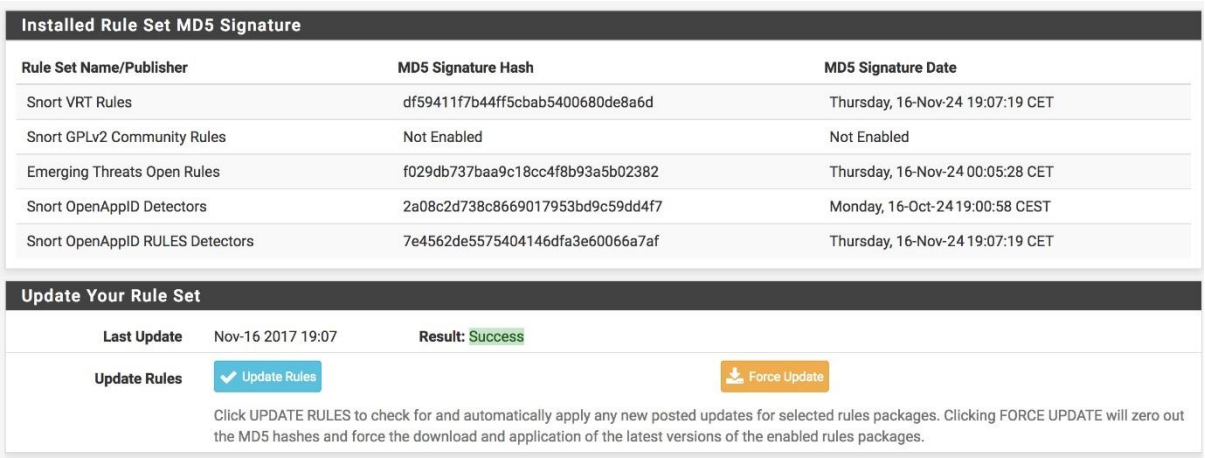

Figura 30. Lista de reguli Snort Pfsense [Sursa: Autorul]

4.2.2 Izolare rețea locală IoT cu Pfsense

PfSense permite crearea de LAN-uri sau VLAN-uri separate cu intervale IP distincte, aplicând reguli stricte de firewall între rețele. Dispozitivele IoT se plasează pe o interfață dedicată (ex. IoT LAN cu adresa 172.250.50.1/24), izolate de LAN-ul principal, limitând astfel răspândirea *malware*-ului și accesul neautorizat.

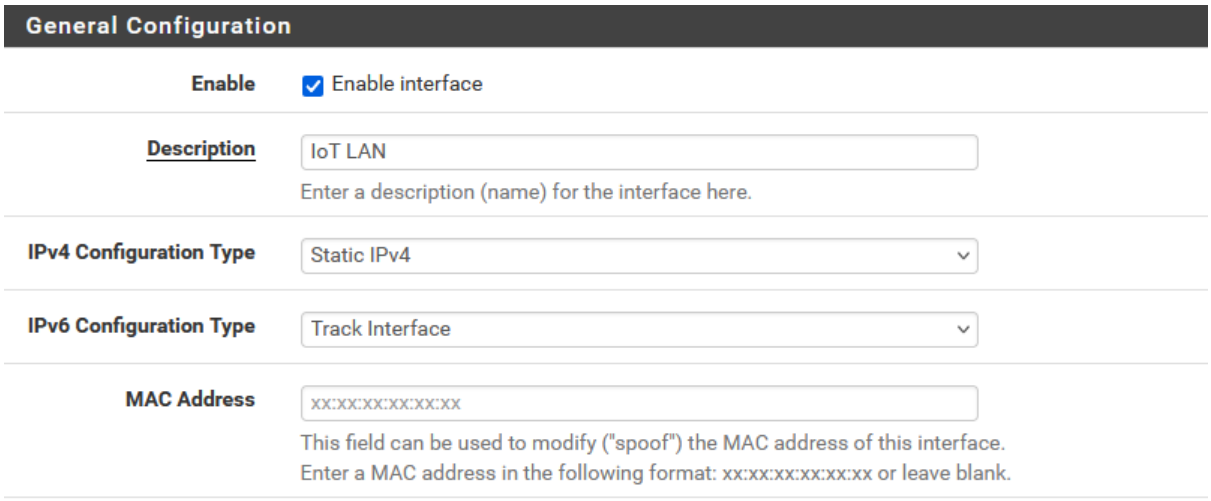

Figura 31. Definirea unei noi interfețe LAN Pfsense [Sursa: Autorul]

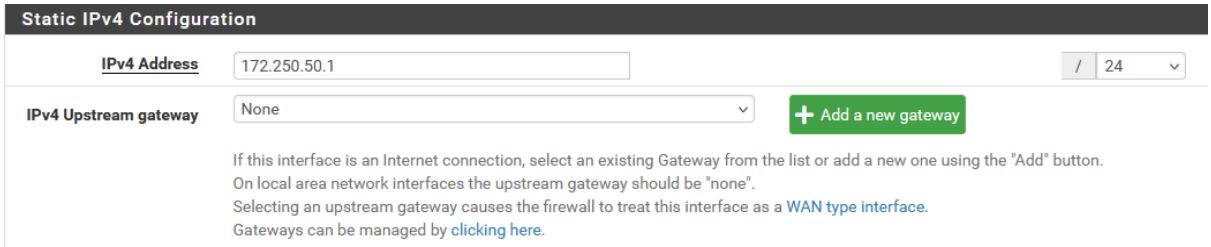

Figura 32. Adresa de IP pentru noua interfață LAN Pfsense [Sursa: Autorul]

4.2.3 Sistem de detecție a intruziunii OPNsense

OPNsense utilizează Suricata ca sistem integrat de prevenire a intruziunilor (IDS). Suricata este un motor *open-source* de înaltă performanță care inspectează traficul de rețea în timp real pentru a detecta și bloca amenințările, cum ar fi scanarea porturilor, programele *malware* și încercările de exploatare. Integrat cu *firewall*-ul OPNsense, Suricata poate aplica reguli de securitate atât la nivelul 3, cât și la nivelul 4, oferind o inspecție profundă a pachetelor și un răspuns automat la activitățile suspecte, îmbunătățind protecția generală a rețelei.

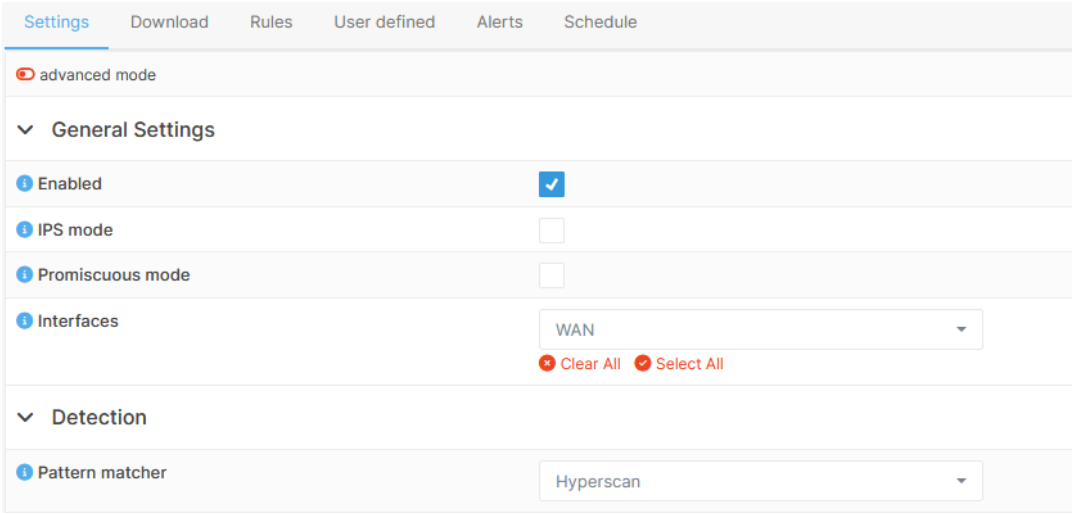

Figura 33. Panoul de configurare Suricata OPNsense [Sursa: Autorul]

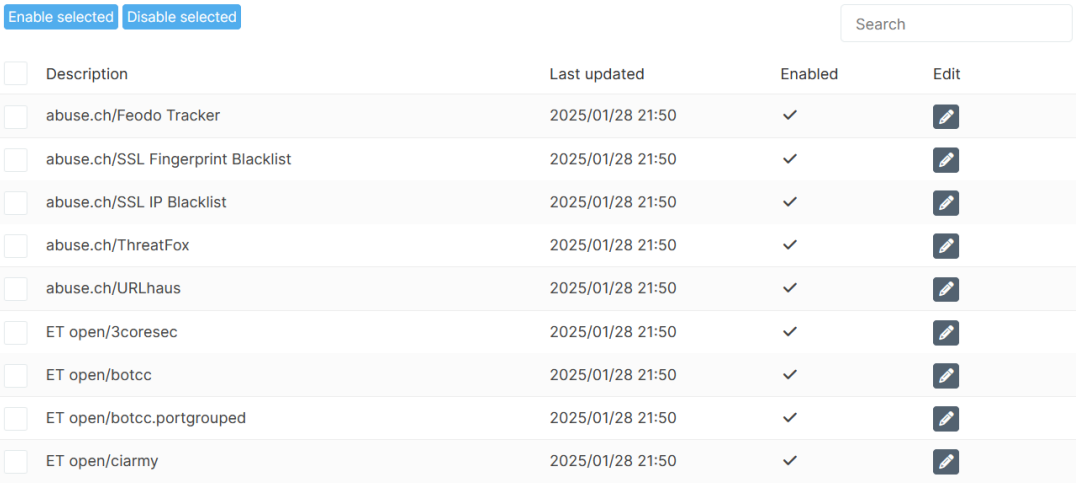

Figura 34. Lista cu reguli Suricata OPNsense [Sursa: Autorul]

4.2.4 Izolare rețea locală IoT cu OPNsense

Similar cu PfSense, OPNsense permite segmentarea traficului IoT prin crearea de interfețe LAN separate cu alocări IP statice (ex. 172.250.50.1/24). Această paradigmă defense-in-depth izolează traficul IoT într-un domeniu de broadcast discret, contracarând propagarea laterală specifică atacurilor precum botnet-ul Mirai și consolidând reziliența față de adversarii cibernetici.

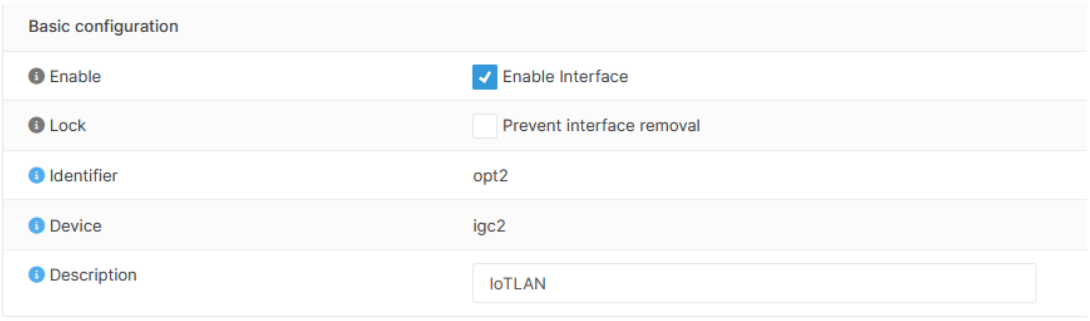

Figura 35. Definirea unei noi interfețe LAN OPNsense [Sursa: Autorul]

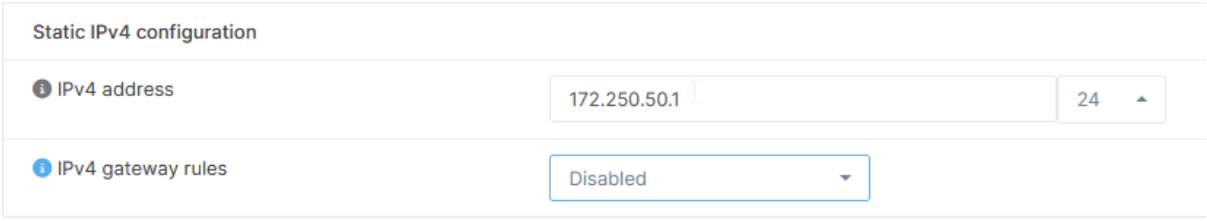

Figura 36. Adresa de IP pentru noua interfață LAN OPNsense [Sursa: Autorul]

4.3 Soluții de securizare și testare performanță la nivelul transport

La nivelul 4 OSI (transport), securizarea datelor se realizează prin TLS pe TCP (criptare *end-to-end* pentru servicii web) și prin WireGuard pe UDP (soluție modernă pentru VPN-uri și sisteme *peer-to-peer*). Ambele abordări asigură confidențialitatea, integritatea și autenticitatea datelor în tranzit.

4.3.1 Securizarea transportului prin TailScale

Tailscale este o soluție VPN bazată pe WireGuard, funcționând la nivelul 4 OSI prin UDP (port 41641). Utilizează criptografie de ultimă generație: Curve25519 pentru DH, BLAKE2s pentru *hashing* și ChaCha20-Poly1305 pentru criptarea AEAD per sesiune. Gestionarea automată a traversării NAT și a cheilor elimină complexitatea VPN-urilor tradiționale. Rețeaua DERP oferă *fallback* pentru NAT-uri simetrice sau *firewall*-uri care blochează UDP. Tunelurile Tailscale bazate pe WireGuard încapsulează datele senzorilor (MQTT sau CoAP) de la *gateway*-uri direct la firewall, menținând segmentarea *zero-trust* fără a expune dispozitivele IoT pe internet. PfSense suportă Tailscale v0.1.4 prin managerul de pachete integrat, cu notificări automate de actualizare.

