Taikomieji moksliniai tyrimai / Applied Scientific Research ISSN 2783-6290
2023, 2(1), 74-81. DOI: https://doi.org/10.56131/tmt.2023.2.1.111 Gauta 2023-05-22. Publikuota 2023-06-08

Saugus nutolusio kliento prisijungimas į kolegijos vidinį kompiuterių tinklą per VPN

Dr. Liudvikas Kaklauskas
Šiaulių valstybinė kolegija, Informatikos mokslų katedros docentas
Šiaulių valstybinė kolegija / Šiauliai State Higher Education Institution, Lithuania; Associate professor of the Department of Informatics Sciences
l.kaklauskas@svako.lt

Dominykas Pugačius
Šiaulių valstybinė kolegija, Informacinių sistemų technologijos studijų programos III kurso studentas
Šiaulių valstybinė kolegija / Šiauliai State Higher Education Institution, Lithuania; Information Systems Technology study program, 3rd course student
dominykas.pugacius@stud.svako.lt

Anotacija

Straipsnyje analizuojama saugaus nutolusio kliento prisijungimo į kolegijos vidinį kompiuterių tinklą problema. Įvertinti dažniausiai naudojami *OpenVPN, Libreswan* ir *WireGuard* sprendimai. Atlikta literatūros analizė parodė, kad OpenVPN sprendimas yra tinkamiausias realizuojant saugaus nutolusių klientų prisijungimo į kolegijos vidinį tinklą sistemą, nes nesudėtingai administruojamas, geba nuskaityti sertifikatus ir privačius raktus iš populiariausių operacinių sistemų, naudoja dvikryptį sertifikatų autentifikavimą. Išanalizuoti ir įvertinti kolegijos vartotojų poreikiai. Atliktas reikalavimų techninei įrangai tyrimas. Parengtas projektuojamos sistemos koncepcinis modelis. Realizuotas ir ištestuotas virtualus suprojektuotos sistemos modelis, panaudojant debesų kompiuterijos sprendimus. Patikrintas vidinio tinklo paslaugų pasiekiamumas, stebėtas ir įvertintas perduodamų duomenų šifravimas.

Reikšminiai žodžiai: VPN, OpenVPN, WireGuard, Libreswan, IPSec

Secure remote client connection to higher education institution internal computer network through VPN

Summary

The article analyzes the problem of secure connection of a remote client to the internal computer network of the higher education institution. The most commonly used OpenVPN, Libreswan and WireGuard solutions were evaluated. The analysis of the literature showed that the OpenVPN solution is the most suitable for implementing a system for secure connection of remote clients to the internal computer network of the higher education institution. OpenVPN is easy to administer, able to read certificates and private keys from the most popular operating systems, uses two-way certificate authentication. Has been analyzed and assessed the needs of higher education institution users. The study of requirements for technical equipment was carried out. A conceptual model of the projected system has been prepared. A virtual model of the designed system was implemented and tested using cloud computing solutions. Checked the availability of internal network services. Evaluated encryption of transmitted data.

Keywords: VPN, OpenVPN, WireGuard, Libreswan, IPSec

Įvadas

Tyrimo aktualumas. Technologijos yra pagrindinis pokyčių pasaulyje katalizatorius. Bagui ir kt. (2017) teigimu, technologijų pažanga suteikia įmonėms, vyriausybinio ir socialinio sektoriaus institucijų darbuotojams papildomas galimybes dirbti komandiruotėse ir iš namų. Daugelis įmonių, siekdamos užtikrinti didesnę komunikavimo saugą, padalinių sujungimui naudoja virtualaus privataus tinklo sprendimus. Naudojantis internetu, vartotojo kompiuteris nuolat keičiasi duomenimis

su nutolusiais tinklo serveriais. Mainų metu labai dažnai perduodama papildoma informacija (IP adresas, naršymo istorija, operacinės sistemos informacija ir kt.). Virtualus privatus tinklas (toliau – VPN (*angl.* Virtual Private Network)) užtikrina saugų prisijungimą prie nutolusių kompiuterių ar serverių, paslepia perteklinę informaciją apie vartotojo kompiuterį (Binkhorst ir kt., 2022). Naudojant VPN sprendimą tarp komunikuojančių nutolusių tinklo objektų sukuriamas saugus virtualus tunelis, naudojant viešus IP adresus. Duomenys perdavimo metu šifruojami, maskuojama siuntėjo ir gavėjo tapatybė, garantuojamas saugus nuotolinis darbas. Pagrindinis tokio sprendimo trūkumas yra duomenų perdavimo greičio lėtėjimas dėl vykdomų kodavimo ir dekodavimo procedūrų (Solisch, 2022, Islam ir kt., 2021).

Tyrimo problema. Straipsnyje analizuojama saugaus prisijungimo prie kolegijos vidinio tinklo iš nutolusio vartotojo kompiuterio problema. Kolegijoje naudojama daug programų sistemų, kurios yra pasiekiamos tik iš vidinio kompiuterių tinklo, vartotojai neturi galimybės saugiai jungtis iš interneto į vidinį kolegijos kompiuterių tinklą ir pasiekti šias programų sistemas. Mokslinės literatūros analizė parodė, kad saugaus duomenų perdavimo iš nutolusio kliento kompiuterio į kolegijos vidinį kompiuterių tinklą per VPN sistema dar nėra analizuota.

