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,
Tîrșu Valentina, conf.univ., dr.

_____

” _____ ” _____ 2025

Analiza transmisiei informației în rețelele de comunicații cu utilizarea tunelului VPN

Teză de master

Student: _____ Lungu Vadim, gr. SISRC-231M

Conducător: _____ Nistiriuc Pavel, conf.univ., dr.

Chișinău, 2025

ADNOTARE

Lungu Vadim, studentul grupei SISRC-231M

Tema tezei – Analiza transmisiei informației în rețelele de comunicații cu utilizarea tunelului VPN.

Teza este constituită din introducere, trei capitole, concluzii și bibliografie.

Cuvinte-cheie: Rețele de comunicații private, securitatea informației, tunel VPN, protocol.

Scopul lucrării constă în analiza transmisiei securizate a informației în rețelele de comunicații private bazate pe tunelul VPN cu utilizarea protocoalelor GRE (Generic Routing Encapsulation) și IPSec (Internet Protocol Security).

Luând în considerare scopului lucrării au fost determinate următoarele obiective:

1. Familiarizarea cu algoritmul de configurare a unui VPN (Virtual Private Network) pe router-ul unui client fizic sau personal;
2. Familiarizarea cu opțiunile A, B, C de interconectare în rețelele MPLS L3VPN (Multiprotocol Label Switching Layer 3 Virtual Private Network);
3. Organizarea într-o rețea de calculatoare a unui tunel VPN cu utilizarea protocolului de tunelare GRE;
4. Analiza securității informației în rețeaua de comunicații VPN din cadrul unei companii private cu utilizarea protocolului IPSec;
5. Analiza asigurării conexiunilor în rețelele de comunicații VPN care vor garanta o comunicare calitativă fără pierderi de pachete cu utilizarea protocolului TCP.

În teză au fost elaborat și examinat algoritmul de configurare a unui VPN pe routerul personal, analizate opțiunile A, B, C de interconectare în rețelele MPLS pentru a crea VPN-uri cu selectarea opțiunii optime, a fost efectuat studiul de caz pentru o rețea de calculatoare în programul Cisco Packet Tracer cu organizarea tunelului VPN ăn baza protocolului GRE, analizată asigurarea unei securități eficiente a datelor pentru rețeaua de comunicații a unei companii private în baza protocolului IPSec, a fost organizat un canal de comunicații securizat prin care se expediază numai pachetele de date cu timpul de viață de 0 ... 255 s, este asigurată o integritate a datelor prin utilizarea protocolului de redundanță VRRP (Virtual Router Redundancy Protocol) au fost determinate mecanismul de verificare la nivelul transport de date, a calității de expediere a pachetelor de date prin utilizarea sumei de control amplsată în antetul protocolului TCP (Transmission Control Protocol) și mecanismul privind utilizarea numărului de validare amplasat în antetul protocolului TCP, care atestă, că succesiunea de pachete cu numerele de ordine respective au fost expediate cu succes, la fel a fost propus protocolul SMTP (Simple Mail Transfer Protocol) pentru a ruta eficient mesajele de e-mail în Internet..

ANNOTATION

Lungu Vadim the student of the group SISRC-231M

The theme of the thesis – Analysis of information transmission in communication networks with the use of VPN tunnel.

The thesis consists of introduction, three chapters, conclusions and bibliography.

Keywords: Private communication networks, information security, VPN tunnel, protocol.

The purpose of the work is to analyze the secure transmission of information in private communication networks based on the VPN tunnel using the GRE (Generic Routing Encapsulation) and IPSec (Internet Protocol Security) protocols.

Taking into account the purpose of the work, the following objectives were determined:

1. Familiarization with the algorithm for configuring a VPN (Virtual Private Network) on the router of a physical or personal client;

2. Familiarization with the A, B, C interconnection options in MPLS L3VPN (Multiprotocol Label Switching Layer 3 Virtual Private Network) networks;

3. Organization in a computer network of a VPN tunnel using the GRE tunneling protocol;

4. Analysis of information security in the VPN communication network within a private company using the IPSec protocol;

5. Analysis of ensuring connections in VPN communication networks that will guarantee qualitative communication without packet loss using the TCP protocol.

