УДК 004.7.056.5

Козюк Ю.Ю.

Салієва О.В.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ТУНЕЛЮВАННЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація. *Дана робота присвячена аналізу використання сучасних технологій створення конфіденційних каналів зв'язку (тунелів) у публічних та приватних комп'ютерних мережах.*

Ключові слова: комп'ютерна мережа; тунель; шифрування; конфіденційність; WireGuard; IPSec; GRE, L2TP; Open VPN; EoIP; IS.

Abstract*. This work is devoted to the analysis of the use of modern technologies for creating confidential communication channels (tunnels) in public and private computer networks..*

Keywords: computer network; tunnel; encryption; confidentiality; WireGuard; IPSec; GRE, L2TP; OpenVPN; EoIP; ISP.

Вступ

Сучасні комп'ютерні мережі характеризуються різноманітністю технологічних засобів і каналів зв'язку. Так, корпоративні мережі підприємств поєднують внутрішні та зовнішні зв'язки для побудови своєї інфраструктури. Питання забезпечення конфіденційності передачі інформації в таких мережах набуває особливого значення. Зміни в робочому середовищі, зокрема збільшення кількості співробітників, що працюють віддалено, сприяють впровадженню захищених зовнішніх каналів зв'язку з інформаційними системами та підсистемами, розташованими у внутрішній приватній частині корпоративної мережі. Постійні вимоги до розробників програмного та апаратного забезпечення для комп'ютерних мереж призводять до впровадження нових програмно-апаратних рішень для забезпечення передачі конфіденційної інформації [1].

Результати дослідження

Враховуючи мету даного дослідження, варто проаналізувати мережеву технологію тунелювання, перевагами якої є: захист приватності, створення безпечних з'єднань, прозорість мережевої інфраструктури та забезпечення доступу до внутрішніх ресурсів. До недоліків тунелювання варто віднести: збільшення навантаження мережі, можливість атаки на протоколи, складність налаштування й підтримки та можливість затримок і втрати пакетів. Незважаючи на ці недоліки, технологія тунелювання залишається важливим інструментом забезпечення безпеки і конфіденційності комп'ютерних мереж, особливо в умовах зростаючих загроз кібербезпеки [2].

Розглянемо найвідоміші технології тунелювання в комп'ютерних мережах.

Тунелювання з використанням протоколу **WireGuard** – це безпечний метод зв'язку для комп'ютерних мереж, що базується на однойменному інноваційному протоколі. WireGuard є простим у використанні, ефективним і безпечним механізмом для створення віртуальних приватних мереж (VPN), заснований на шифруванні трафіку та обміну ключами. Протокол є привабливим варіантом для використання в сучасних комп'ютерних мережах, оскільки забезпечує швидку передачу даних і мінімізує затримки. Тунелі з використанням WireGuard можна створювати як між окремими пристроями, так і між мережами, забезпечуючи безпеку і конфіденційність під час передачі даних через такі мережі як Інтернет [3].

Тунелювання з використанням **Generic Routing Encapsulation (GRE) та Internet Protocol Security** (IPSec) – це спосіб безпечного з'єднання двох або більше мереж або пристроїв через загальнодоступну мережу. GRE використовується для пакування даних з протоколу в мережеві пакети IP і їх відправки через мережу, яка не підтримує цей протокол. IPSec забезпечує безпеку і конфіденційність даних, що передаються по мережі. При цьому GRE використовується для створення тунелю між віддаленими мережами або пристроями, а IPSec – для шифрування і аутентифікації мережевого трафіку.

Тунелювання з використанням протоколу тунелювання 2-го рівня **(L2TP**) і захисту інтернет-протоколу (IPSec) – це метод безпечного з'єднання двох точок комп'ютерної мережі через загальнодоступну мережу. L2TP використовується для створення віртуального тунелю між двома вузлами мережі, а IPSec використовується для шифрування і захисту цих тунельних з'єднань. При використанні цього методу, L2TP використовується для створення логічного з'єднання між двома кінцями тунелю, що дозволяє передавати дані між двома вузлами в непублічній мережі. IPSec дозволяє шифрувати дані, що надсилаються через цей тунель, і забезпечує їх автентичність та цілісність. Тунелі з використанням L2TP + IPSec широко використовуються для створення захищених з'єднань між віддаленими користувачами і корпоративними мережами, а також для забезпечення безпеки і конфіденційності даних, що передаються через ці з'єднання. Такий підхід дозволяє ефективно захищати мережевий трафік і забезпечує безпечний доступ до мережевих ресурсів з будь-якої точки, де є інтернет-з'єднання [4].