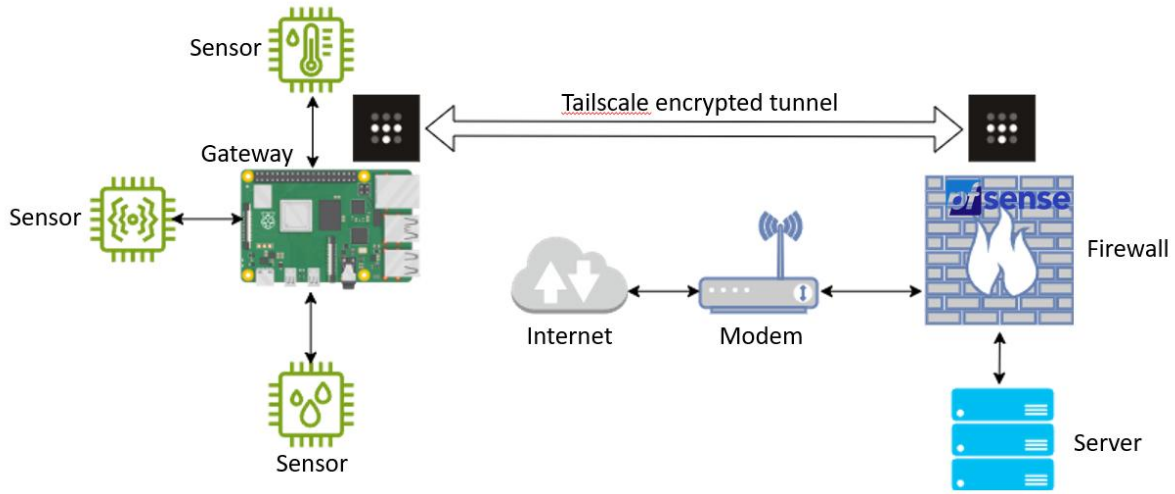

Figura 37. Modul de securizare a transportului de date cu TailScale [Sursa: Autorul][96]

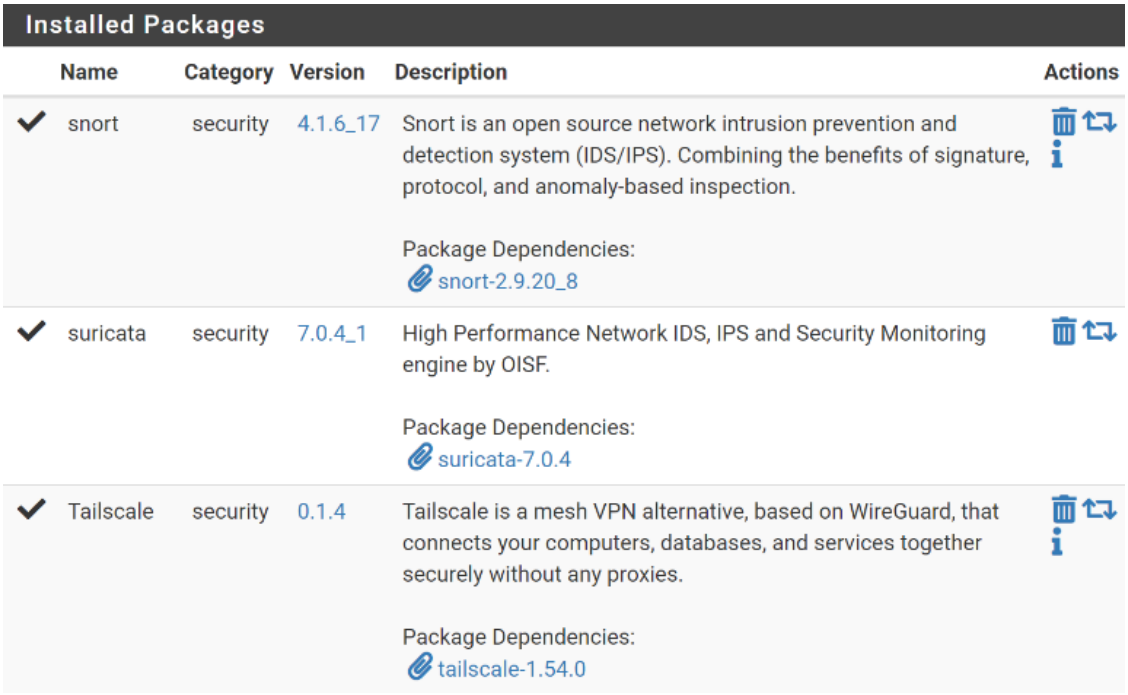

Figura 38. Panoul managerului de pachete Pfsense [Sursa: Autorul][96]

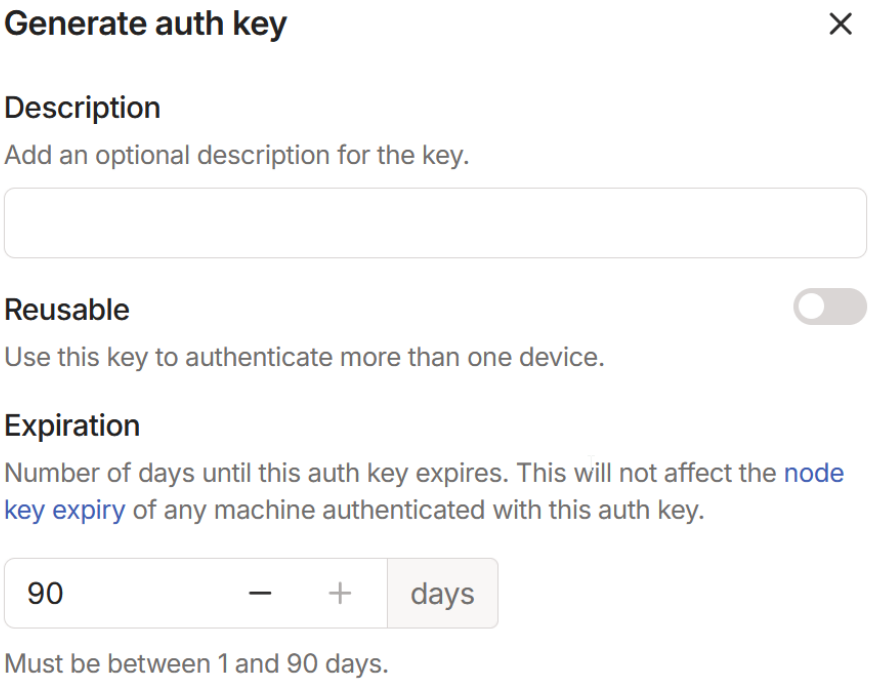

Figura 39. Generarea cheii de autentificare din panoul Tailscale [Sursa: Autorul][96]

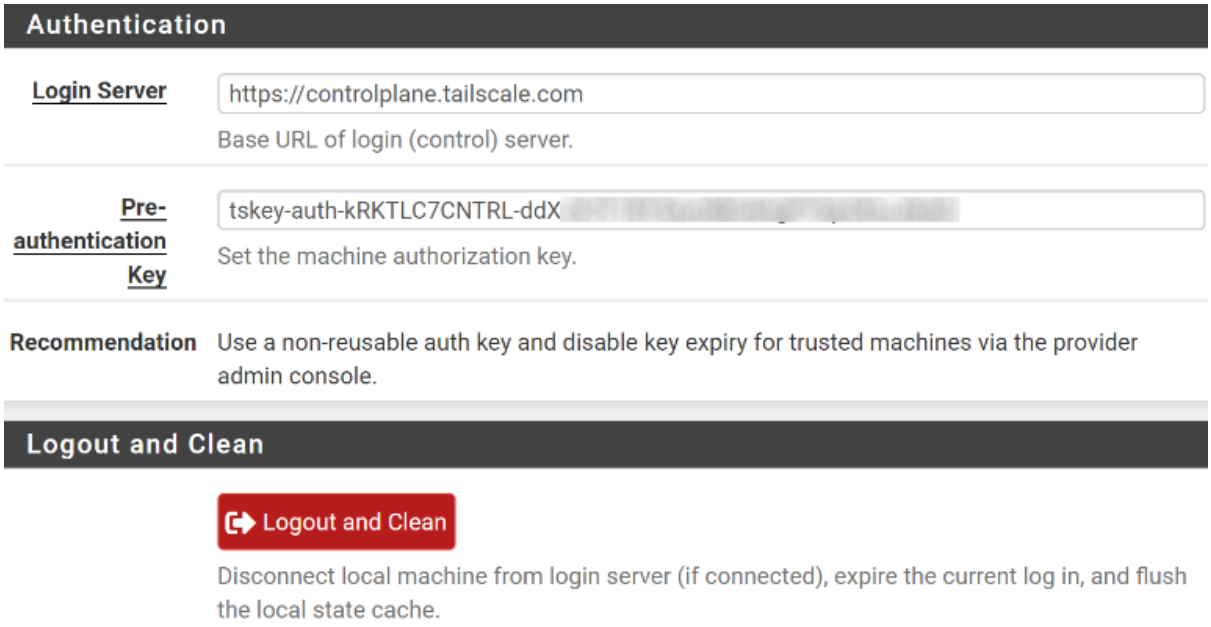

Figura 40. Panoul de autentificare în rețeaua Tailscale Pfsense [Sursa: Autorul][96]

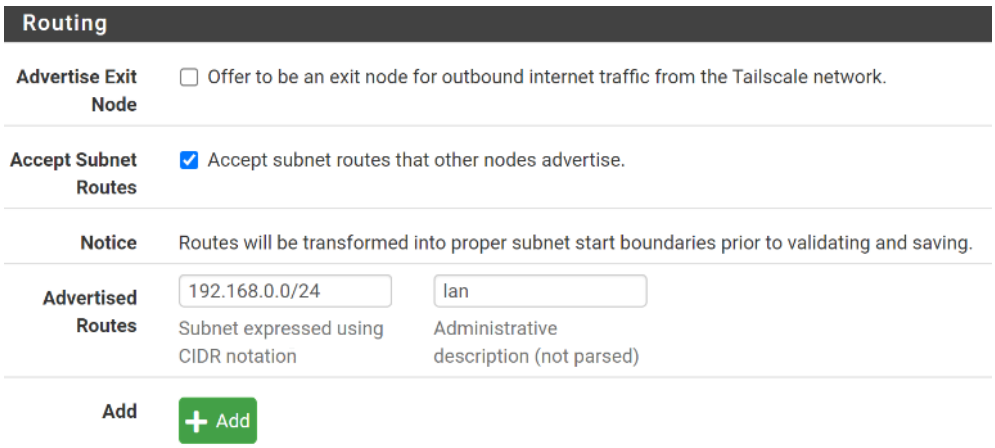

Figura 41. Expunerea subrețelei Pfsense în rețeaua Tailscale [Sursa: Autorul][96]

4.3.2 Securizarea transportului prin ZeroTier

ZeroTier One este o soluție SDN la nivelul 4 OSI, utilizând UDP pentru rețele suprapuse virtuale care se comportă ca Ethernet local. Fiecare nod are o identitate criptografică unică, cu XSalsa20-Poly1305 pentru criptarea autentificată a traficului și criptografie cu cheie publică pentru identitate. Traversarea inteligentă a NAT și criptarea AES-256 asigură confidențialitatea chiar în medii de rețea neîncrezătoare. Senzorul de teren stabilește o conexiune securizată la gateway traversând tunelul ZeroTier One care se termină la *firewall*, de unde traficul ajunge la platforma IoT. OPNsense suportă ZeroTier v1.12.2 prin secțiunea *System/Firmware/Plugins*, autorizarea nodurilor realizându-se din panoul ZeroTier Central prin bifarea opțiunii "*Auth*?".

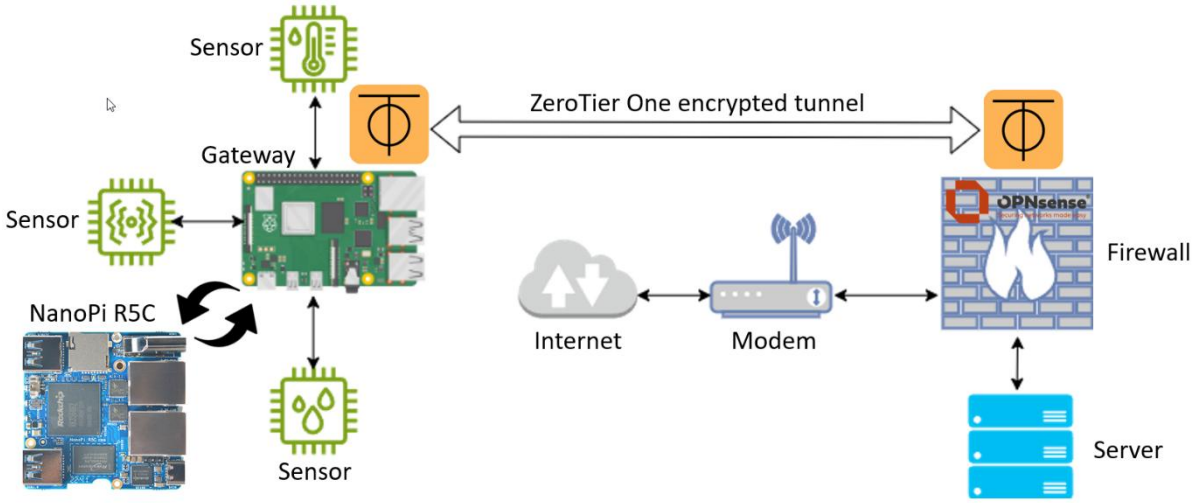

Figura 42. Modul de securizare a transportului de date cu ZeroTier [Sursa: Autorul][95]

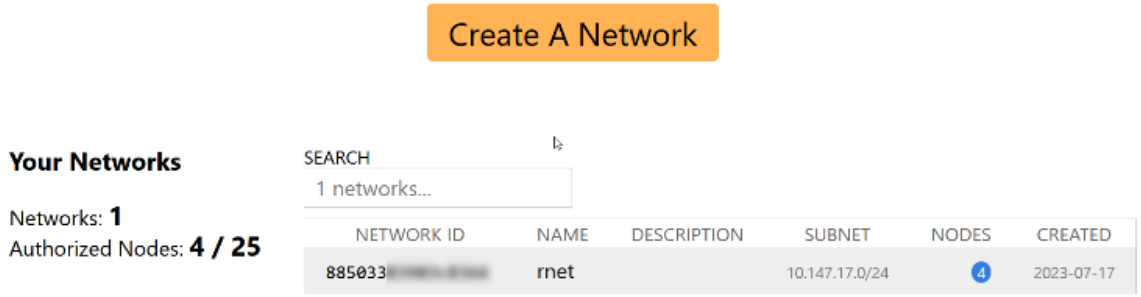

Figura 43. Rețelele create din panoul principal ZeroTier [Sursa: Autorul][95]

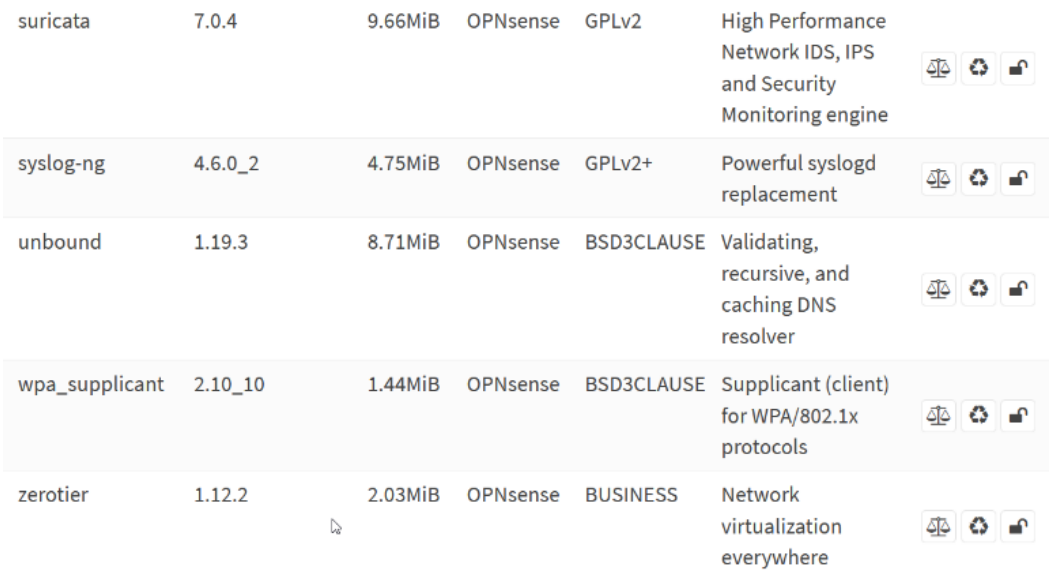

Figura 44. Managerul de scripturi suplimentare OPNsense [Sursa: Autorul][95]