Tyrimo tikslas: suprojektuoti ir testuoti kolegijos kompiuterių tinklo posistemį, užtikrinantį saugų nutolusių kolegijos darbuotojų ir studentų prisijungimą prie vidinio kompiuterių tinklo programų sistemų ir paslaugų.

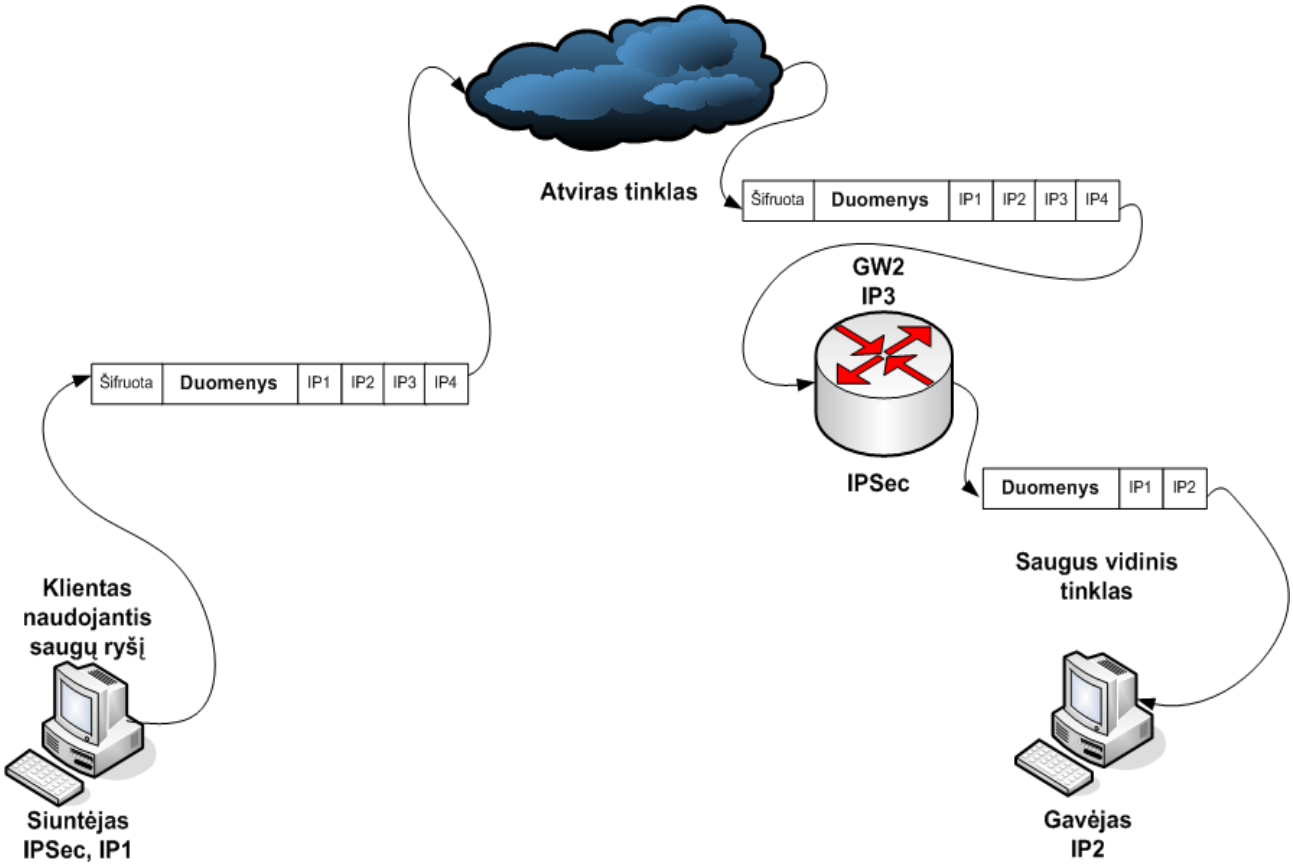
Tyrimo metodai: mokslinės literatūros analizė, modeliavimas, ekspertų interviu metodas (Baležentis, Žalimaitė, 2011).

Saugaus prisijungimo iš interneto į vidinį kolegijos tinklą teorinių sprendimų analizė

Vadovaujantis mokslinės literatūros analize, nustatyta, kad yra rekomenduojami šie populiariausi *VPN* sprendimai: *PPTP* (angl. Point-to-Point Tunneling Protocol) – minimaliai saugus *VPN*, palaiko visos operacinės sistemos; *L2TP* ir *IPsec* (angl. Layer 2 Tunneling Protocol, Internet Protocol Security) – tai didesnės *VPN* saugos protokolai; *SSL* (angl. Secure Sockets Layer) – protokolas perduodamus duomenis apsaugo juos šifruojant; *OpenVPN* – atvirojo kodo projektas, kuriantis programinį *VPN* (Yang, 2022, Gentile ir kt., 2022).

