ЦИФРОВА ЕКОНОМІКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
Digital Economy and Information Technologies

УДК 004.7

Микита Капустін,

Провідний інженер комп'ютерних систем, Fozzy Group,
Запоріжжя, Україна

МЕТОДИКА ВИБОРУ ПРОТОКОЛУ VPN ПРИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ В КОРПОРАТИВНИХ МЕРЕЖАХ

Анотація — Метою роботи став аналіз і порівняння продуктивності сучасних рішень віртуальних приватних мереж в умовах стабільного та ненадійного мережевого з'єднання, а також розробка рекомендацій для вибору найліпшого рішення для організації віддаленого доступа в корпоративних мережах.
Для цього були досліджені проблеми вибору протоколу віртуальної приватної мережі; визначений перелік протоколів для порівняльного аналізу; визначені метрики та інструменти для вимірювання продуктивності; проведені експериментальні дослідження продуктивності, що дозволилоі порівняти продуктивність різних рішень, у різних середовищах та умовах застосування та обґрунтувати рекомендації з вибору найліпшого протоколу.

Ключові слова— IPERF, IPSEC, L2TP, OPENVPN, VPN, WIREGUARD, віддалений доступ, ненадійність, продуктивність, протокол

I. ВСТУП

В останні роки значна кількість працівників компаній переходять на віддалений режим роботи, який надає багато переваг, таких як гнучкість організації роботи та безперервність робочих процесів. При цьому сам процес забезпечення віддаленого доступу до мережі компанії пов'язаний із багатьма викликами. Віддалені співробітники отримують доступ до даних і програм компанії за межами корпоративної мережі, в результаті чого вони піддаються багатьом ризикам безпеки, а також наражають дані та системи своїх роботодавців та співробітників на такі ризики. Рішення віддаленого доступу оптимізують те, як компанії надають доступ до даних і програм віддаленим співробітникам, але розгортання таких систем і їх обслуговування може виявитися складним.

Одним з традиційних і найвідоміших рішень проблеми організації безпечної віддаленої роботи є віртуальні приватні мережі (Virtual Private Network, VPN). VPN встановлює зашифрований тунель між системою, на якій працює клієнт VPN, і сервером VPN, який потім передає трафік через тунель до решти корпоративної мережі. Система, на якій працює VPN-клієнт, фактично стає розширенням корпоративної мережі, що існує всередині цієї мережі з доступом до ресурсів, який загалом еквівалентний будь-якій іншій системі корпоративної мережі (рис. 1).

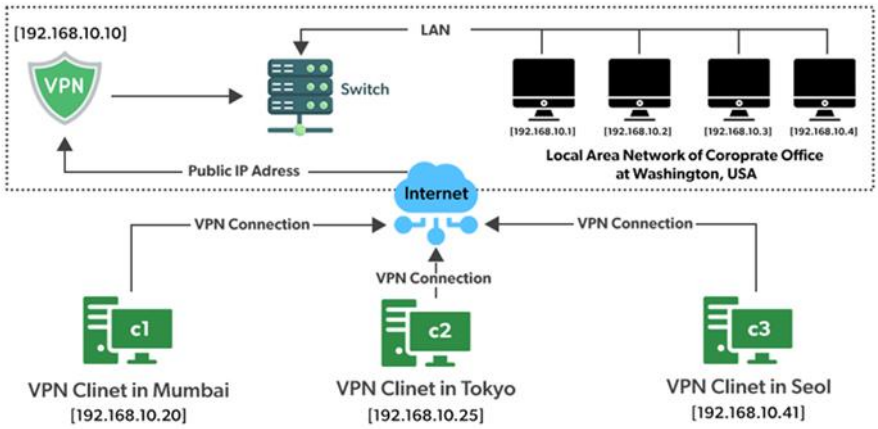

Рисунок 1 – Схема організації VPN

Таким чином, віртуальна приватна мережа – це спосіб розширення приватної мережі через загальнодоступну мережу, таку як Інтернет. Вона називається віртуальною тому, що залежить від використання тимчасових з’єднань, які не мають реальної фізичної присутності, але складаються з маршрутизованих пакетів. Технології VPN, а також способи їх встановлення, конфігурації та використання детально описані Ч. Скоттом, П. Вулфом та М. Ервіном у книзі «Віртуальні приватні мережі». [1]