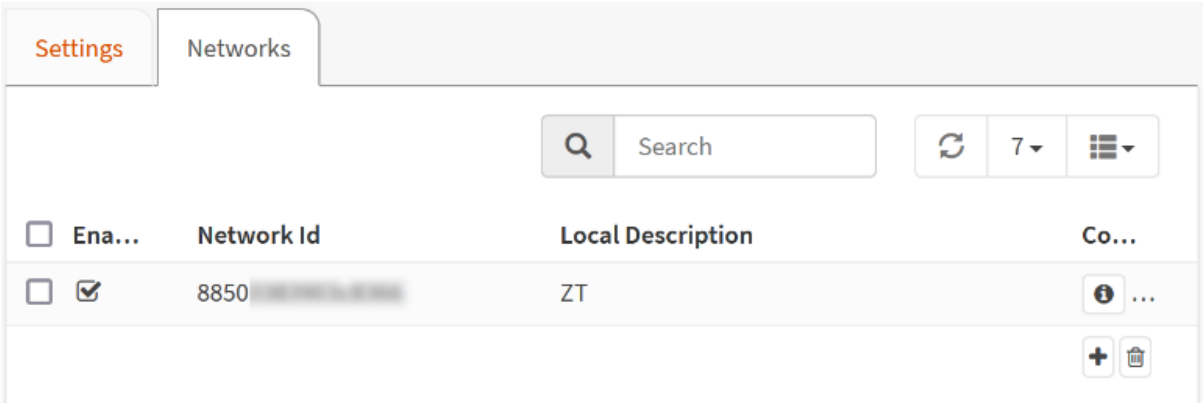

Figura 45. Panoul de autentificare în rețeaua ZeroTier OPNsense [Sursa: Autorul][95]

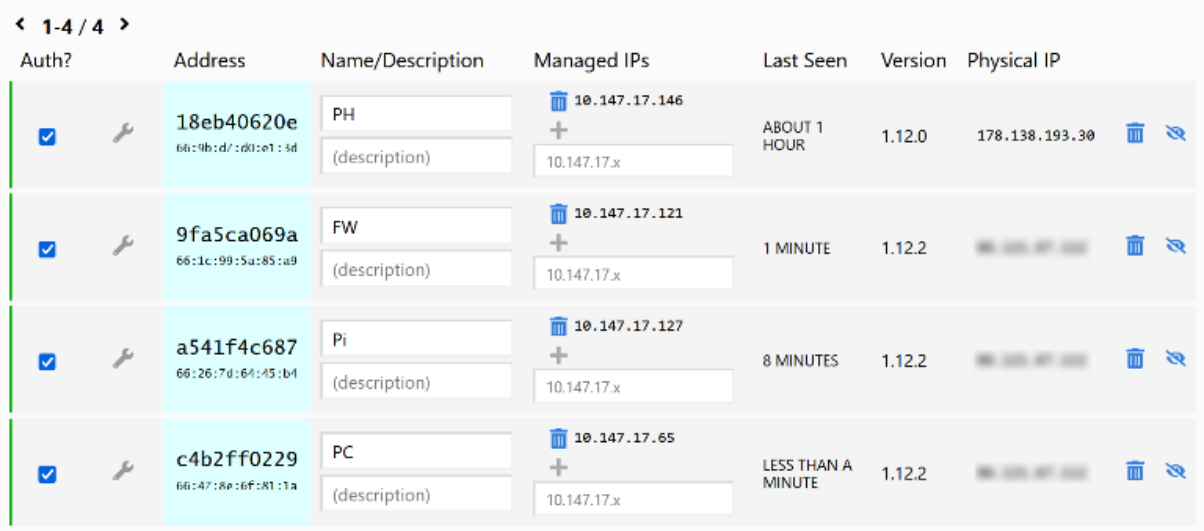

Figura 46. Panoul de autorizare în rețeaua ZeroTier [Sursa: Autorul][95]

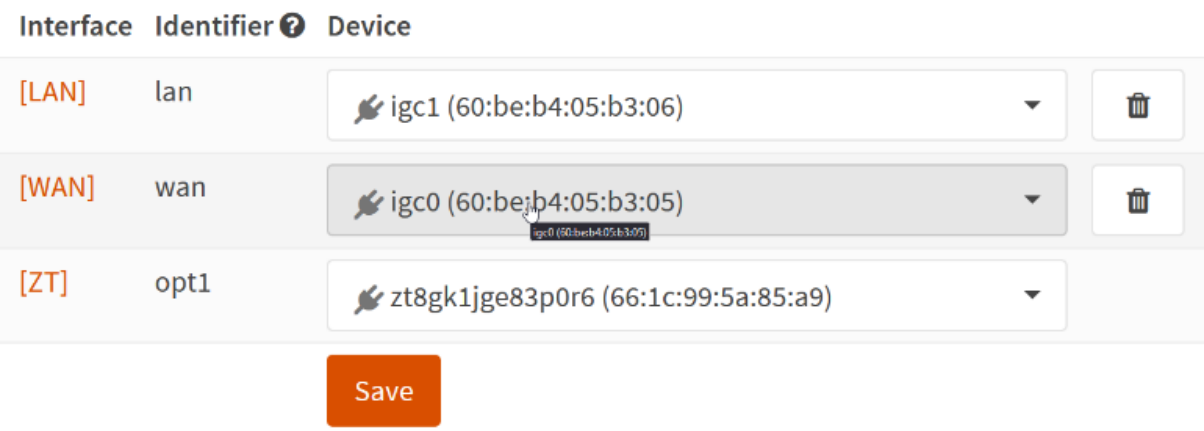

Figura 47. Alocarea interfeței OPNsense pentru scriptul ZeroTier [Sursa: Autorul][95]

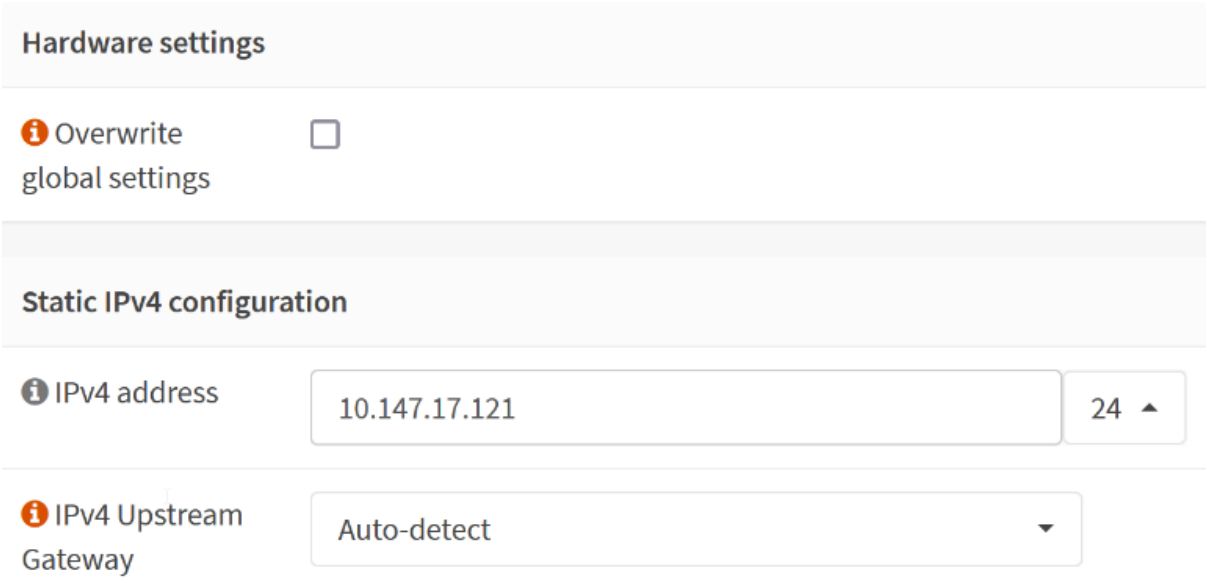

Figura 48. Configurarea adresei IP a interfeței pentru rețeaua ZeroTier [Sursa: Autorul][95]

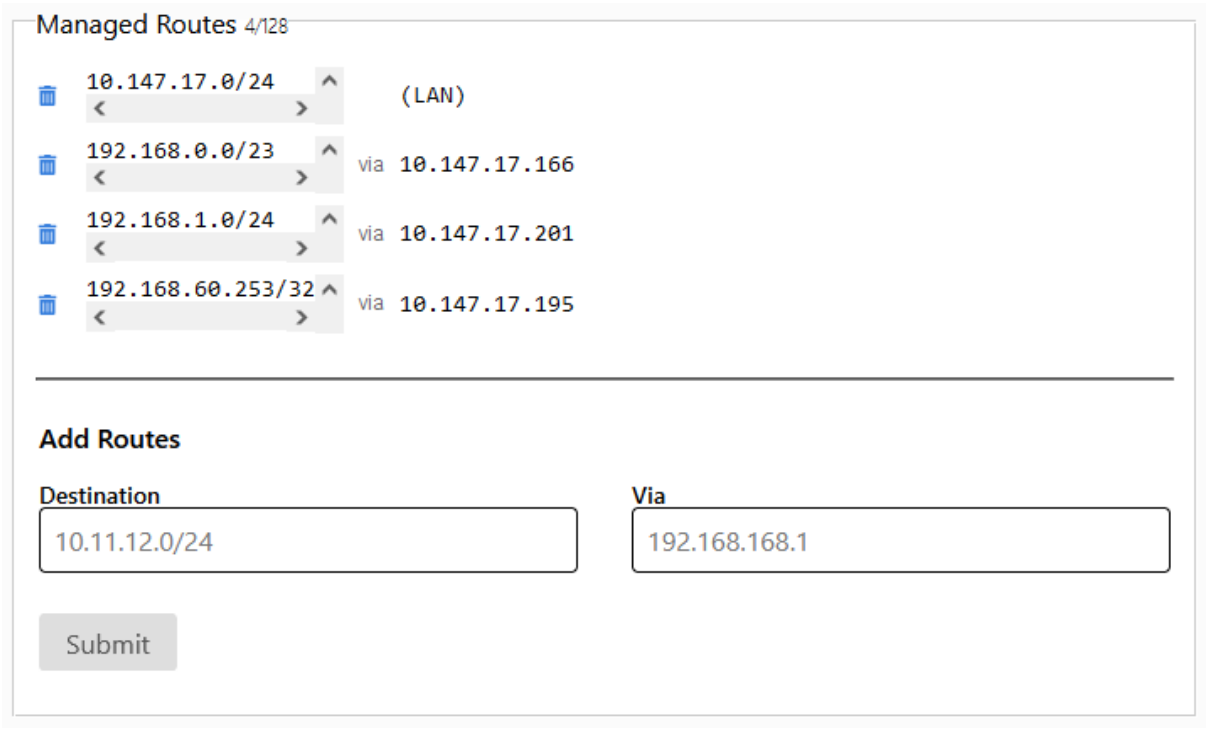

Figura 49. Expunerea subrețelei OPNsense în rețeaua ZeroTier [Sursa: Autorul][95]

OPNsens după conectarea la rețeaua privată ZeroTier, are nevoie de rutarea precum în figura 49 care arată cum se adaugă o subrețea care în interiorul *firewall*-ului este asociată cu o interfață care oferă conexiune la internet pentru dispozitivele conectate la aceasta. În mediile IoT, interfața ar putea fi izolată pentru a nu putea compromite întreaga rețea gestionată de *firewall*. Aceasta este o bună practică suplimentară pentru consolidarea securității în interiorul unei rețele.

În *gateway* fie cel bazat pe Raspberry Pi sau pe NanoPi R5C după instalarea clientului ZeroTier este și acolo nevoie de autorizare în intetriorul rețelei private [95].

4.3.3 Testare performanță servicii VPN

Studiul evaluează comparativ patru servicii VPN OpenVPN, WireGuard, Tailscale și ZeroTier One în contextul securizării mediilor IoT, măsurând latența (ping) și rata de transfer (Iperf3 v3.17) atât pe fibră optică, cât și pe GSM 4G (Digi 100 Mbit/s). OpenVPN și WireGuard necesită porturi deschise pe router (443, respectiv 51820), pe când Tailscale și ZeroTier stabilesc tuneluri *peer-to-peer* prin servere securizate, fără porturi deschise.

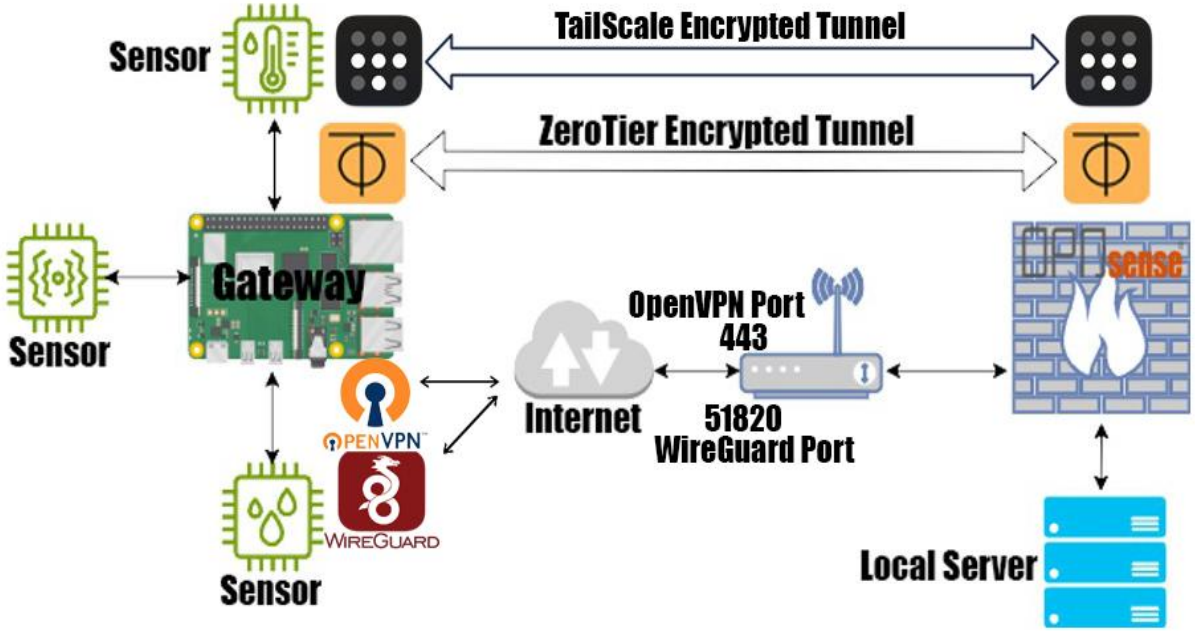

Figura 50. Prezentare generală a diagramei arhitecturii de testare [Sursa: Autorul][101]

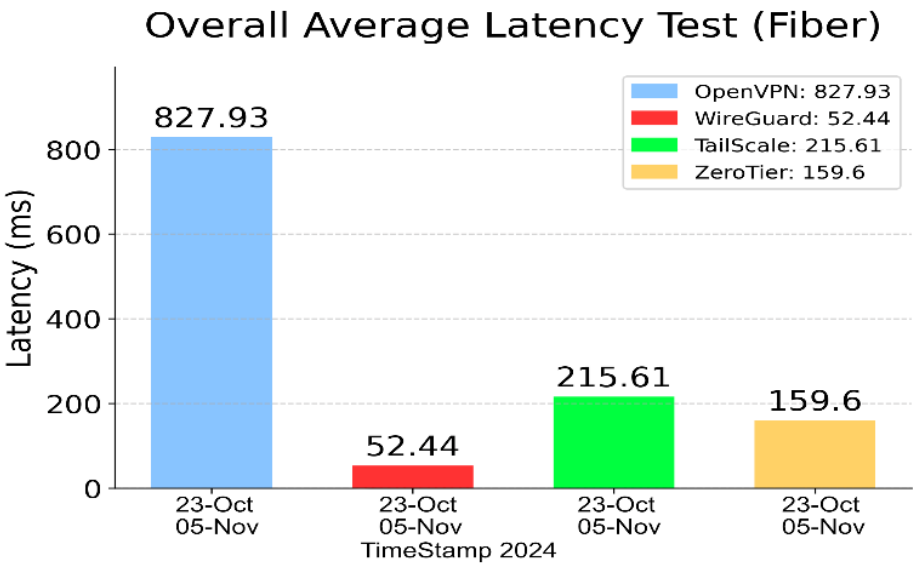

Figura 51. Test zilnic de latență utilizând o conexiune prin fibră optică [Sursa: Autorul][101]