Vienas iš paprasčiausių sprendimų organizacijai – pasinaudoti specializuotų įmonių teikiamomis *VPN* paslaugomis (Ramesh ir kt., 2022, Zakaria ir kt., 2022). Khan ir kt. (2023) įvardino aštuonis populiariausius *VPN* paslaugos tiekėjus. Išsamesnei teikiamų komercinių *VPN* paslaugų struktūros analizei pasirinktos trys įmonės: *NordVPN*, *Surfshark* ir *ExpressVPN* (NordVPN, 2023; Surfshark, 2023; ExpressVPN, 2023). Šios įmonės nuomoja serverius, užtikrinant saugų vartotojų naršymą internete. NordVPN siūlo sprendimus, taikomus daugeliui kompiuterių tinklo įrenginių. *NordVPN* nukreipia vartotojų interneto srautą per nuotolinį serverį, paslepia IP adresą, šifruoja duomenis. Šifravimui naudojama *OpenVPN* ir *Internet Key Exchange v2/IPsec* technologija. Nuo 2019 m. įmonė pristatė ir užpatentavo savo *NordLynx* technologiją, grįstą *WireGuard* protokolu. *NordLynx* užtikrina geresnį sistemos našumą nei *IPsec* ar *OpenVPN* tuneliavimo protokolai. *Surfshark* siūlo naršyklės plėtinius, skirtus *Chrome* ir *Firefox*. *Surfshark VPN* pagrindinį dėmesį skiria privatumui, leidžia jungti neribotą įrenginių skaičių. Saugaus *VPN* prisijungimo kūrimui naudojamas *OpenVPN* sprendimas ir *WireGuard* protokolas. *ExpressVPN* skirta namų vartotojams, ją galima įdiegti į maršrutizatorių. Sistema naudoja *AES-256* šifravimo būdą. *VPN* kūrimui taip pat naudojamas *Lightway* arba *OpenVPN* sprendimas (Khan ir kt., 2023).

Čia analizuotos sistemos naudoja *OpenVPN* sprendimą, kuris realizuoja saugius privačius sujungimus per internetą, naudojant SSL/TLS protokolą. Šis protokolas palaiko lanksčius kliento autentifikavimo metodus, grįstus sertifikatais, intelektualiosiomis kortelėmis ir/arba vartotojo vardo/slaptažodžio kredencialais ir leidžia taikyti konkrečias vartotojo ar grupės prieigos kontrolės strategijas. VPN sujungimą galima realizuoti trimis skirtingais būdais: *tinklo klientas – tinklo mazgas, tinklo mazgas – tinklo mazgas* ir retai naudojamas būdas *tinklo klientas – tinklo klientas* (Ravindran ir kt., 2006; Hara ir kt., 2003; Braun ir kt., 1999). Straipsnyje analizuojamas *tinklo klientas – tinklo mazgas VPN* jungimo atvejis. Čia iš nutolusių klientų kompiuterių jungiamasi į kolegijos vidinį tinklą per *WAN-LAN* tinklo mazgą į *VPN* serverį.



1 pav. Kliento prijungimas per *VPN* į organizacijos vidinį kompiuterių tinklą

1 pav. matome, kad tinklo klientas iš savo kompiuterio jungiasi į kolegijos kompiuterių tinklą. Šiuo atveju vartotojo kompiuterio apkrova yra didesnė nei įprasta, nes jis turi užšifruoti ir dešifruoti perduodamus duomenų paketus į kolegijos kompiuterių tinklą. Duomenų gavėjo tinklo mazge yra integruotas *VPN* serveris, kuris taip pat atlieka užšifravimo ir dešifravimo veiksmus. 1 pav. matome, kad *IP3* ir *IP4* yra viešieji *IP* adresai, garantuojantys saugų *VPN* sujungimą iš kliento kompiuterio į tinklo mazgą.

Išanalizavus mokslinę literatūrą, nustatyta, kad joje analizuotas saugus įmonės padalinių apjungimas (Pilipavičius ir kt., 2016), vertinti saugos užtikrinimo sprendimai, jungiantis į universiteto kompiuterių tinklą per IPSec (Sharma, 2021; Jing ir kt., 2016), aptarti saugaus prisijungimo sprendimai (Khan ir kt., 2023; Yang, 2022; Gentile ir kt., 2022; Ravindran ir kt., 2006; Hara ir kt., 2003; Braun ir kt., 1999).