VPN віддаленого доступу працює шляхом створення віртуального тунелю між пристроєм співробітника та мережею компанії. Цей тунель проходить через загальнодоступний Інтернет, але дані, що надсилаються туди й назад, захищені протоколами шифрування та безпеки, щоб зберегти їх конфіденційність. Важливість збереження безпеки при реалізації VPN, а також засоби захисту даних, які використовуються у цих технологіях, детально розглянуті С. Брауном у книзі «Впровадження віртуальних приватних мереж». [2]

Згідно з нашим дослідженням трьома найпоширенішими протоколами, які сьогодні використовуються у VPN віддаленого доступу, є Ipsec, OpenVPN та WireGuard.

IPSec зазвичай використовується разом із протоколом L2TP (Layer 2 Tunneling Protocol, L2TP). L2TP забезпечує тунелювання шляхом інкапсуляції корисного навантаження з однієї точки в іншу, але не надає можливості шифрування. IPSec доповнює його, виконуючи автентифікацію і шифрування пакетів даних, і відповідно підвищує рівень безпеки. Але, через те, що дані інкапсулюються двічі, це безпосередньо впливає на швидкість передачі даних. L2TP/IPSec підтримується всіма сучасними операційними системами.

OpenVPN є універсальним протоколом, який підтримує різні алгоритми шифрування і працює на великій кількості платформ. OpenVPN пройшов декілька незалежних експертиз безпеки, що підтвердили у нього відсутність серйозних вразливостей. Головним недоліком OpenVPN вважається складність налаштування VPN за цим протоколом.

Відносно новий протокол WireGuard розроблявся з метою замінити обидва вищеназвані протоколи і забезпечити більшу продуктивність, у порівнянні з попередніми реалізаціями. Незважаючи на те, що WireGuard сьогодні займає не надто помітне місце в індустрії VPN, він є протоколом, який уникає складності IPsec і має ліпшу продуктивність за OpenVPN. Спершу WireGuard був написаний виключно для Linux, але зараз цей протокол доступний для великої кількості платформ.

Незважаючи на розповсюдженість використання цих технологій, мережеві адміністратори стикаються з проблемою обґрунтованого вибору протоколу VPN. Існуючі протоколи пропонують різні можливості налаштування та безпеки, а також по-

різному впливають на продуктивність віртуальної приватної мережі. У відкритих джерелах часто міститься інформація про застарілі та потенційно скомпрометовані протоколи, натомість дослідження сучасних протоколів зустрічається значно рідше.

Вплив рішень віртуальних приватних мереж на продуктивність мережі досліджується у працях Ш. Нарайяна, К. Брукінга та С. де Вере [3], К. Навея та Ш. Ду [4]. Порівняння рішень з погляду продуктивності наводиться у роботі А. Абдулазіза, Б. Саліма, Д. Зібарі та Д. Доградмачі [5], а також Л. Оссвальда, М. Хеберле та М. Мента [6]. Вимірювання продуктивності мережі за умов ненадійності мережевого з’єднання виконується у роботах Д. Брассіла, Р. Макгіра, Р. Раджагопалана, Е. Бав’єра, Л. Робертса, Б. Марка та С. Шваба [7], а також Д. Коула та В. Тейна [8], однак аналіз джерел не дозволив знайти досліджень, у яких би порівнювалась продуктивність рішень віртуальних приватних мереж в умовах стабільного та ненадійного мережевого з’єднання, в залежності від використовуваної платформи. Тому, в цій статті викладається розроблена методика порівняльного аналізу сучасних протоколів VPN та результати її використання, які дозволяють обґрунтовувати вибір найбільш продуктивного протоколу в певних умовах застосування.

II. МОДЕЛІ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Розроблена методика передбачає:

- виокремлення метрик, за якими вимірюється продуктивність рішень VPN,
- обґрунтування інструментів вимірювання,
- опис експериментів та обробку їх результатів,
- узагальнення результатів цих експериментів для складання рекомендацій з метою обґрунтування вибору найбільш продуктивного з рішень в конкретних умовах.