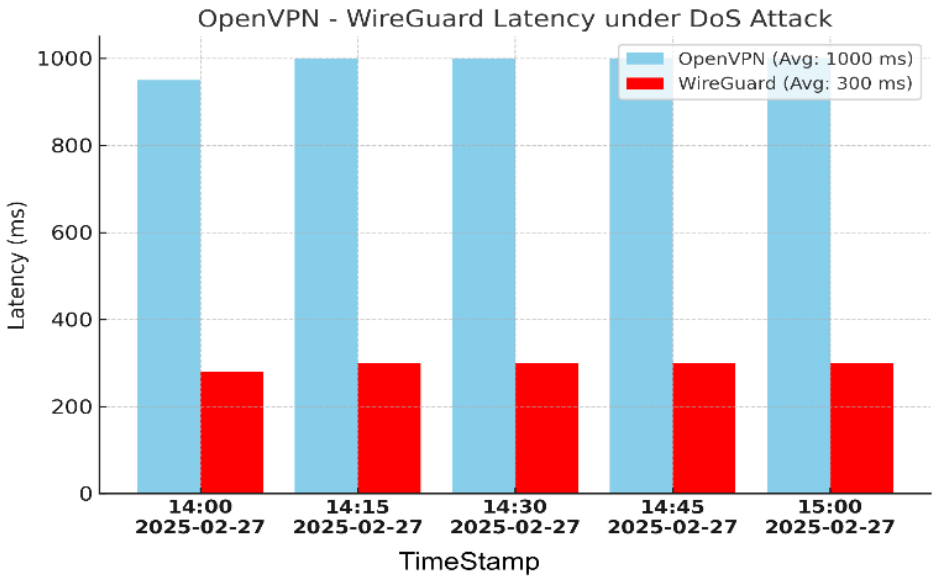

Figura 52. Test de latență conexiune prin fibră optică sub atac DoS [Sursa: Autorul][101]

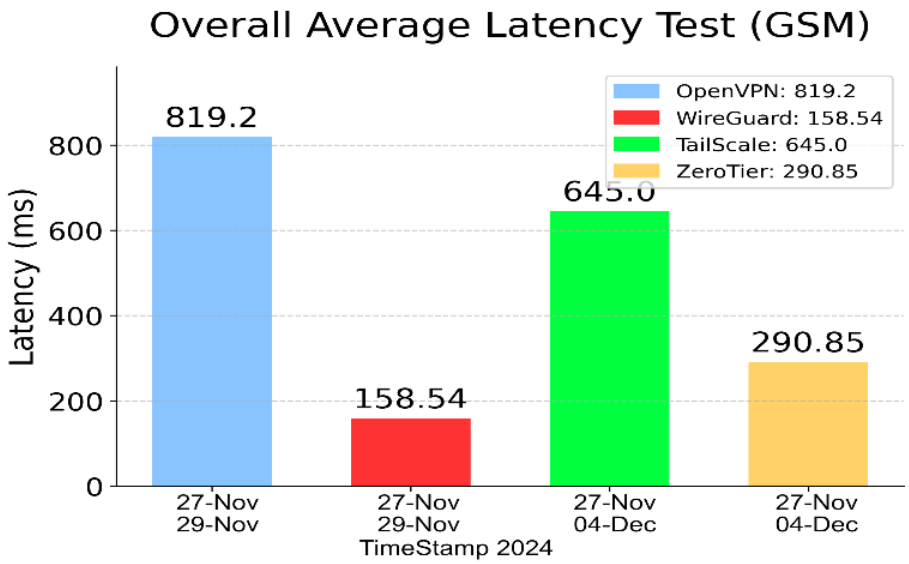

Figura 53. Test zilnic de latență utilizând o conexiune GSM (4G) [Sursa: Autorul][101]

TABEL VII. REZULTATELE TESTULUI TRANSFERULUI DE DATE IPERF3 FIBRĂ [SURSA: AUTORUL][101]

Tehnologii Testate	**Medie. Bitrate Server** Mbits/sec	**Medie. Bitrate Client** Mbits/sec	**Medie. Transfer Server** Mbytes	**Medie. Transfer Client** Mbytes
ZeroTier	10.32	14.81	1.24	1.77
TailScale	10.20	13.56	1.22	1.62
WireGuard	41.27	41.96	4.92	5.00
OpenVPN	32.28	32.44	3.85	3.87

TABEL VIII. REZULTATELE TESTULUI TRANSFERULUI DE DATE IPERF3 4G GSM [SURSA: AUTORUL][101]

Tehnologii Testate	**Medie. Bitrate Server** Mbits/sec	**Medie. Bitrate Client** Mbits/sec	**Medie. Transfer Server** Mbytes	**Medie. Transfer Client** Mbytes
ZeroTier	4.37	4.73	0.47	1.08
TailScale	5.61	12.75	0.68	1.52
WireGuard	24.06	24.09	2.87	2.87
OpenVPN	21.02	21.22	2.51	2.53

4.4 Soluții de securizare la nivelul aplicație

La nivelul 7 OSI, traficul HTTP este expus atacurilor SQLi, XSS și CSRF. *Web Application Firewalls* (WAF) efectuează inspecție profundă a cererilor HTTP, evaluând *payload*-ul, antetele și semnăturile de atac prin reguli euristice și *machine learning*. Proxy-urile inverse și gateway-urile API adaugă autentificare multi-factor, *rate limiting* și sanitizarea intrărilor.

4.4.1 Securizarea platformelor IoT prin Kemp LoadMaster

Kemp LoadMaster funcționează ca *load balancer* și *reverse proxy* la nivelul 7, cu descărcare TLS, WAF integrat (ModSecurity/OWASP CRS pentru SQLi/XSS), Adaptive SYN Checking și SYN Flood Protection. Cloudflare asigură proxy invers distribuit (anycast), ascunzând IP-ul de origine și aplicând filtrare L4/L7 și WAF. Proxy-urile edge efectuează terminarea TLS 1.3 cu certificate ECC P-384, urmate de validare mutuală mTLS cu load *balancer*-ul, consolidând rezistența la atacuri *man-in-the-middle*.

Virtual Service-ul se configurează pe portul 443 TCP la nivelul 7, cu certificat *wildcard* Cloudflare. Regulile de conținut (Content Rules) utilizează expresii regex (ex. ^/tbg/(.*)) și predicate SNI pentru rutarea către servicii *backend* specifice (ThingsBoard port 8080, Node-RED port 1880). Testele Nmap confirmă că, cu soluția activă, adresa IP vizibilă este a *proxy*-ului Cloudflare (188.114.96.16), nu a serverului local, expunând doar porturile 80, 443, 8080 și 8443 Cloudflare.

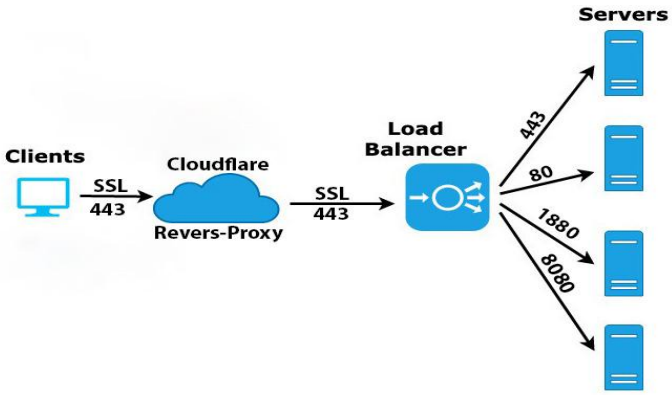

Figura 54. Arhitectura soluției implementate [Sursa: Autorul][93]

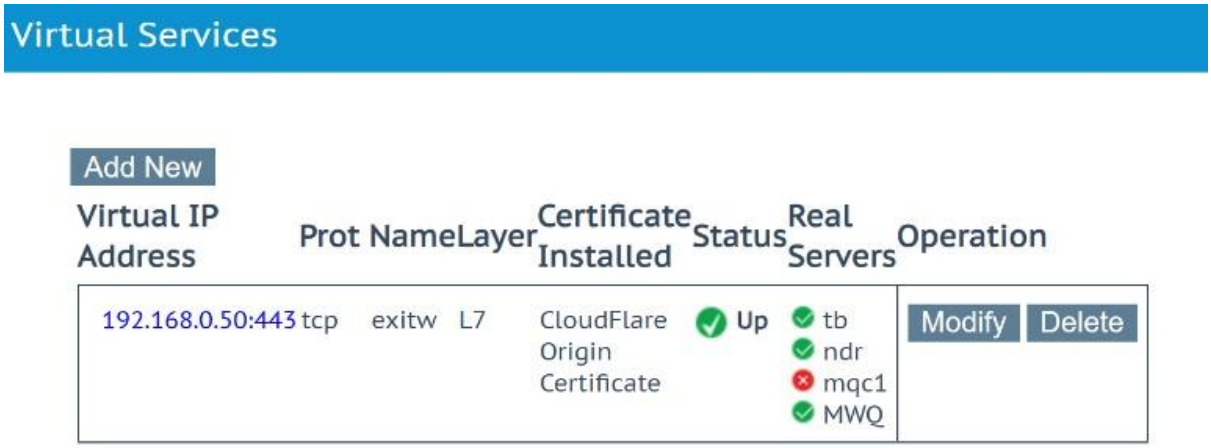

Figura 55. Panoul de gestionare serverelor virtualizate [Sursa: Autorul][93]

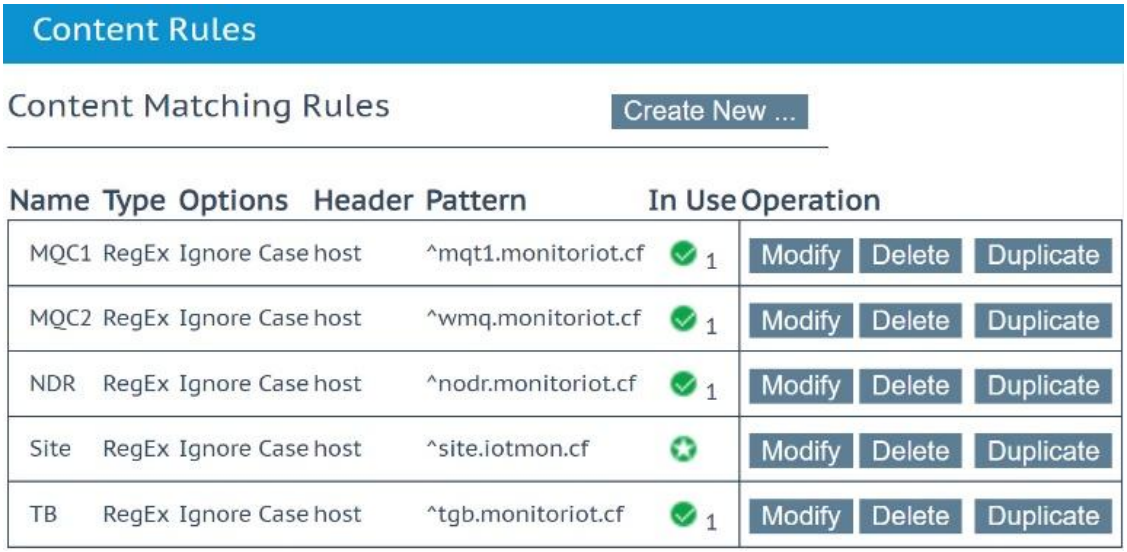

Figura 56. Panoul de gestionare al regulilor înregistrărilor DNS [Sursa: Autorul][93]

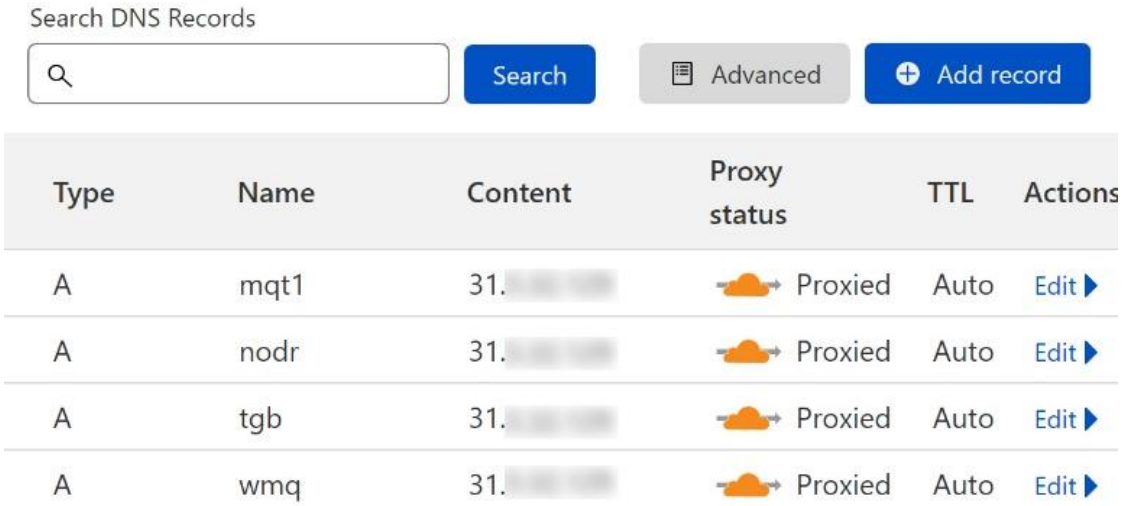

Figura 57. Panoul de gestionare al înregistrărilor DNS în Cloudflare [Sursa: Autorul][93]

```
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
┌──(hdsec㉿HDSec)-[~]
└─$ nmap tgb.monitoriot.cf
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-04 23:11 EEST
Nmap scan report for tgb.monitoriot.cf (188.114.96.16)
Host is up (0.0093s latency).
Other addresses for tgb.monitoriot.cf (not scanned): 2a06:98c1:3120::10 2a06:98c1:3121::10 188.114.97.16
Not shown: 640 filtered tcp ports (no-response), 356 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

Figura 58. Test Nmap cu soluția load balancer activă [Sursa: Autorul]