Тунелювання з використанням **Ethernet over IP (EoIP)** і Internet Protocol Security (IPSec) – це спосіб забезпечити безпеку і конфіденційність з'єднання між двома мережами або пристроями через загальнодоступну мережу. EoIP використовується для створення віртуального рівня Ethernet поверх IP-мережі для передачі кадрів Ethernet між вузлами мережі, тоді як IPSec використовується для шифрування і захисту цього тунельного з'єднання. При використанні цього методу, EoIP використовується для імітації рівня Ethernet поверх IP-мережі, що дозволяє передавати дані між вузлами мережі, навіть якщо вони знаходяться в різних локальних мережах або віддалених місцях. IPSec використовується для шифрування і захисту переданих даних. Тунелі EoIP + IPSec часто використовуються для з'єднання віддалених мереж і філій з центром та для забезпечення безпеки і конфіденційності даних, що передаються через ці з'єднання.

Тунелювання за допомогою **OpenVPN** – це метод забезпечення безпечного з'єднання між двома точками комп'ютерної мережі через публічну мережу. OpenVPN використовується для створення віртуального приватного з'єднання, яке забезпечує шифрування і безпечне передавання даних. OpenVPN створює тунель, що забезпечує безпечну передачу даних між вузлами мережі. OpenVPN використовує протокол TLS/SSL для шифрування та аутентифікації даних, забезпечуючи високий ступінь безпеки. Тунелі з використанням OpenVPN широко застосовують для забезпечення безпеки та конфіденційності даних у корпоративних мережах і для захисту особистих даних користувачів у віртуальних приватних мережах. Такий підхід забезпечує безпечний доступ до мережевих ресурсів з будь-якого місця, де є під'єднання до Інтернету, і гарантує захист даних під час передавання за межі приватної мережі [5].

Здійснимо порівняльний аналіз описаних методів тунелювання, використовуючи рейтингову шкалу показників (табл.1).

Таблиця 1 – Порівняльний аналіз сучасних методів тунелювання

Метод тунелювання	Швидкодія	Рівень безпеки	Складність налаштування	Сумісність з різними платформами
WireGuard	Висока	Високий	Низька	Середня
L2TP + IPSec	Середня	Високий	Середня	Висока
EoIP + IPSec	Середня	Високий	Середня	Висока
OpenVPN	Середня-Висока	Високий	Висока	Висока
GRE + IPSec	Середня	Високий	Висока	Низька

Таким чином, можна зробити висновок, що WireGuard виділяється як метод тунелювання з високою швидкодією та низькою складністю налаштування, що робить його привабливим вибором для різноманітних сценаріїв. В свою чергу, OpenVPN вражає високою сумісністю з різними платформами та високим рівнем безпеки.

Висновки

Отже, сучасні комп'ютерні мережі вимагають надійних і безпечних методів передачі даних. Тунелювання є одним з таких методів, який гарантує конфіденційність та захист інформації під час

передачі через публічні мережі. У даній роботі було проаналізовано декілька сучасних методів тунелювання, зокрема WireGuard, L2TP+IPSec, EoIP+IPSec, OpenVPN та GRE+IPSec. Кожен із них має свої переваги та недоліки, але найпростішим у використанні виявився досліджуваний метод WireGuard.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комп'ютерні мережі: навчальний посібник, Одеса : Фенікс, 2022, 189 с. ISBN 978-966-928. [Електронний ресурс] – Режим доступу до ресурсу: http://dspace.onua.edu.ua/handle/11300/19423 (Дата звернення 01.05.2024 р.).
2. Generic Routing Encapsulation (GRE) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.rfc-editor.org/rfc/pdfrfc/rfc2784.txt.pdf. (Дата звернення 01.05.2024).
3. Комп'ютерні мережі: підручник з дисципліни «Комп'ютерні мережі» / Блозва А. І. , Матус Ю. В., Касаткін Д. Ю.; Нац. ун-т біоресурсів і природокористування України, Каф. комп'ютер. систем і мереж. – Київ: Компринт, 2019. Т. 2. – 2019.– с. 382 (Дата звернення 04.05.2024).
4. Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації/ Є. В. Риндич, Т. А. Петренко, Л. Г. Черниш, С.М. Семендяй, Г.С. Біленький//Технічні науки та технології. –2020. –N 2(20). –С. 229–236. (Дата звернення 04.05.2024).
5. Protocol Compatibility // [Електронний ресурс]. – Режим доступу до ресурсу: https://openvpn.net/index.php/open-source/documentation/miscellaneous/protocol-compatibility.html (Дата звернення 04.05.2024).

Козюк Юлія Юріївна – студентка групи УБ-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: juliakozyk999@gmail.com

Салієва Ольга Володимирівна − доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Koziuk Yuliia Y. – student of the UB-21b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: juliakozyk999@gmail.com

Saliieva Olha V. − Doctor of Philosophy (PhD) in 125 "Cybersecurity", Senior Lecturer, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@vntu.edu.ua