MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admis la susținere
Șefă departament TSE:
Valentina TÎRȘU, conf.univ.,dr.

_____

”_____”_____2025

SECURIZAREA CONEXIUNILOR VPN PRIN INTERMEDIUL PROTOCOALELOR IPSEC

Student: **Tornea Mihail**

Conducător: **Sava Lilia**
conf. univ. dr.

Chișinău 2025

ADNOTARE

Autor: Tornea Mihail

Tema lucrării: SECURIZAREA CONEXIUNILOR VPN PRIN INTERMEDIUL PROTOCOALELOR IPSEC și se concentrează pe analiza și implementarea unei soluții de securizare a comunicațiilor VPN site-to-site folosind protocoalele IPSec și IKEv2.

Structura lucrării: Introducere, 3 Capitole, Concluzii, Bibliografie, 3 Anexe, 19 Imagini.

Cuvinte cheie: IPSec, IKEv2, VPN, criptare AES-256, Perfect Forward Secrecy, securitate cibernetică, Mikrotik.

Scopul lucrării: Demonstrarea importanței implementării unor protocoale de securitate robuste pentru protejarea datelor transmise prin rețele VPN, prin configurarea și evaluarea unei soluții care asigură confidențialitatea, integritatea și autenticitatea comunicațiilor.

Rezultatele obținute: Rezultatele obținute evidențiază faptul că implementarea protocoalelor IPSec/IKEv2 împreună cu criptarea AES-256 și rotația periodică a cheilor asigură un nivel ridicat de protecție împotriva atacurilor cibernetice.

Lucrarea începe cu o introducere, care descrie provocările moderne în domeniul securității cibernetice, evidențiază riscurile majore și costurile mari suferite de organizații în cazul unor atacuri cibernetice de succes purtate de răufăcători.

Primul capitol reprezintă partea teoretică, în care sunt descrise conceptele de bază ale rețelelor VPN, algoritmii de criptare și mecanismele de autentificare, precum și modul de conlucrare între IPSEC și IKEv2.

Al doilea capitol detaliază procesul de configurare și testare a unei conexiuni VPN securizate IPSec/IKEv2 pe echipamente de rețea Mikrotik, cu un algoritm de criptare puternic AES-256, precum și necesitatea configurării NAT pentru a asigura funcționalitatea sistemului.

Al treilea capitol reprezintă o analiză a performanțelor conexiunii prin testarea și validarea corectitudinii configurărilor descrise în capitolul doi.

ANNOTATION

Author: Tornea Mihail

Theme: SECURING VPN CONNECTIONS THROUGH IPSEC PROTOCOLS and focuses on the analysis and implementation of a solution for securing site-to-site VPN communications using IPSec and IKEv2 protocols.

Structure of the work: Introduction, 3 Chapters, Conclusions, Bibliography, 3 Appendices, 19 Images.

Keywords: IPSec, IKEv2, VPN, AES-256 encryption, Perfect Forward Secrecy, cybersecurity, Mikrotik.

Purpose of the work: To demonstrate the importance of implementing robust security protocols to protect data transmitted over VPN networks, by configuring and evaluating a solution that ensures confidentiality, integrity and authenticity of communications.

Results of the work: The results show that the implementation of IPSec/IKEv2 protocols together with AES-256 encryption and periodic key rotation provide a high level of protection against cyber-attacks.

The paper starts with an introduction, which describes the modern challenges in cybersecurity, outlines the major risks and high costs incurred by organizations in case of successful cyber-attacks by malicious actors.
The first chapter is the theoretical part, describing the basic concepts of VPNs, encryption algorithms and authentication mechanisms, and how IPSEC and IKEv2 work together.

The second chapter details the process of setting up and testing a secure IPSec/IKEv2 VPN connection over Mikrotik network equipment with a strong AES-256 encryption algorithm, and the need for NAT configuration to ensure system functionality.

The third chapter is an analysis of the connection performance by testing and validating the correctness of the configurations described in chapter two.

CUPRINS

INTRODUCERE

În era digitală, evoluția accelerată a tehnologiilor informaționale a transformat profund modul în care organizațiile și indivizii interacționează cu mediul digital. Extinderea rețelelor de comunicații, utilizarea masivă a serviciilor de cloud și proliferarea dispozitivelor conectate au dus la creșterea semnificativă a volumului de date transmise zilnic. În acest context, securitatea informației a devenit o prioritate absolută, pe fondul creșterii alarmante a atacurilor cibernetice, care generează pierderi financiare și reputaționale uriașe.

Conform estimărilor, costurile globale ale criminalității informatice vor atinge 10,5 trilioane USD anual până în 2025, depășind daunele provocate de dezastre naturale sau alte amenințări economice. În acest peisaj, rețelele virtuale private (VPN) și protocoalele avansate de securitate, precum IP Sec (Internet Protocol Security), devin soluții esențiale pentru protejarea confidențialității și integrității datelor transmise între locații diferite. IP Sec s-a impus ca standard de referință datorită nivelului său ridicat de securitate și a compatibilității extinse cu diverse platforme și dispozitive.