Під час вимірювання продуктивності мережі використовувалися три показники: пропускна здатність, затримка та втрата пакетів. Пропускна здатність – це обсяг даних, що надсилається з однієї точки в іншу протягом певного періоду часу. Пропускна здатність зазвичай вимірюється в бітах на секунду (біт/с). На цей показник впливають характеристики фізичного середовища та обчислювальна потужність системи. Затримка визначається як час, необхідний для передачі пакета в одному напрямку, наприклад, від клієнта до сервера. Під час тестування VPN затримка є значенням часу, що зазвичай вимірюється у мілісекундах (мс). Втрата пакетів вказує на кількість пакетів, що не надійшли від джерела до місця призначення. Це може бути викликано, наприклад, перевантаженням мережі. Цей показник вимірюється як відсоток втрачених пакетів відносно надісланих пакетів (%).

В якості програмного інструмента для організації експериментів використовувався iPerf, який дозволяє виконувати стандартизовані вимірювання продуктивності для будь-якої мережі. Типовий вихід iPerf містить звіт із міткою часу про кількість переданих даних і виміряну пропускну здатність. Цей інструмент широко використовується для вимірювання продуктивності мереж, зокрема в дослідженнях, цитованих раніше у цій роботі.

Експериментальна установка містить одну машину, яка працює як програмний маршрутизатор під керуванням pfSense. pfSense є спеціалізованим дистрибутивом операційної системи FreeBSD з відкритим кодом, що призначений виконувати функції мережевого екрана та мережевого маршрутизатора. [9]

Маршрутизатор має два контролери мережевого інтерфейсу (Network Interface Controller, NIC), один з яких може працювати зі швидкістю до 1 Гбіт/с, інший – до 2.5 Гбіт/с. Перший порт було підключено до комутатора, що з’єднує клієнтську мережу, другий – до сервера VPN. Комутатор між маршрутизатором та клієнтами використовувався в експериментальній установці для того, щоб спростити тестування, оскільки маршрутизатор мав лише два порти, і тому його потрібно було вручну відключати та підключати щоразу, коли виконувалось тестування на іншому клієнті. Якби комутатор створив будь-яку затримку, вона була б однаковою для всіх клієнтів та VPN, тому її додавання є незначним для цього експерименту.

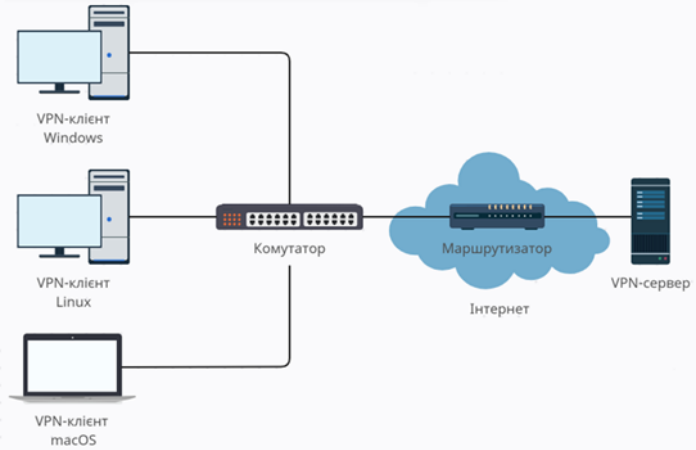

Рис. 2 – Топологія мережі в експерименті

Параметри мережі, що були визначені як важливі для тестування:

– затримка, 400 мс, згідно з документом служби підтримки Cisco[10] (перша ненадійність);

– втрата пакетів, 1%, згідно з дослідженням Ю. Полацького [11] (друга ненадійність).

Тестування було розроблено для запуску тестів по одному клієнту за раз. Один стандартний тест iPerf складається з 10-секундного безперервного тестування та звітування про пропускну здатність з інтервалом в 1 секунду. iPerf працює, записуючи масив певного обсягу байтів, певну кількість разів. За замовчуванням цей обсяг становить 128 КБ для TCP та 8 КБ для UDP. Це означає, що застосунок надсилає пакети через мережу з фіксованим розміром вікна, по суті, буфером кількості даних, надісланих до того, як їх підтвердить одержувач. Крім того, застосунок працює в пам’яті, тому диск взагалі не задіяний під час вимірювання, а дані, що надсилаються, є шумом (випадковими даними). iPerf має дуже просту архітектуру, де одна кінцева точка є сервером, а інша – клієнтом. Будь-яка з цих точок може бути сервером або клієнтом.