In the thesis, the algorithm for configuring a VPN on a personal router was developed and examined, options A, B, C for interconnection in MPLS networks were analyzed to create VPNs with the selection of the optimal option, a case study was conducted for a computer network in the Cisco Packet Tracer program with the organization of the VPN tunnel based on the GRE protocol, ensuring effective data security for the communications network of a private company based on the IPSec protocol was analyzed, a secure communications channel was organized through which only data packets with a lifetime of 0 ... 255 s are sent, data integrity is ensured by using the VRRP redundancy protocol (Virtual Router Redundancy Protocol), the verification mechanism at the data transport level of the quality of sending data packets by using the checksum placed in the TCP protocol header (Transmission Control Protocol) and the mechanism regarding the use of the validation number placed in the TCP protocol header, which certifies that the sequence of packets with the respective sequence numbers were successfully sent, and the SMTP (Simple Mail Transfer Protocol) protocol was proposed to efficiently route e-mail messages on the Internet.

CUPRINS

INTRODUCERE

Actualmente mediul de afaceri are nevoie de rețele sigure și rapide de transport date. Soluția optimă pentru rețelele corporative este rețeaua virtuală privată – VPN (Virtual Private Network).

Virtual Private Network este un serviciu de transport date ce permite conectarea mai multor calculatoare într-o rețea privată virtuală, indiferent unde sunt amplasate teritorial. Utilizarea infrastructurii operatorilor de comunicaţii electronice permite clienţilor VPN să-şi formeze reţeaua privată între sediile companiei sale aflate pe teritoriul țării indiferent de distanţă. Rețelele VPN posedă o serie de avantaje, după cum sunt: o reţea securizată între sediile companiei; funcţionarea în regim non-stop fără blocaje; posibilitatea utilizării aplicaţiilor de tip client-server; posibilitatea conectării reţelei la Internet; preţul de conectare şi abonament avantajos; securitate informațională sporită; transfer de date în timp real la viteze constante.

Un VPN este o rețea de comunicații privată, folosită de obicei în cadrul uneia sau mai multor organizații, pentru a comunica în mod confidențial, prin intermediul unei rețele publice.
Mesajele din traficul VPN pot fi transmise prin intermediul infrastructurii unei rețele publice de date, precum Internet-ul, folosind protocoalele standard, sau prin intermediul unei rețele private a furnizorului de servicii Internet.

VPN-ul este o soluție eficientă din punctul de vedere al costurilor, pentru ca diferite organizații să poată asigura accesul la rețeaua internă pentru angajații şi colaboratorii aflați la distanță, şi pentru a permite confidențialitatea datelor schimbate între punctele de lucru aflate la distanţă.

Multe din programele-client ale VPN- ului pot fi configurate în aşa fel încât să ceară dirijarea întregului trafic printr-un tunel, atâta timp cât conexiunea VPN este activă, sporind astfel siguranța conexiunii. Atâta vreme cât conexiunea VPN este activă, accesul din afara rețelei sigure se
face prin acelaşi firewall, ca şi cum utilizatorul ar fi conectat din interiorul rețelei private. Acest fapt reduce riscurile unei posibile accesări din partea unui atacator, de interceptare şi de urmărire a pachetelor. Un tunel reprezintă o conexiune ”punct-la-punct” între două calculatoare sau două rețele pentru care se utilizează diferite protocoale de rutare prin care se stabileşte calea pe care este trimis pachetul de la sursă la destinație.

Termenul de VPN descrie două modalități de abordare a problemei rețelelor private care au ca suport o rețea publică, din punctul de vedere al accesibilității:
1. VPN-uri realizate între mai multe rețele locale (LAN-to-LAN VPNs, cunoscute şi sub denumirea de Site-to-Site VPNs) care conectează la un nod central mai multe LAN-uri diferite aflate la mare distanță unele față de altele dar care fac parte din acelaşi intranet, astfel încât să asigure conectivitatea între ele;
2. VPN-uri de acces de la distanță (Remote Access VPNs) care asigură accesul de la distanță la o rețea

privată, de exemplu pentru utilizatorii de Internet mobil. Se pot folosi diverse tehnologii de implementare a VPN-urilor. Alegerea uneia anume depinde de criteriile impuse prin politica de securitate a rețelei.

Scopul lucrării constă în analiza transmisiei securizate a informației în rețelele de comunicații private bazate pe tunelul VPN cu utilizarea protocoalelor GRE (Generic Routing Encapsulation) și IPSec (Internet Protocol Security).