Saugaus prisijungimo teoriniai sprendimai

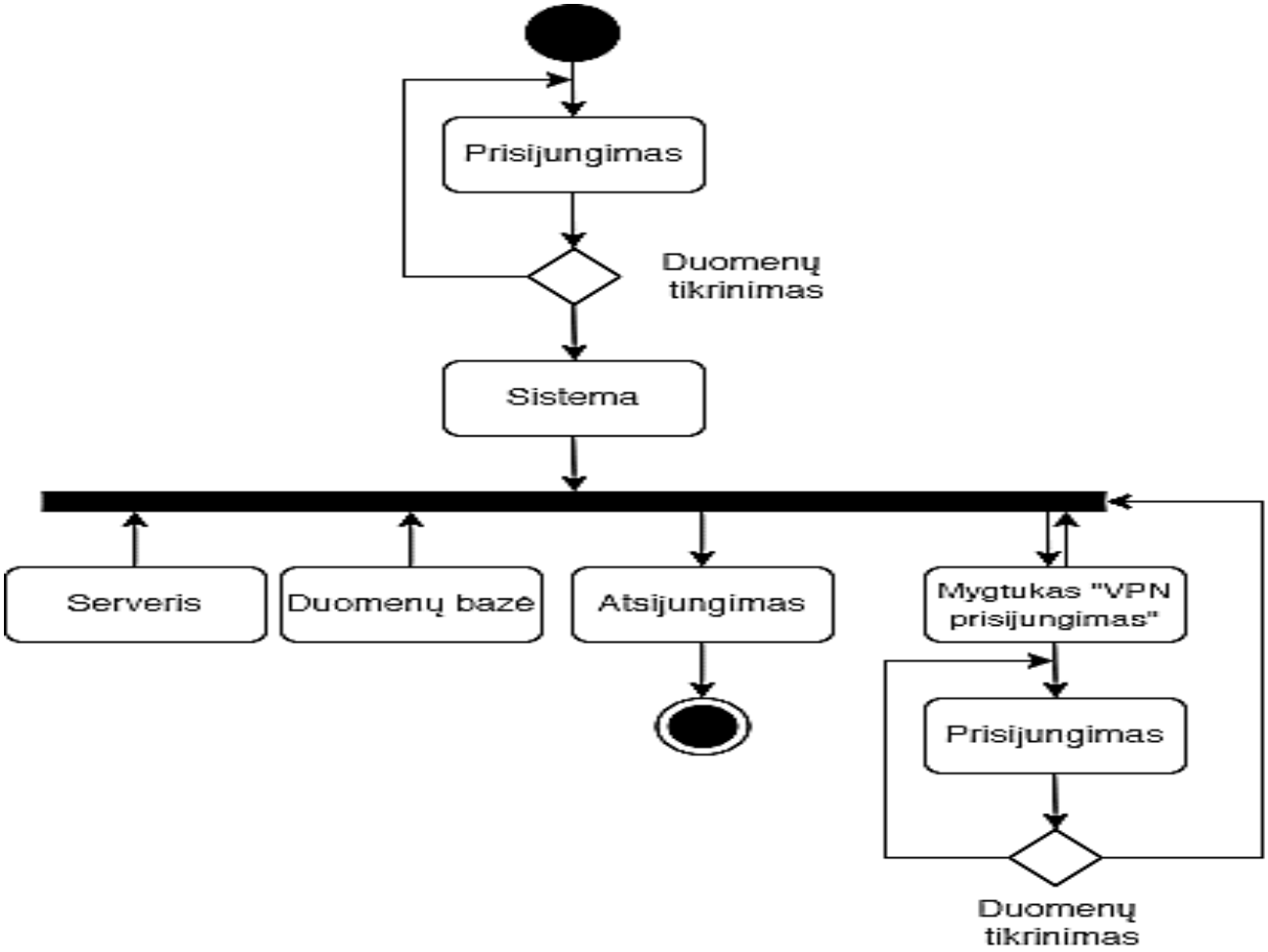
Įvertinus *VPN* paslaugas teikiančių įmonių sistemas, nustatyta, kad į jas dažnai integruojami *OpenVPN* (OpenVPN, 2023), *Libreswan* (LibreswanVPN, 2023) ir *WireGuard* (WireGuard, 2023) sprendimai (Ramesh ir kt., 2022; Zakaria ir kt., 2022). Nustatyta, kad dažniausiai naudojamas *OpenVPN* sprendimas, taikantis šifravimą bei kitas saugos priemones duomenų apsaugai ir privatumui užtikrinti. *OpenVPN* palaiko Windows, MacOS, Linux ir iOS operacines sistemas. Galima rinktis AES, Blowfish ar SSL/TLS šifravimo algoritmą. *OpenVPN* pasižymi patikimumu ir stabilumu (OpenVPN, 2023; Sha, 2020). *Libreswan* sprendimas pagrįstas populiariais IPsec ir IKE protokolais, lengvai diegiamas į *Linux*, *FreeBSD* ir *Apple OSX* tinklo operacines sistemas, tačiau šios sistemos administravimas pakankamai sudėtingas. *WireGuard* naudoja pažangiausius kriptografinius sprendimus, pakankamai greita, tačiau yra dar besivystanti technologija, todėl, ją taikant, gali kilti keblumų praktiniame darbe (Xue ir kt., 2022; Sha, 2020; Abdulazeez ir kt., 2020).

Apibendrinant *VPN* sprendimų analizę, nuspręsta pasirinkti *OpenVPN*, nes programos diegimas

ir dinaminių IP adresų palaikymas yra nesudėtingas, turi pakankamai paprastą administravimo sąsają, kurią galima naudotis nuotoliniu būdu. *Windows* operacinėje sistemoje *OpenVPN* geba nuskaityti sertifikatus ir privačius raktus iš pačios operacinės sistemos, kuri palaiko *Windows Crypto API* funkciją (Abbas ir kt., 2023).