Тест за замовчуванням, який використовувався в цьому дослідженні, – це завантаження даних із клієнта на сервер. Кожен тест повторювався 50 разів. Перший 1-секундний інтервал тесту було видалено з набору даних, щоб дати можливість встановити належне з’єднання, оскільки тест розпочинався одразу після ввімкнення VPN.

Щоб мінімізувати ймовірні перешкоди, під час тестування одного з протоколів VPN всі інші були вимкнені, і клієнти, і сервер були перезапущені та залишені в режимі очікування на 10 хвилин, щоб дозволити будь-які автоматичні оновлення та стабілізувати роботу вузлів.

Для імітації деградацій мережі використовуються затримка та втрата пакетів, оскільки основна увага приділяється VoIP. VoIP є звичайним випадком застосування для віддалених працівників, водночас чутливим до швидкості мережі, коли

використовується через VPN або загалом в мережі Інтернет. Це відрізняє VoIP від, наприклад, перегляду сторінок, оскільки на завантаження сторінок затримка та втрата пакетів впливають значно менше, в той час як потокове передавання VoIP чутливіше до таких деградацій.

Блок-схему, що відображає порядок проведення експерименту, наведено на рисунку (Рисунок 3).

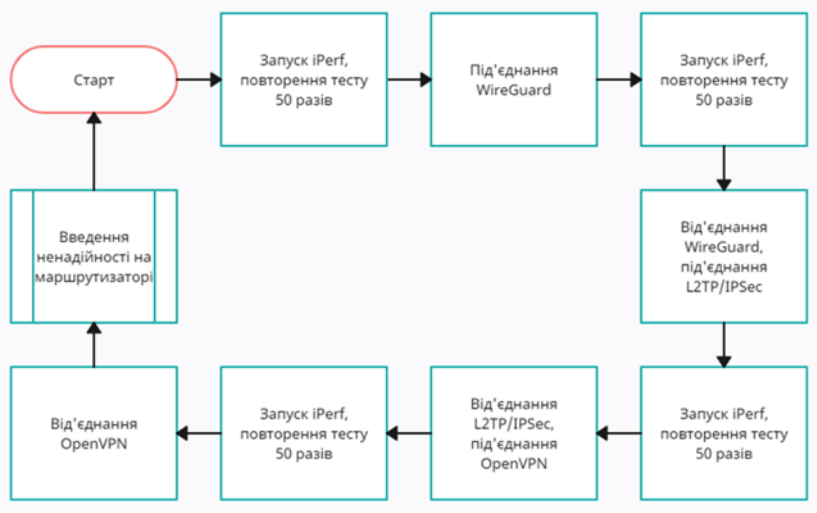

Рис. 3 – Блок-схема експерименту

Далі, були оброблені дані всіх експериментів, зроблені висновки та розроблені рекомендації.

III. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Представлені результати є значеннями, отриманими на момент, коли iPerf надсилає пакети на сервер, а сервер отримує та відображає значення. Усі результати є усередненими значеннями 50 тестів, що проводились для кожного випадку тестування. Як було зазначено у методиці експерименту, тестування проводилось у 36 різних випадках. Наприклад, тестування рішення WireGuard в операційній системі Windows без деградації мережі – це один випадок.

Узагальнені результати тестування пропускної здатності, отримані в усіх 36 випадках, наведені у таблиці (Таблиця 1).

Таблиця 1 - Результати тестування пропускної здатності (Мбіт/с)

Операційні системи	Без VPN	WireGuard	L2TP/IPSec	OpenVPN
	Без деградацій мережі			
Windows	908,5	749,5	309,9	270,7
Ubuntu	924,6	847,9	816,7	366,4
macOS	879,4	599,3	758,3	227,7
	Перша ненадійність – затримка			
Windows	3,9	3,7	0,7	1,2
Ubuntu	51,6	48,9	49,4	4,3
macOS	27,1	5,7	16,1	22,6
	Друга ненадійність – втрата пакетів			
Windows	96,1	91,6	81,9	91,4
Ubuntu	267	171,3	141,8	91,7

macOS	106,2	79,8	63,5	69,8

Далі наведемо більш докладні результати:

Спершу було виміряно базову продуктивність – значення пропускної здатності в стабільній мережі, без під’єднання VPN.