```
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds

┌──(hdsec㉿HDSec)-[~]
└─$ nmap 31.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-04 23:13 EEST
Nmap scan report for 31.
Host is up (0.0092s latency).
Not shown: 634 filtered tcp ports (no-response), 363 filtered tcp ports (host-unreach)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  closed http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
```

Figura 59. Test Nmap cu soluția load balancer dezactivată [Sursa: Autorul]

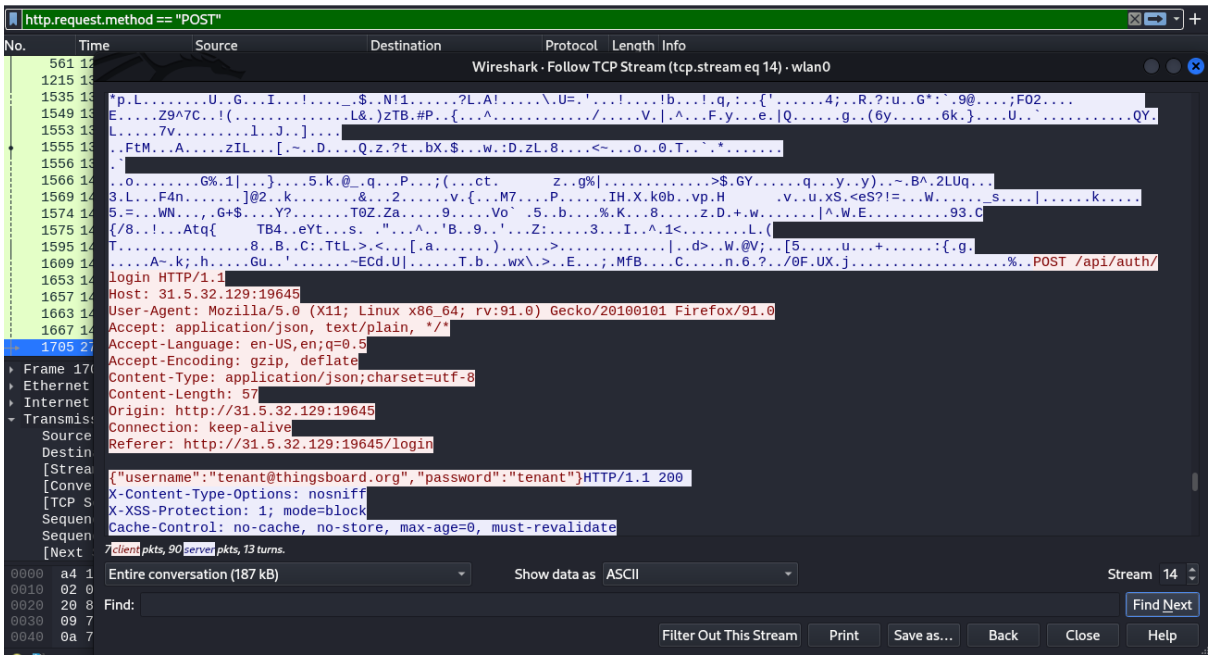

Figura 60. Test simulare atac man in the middle [Sursa: Autorul]

Testul MITM cu EtterCap (ARP poisoning) demonstrează că, dacă rețeaua IoT nu este izolată și traficul este necriptat, credențialele pot fi extrase din cererile HTTP POST. Soluția *load balancer* cu Cloudflare elimină acest risc prin criptare *end-to-end* și ascunderea IP-ului real al *server*-ului.

4.4.2 Securizarea platformelor IoT prin Nginx Proxy Manager și TailScale

Nginx Proxy Manager (NPM) rulat ca container Docker pe o instanță Oracle Cloud VPS (gratuit: 1 CPU, 1 GB RAM, 50 GB stocare, Ubuntu 22.04) funcționează ca *reverse proxy* și *load balancer*. Traficul este criptat TLS între client și instanța *cloud* (Cloudflare), iar de la *cloud* la *server*-ul local prin tunelul WireGuard Tailscale (latență adăugată 15-25 ms). NPM gestionează certificatele Let's Encrypt prin clientul ACME integrat (HTTP-01/DNS-01), cu reînnoire automată la 90 de zile. *Server*-ul local, pozitionat în spatele CGNAT, este conectat la instanța VPS prin rețeaua Tailscale, desemnat ca *router* de subrețea (tag "Subnet"). Înregistrările DNS Cloudflare de tip A sunt configurate cu *proxy* activat (portocaliu) pentru fiecare subdomeniu, direcționând traficul spre IP-ul public al VPS-ului Oracle și mascând *server*-ul de origine. Abordarea se aliniază principiilor *zero-trust* fără a necesita echilibratoare de sarcină *hardware*.

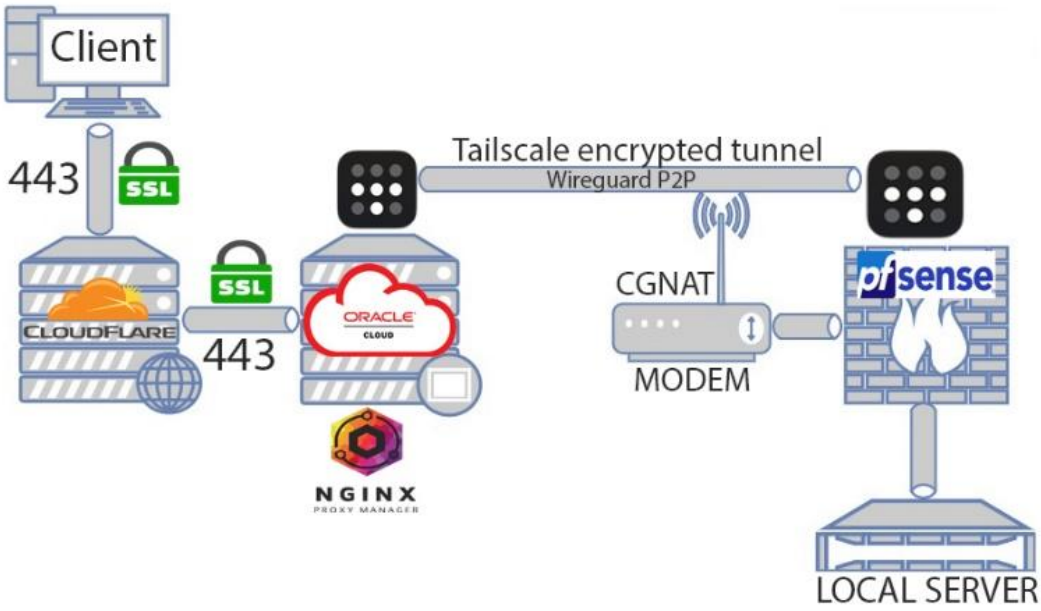

Figura 61. Arhitectura soluției implementate [Sursa: Autorul][94]

Create instance | Actions

Name	State	Public IP	Private IP	Shape	OCPU count	Mem
Server1 Always Free	Running	[redacted]9.71	10.0.0.165	VM.Standard.E2.1.Micro	1	1
Server2 Always Free	Running	[redacted]4.120	10.0.0.155	VM.Standard.E2.1.Micro	1	1

0 selected | Showing 2 items | 1 of 1

Figura 62. Panoul de control al instanței VPS [Sursa: Autorul][94]

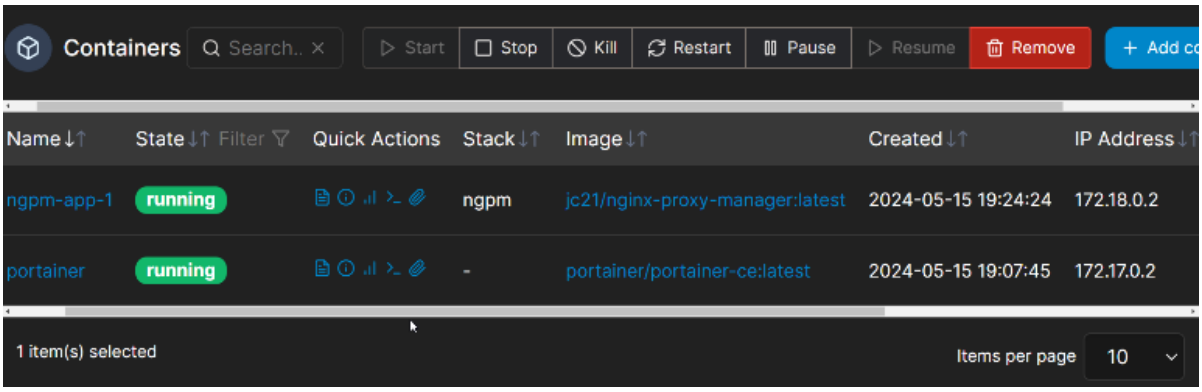

Figura 63. Rularea containerului docker în interiorul Portainer [Sursa: Autorul][94]

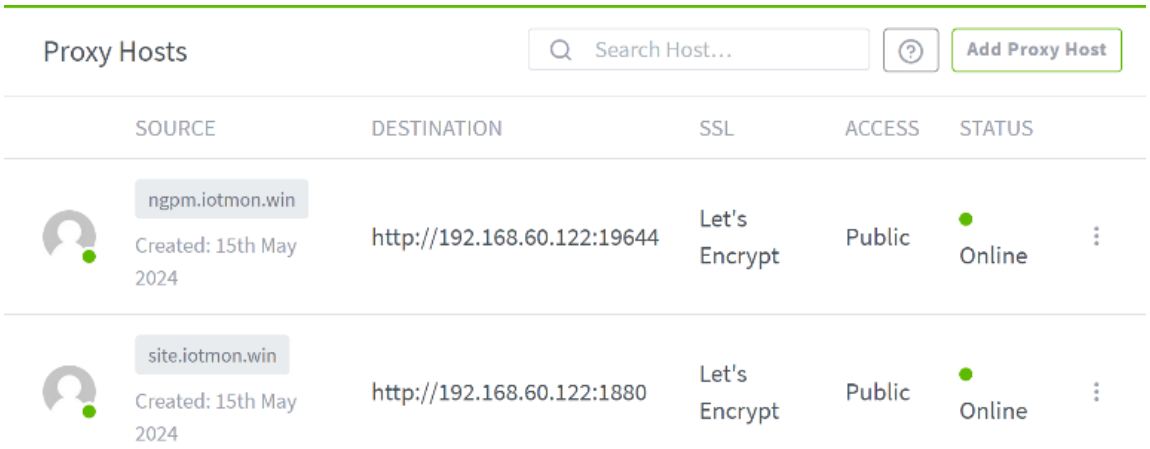

Figura 64. Panoul de gestionare a serviciilor găzduite cu proxy [Sursa: Autorul][94]

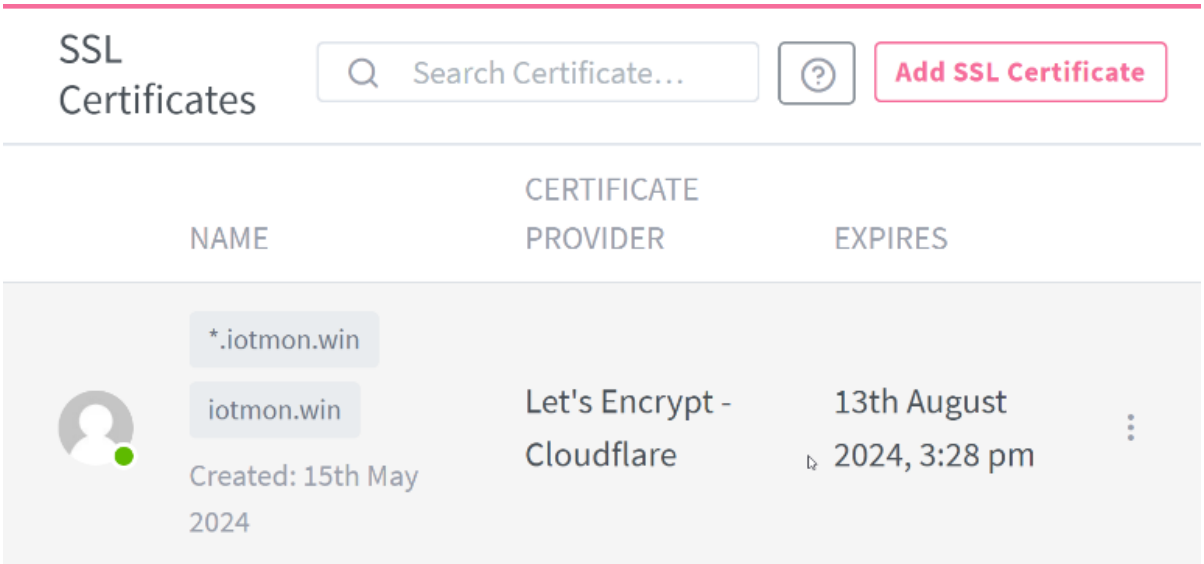

Figura 65. Panoul de gestionare a certificatelor TLS [Sursa: Autorul][94]

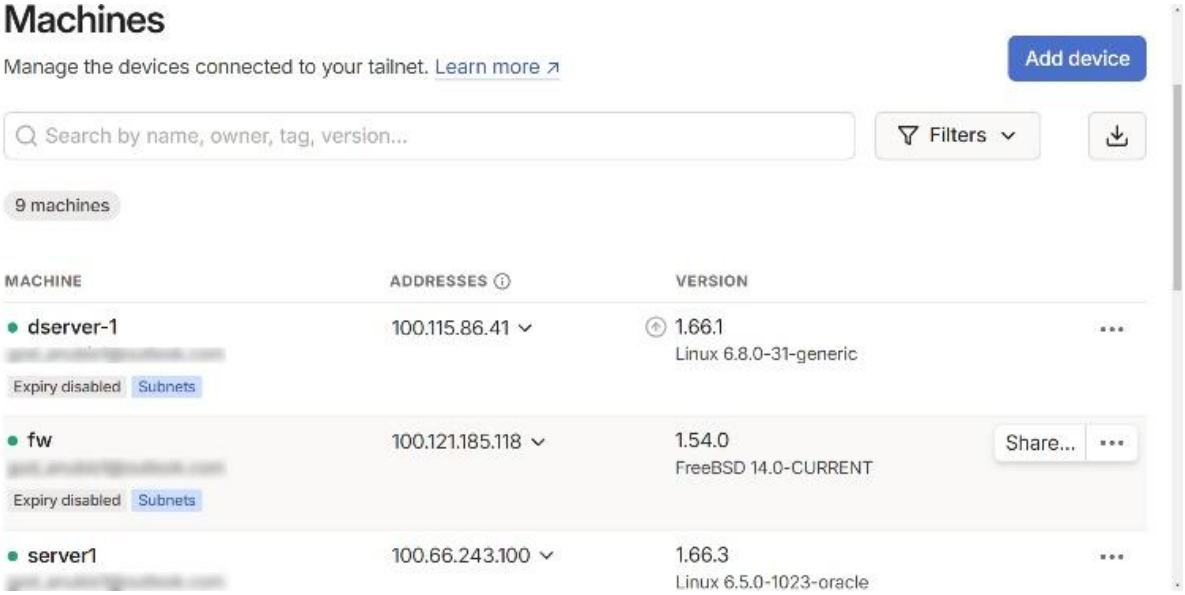

Figura 66. Panoul de control TailScale cu cele 2 servere active [Sursa: Autorul][94]

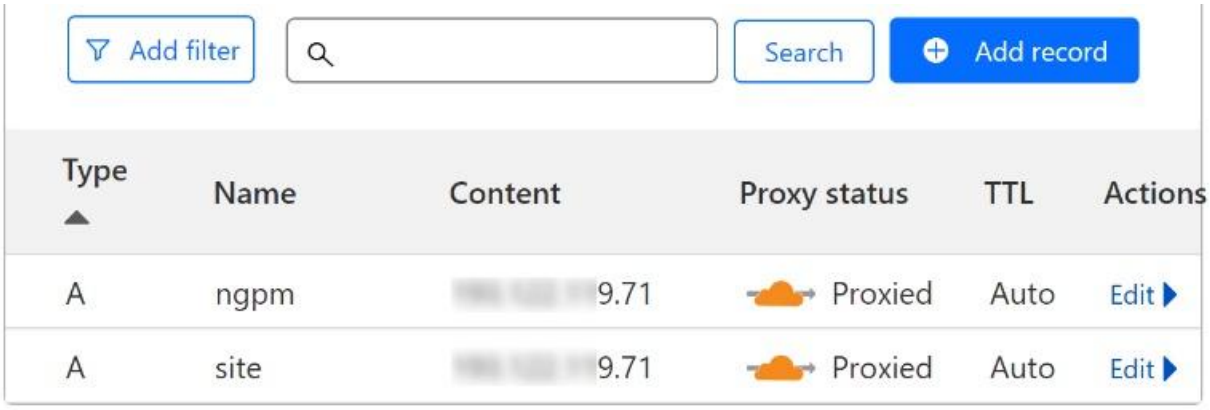

Figura 67. Panoul de gestionare a înregistrările DNS din Cloudflare [Sursa: Autorul][94]

Așa cum se arată în Figura 67, înregistrările de „A”, au fost configurate meticulos pentru fiecare subdomeniu corespunzător serviciilor găzduite prin Nginx Proxy Manager, toate intrările DNS redirecționând către adresa IP publică a instanței VPS Oracle Cloud. Pentru a spori securitatea, opțiunea de *proxy* Cloudflare care utilizează capacitățile CDN și de atenuare a atacurilor DDoS ale Cloudflare a fost activată pentru fiecare subdomeniu, interpunând un strat suplimentar de protecție care ascunde serverul de origine și filtrează traficul rău intenționat.

Această configurație permite o evaluare riguroasă folosind aceleași teste de evaluare a vulnerabilităților utilizate pentru implementarea bazată pe Kemp LoadMaster, în special tehnicile de scanare a porturilor deschise, pe care adversarii le exploatează de obicei pentru a enumera serviciile, a identifica configurările greșite sau a orchestra atacuri *Denial-of-Service* (DoS). Indicatorii cantitativi, cum ar fi expunerea porturilor, timpii de răspuns și suprasarcina indusă de *proxy*, pot fi comparați sistematic între implementări pentru a valida starea de securitate.

Deși această *proxy* introduce o latență crescută, atribuibilă salturilor de rețea suplimentare prin infrastructura globală a Cloudflare, aceasta constituie un compromis pragmatic și accesibil pentru implementările limitate de absența unei adrese IP publice dedicate, democratizând astfel accesul securizat la distanță pentru mediile IoT [94].

5. Concluzii generale și perspective

Proliferarea rapidă a ecosistemelor internetului obiectelor (IoT) în domeniile industrial, medical și al infrastructurilor critice a precipitat un peisaj al amenințărilor din ce în ce mai sofisticat și eterogen. Implementările IoT contemporane sunt caracterizate de fragmentarea protocoalelor, de puncte terminale cu resurse limitate și de absența unor cadre de securitate unificate care să acopere întregul model de referință OSI. Aceste deficiențe structurale fac ca soluțiile existente să fie în mod inerent incomplete, abordând straturi izolate în mod izolat, în loc să ofere o protecție coerentă multinivel.

Prezenta teză abordează această lacună printr-un program de cercetare în trei etape: (1) identificarea sistematică și clasificarea taxonomică a vulnerabilităților de securitate ale IoT în toate cele șapte straturi OSI; (2) selectarea și justificarea pe bază de dovezi a unui pachet tehnologic *hardware* și *software* capabil să atenueze categoriile de amenințări identificate; și (3) implementarea experimentală, măsurarea și validarea empirică a arhitecturii propuse în condiții de atac simulate în lumea reală. Cercetarea demonstrează că reziliența cibernetică de nivel industrial a IoT poate fi obținută prin orchestrarea inteligentă a componentelor *open-source* și accesibile din punct de vedere al costurilor, fără a depinde de soluții brevetate sau cu buget mare.

Prima contribuție originală a acestei teze constă într-o sinteză analitică cuprinzătoare, structurată critic, a stadiului actual al tehnologiei în domeniul securității IoT, realizată prin revizuirea sistematică a literaturii științifice primare, a rapoartelor de informații privind amenințările (ENISA 2024) și a datelor empirice privind incidentele. Această contribuție vine în ajutorul interpretării studiilor din literatura de specialitate prin introducerea unui cadru analitic cu două axe care corelează clasele de vulnerabilități cu frecvența exploatării lor în lumea reală și mapează fiecare lacună direct la o contramăsură arhitecturală propusă. În literatura de specialitate au fost identificate patru categorii structurale de deficiențe metodologice:

- **Absența soluțiilor hibride integrate la nivelul întregii stive OSI**. Literatura de specialitate abordează în mod predominant securitatea la un singur nivel de protocol sau în mod izolat. Evaluările experimentale care combină întărirea *gateway*-ului fizic, IDS-ul la nivelul rețelei, VPN-ul la nivelul transportului și echilibrarea sarcinii la nivelul aplicației - exact arhitectura propusă aici - sunt absente din *corpus*-ul analizat.
- **Lipsa evaluărilor de performanță în condiții de atac activ**. Studiile teoretice încorporează rareori măsurători de latență și debit obținute în timpul simulării DoS sau *botnet live*, lăsând un gol empiric critic pentru scenariile hibride VPN și *reverse-proxy*.
- **Constrângeri de scalabilitate Zero-Trust pentru puncte finale eterogene, cu resurse limitate**. Implementările Zero-Trust existente presupun dispozitive cu suficientă memorie RAM pentru re-autentificare continuă, ceea ce le face inaplicabile pentru nodurile MCU cu mai puțin de 32 KB RAM.
- **Nepotrivire între prioritizarea amenințărilor în mediul academic și realitatea operațională**. Conform ENISA-24, acreditările implicite și *botnet*-urile DDoS reprezintă amenințările reale cu cea mai mare frecvență; cu toate acestea, literatura academică se concentrează în mod disproporționat asupra vectorilor de atac avansați (canal lateral, post-cuantum, gaura de vierme RPL), creând un decalaj între cercetare și practică cu consecințe industriale semnificative.

Pe baza acestor constatări, au fost derivate formal și operaționalizate cinci cerințe funcționale normative (C1–C5), constituind cadrul de evaluare aplicat în capitolele 3 și 4. Standardele criptografice moderne - inclusiv profilurile EDHOC, OSCORE și DTLS 1.3 - s-au dovedit a fi viabile pe dispozitive cu resurse limitate, cu toate că au costuri suplimentare măsurabile de energie și latență. Abordările ML/IDS federative au fost identificate ca introducând provocări legate de robustețea adversarilor, subliniind în mod colectiv necesitatea unor arhitecturi coerente multistrat în locul unor soluții punctuale izolate.

A doua contribuție originală constă în selectarea sistematică, bazată pe criterii și sinteza integrativă a unui ecosistem *hardware-software* complet pentru securitatea IoT industrială, guvernat de trei principii de proiectare generale: apărare în profunzime (fiecare componentă acoperă un segment de strat OSI distinct, care nu se suprapune), accesibilitate economică (utilizarea exclusivă a *software*-ului *open-source* și a *hardware*-ului recondiționat sau *low-cost*) și aliniere la economia circulară (extinderea ciclului de viață al hardware-ului industrial la sfârșitul ciclului de viață).

Stiva *hardware* cuprinde: PC-uri industriale Beckhoff care execută pfSense/OPNsense ca firewall-uri perimetrale (L1-L3); servere HP ProLiant DL360 G7 care asigură virtualizarea VMware ESXi pentru izolarea serviciilor (L3-L7); *gateway*-uri de teren Raspberry Pi 3B+ și NanoPi R5C care rulează OpenWRT cu WPA3 și tuneluri VPN WireGuard/Tailscale (L2-L4); *modem*-uri USB Huawei LTE pentru conectivitate GSM/4G de rezervă (L1-L2); și Netgear ReadyNAS 3000 pentru stocare persistentă decuplabilă (L7). Toate echipamentele hardware sunt reutilizate în proporție de 100% sau achiziționate la mâna a doua, demonstrând că reziliența cibernetică de nivel industrial nu necesită achiziții de capital intensive.

Stiva de *software* cuprinde: pfSense/OPNsense cu Snort/Suricata IDS/IPS în linie (L2-L4); WireGuard, ZeroTier, Tailscale și OpenVPN evaluate comparativ pentru securitatea transportului (L4); Kemp LoadMaster și Nginx Proxy Manager pentru terminarea TLS și servicii de *proxy* invers (L5-L7); și Cloudflare DNS/*Proxy* pentru absorbția DDoS, mascarea IP de origine și gestionarea automată a certificatelor (L7). Aceasta reprezintă o paradigmă a orchestrării inteligente a resurselor ca determinant principal al posturii de securitate, independent de amploarea bugetului.