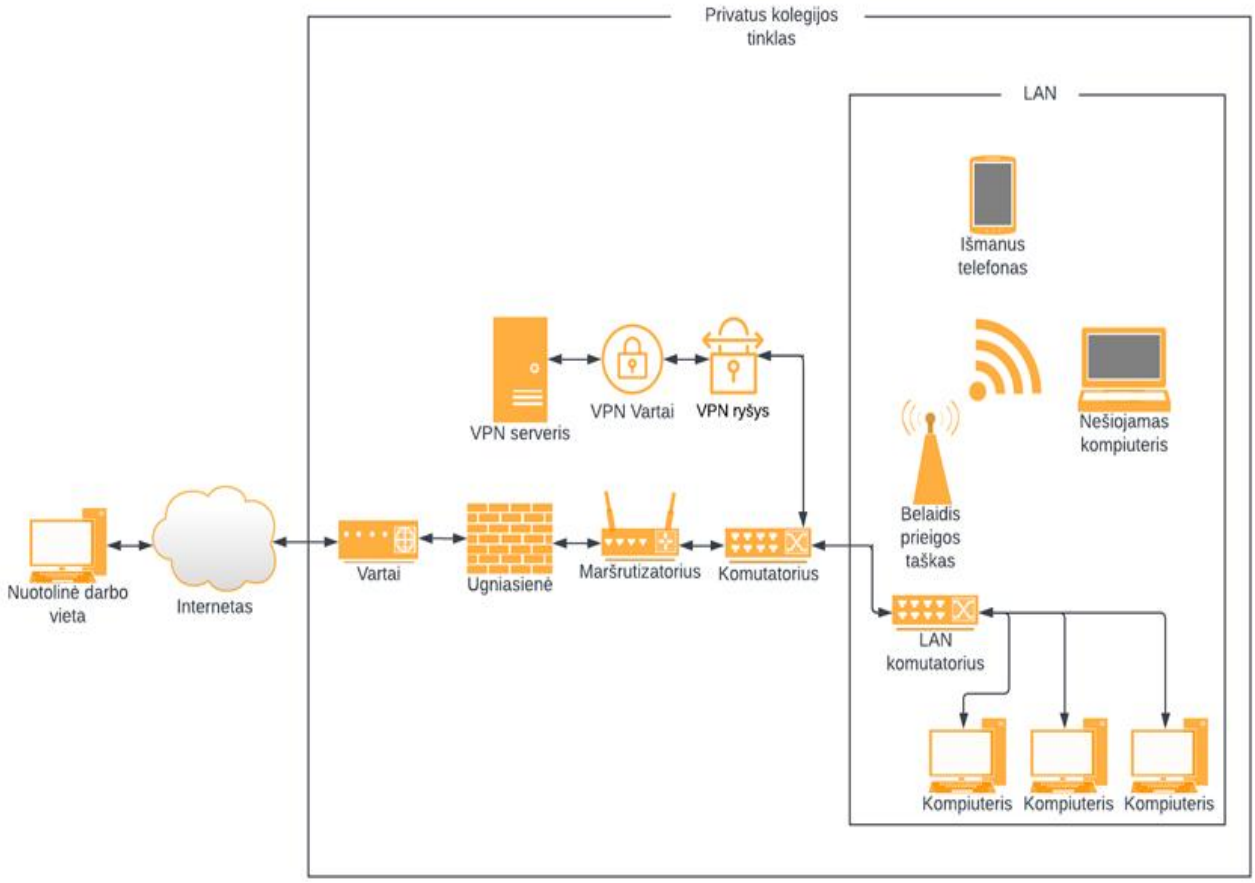
Saugaus prisijungimo sistemos projektavimas

Reikalavimų techninei įrangai analizė parodė, kad OpenVPN produktyviam darbui rekomenduojamas procesorius su 4 branduoliais, kurių minimali sparta 3GHz. Darbinės atminties apimtis priklauso nuo prijungtų įrenginių skaičiaus ir duomenų srauto. Nurodoma, kad 1 GB darbinės atminties efektyviai aptarnauja iki 150 prie VPN prijungtų įrenginių. Nustatyta, kad kolegijoje dirba ir studijuoja apie 1650 žmonių. Vadinasi, reikia ne mažiau nei 11 GB darbinės atminties, užtikrinant stabilų programinės įrangos darbą. Kolegijoje naudojamas interneto prieigos srautas yra ne mažesnis nei 3Gbps, jo pilnai pakanka kolegijos tinklo klientų aptarnavimui. Kietajame VPN serverio diske turi būti ne mažiau nei 16 GB vietos.