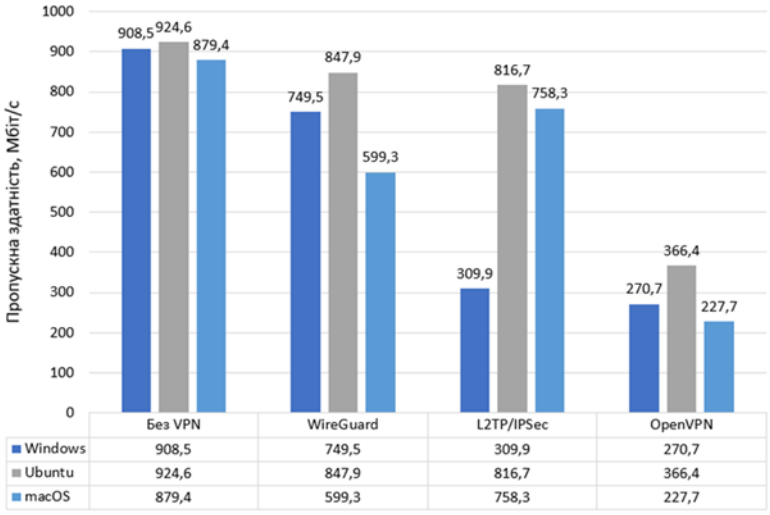

Рис. 3 – Тестування без деградацій мережі

Як і очікувалося, після під’єднання VPN пропускна здатність мережі знижувалась. Крім того, у порівнянні з базовою продуктивністю мережі, спостерігалися декілька очевидних тенденцій.

Найбільшого впливу на продуктивність мережі завдав OpenVPN, знизивши пропускну здатність в середньому на 60% в Ubuntu, на 70% у Windows та на 74% у macOS. OpenVPN виявився найповільнішим в усіх трьох операційних системах, причому майже в усіх випадках тестування пропускна здатність була у кілька разів нижчою у порівнянні з іншими рішеннями. У найгіршому випадку тестування, під час під’єднання OpenVPN у macOS, пропускна здатність впала з 879,4 Мбіт/с у базових тестах до 227,7 Мбіт/с у тестах з VPN.

L2TP/IPSec став найпродуктивнішим рішенням для macOS, разом з ним пропускна здатність знизилась на 14%, і в середньому становила 758,3 Мбіт/с. Найкраще він продемонстрував себе в Ubuntu, знизивши пропускну здатність всього на 12%, проте поступився першістю в цій операційній системі іншому рішенню. Несподівано, найменш продуктивним L2TP/IPSec виявився у Windows, пропускна здатність становила в середньому 309,9 Мбіт/с, що на 66% менше за базову продуктивність.

Найліпшу продуктивність у Windows та Ubuntu продемонстрував WireGuard, з цим рішенням середня пропускна здатність становила 749,5 Мбіт/с та 847,9 Мбіт/с відповідно. У найкращому випадку тестування, під час під’єднання WireGuard в Ubuntu, пропускна здатність знизилась лише на 8%. Найменш ефективним WireGuard виявився для macOS, знизивши пропускну здатність на 32%, в середньому до 599,3 Мбіт/с, та все ж це непоганий результат, особливо в порівнянні з OpenVPN.

Усереднені результати вимірювань пропускної здатності з першою ненадійністю наведені на рисунку (Рисунок 4).