Luând în considerare scopului lucrării au fost determinate următoarele obiective:

1. Familiarizarea cu algoritmul de configurare a unui VPN (Virtual Private Network) pe router-ul unui client fizic sau personal;
2. Familiarizarea cu opțiunile A, B, C de interconectare în rețelele MPLS L3VPN (Multiprotocol Label Switching Layer 3 Virtual Private Network);
3. Organizarea într-o rețea de calculatoare a unui tunel VPN cu utilizarea protocolului de tunelare GRE;
4. Analiza securității informației în rețeaua de comunicații VPN din cadrul unei companii private cu utilizarea protocolului IPSec;
5. Analiza asigurării conexiunilor în rețelele de comunicații VPN care vor garanta o comunicare calitativă fără pierderi de pachete cu utilizarea protocolului TCP.

BIBLIOGRAFIE

1. MOHAMMADY, SOMAYEH. Multiplexing: Recent Advances and Novel Applications. ITexLi, 2022.
2. ȚURCANU, D., ALEXEI, A., NISTIRIUC, P., BEREGOI, E., BÂRZOI, O. Estimarea eficienţei de organizare a tunelelor în reţelele de comunicaţii MPLS. In: Materialele Conferinţei Naţionale de Telecomunicaţii, Electronică și Informatică. Chişinău: UTM, 2006. – p.84-88. https://utm.md/wp-content/uploads/2023/09/estimarea-eficientei-de-organizare-a-tunelelor-in-retelele-de-comunicatii-mpls.pdf
3. FANINACCI, D. LISP Network, The: Evolution To The Next-Generation of Data Networks. Cisco Press, New York, 2019.
4. ZHANG, P. Practical Guide to Large Database Migration. CRC Press, 2019.
5. ȚURCANU, D., SPINU, N., POPOVICI, S., ȚURCANU, T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. In: Journal of Social Sciences. 2021, IV (1), pp. 74–83. https://doi.org/10.52326/jss.utm.2021.4(1).10
6. COZZO, E. Multiplex Networks. Springer, 2018.
7. BOUILLARD, A. Deterministic Network Calculus: From Theory to Practical Implementation. New York: Wiley-ISTE, 2018.
8. TOGAN, M. Infrastructuri de Securitate pentru servicii electronice în Internet. București: Matrix Rom, 2017.
9. BHATNAGAR, S., K. Network Analysis Tehnique. John Wiley & Sons. New York, 2016.
10. https://gns3.com/gns3-vs-cisco-packet-tracer
11. https://www.wireshark.org/
12. https://labex.io/tutorials/cybersecurity-how-to-select-the-correct-network-interface-in-wireshark-for-capturing-traffic-417627
13. CITTADINI, L. MPLS Virtual Private Networks. Cisco Press, New York, 2013.
14. SNADER, J., C. VPN Illustrated: Tunnels, VPN and IPSec. Cisco Press, New York, 2010.
15. 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
16. 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. – Chişinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-812-2. http://repository.utm.md/handle/5014/20549

17. LEWIS, M. Comparing, Designing and Deploying VPN. Cisco Press, New York, 2010.
18. ANDERSON, NELL. Cisco Networking Simplified. Cisco Press. 2008.
19. DORASSWAMY, N., HARKINS, D. IPSec. The New Security Standard for the Internet, Intranets and Virtual Private Networks. Cisco Press. New York, 2008.
20. CARMOUCHE, J., H. IPSec Virtual Private Network Fundamentals. Cisco Press, New York, 2006.
21. HENRY, J. IPSec Virtual Private Networks Fundamentals. Cisco Press, New York, 2006.
22. DOROASWAMY, N. IPSec – The New Security Standard for the Internet, Intranets and Virtual Private Networks. Prentice Hall. New York, 2003.
23. MASON, A., G. Cisco Secure Virtual Private Networks. Cisco Press, New York, 2002.
24. RUIXI, Y. Virtual Private Networks: Technologies and Solutions. Addison-Weseley Professional, New York, 2001.
25. 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
26. 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
27. 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.
28. 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/
29. NISTIRIUC P., MIROVSKI Vl., CHIHAI A., ȚURCANU D., SAVA L., TÎRȘU V. Variable optical attenuator. În: CEM 2024 The 14th International Workshop on Electromagnetic Compatibility, p.30-31. Romania, Sibiu: print ISSN-L2537-222X.
30. ȚURCANU, D. Quality of Services in MPLS Networks. In: Journal of Engineering Science, 2020, Vol. XXVII (3). pp.102-110. https://zenodo.org/record/3949674