A treia și principala contribuție originală a acestei teze este proiectarea, implementarea și evaluarea experimentală riguroasă a arhitecturii de securitate stratificate propuse, atât în condiții normale de funcționare, cât și în scenarii de adversitate simulate. Această contribuție acoperă în mod direct lacuna empirică identificată în contribuția I și validează toate cele cinci cerințe C1-C5 prin indicatori-cheie de performanță (KPI) măsurabili.

Tabelul 15 oferă o sinteză integrată a contribuțiilor originale ale acestei teze, structurată pe nivel sau strat OSI. Pentru fiecare nivel, sunt prezentate principalul vector de amenințare, soluția tehnologică pusă în aplicare, rezultatul măsurabil obținut și cerința de cercetare abordată, permițând o evaluare sistematică de către comitetul de evaluare.

TABEL IX. SINTEZA CONTRIBUȚIILOR AUTORULUI ȘI SOLUȚIILE PROPUSE PE MODELUL OSI [SURSA: AUTORUL]

Nivel OSI	Amenințările principale	Soluții implementate	Rezultat empiric / KPI	Cerințe	Capitole
L1	Interceptarea semnalelor, bruiajul, atacurile pe canale laterale, sabotaj fizic	Platfome (SBC) ca gateway fizic securizat; modem Huawei LTE pentru redundanță GSM/4G failover, dulap închis	Timp de funcționare continuu; failover LTE operațional, împiedicarea accesului persoanelor fără cheie acces la dulap	C1	3 și 4
L2	ARP poisoning, MAC spoofing	Segmentarea VLAN pfSense/OPNsense; VLAN IoT dedicat; WPA2/WPA3 pe gateway-uri de teren (Raspberry pi / NanoPi R5C)	Izolarea L2 completă confirmată; rezistența la atacurile MITM/ISP	C1 și C2	3 și 4
L3	RPL rank/sinkhol e/wormhole, Sybil, botnet C2 (Frecvență ridicată)	Inline Snort/Suricata IDS pe gateway SBC; pfSense stateful firewall; Cloudflare DDoS absorption	Firewall + IDS latență <2 ms la 1 Gbps; semnături Mirai/Modbus detectate; 87% reducere a suprafeței de atac	C2 și C5	3 și 4
L4	MQTT fără TLS, UDP spoofing, TCP overhead, DdoS botnets (Frecvență foarte mare)	WireGuard (VPN principal); ZeroTier (mesh overlay); Tailscale (gestionat prin MFA); OpenVPN (referință de bază); teste de sarcină iperf3	WireGuard: 41.96 Mbps /52.44 ms; OpenVPN: 32.44 Mbps / 827 ms; ZeroTier: 14.81 Mbps /159.6 ms; Tailscale: 13.56 Mbps / 215.61 ms	C3 și C5	4
L5-L6	Sesiuni neautentificate, fluxuri de date necriptate, certificate expirate	Kemp LoadMaster Terminare TLS cu sesiuni lipicioase; Nginx Proxy Manager cu reînnoire automată Let's Encrypt; Cloudflare wildcard TLS	TLS 1.3 aplicat end-to-end; zero intervenții manuale asupra certificatelor; reînnoire automată validată	C4	3 și 4
L7	Autentificări implicite, atacuri prin injectare, chei hardcoded, firmware vulnerabil (Critic – cel mai exploatat)	Reverse-proxy TLS (Nginx / Kemp); mascarea IP-ului de origine Cloudflare; izolarea containerizată (Docker/Portainer); căi de expunere dual; Oracle Cloud overlay	Expunere exclusivă la portul 443; latență suplimentară de 15-25 ms pentru calea containerizată; +53% creștere DdoS absorbită; 87% reducere a suprafeței de atac confirmată [107]	C4 și C5	3 și 4

Perspectivele și direcțiile de cercetare viitoare vor fi fundamentate pe analiza critică a literaturii, experimentele anterioare și lacunele metodologice identificate. Fiecare direcție este însoțită de KPI măsurabili, iar orizonturile temporale reflectă maturitatea tehnologică (TRL) și standardele internaționale relevante (NIST, ETSI, IEEE). În primă fază se vor menționa care sunt soluțiile viitorului, iar mai apoi se menționează o foaie de parcurs pentru următorii ani.

1. Adaptare dinamică a criptării coordonată de inteligență artificială

Direcția vizează un sistem de criptare adaptivă în care modele ML supervizate antrenate pe date telemetrice Suricata analizează în timp real profilul de risc al fluxurilor IoT și ajustează dinamic nivelul criptografic (AES-128 vs. AES-256) și parametrii TLS. Metodologic, se propun modele multi-clasă (Random Forest, XGBoost) cu validare k-fold. Ipoteza testabilă: mecanismul adaptiv reduce consumul energetic cu ≥20% față de AES-256 static, fără degradarea securității.

2. Detectarea distribuită a intruziunilor prin învățare federată (FL-IDS)

Arhitecturile *Federated Learning* permit antrenarea colaborativă a modelelor IDS pe jurnalele Suricata EVE JSON locale, fără transfer de date brute. Cercetările viitoare vor investiga reziliența algoritmilor FedAvg/FedProx la atacuri de gradient poisoning și impactul procentului de participanți compromiși. Comunicația *inter-gateway* (mTLS cu certificate rotative) va fi analizată separat pentru *overhead*-ul de rețea indus.

3. Optimizarea rutării prin învățare prin întărire în suprapuneri VPN

Integrarea algoritmilor *Deep Q-Network* (DQN) în planul de control WireGuard/ZeroTier vizează rutarea predictivă capabilă să anticipeze congestia și să evite vectorii de atac LoRaWAN. Definirea spațiului de stare (latență, jitter, pierdere pachete, scor Suricata) și a funcției de recompensă rămân provocări deschise. Evaluarea comparativă față de OSPF/BGP pe topologii reprezentative este o cerință metodologică fundamentală.

4. Migrarea către criptografia post-cuantică în tunelurile VPN

Standardizarea NIST a CRYSTALS-Kyber (ML-KEM) și CRYSTALS-Dilithium (ML-DSA) în 2024 deschide calea consolidării VPN împotriva amenințărilor cuantice. Cercetările propuse vizează testarea sintetică a schimburilor hibride X25519+Kyber pe microcontrolere ARM Cortex-M, cu obiectivul menținerii latenței *handshake* sub 10 ms. Interoperabilitatea cu stivele TLS existente (OpenSSL, wolfSSL) și impactul asupra *overhead*-ului LPWAN vor fi evaluate distinct [111].

5. Accelerare eBPF/XDP și generarea regulilor de firewall prin ML

Tehnologiile eBPF/XDP permit procesarea pachetelor în *kernel* cu latențe sub-microsecundă, esențiale pentru scalare la debitele 6G/IoT masiv (10–40 Gbps). Direcția propusă automatizează generarea și actualizarea regulilor eBPF prin modele ML antrenate pe profiluri Suricata. Complementar, atestarea SBOM ancorată în *blockchain* (*Hyperledger Fabric, Proof-of-Stake*) securizează lanțul de aprovizionare al dispozitivelor IoT de margine.

6. Explicabilitate AI (XAI) și autentificare Zero-Knowledge

Tehnicile XAI (SHAP, LIME) integrate cu alertele Suricata generează explicații interpretabile pentru operatorii SOC, reducând alert fatigue. Utilitatea explicațiilor va fi validată prin studii cu operatori, folosind *System Usability Scale* (SUS). Protocoalele zkSNARK (Circom/SnarkJS), combinate cu biometria comportamentală AI, minimizează scurgerile de metadate în *handshake*-urile mTLS IoT, cu aplicabilitate în infrastructuri critice.

7. Modelare Tehnico-Economică și Simulare Adversarială prin GAN

Modelele TCO (optimizare multi-obiectiv sau regresie ML) vor ghida selecția configurației optime WireGuard vs. ZeroTier L2 în funcție de constrângerile specifice contextului de implementare. Rețelele GAN antrenate pe trafic de atac real vor sintetiza noi vectori de atac, utilizabili în exerciții de red-team automatizate pentru consolidarea proactivă a posturii de securitate.

TABEL X. INDICATORI CHEIE DE PERFORMANȚĂ (KPI) PENTRU DIRECȚIILE DE CERCETARE PROPUSE [SURSA: AUTORUL]

Direcție de Cercetare	KPI Principal	Valoare Țintă	Orizont Temporal	Metodă de Validare	TRL
Criptare dinamică AI (AES-128/256 adaptiv)	Latență re-criptare	<30 ms (p95)	2026–2027	Testare A/B, Suricata EVE	4–5
Învățare federată FL-IDS	Acuratețe detectare	≥94% F1-score	2027–2028	NSL-KDD / CICIDS2018	3-4
Rutare AI DQN (WireGuard/ZeroTier)	Reducere congestie	<15% packet loss	2027–2028	Simulare LoRaWAN + bruiaj	3-4
Criptografie post-cuantică X25519+Kyber	Latență handshake TLS	<10 ms ARM Cortex-M	2028	Conformitate NIST PQC R3	4
Accelerare eBPF/XDP + ML	Debit firewall 6G/IoT	10–40 Gbps	2028–2029	Kernel Linux 6.x	3
SBOM blockchain (Hyperledger Fabric)	Timp tranzacție audit	<1 s (PoS)	2026–2027	Prototip Raspberry Pi 4/5	3-4
XAI pentru alerte Suricata	Înțelegere operator (SUS)	SUS ≥75/100	2027–2028	Studiu utilizare SOC	3
Autentificare zkSNARKs + biometrie	Scurgeri metadate mTLS	≤5% expuse	2028–2029	Wireshark + Circom	2-3
Modelare TCO bazată pe AI	Precizie predicție cost	MAPE ≤10%	2029–2030	Studii de caz industriale	3
Simulare adversarială GAN	Detecție atacuri zero-day	≥88% detecție	2029–2030	Red-team cu date GAN	3

8. Foaie de parcurs tehnologică (2026–2030).

Faza I – 2026–2027: Standardizare și Prototipare
Implementarea prototipurilor de *blockchain* ușor (Hyperledger Fabric v2.x cu Proof-of-Stake) pe dispozitive SBC (Raspberry Pi 4/5) pentru distribuirea descentralizată a cheilor și generarea de piste de audit imuabile. Obiectiv: finalizarea tranzacțiilor sub 1 s, consum <5 W/nod. Livrabile: articol IEEE/ACM, cod *open-source* pe GitHub.

Faza II – 2028: Integrare Post-Cuantică și Detectare Federată
Implementarea hibridă CRYSTALS-Kyber + X25519 pe microcontrolere cu constrângeri, combinată cu agenți FL de margine pentru detectarea anomaliilor în timp real (modele TinyML sub 256 kB). Obiectiv: latență *handshake* <10 ms, F1-score ≥94%. Livrabile: articol jurnal Q1 (IEEE IoT / Computers & Security), raport tehnic ETSI.

Faza III – 2029: Piloturi în Medii Reale
Piloturi în *smart-city* (iluminat public, monitorizare trafic) și sănătate (monitorizare pacient) în cadrul ETSI oneM2M și Matter 1.2, validând modelele TCO în condiții reale. Obiectiv: MAPE-TCO ≤10%, SUS ≥75/100. Livrabile: raport pilot, propunere H2020/Horizon Europe.

Faza IV – 2030: Adoptare Industrială și Certificare
Tranziția de la prototip la produs prin API-uri independente de furnizor și obținerea certificărilor UE (EN 18031, Legea Securității Cibernetice). Convergența cu MQTT 5.0 PSK, TSN și segmentarea 6G poziționează arhitecturile AI ca fundament al IoT de generație următoare. Livrabil final: recomandare de standard sau contribuție la un grup de lucru IEEE/ETSI.

Diseminare rezultatelor cercetării

1. **The Role of Load Balancer Mechanisms in Securing IoT Platforms**
   DOI: 10.1109/RoEduNet57163.2022.9921059

   Autori: Daniel-Florin Hrițcan, Doru Balan
   2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet)
   Publicat: 21 Octombrie 2022
   ISBN: 978-1-6654-5528-2 și **ISSN:** 2247-5443

2. **Using Tailscale and PfSense for Security and Anonymity of IoT Environments**
   DOI: 10.1109/DAS61944.2024.10541192

   Autori: Daniel-Florin Hrițcan, Doru Balan
   2024 International Conference on Development and Application Systems (DAS)
   Publicat: 31 Mai 2024
   ISBN: 979-8-3503-4929-0

3. **Exposing IoT Platforms Securely and Anonymously Behind CGNAT**
   DOI: 10.1109/RoEduNet64292.2024.10722287

   Autori: Daniel-Florin Hrițcan, Doru Balan
   2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)