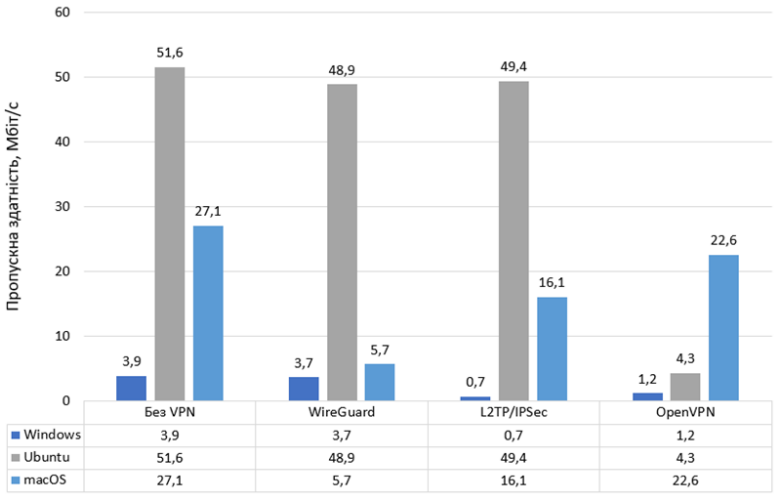

Рис. 4 – Тестування з першою ненадійністю

Після введення затримки істотне зниження пропускної здатності спостерігалося в усіх трьох операційних системах. Найкращі результати у тестах без VPN з цим варіантом ненадійності продемонструвала Ubuntu – в середньому 51,6 Мбіт/с проти 27,1 Мбіт/с у macOS та 3,9 Мбіт/с у Windows. MacOS мала посередні результати як у тестах без VPN, так і у тестах з будь-яким рішенням VPN. Windows мала найгірші результати в усіх випадках тестування.

L2TP/IPSec найліпше впорався із затримкою в Ubuntu, разом з ним середня пропускна здатність була трохи меншою, ніж у тестах без VPN, і становила 49,4 Мбіт/с. У macOS він мав посередні результати, знизивши пропускну здатність на 41%, в середньому до 16,1 Мбіт/с, але інше рішення у цій операційній системі виявилось кращим.

Найпродуктивнішим під час тестування із затримкою у macOS виявився OpenVPN, середня пропускна здатність з цим рішенням знизилась лише на 17%, порівняно з тестами без VPN, і становила 22,6 Мбіт/с. Проте у Windows та Ubuntu результати були невтішні, пропускна здатність разом з OpenVPN знизилась на 69% та 92% відповідно.

WireGuard впорався із затримкою в Ubuntu так само добре, як і L2TP/IPSec. Пропускна здатність становила в середньому 48,9 Мбіт/с, тобто різниця із тестами без VPN становила близько 5%. У macOS пропускна здатність була на 79% нижчою, у порівнянні з тестами без VPN, і становила в середньому 5,7 Мбіт/с, що є найнижчим результатом у цій операційній системі. Зауважу, що WireGuard продемонстрував кращі результати у Windows, ніж OpenVPN та L2TP/IPSec, знизивши пропускну здатність лише на 5%, та попри це вона була дуже низькою.

Далі за допомогою маршрутизатора в експериментальній мережі було усунена перша ненадійність, і додана друга – 1% втрати пакетів. Порядок тестування залишився таким самим, як і у попередньому випадку, спочатку проводились тести без VPN, а потім окремо з кожним рішенням.

Усереднені результати вимірювань пропускної здатності з другою ненадійністю наведені на рисунку (Рисунок 5).

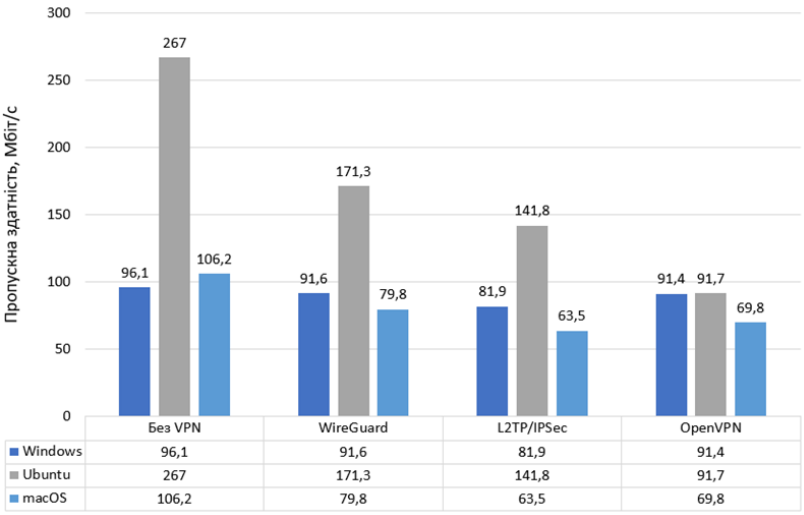

Рис. 5 – Тестування з другою ненадійністю

Після додавання втрати пакетів так само спостерігалося зниження пропускної здатності в усіх трьох операційних системах, щоправда воно було не таким значним, як у випадку із затримкою. У тестах без VPN з цим варіантом ненадійності найкращі результати знову продемонструвала Ubuntu, пропускна здатність становила в середньому 267 Мбіт/с. Для порівняння, результати у macOS та Windows були у кілька разів меншими – 106,2 Мбіт/с та 96,1 Мбіт/с відповідно.