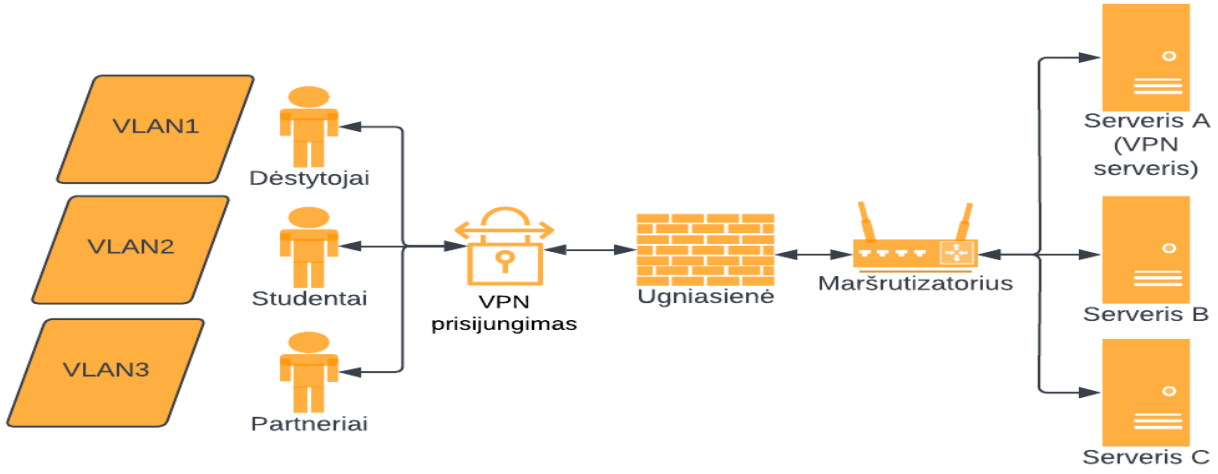
2 pav. Vartotojo veiklos diagrama

Taikant ekspertų interviu metodą (Baležentis, Žalimaitė, 2011), išsiaiškinti klientų saugaus prisijungimo į kolegijos vidinį tinklą poreikiai. Apklausti keturi ekspertai. Išanalizavus tyrimo rezultatus, išsiaiškintos pagrindinės projektuojamos *VPN* sistemos funkcijos: registravimas; prisijungimas; statuso peržiūra; aktyvių vartotojų peržiūra; ataskaitos; klasteris; *TLS* parametrai; tinklo parametrai; *VPN* parametrai; vartotojų valdymas; autentifikavimo parametrai. *VPN* sistemos funkcijos realizuotos projektuojamos sistemos modelyje, numatyti sistemos vartotojų veiksmai. Norint prisijungti prie sistemos, nutolęs vartotojas pirmiausiai turi įsidiegti kliento *VPN* programą. Ji naudojama prisijungimui prie kolegijos *VPN* serverio. Sėkmingai prisijungęs, vartotojas matys kolegijos vidinį kompiuterių tinklą. 2 pav. matome vartotojo veiklos diagramą, kur apibrėžti jo galimi veiksmai, naudojant *VPN* sistemą.



3 pav. Koncepcinis kolegijos *VPN* sistemos modelis

3 pav. matyti, kad nutolęs *VPN* klientas per kolegijos vartus (angl. Gateway from WAN to LAN) iš interneto jungiasi į *VPN* serverį. Čia jis gauna vartotojo identifikatorių su aprašytomis prieigos teisėmis. Tada jis gali patekti į kolegijos *LAN* ir pasinaudoti šio tinklo jam teikiamomis ir leidžiamomis naudoti paslaugomis. Realizuotoje sistemoje visi duomenys keliauja per vieną mazgą (4 pav.). Vartotojų grupių atskyrimui pagal teises panaudotas *VLAN* protokolas. *VLAN* sprendimas garantuoja, kad *Studentas,* priskirtas prie *VLAN2* tinklo, galės pasiekti tik *Serverio B* resursus. *Dėstytojai* galės matyti serverius, kurie priklauso *VLAN1*. Sistemos duomenų apsaugai taikomas *AES-256* duomenų šifravimo protokolas. Naudojamas dvikryptis autentifikavimo sertifikatas, kuris reikalauja kliento autentifikuoti serverio sertifikatą, o serveris turi autentifikuoti kliento sertifikatą, taip užtikrinamas abipusis pasitikėjimas.