   Publicat: 23 Octombrie 2024
   ISBN: 979-8-3315-4038-8 și **ISSN:** 2247-5443

4. **Securing IoT Environments Using ZeroTier and OPNsense** –
   DOI: 10.1109/RoEduNet64292.2024.10722755

   Autori: Daniel-Florin Hrițcan, Adrian Graur, Doru Balan
   2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)
   Publicat: 23 Octombrie 2024
   ISBN: 979-8-3315-4038-8 și **ISSN:** 2247-5443

5. **Securing IoT Devices: A Literature Survey with Experimental Insights into Threat Detection and Mitigation**
   DOI: 10.4316/AECE.2025.02008

   Autori: Edi Marian Timofte, Mihai Dimian, Adrian Graur, Alin Dan Potorac, Doru Gabriel Balan, Daniel Hrițcan, Marcel Pușcașu
   Advances in Electrical and Computer Engineering, vol.25, no.2, pp.69-80, 2025
   Publicat: 2025-06-30
   ISSN: 1582-7445

6. **A Performance Analysis of VPN Technologies Used in an IoT Environment**
DOI: 10.4316/AECE.2025.02009

Autori: Daniel Hrițcan, Adrian Graur, Doru Gabriel Balan, Edi Marian Timofte
Advances in Electrical and Computer Engineering, vol.25, no.2, pp.81-88, 2025
Publicat: 2025-06-30
ISSN: 1582-7445

7. **Federated Learning for Cybersecurity: A Privacy-Preserving Approach**
DOI: 10.3390/app15126878

Autori: Edi Marian Timofte, Mihai Dimian, Adrian Graur, Alin Dan Potorac, Doru Gabriel Balan, Ionuț Croitoru, Daniel Hrițcan, Marcel Pușcașu
Applied Sciences Volume 15, Issue 12, article 6878, 2025
Publicat: 18 Iunie 2025
ISSN: 2076-3417

8. **ARGUS: An Autonomous Robotic Guard System for Uncovering Security Threats in Cyber-Physical Environments**
DOI: doi.org/10.3390/jcp5040078

Autori: Edi Marian Timofte, Mihai Dimian, Alin Dan Potorac, Doru Gabriel Balan, Daniel Hrițcan, Marcel Pușcașu, Ovidiu Chiraș
Journal of Cybersecurity and Privacy Volume 5, Issue 4, article 78, 2025
Publicat: 1 Octombrie 2025
ISSN: 2624-800X

9. **A Study of Cybersecurity in the Healthcare Sector: Threat and Vulnerability Mapping**
DOI: 10.1109/Cyber-AI66431.2025.11233388

Autori: Marcel Pușcașu, Mihai Dimian, Doru Balan, Timofte Edi Marian, Daniel-Florin Hrițcan
2025 International Conference on Cybersecurity and AI-Based Systems (Cyber-AI)
Publicat: 14 Noiembrie 2025
ISBN: 979-8-3315-6631-9

Bibliografie

[1]. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 2023, 23, 4117. https://doi.org/10.3390/s23084117

[2]. Alotaibi, B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. Sensors 2023, 23, 7470. https://doi.org/10.3390/s23177470

[3]. M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," Wireless Communications and Mobile Computing, vol. 2022, Art. no. 8669348, 2022. doi: 10.1155/2022/8669348.

[4]. H. Ruotsalainen, G. Shen, J. Zhang, and R. Fujdiak, "LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review," Sensors, vol. 22, no. 9, Art. no. 3127, 2022. doi: 10.3390/s22093127.

[5]. O. O. Amoo, F. Osasona, A. Atadoga, B. S. Ayinla, O. A. Farayola and T. O. Abrahams, "Cybersecurity threats in the age of IoT: A review of protective measures," International Journal of Science and Research Archive, vol. 11, no. 1, pp. 1304-1310, Feb. 2024, Dublin, Ireland. DOI: 10.30574/ijsra.2024.11.1.0217.

[6]. M. Hammouti, O. Moussaoui, M. Hassine, and A. Betari, "Exploring open source and proprietary LoRa mesh technologies," Indonesian Journal of Electrical Engineering and Computer Science, vol. 34, no. 2, pp. 960–969, May 2024. doi: 10.11591/ijeecs.v34.i2.pp960-969.

[7]. Almuhaya, M.A.M.; Jabbar, W.A.; Sulaiman, N.; Abdulmalek, S. A Survey on LoRaWAN Technology: Recent Trends, Opportunities, Simulation Tools and Future Directions. Electronics 2022, 11, 164. https://doi.org/10.3390/electronics11010164

[8]. Ruotsalainen, H.; Shen, G.; Zhang, J.; Fujdiak, R. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. Sensors 2022, 22, 3127. https://doi.org/10.3390/s22093127.

[9]. Ntshabele, K.; Isong, B.; Gasela, N.; Abu-Mahfouz, A.M. A Comprehensive Analysis of LoRaWAN Key Security Models and Possible Attack Solutions. Mathematics 2022, 10, 3421. https://doi.org/10.3390/math10193421

[10]. W. Andreas, A. G. de la Fuente, C. Lipps, and M. Karrenbauer, "Physical Layer Security based Key Management for LoRaWAN," arXiv preprint arXiv:2101.02975, 2021.

[11]. N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," arXiv preprint arXiv:2402.00356, 2024.

[12]. M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," Wireless Communications and Mobile Computing, vol. 2022, Art. no. 8669348, 2022. doi: 10.1155/2022/8669348.

[13]. S. Jin, M. Xu, and Y. Cai, “Energy Efficient Obfuscation of Side-Channel Leakage for Preventing Side-Channel Attacks,” arXiv preprint arXiv:2208.09140, 2022.

[14]. B. Zhao, S. Ji, J. Xu, Y. Tian, Q. Wei, Q. Wang, C. Lyu, X. Zhang, C. Lin, J. Wu, and R. Beyah, “One Bad Apple Spoils the Barrel: Understanding the Security Risks Introduced by Third-Party Components in IoT Firmware,” arXiv preprint arXiv:2212.13716, Dec. 2022. doi: 10.48550/arXiv.2212.13716.

[15]. M. Rosendo and J. Granjal, “Energy Aware Security Adaptation for Low Power IoT Applications,” Network, vol. 2, no. 1, pp. 36 52, 2022. doi: 10.3390/network2010003.

[16]. A. Ahmed, B. Quoitin, A. Gros, and V. Moeyaert, “A Comprehensive Survey on Deep Learning Based LoRa Radio Frequency Fingerprinting Identification,” Sensors, vol. 24, no. 13, Art. no. 4411, 2024. doi: 10.3390/s24134411.

[17]. S. Jin, M. Xu, and Y. Cai, “Energy Efficient Obfuscation of Side Channel Leakage for Preventing Side Channel Attacks,” arXiv preprint arXiv:2208.09140, 2022.

[18]. M. Hammouti, O. Moussaoui, M. Hassine, and A. Betari, “Exploring open source and proprietary LoRa mesh technologies,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 34, no. 2, pp. 960–969, May 2024. doi: 10.11591/ijeecs.v34.i2.pp960-969.

[19]. O. Freitas, F. Taffarel, A. L. dos Santos, and L. A. P. Júnior, “Uncovering Hidden Risks in IoT devices: A Post-Pandemic National Study of SOHO Wi-Fi Router Security,” Journal of Internet Services and Applications, vol. 15, no. 1, pp. 485–495, 2024. doi: 10.5753/jisa.2024.3834.

[20]. S. Amanlou and K. A. Abu Bakar, “Lightweight Security Mechanism over MQTT Protocol for IoT Devices,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 7, 2020. doi: 10.14569/IJACSA.2020.0110726.

[22]. A. Ghobakhlou, D. Z. Al-Hamid, S. Zandi, and J. Cato, “A Comprehensive Analysis of Security Challenges in ZigBee 3.0 Networks,” Sensors, vol. 25, Art. no. 4606, 2025. doi: 10.3390/s25154606.

[23]. T. Bakhshi, B. Ghita, and I. Kuzminykh, “A Review of IoT Firmware Vulnerabilities and Auditing Techniques,” Sensors, vol. 24, no. 2, Art. no. 708, 2024. doi: 10.3390/s24020708.

[24]. B. Zhao et al., "One Bad Apple Spoils the Barrel: Understanding the Security Risks Introduced by Third-Party Components in IoT Firmware," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 3, pp. 1372-1389, May-June 2024, doi: 10.1109/TDSC.2023.3279846.

[25]. X. Fang, L. Zheng, X. Fang, W. Chen, K. Fang, L. Yin, H. Zhu, “Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks,” Scientific Reports, vol. 14, Art. no. 13931, 2024. doi: 10.1038/s41598-024-64895-8.

[26]. C. T. Hager and S. F. Midkiff, "An analysis of Bluetooth security vulnerabilities," 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003., New Orleans, LA, USA, 2003, pp. 1825-1831 vol.3, doi: 10.1109/WCNC.2003.1200664.

[27]. A. A. Ahmed, “Lightweight Digital Certificate Management and Efficacious Symmetric Cryptographic Mechanism over Industrial Internet of Things,” Sensors, vol. 21, no. 8, Art. no. 2810, 2021. doi: 10.3390/s21082810.

[28]. M. Sahni and S. Tripathi, “Constrained Application Protocol (CoAP) Transfer for the Certificate Management Protocol,” RFC 9482, Proposed Standard, Nov. 2023. doi: 10.17487/RFC9482.

[29]. F. Ullah, A. Turab, S. Ullah, D. Cacciagrano, and Y. Zhao, “Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory,” Sensors, vol. 24, no. 13, Art. no. 4152, 2024. doi: 10.3390/s24134152.

[30]. D. Torre, A. Chennamaneni, J. Jo, G. Vyas, and B. Sabrsula, “Toward Enhancing Privacy Preservation of a Federated Learning CNN Intrusion Detection System in IoT: Method and Empirical Study,” ACM Transactions on Software Engineering and Methodology, vol. 34, no. 2, Article No. 53, 2025. doi: 10.1145/3695998.

[31]. A. F. Gentile, D. Macrì, D. L. Carnì, E. Greco, and F. Lamonaca, “A Performance Analysis of Security Protocols for Distributed Measurement Systems Based on Internet of Things with Constrained Hardware and Open Source Infrastructures,” Sensors, vol. 24, no. 9, Art. no. 2781, 2024. doi: 10.3390/s24092781.

[32]. S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, “A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things,” Sensors, vol. 22, no. 18, Art. no. 7052, 2022. doi: 10.3390/s22187052.

[35]. F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, “Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning,” Sensors, vol. 22, no. 18, Art. no. 6765, 2022. doi: 10.3390/s22186765.

[36]. K. Xu, L. Chen, and S. Wang, “Wormhole: Concept-Aware Deep Representation Learning for Co-Evolving Sequences,” arXiv preprint arXiv:2409.13857, 2024.

[37]. P. P. Ioulianou, V. Vasilakis, and S. F. Shahandashti, “A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks,” Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 124–153, Mar. 2022. doi: 10.3390/jcp2010009.

[38]. R. Khan, N. Tariq, M. Ashraf, F. A. Khan, S. Shafi, and A. Ali, “FL DSFA: Securing RPL Based IoT Networks against Selective Forwarding Attacks Using Federated Learning,” Sensors, vol. 24, no. 17, Art. no. 5834, 2024. doi: 10.3390/s24175834.

[40]. N. Alfriehat, M. Anbar, M. A. Aladaileh, I. Hasbullah, T. A. Shurbaji, S. Karuppayah, and A. Almomani, “RPL based attack detection approaches in IoT networks: review and taxonomy,” Artificial Intelligence Review, vol. 57, Art. no. 248, 2024. doi: 10.1007/s10462-024-10907-y.

[41]. C. Tagliaro, M. Komsic, A. Continella, K. Borgolte, and M. Lindorfer, “Large Scale Security Analysis of Real World Backend Deployments Speaking IoT Focused Protocols,” arXiv preprint arXiv:2405.09662, 2024.

[42]. L. Verderame, A. Ruggia, and A. Merlo, “PARIOT: Anti Repackaging for IoT Firmware Integrity,” arXiv preprint arXiv:2109.04337, 2021.

[43]. K. Nedergaard, B. Singh, and B. Andersen, “Evaluating CoAP, OSCORE, DTLS and HTTPS for Secure Device Communication,” in Proceedings of EAI International Conference on the Internet of Everything, T. Pereira, J. Impagliazzo & H. Santos, Eds.,

Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, vol. 458, Springer, 2023, pp. 117–132. doi: 10.1007/978-3-031-25222-8_10.