Avansurile tehnologice din domeniul supercalculatoarelor accentuează necesitatea unor măsuri stricte de securitate în rețelele VPN, iar deschiderea rețelelor interne ale întreprinderilor și organizațiilor fără VPN ar trebui să fie reglementată de către autorități pentru protejarea acestora deoarece majoritatea echipamentelor din rețelele întreprinderilor precum printere de rețea, sisteme de monitorizare video, sau chiar parolele de access către sistemul de operare a terminalelor de lucru nu au nici o șansă să reziste unui atac ce ar utiliza un astfel de supercalculator. Un supercalculator de puterea NVIDIA GB200 NVL72 sau chiar mai mare ar putea reprezenta o amenințare semnificativă pentru securitatea globală dacă ar ajunge în posesia unui grup criminal cibernetic sau a unui stat autoritar precum Federația Rusă (Atacurile cibernetice atribuite autorităților ruse au crescut semnificativ în ultimii ani, vizând atât state membre NATO, cât și alte țări, inclusiv România și Republica Moldova. Conform unui raport al companiei Google, în 2022, numărul acestor atacuri a crescut cu 300% în țările NATO și cu 250% în Ucraina, comparativ cu 2020). Capacitatea de procesare masivă pe care o oferă un astfel de echipament ar putea fi utilizată pentru a desfășura atacuri cibernetice extrem de sofisticate, compromițând sisteme critice și generând pagube financiare, politice și sociale de proporții. În primul rând, utilizarea unui astfel de supercalculator în scopuri malițioase ar permite desfășurarea unor atacuri brute-force rapide asupra unor sisteme de securitate informatice bazate pe criptografie. Deși cheile de securitate mai lungi, de 16 caractere sau mai mult, oferă o protecție semnificativă, un calculator cu puterea de procesare a GB200 NVL72 poate compromite chei mai scurte în doar câteva secunde. Aceasta ar deschide calea spre accesarea neautorizată a rețelelor, comunicațiilor securizate sau datelor financiare, iar decriptarea avansată a

protocoalelor criptografice complexe ar putea deveni posibilă, expunând chiar și rețele considerate anterior invulnerabile.

Tema abordată în această lucrare este de actualitate, fiind motivată de nevoia crescută de a securiza comunicațiile în rețelele moderne. Lucrarea își propune să demonstreze, printr-un studiu practic, eficiența utilizării protocoalelor IP Sec în implementarea unei conexiuni VPN de tip site-to-site, utilizând echipamente Mikrotik.

Scopul lucrării este de a evidenția aplicabilitatea practică a protocoalelor IP Sec/IKEv2 în crearea unei soluții viabile și eficiente pentru protejarea comunicațiilor intersite, subliniind totodată rolul acestora în asigurarea unui mediu digital sigur.

Pentru atingerea acestui scop, lucrarea urmărește următoarele **obiective**:

1. Analiza conceptelor fundamentale ale rețelelor VPN și a principiilor de securitate cibernetică relevante;
2. Explorarea fluxului de negociere și securizare IP Sec/IKEv2, incluzând mecanismele de criptare și autentificare;
3. Implementarea practică a unei conexiuni VPN IP Sec/IKEv2 de tip site-to-site utilizând echipamente Mikrotik, cu configurarea regulilor Firewall și NAT necesare;
4. Evaluarea performanțelor conexiunii implementate, identificarea eventualelor limitări și propunerea de soluții de optimizare;
5. Formularea concluziilor și a recomandărilor pentru utilizarea extinsă a soluțiilor IP Sec în mediile corporative și organizaționale.

Lucrarea se structurează pe două mari direcții: prima, teoretică, ce abordează fundamentele securității cibernetice și protocoalele VPN, și a doua, practică, care constă în implementarea și evaluarea soluției propuse. Această abordare combinată oferă atât o înțelegere teoretică profundă, cât și o contribuție practică, utilă pentru specialiștii în domeniul rețelelor și telecomunicațiilor.

Prin intermediul acestei cercetări, se evidențiază importanța utilizării unor soluții robuste pentru securizarea comunicațiilor în rețelele moderne, contribuind astfel la dezvoltarea unui mediu digital sigur și eficient.

BIBLIOGRAFIE

[1] Revista Intelligence, "Revoluția tehnologică, mega trendul începutului de secol XXI," 2021. [Online]. Disponibil la: https://intelligence.revista.ro. [Accesat: 22-dec-2024].

[2] EUR-Lex, "Regulament 2016/679 - EN - GDPR," 2016. [Online]. Disponibil la: https://eur-lex.europa.eu. [Accesat: 22-dec-2024].

[3] Your Europe, "Protecția datelor și a vieții private în mediul on-line," 2023. [Online]. Disponibil la: https://europa.eu/youreurope. [Accesat: 22-dec-2024].