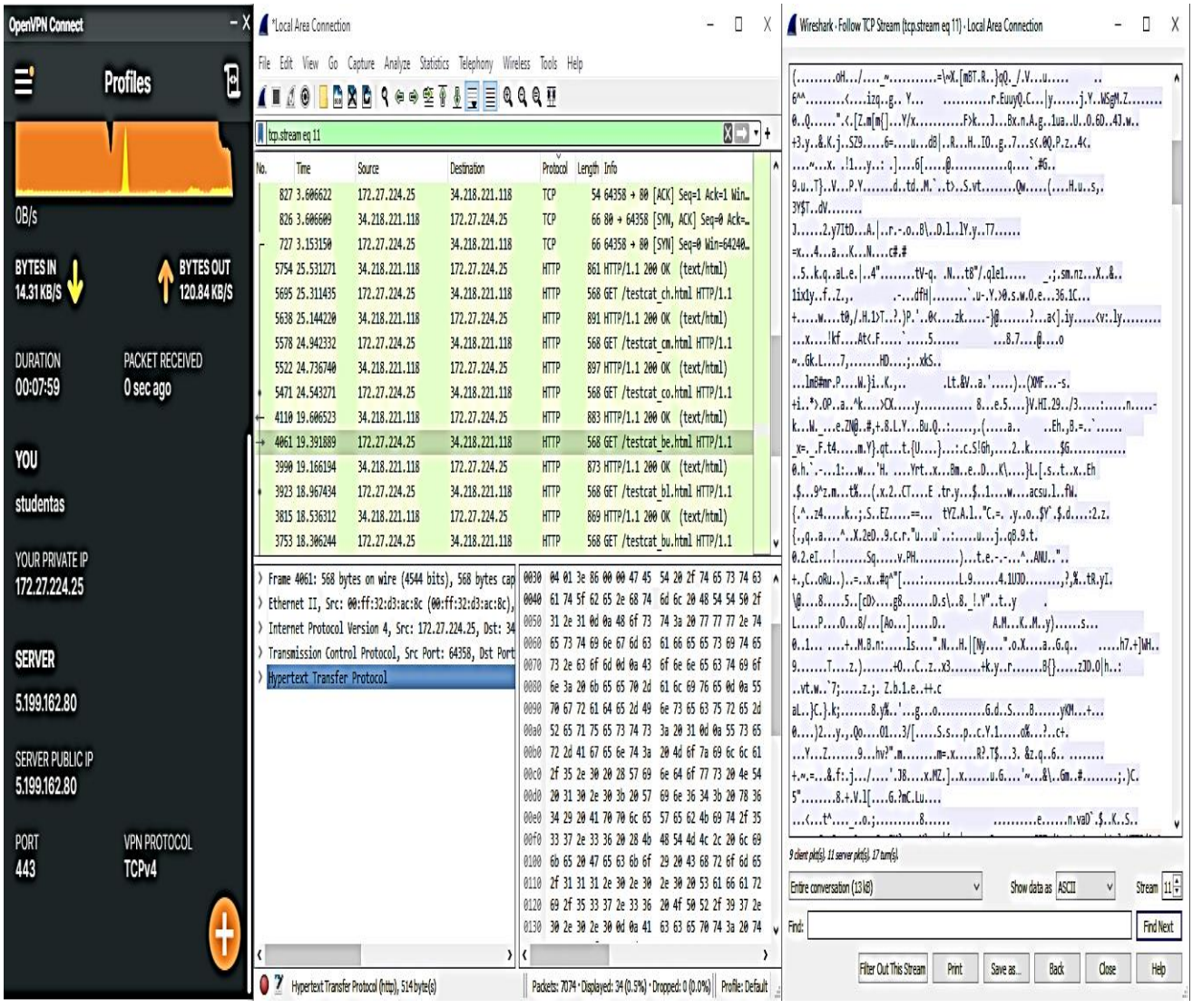


4 pav. Kliento prisijungimo prie kolegijos *VPN* serverio schema

Saugaus prisijungimo sistemos testavimas

Naudojant debesų kompiuterijos paslaugas, suprojektuotas ir parengtas virtualus sistemos testavimo modelis. Kolegijos kompiuterių tinklą ir jo funkcijas imitavo *Linux Ubuntu* serveris, o klientą imitavo Linux *Ubuntu Desktop* su *Gnome* grafine aplinka. Naudojant *Uncomplicated Fireewall* taisykles, suderinta užkarda. Diegiant *OpenVPN* paketus, įkelti sertifikatai bei kitos prisijungimo saugą užtikrinančios priemonės. Sukurta administratoriaus vartotojo sąsaja. Sukonfigūruotas transporto protokolas. *TCP* pakeistas į *UDP*, taip užtikrinant didesnę komunikavimo spartą sistemoje. Kliento kompiuteryje suderinta nutolusio kliento *OpenVPN* dalis.

Egzistuojančių *LAN* paslaugų kolegijoje imitavimui serveryje suderintas *LAMP* posistemis. Įdiegta *MySql* duomenų bazė ir suderinti jos sąryšiai su kitomis sistemomis. Suderinta turinio valdymo sistema, imituojanti paslaugas, teikiamas kolegijos vidiniame tinkle. Tam panaudota *WordPress* turinio valdymo sistema, kuri imituoja kolegijos vidiniame tinkle naudojamas paslaugas. Šios paslaugos yra pasiekiamos tik per kolegijos vidinius *IP* adresus arba per vidiniame *DNS* serveryje registruotus domenus.



5 pav. Sistemos saugos testavimas

Pirmiausia virtualiame sistemos testavimo modelyje patikrinta, ar tinkamai veikia *VPN* tunelis. Tam iš *OpenVPN* kliento prisijungta į *VPN* serverį. Tada, naudojant vidinius imituojamo kolegijos tinklo adresus, prisijungta prie tik iš vidinio tinklo pasiekiamos *TVS WordPress* paslaugos. *VPN* saugos testavimui panaudota *Wireshark* programa, kuri stebėjo duomenų srautus, keliaujančius per *VPN* tunelį. Iš surinktų kompiuterių tinklo srauto paketų išfiltravus tik per *VPN* tunelį keliaujančius paketus, matyti, kad jų turinys užkoduotas (žr. 5 pav.).

Išvados

Vadovaujantis atlikta mokslinės literatūros analize nustatyta, kad *OpenVPN* sprendimas yra tinkamiausias, realizuojant saugaus nutolusių klientų prisijungimo į kolegijos vidinį tinklą sistemą, nes nesudėtingai administruojamas, geba nuskaityti sertifikatus ir privačius raktus iš populiariausių operacinių sistemų, naudoja dvikryptį sertifikatų autentifikavimą.

Parengtas koncepcinis kolegijos VPN sistemos modelis, realizuotas virtualus šios sistemos prototipas, jis ištestuotas: patikrintas vidinio tinklo paslaugų pasiekiamumas; stebėtas ir įvertintas perduodamų duomenų šifravimas.