[44]. G. Selander, J. Mattsson, F. Palombini, and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)," RFC 8613, Standards Track, July 2019. doi: 10.17487/RFC8613.

[45]. G. Selander, J. Preuß Mattsson, and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)," RFC 9528, March 2024. doi: 10.17487/RFC9528.

[46]. S. Rafique, A. Abdallah, S. Alhosani, and N. Jamil, "A Review of AMQP Protocol: Characteristics, Security Challenges and Proposed Enhancement," JOIV: International Journal on Informatics Visualization, vol. 9, no. 3, pp. 1283–1297, May 2025. doi: 10.62527/joiv.9.3.3043.

[47]. M. Husnain, K. Hayat, E. Cambiaso, U. U. Fayyaz, M. Mongelli, H. Akram, S. G. Abbas and G. A. Shah, "Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System," Sensors, vol. 22, no. 2, Art. no. 567, 2022. doi: 10.3390/s22020567.

[48]. A. F. Gentile, D. Macrì, D. L. Carnì, E. Greco, and F. Lamonaca, "A Network Performance Analysis of MQTT Security Protocols with Constrained Hardware in the Dark Net for DMS," Applied Sciences, vol. 14, no. 18, Art. no. 8501, 2024. doi: 10.3390/app14188501.

[50]. S. G. Oliver and T. Purusothaman, "Lightweight and Secure Mutual Authentication Scheme for IoT Devices Using CoAP Protocol," Computer Systems Science and Engineering, vol. 41, no. 2, pp. 767–780, 2022. doi: 10.32604/csse.2022.020888.

[51]. X. Gong and T. Feng, "Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things," Sensors, vol. 22, no. 19, Art. no. 7191, 2022. doi: 10.3390/s22197191.

[53]. H. Tschofenig, T. Fossati and M. Richardson, "TLS/DTLS 1.3 Profiles for the Internet of Things," Internet Draft draft-ietf-uta-tls13-iot-profile, Work in Progress, Mar. 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-uta-tls13-iot-profile/

[54]. D. Forsberg, H. Tschofenig, and R. Watsen, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things," IETF Internet-Draft, 2023. [Online]. Available: https://www.ietf.org/archive/id/draft-ietf-uta-tls13-iot-profile-08.html

[55]. P. Maurya, A. Hazra, P. Kumari, T. B. Sørensen, and S. K. Das, "A Comprehensive Survey of Data Driven Solutions for LoRaWAN: Challenges and Future Directions," ACM Transactions on Internet of Things, vol. 6, no. 1, 2025. doi: 10.1145/3711953.

[56]. S. Pattasani, S. Mohapatra, and A. Jyoti, "IoT Based Social Device Network with Cloud Computing Architecture: A Systematic Review," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 14, no. 8, pp. 19–23, Jul. 2025. doi: 10.35940/ijitee.G1106.14080725.

[57]. L. Catuogno and C. Galdi, "Secure Firmware Update: Challenges and Solutions," Cryptography, vol. 7, no. 2, Art. no. 30, 2023. doi: 10.3390/cryptography7020030.

[58]. H. Brockhaus, D. von Oheimb, and S. Fries, “Lightweight Certificate Management Protocol (CMP) Profile,” RFC 9483, Internet Standards Track, Nov. 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc9483

[59]. M. Sahni and S. Tripathi, “Constrained Application Protocol (CoAP) Transfer for the Certificate Management Protocol,” RFC 9482, Internet Standards Track, Nov. 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc9482

[60]. J. Göppert, A. Walz, and A. Sikora, “A Survey on Life Cycle Oriented Certificate Management in Industrial Networking Environments,” Journal of Sensor and Actuator Networks, vol. 13, no. 2, Art. no. 26, 2024. doi: 10.3390/jsan13020026.

[62]. J. Ahn, E. Yi, and M. Kim, “Blockchain consensus mechanisms: A bibliometric analysis (2014–2024) using VOSviewer and R Bibliometrix,” Information, vol. 15, no. 10, p. 644, 2024, doi: 10.3390/info15100644.

[63]. S. Safeer, G. De Mastro, and C. Pulvento, “IoT based climate smart agriculture succeeded by blockchain database — A bibliometric analysis,” Frontiers in Sustainable Food Systems, vol. 8, 2024, doi: 10.3389/fsufs.2024.1406871.

[64]. W. Wen and X. Han, “An introduction of transaction session-induced security scheme using blockchain technology: Understanding the features of Internet of Things-based financial security systems,” Managerial and Decision Economics, vol. 45, no. 4, pp. 1817–1834, 2024, doi: 10.1002/mde.4043.

[65]. Andronie, M., Blažek, R., Iatagan, M., Skypalova, R., Uță, C., Dijmărescu, A., Kovacova, M., Grecu, G., Pârvu, I., Strakova, J., Guni, C., Zabojnik, S., Chiru, C., Sedláčková, A. N., Novák, A., & Dijmărescu, I. (2024). “Generative artificial intelligence algorithms in Internet of Things blockchain-based fintech management.” Oeconomia Copernicana, 15(4), 1349-1381. https://doi.org/10.24136/oc.3283.

[66]. G. Dhiman and A. K. Nagar, “Editorial: Blockchain based 6G and industrial internet of things systems for Industry 4.0/5.0,” Expert Systems, vol. 39, no. 10, 2022. doi: 10.1111/exsy.13162.

[67]. S. Selvarajan, A. Shankar, M. Uddin, A. S. Alqahtani, T. Al Shehari, W. Viriyasitavat, “A smart decentralized identifiable distributed ledger technology based blockchain (DIDLT BC) model for cloud IoT security,” Expert Systems, vol. 42, no. 1, 2025. doi: 10.1111/exsy.13544.

[68]. P. Modi, “Towards Efficient Machine Learning Method for IoT DDoS Attack Detection,” arXiv preprint arXiv:2408.10267, Aug. 2024. doi: 10.48550/arXiv.2408.10267.

[69]. M. Aljabri, A. Shaahid, F. Alnasser, A. Saleh, D. Alomari, M. Aboulnour, W. Al Eidarous and A. Althubaity, “IoT Attacks Detection Using Supervised Machine Learning Techniques,” HighTech and Innovation Journal, vol. 5, no. 3, pp. 534–550, Sep. 2024. doi: 10.28991/HIJ 2024 05 03 01.

[70]. D. Torre, A. Chennamaneni, J. Jo, G. Vyas, and B. Sabrsula, “Toward Enhancing Privacy Preservation of a Federated Learning CNN Intrusion Detection System in IoT: Method and Empirical Study,” ACM Transactions on Software Engineering and Methodology, vol. 34, no. 2, pp. 1 48, Feb. 2025. doi: 10.1145/3695998.

[71]. H. Meziane and N. Ouerdi, “A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems,” Scientific Reports, vol. 13, no. 1, p. 21255, 2023. doi: 10.1038/s41598 023 46640 9.

[72]. P. Chadha, R. Gera, Y. Sharma, and S. Dixit, “Artificial Intelligence in Cyber Security: A Bibliometric Analysis,” in Applications of Artificial Intelligence in Business and Finance 5.0, 1st ed., Apple Academic Press, 2024, pp. 25. doi: 10.1201/9781003535133 12.

[74]. K. Sundaram and Y. Perumalsamy, “A Novel Hybrid Feature Selection with Cascaded LSTM: Enhancing Security in IoT Networks,” Wireless Communications and Mobile Computing, vol. 2024, Article ID 5522431, 2024. doi: 10.1155/2024/5522431.

[76]. A. Bensaoud and J. Kalita, “Optimized detection of cyber attacks on IoT networks via hybrid deep learning models,” Ad Hoc Networks, vol. 170, Apr. 2025, Art. no. 103770. doi: 10.1016/j.adhoc.2025.103770.

[78]. M. A. Akif, I. Butun, A. Williams, and I. Mahgoub, “Hybrid Machine Learning Models for Intrusion Detection in IoT: Leveraging a Real World IoT Dataset,” arXiv preprint arXiv:2502.12382, 2025.

[80]. A. Churcher, R. Ullah, J. Ahmad, S. ur Rehman, F. Masood, M. Gogate, F. Alqahtani, B. Nour, and W. J. Buchanan, “An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks,” arXiv preprint arXiv:2101.12270, Jan. 2021. doi: 10.48550/arXiv.2101.12270.

[81]. J. Vitorino, I. Praça and E. Maia, “Towards Adversarial Realism and Robust Learning for IoT Intrusion Detection and Classification,” arXiv preprint arXiv:2301.13122, Mar. 2023. doi: 10.48550/arXiv.2301.13122.

[93]. **D. -F. Hrițcan** and D. Balan, "The Role of Load Balancer Mechanisms in Securing IoT Platforms," 2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet), Sovata, Romania, 2022, pp. 1-4, doi: 10.1109/RoEduNet57163.2022.9921059.

[94]. **D. -F. Hriţcan** and D. Balan, "Exposing IoT Platforms Securely and Anonymously Behind CGNAT," 2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2024, pp. 1-4, doi: 10.1109/RoEduNet64292.2024.10722287.

[95]. **D. -F. Hriţcan**, A. Graur and D. Balan, "Securing IoT Environments Using ZeroTier and OPNsense," 2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2024, pp. 1-4, doi: 10.1109/RoEduNet64292.2024.10722755.

[96]. **D. -F. Hrițcan** and D. Balan, "Using Tailscale and PfSense for Security and Anonymity of IoT Environments," 2024 International Conference on Development and Application Systems (DAS), Suceava, Romania, 2024, pp. 91-94, doi: 10.1109/DAS61944.2024.10541192.

[101]. **D. -F. Hritcan**, A. Graur, D. G. Balan, E. M. Timofte, "A Performance Analysis of VPN Technologies Used in an IoT Environment," Advances in Electrical and Computer Engineering, vol.25, no.2, pp.81-88, 2025, doi:10.4316/AECE.2025.02009.

[102]. E. M. Timofte, M. Dimian, A. Graur, A. D. Potorac, D. G. Balan, **D. Hritcan**, and M. Puscasu, "Securing IoT Devices: A Literature Survey with Experimental Insights into

Threat Detection and Mitigation," Adv. Electr. Comp. Eng., vol. 25, no. 2, pp. 69–80, Jun. 2025, doi: 10.4316/AECE.2025.02008.

[103]. E. M. Timofte, M. Dimian, A. Graur, A. D. Potorac, D. Balan, I. Croitoru, **D.-F. Hrițcan** și M. Pușcașu, „Federated Learning for Cybersecurity: A Privacy-Preserving Approach”, Appl. Sci., vol. 15, nr. 12, p. 6878, iun. 2025, doi: 10.3390/app15126878.

[104]. M. Puscasu, M. Dimian, E. M. Timofte, D. G. Balan, and **D.-F. Hritcan**, "A Study of Cybersecurity in the Healthcare Sector: Threat and Vulnerability Mapping," 2025 International Conference on Cybersecurity and Artificial Intelligence (Cyber-AI), pp. 1‑6, 2025, doi: 10.1109/Cyber-AI66431.2025.11233388.

[105]. E. M. Timofte, M. Dimian, A. D. Potorac, D. Balan, **D.-F. Hrițcan**, M. Pușcașu și O. Chiraș, „ARGUS: An Autonomous Robotic Guard System for Uncovering Security Threats in Cyber-Physical Environments”, J. Cybersecur. Priv., vol. 5, nr. 4, p. 78, oct. 2025, doi: 10.3390/jcp5040078.

[106]. ENISA, "ENISA Threat Landscape 2024," Sep. 19, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[107]. Cloudflare, "DDoS Threat Report for 2024 Q4," The Cloudflare Blog, Jan. 21, 2025. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/

[108]. NIST, „NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” National Institute of Standards and Technology, 13 aug. 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[109]. J. Lopez, V. Cadena, and M. S. Rahman, “Evaluating Post-Quantum Cryptographic Algorithms on Resource-Constrained Devices,” 2025, arXiv:2507.08312. doi: 10.48550/arXiv.2507.08312.

[110]. M. O. Ozmen, A. A. Yavuz, „Systematic Literature Review of IoT Botnet DDoS Attacks and Evaluation of Detection Techniques,” Sensors, vol. 24, nr. 11, art. 3571, iun. 2024, doi: 10.3390/s24113571.

[111]. O. Alnaseri, Y. Himeur, S. Atalla, W. Mansoor, „Complexity of Post-Quantum Cryptography in Embedded Systems and Its Optimization Strategies,” 2025, arXiv:2504.13537. doi: 10.48550/arXiv.2504.13537.