[4] Hackout, "Costurile ascunse ale atacurilor cibernetice: Impactul financiar neașteptat pentru companii," 2024. [Online]. Disponibil la: https://hackout.ro. [Accesat: 22-dec-2024].

[5] Forbes Advisor, "VPN Pros And Cons In 2024," 2024. [Online]. Disponibil la: https://www.forbes.com/advisor. [Accesat: 22-dec-2024].

[6] OpenVPN, "Site-to-Site VPN," 2023. [Online]. Disponibil la: https://openvpn.net. [Accesat: 22-dec-2024].

[7] pfSense Documentation, "Choosing a VPN solution," 2023. [Online]. Disponibil la: https://docs.netgate.com. [Accesat: 22-dec-2024].

[8] Cybersecurity Ventures, "Top 10 Cybersecurity Predictions and Statistics For 2024," 2024. [Online]. Disponibil la: https://cybersecurityventures.com. [Accesat: 22-dec-2024].

[9] M. A. N. Rahman, "How to Deploy IPsec/IKEv2 on Mikrotik," 2024. [Online]. Disponibil la: https://mikrotik.tutorials.com. [Accesat: 22-dec-2024].

[10] MikroTik Documentation, "IPsec - RouterOS," 2023. [Online]. Disponibil la: https://wiki.mikrotik.com. [Accesat: 22-dec-2024].

[11] PECA, L., ȚURCANU, D. Computer networks: Practical examples solved to be introduced in computer networks. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chișinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-812-2. http://repository.utm.md/handle/5014/20549

[12] World Economic Forum, "These are the world's top 10 fastest supercomputers," 2023. [Online]. Disponibil la: https://www.weforum.org. [Accesat: 22-dec-2024].

[13] Tom's Hardware, "NVIDIA's new GB200 Superchip costs up to $70,000: Full B200 NVL72 AI server costs $3 million," 2024. [Online]. Disponibil la: https://www.tomshardware.com. [Accesat: 22-dec-2024].

[14] B. Limani, D. Jahiri, and D. Morina, "IPSecurity (IPSec)," ResearchGate, 2020. [Online]. Disponibil la: https://www.researchgate.net. [Accesat: 22-dec-2024].

[15] Tîrșu V., Sava L**.** Integrating elasticsearch and kibana in ict management *processes for economic efficiency in multimedia content administration.* In: The scientific heritage. Economic Sciences.,

Vol.1 № 142 (142), 2024, p.15-20 . Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: http://www.scientific-heritage.com/ru/arhiv/

[16] Tîrșu V., Cerbu O. *Interactive visualization of geographical data using proxmox and modern technologies.* In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.21-26. Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: http://www.scientific-heritage.com/ru/arhiv/

[17] Sava L., Tîrșu V., Plămădeală C**.** *Performance evaluation of microtik routers according to electromagnetic compatibility testing standards.* În: Electrotehnica, Electronica, Automatica, vol.72/4, p.57-61. Romania, Sibiu: ISSN: 2392-828X, categoria B+. Disponibil: https://eea-journal.ro/articles-and-issues/current-issues/

[18] PECA, L., ȚURCANU, D. Network security: Practical examples solved to be introduced in network security. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chișinău: Tehnica-UTM, 2023. – 243 p. ISBN 978-9975-45-941-9. http://repository.utm.md/handle/5014/22819

[19] Tîrșu, V., Cristea E. Baze de date : Ghid metodic pentru lucrările de laborator. Chișinău: Ed. "Tehnica-UTM", 2024, 112 pag. ISBN 978-9975-64-392-4. Disponibil: https://library.utm.md/items/?biblionumber=2628876

[20] Tîrșu, V. Programare : Ghid metodic pentru lucrări de laborator. Chișinău: Ed. "Tehnica-UTM", 2022, pag.130, ISBN 978-9975-45-861-0. Disponibil: https://library.utm.md/items/?biblionumber=2619626

[21] Sava, L., Vortolomei, D. Organizarea şi analiza activităţii economice în domeniul telecomunicaţiilor. Note de curs, Chişinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.

[22] MikroTik, "RouterOS Configuration Examples," 2024. [Online]. Disponibil la: https://wiki.mikrotik.com/examples. [Accesat: 22-dec-2024].

[23] Gartner, "VPN Adoption and Trends," 2023. [Online]. Disponibil la: https://www.gartner.com. [Accesat: 22-dec-2024].

[24] ENISA, "Threat Landscape 2024," European Union Agency for Cybersecurity, 2024. [Online]. Disponibil la: https://www.enisa.europa.eu. [Accesat: 22-dec-2024].

[25] Cloudflare, "Understanding IPsec and IKEv2," 2024. [Online]. Disponibil la: https://www.cloudflare.com. [Accesat: 22-dec-2024].

[26] IEEE, "Standards for IPsec and Cryptography," 2024. [Online]. Disponibil la: https://standards.ieee.org. [Accesat: 22-dec-2024].