Literatūra

1. Abbas, H., Emmanuel, N., Amjad, M. F., Yaqoob, T., Atiquzzaman, M., Iqbal, Z., Shafqat N., Shahid W. B., Tanveer A., & Ashfaq, U. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. *ACM Computing Surveys*. https://doi.org/10.1145/3579162
2. Abdulazeez, A., Salim, B., Zeebaree, D., & Doghramachi, D. (2020). *Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol*. The Learning & Technology Library. https://www.learntechlib.org/p/218341/
3. Bagui, S., Fang, X., Kalaimannan, E., Bagui, S. C., & Sheehan, J. (2017). Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features. *Journal of Cyber Security Technology*, 1(2), 108–126.
4. Baležentis, A., Žalimaitė, M. (2011). Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. *Vadybos mokslas ir studijos – kaimo verslų ir jų infrastruktūros plėtrai*, 3(27), 23–31.
5. Binkhorst, V., Fiebig, T., Krombholz, K., Pieters, W., & Labunets, K. (2022). Security at the End of the Tunnel: The Anatomy of {VPN} Mental Models among Experts and {Non-Experts} in a Corporate Context. In *31st USENIX Security Symposium (USENIX Security 22)*, pp. 3433–3450. https://www.usenix.org/conference/usenixsecurity22/presentation/binkhorst
6. Braun, T., Günter, M., Kasumi, M., & Khalil, I. (1999). Virtual private network architecture. *Charging and Accounting Technology for the Internet (Aug. 1, 1999)(VPNA)*. https://home.inf.unibe.ch/~rvs/research/pub_files/BGKK99.pdf
7. ExpressVPN. (2023). https://www.expressvpn.com
8. Gentile, A. F., Macrì, D., De Rango, F., Tropea, M., & Greco, E. (2022). A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment. *Future Internet*, 14(9), 264. https://doi.org/10.3390/fi14090264
9. Hara, Y., Ohsaki, H., Imase, M., Tajima, Y., Maruyoshi, M., Murayama, J., & Matsuda, K. (2003, November). VPN architecture enabling users to be associated with multiple VPNs. In *Proceedings of the 5th Asia–Pacific Symposium on Information and Telecommunication Technologies (APSITT 2003)*, pp. 195–200.
10. Islam, M. Z., Khan, M. A. R., Hossain, M. I., & Hossain, R. (2021). Analysis the importance of VPN for Creating a Safe Connection Over the World of Internet. *International Journal of Advanced Research in Computer and Communication Engineering*, 10(10), 86–92.
11. Jing, S., Qi, Q., Sun, R., & Li, Q. (2016, December). Study on VPN solution based on multi-campus network. In *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, pp. 777–780. IEEE. DOI: 10.1109/ITME.2016.0180
12. Khan, E., Sperotto, A., van der Ham, J., & van Rijswijk-Deij, R. (2023, March). Stranger VPNs: Investigating the Geo-Unblocking Capabilities of Commercial VPN Providers. In *Passive and Active Measurement: 24th International Conference, PAM 2023, Virtual Event*, March 21–23, 2023, Proceedings, pp. 46-68. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28486-1_3
13. LibreswanVPN. (2023). https://libreswan.org
14. NordVPN. (2023). https://nordvpn.com
15. OpenVPN. (2023). https://openvpn.net
16. OpenVPN. (2023). *OpenVPN Access Server system requirements*. https://openvpn.net/vpn-server-resources/openvpn-access-server-system-requirements/#hardware-requirements
17. Pilipavičius, M., Kaklauskas, L. (2016). Tuneliavimo metodų tyrimas, užtikrinant saugius informacijos mainus tarp nutolusių įmonės padalinių. *Studijos modernioje visuomenėje*. *Mokslo darbai*, 7(1), 233–238. https://www.slk.lt/sites/default/files/studijos_siuolaikineje_visuomeneje_2016.pdf#page=233

18. Ramesh, R., Vyas, A., & Ensafi, R. (2022). "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers. arXiv preprint arXiv:2208.03505. https://www.usenix.org/system/files/sec23summer_147-ramesh-prepub.pdf
19. Ravindran, R. S., Huang, C., & Thulasiraman, K. (2006, June). A dynamic managed VPN service: architecture and algorithms. In *2006 IEEE International Conference on Communications*, 2, pp. 664–669. IEEE. DOI: 10.1109/ICC.2006.254783
20. Sha, A. (2020). OpenVPN vs WireGuard: The Best VPN Protocol. https://beebom.com/openvpn-vs-wireguard/
21. Sharma, G. (2021). Secure Remote Access IPSEC Virtual Private Network to University Network System. *Journal of Computer Science Research*, 3(1), 16–27.
22. Solisch, T. (2022). Comparison of VPN Technologies. FMS-BERICHTE.
23. Surfshark. (2023). https://surfshark.com
24. WireGuard. (2023). https://www.wireguard.com
25. Xue, D., Ramesh, R., Jain, A., Kallitsis, M., Halderman, J. A., Crandall, J. R., & Ensafi, R. (2022). {OpenVPN} is Open to {VPN} Fingerprinting. In *31st USENIX Security Symposium (USENIX Security 22)*, pp. 483–500.
26. Yang, H. (2022). Application of hybrid encryption algorithm in hardware encryption interface card. *Security and Communication Networks*, 2022. https://doi.org/10.1155/2022/7794209
27. Zakaria, M. I., Norizan, M. N., Isa, M. M., Jamlos, M. F., & Mustapa, M. (2022). Comparative analysis on virtual private network in the internet of things gateways. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(1), 488–497.