Найліпше з втратою пакетів впорався WireGuard, причому в усіх трьох операційних системах. У Windows пропускна здатність знизилась на несуттєві 5%, в середньому до 91,6 Мбіт/с, хоча справедливо буде відзначити, що у Windows всі три рішення продемонстрували майже однакові результати. У macOS перевага WireGuard була помітнішою, пропускна здатність знизилась на 25%, і становила в середньому 79,8 Мбіт/с, в той час, як з іншими рішеннями відсоток зниження був більшим. В Ubuntu середня пропускна здатність становила 171,3 Мбіт/с, що на 36% менше, у порівнянні з тестами без VPN, і це найкращий результат у цій операційній системі.

OpenVPN, як і WireGuard, непогано впорався з втратою пакетів у Windows, різниця з тестами без VPN не перевищила 5%. Він мав посередні результати в macOS, знизивши пропускну здатність на 34%. В Ubuntu OpenVPN виявився найменш продуктивним, пропускна здатність становила в середньому 91,7 Мбіт/с, у порівнянні з тестами без VPN це на 66% менше.

L2TP/IPSec продемонстрував найнижчі результати у Windows та macOS, знизивши пропускну здатність в середньому до 81,9 Мбіт/с та 63,5 Мбіт/с відповідно. Для Windows різниця з тестами без VPN склала 15%, для macOS – близько 40%. В Ubuntu результати були посередніми, пропускна здатність знизилась на 47%, але загалом різниця з іншими рішеннями була невелика.

IV. ВИСНОВКИ

На основі результатів проведеного дослідження були обґрунтовані рекомендації з вибору найліпшого з погляду продуктивності протоколу VPN для забезпечення віддаленого доступу з різних операційних систем, за різних умов надійності мережевого з’єднання.

Якщо сервіс VPN розгортається у надійному мережевому з’єднанні в середовищі Windows, відповідно до результатів цього дослідження, рекомендовано використовувати WireGuard.

Якщо це середовище на базі Linux (наприклад, Ubuntu), з надійним мережевим з’єднання рекомендовано використовувати WireGuard або L2TP/IPSec. Обидва рішення є ефективними на Linux, для найкращих результатів рекомендується WireGuard.

Якщо середовище складається переважно з пристроїв під керуванням macOS, за умов надійного мережевого з’єднання рекомендовано використовувати L2TP/IPSec.

Якщо розгортати VPN у ненадійному мережевому з’єднанні, де очікується затримка, у середовищі Windows, рекомендовано використовувати WireGuard.

Якщо середовище базується на Linux, з ненадійним мережевим з’єднанням, схильним до затримки, рекомендовано використовувати L2TP/IPSec або WireGuard. Ці два рішення у цьому дослідженні майже однаково ефективно впорались із затримкою на Linux, для найкращих результатів рекомендується L2TP/IPSec.

Якщо середовище працює під керуванням macOS, а мережеве з’єднання так само ненадійне і схильне до затримки, рекомендовано використовувати OpenVPN або L2TP/IPSec. Для найкращих результатів рекомендується OpenVPN, оскільки він дещо краще впорався із затримкою на macOS у цьому дослідженні.

Якщо розгортання VPN виконується у ненадійному мережевому з’єднанні, де очікується втрата пакетів, у всіх трьох середовищах рекомендовано використовувати WireGuard для найкращих результатів.

Якщо це середовище Windows, OpenVPN буде так само ефективним, як і WireGuard, тому він також рекомендований до використання.

V. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У майбутніх дослідженнях доцільно було б протестувати рішення VPN на іншому апаратному забезпеченні для сервера, маршрутизатора та клієнтів, виміряти та порівняти використання обчислювальних ресурсів під час виконання тестів, розмістити VPN-сервер на іншій операційній системі, наприклад, Windows Server.

У тестах з ненадійностями мережі можна використовувати різні значення керованих метрик, таких як затримка та втрата пакетів. Так, наприклад, можна протестувати, як рішення VPN впораються з меншою або більшою затримкою, або з вищим відсотком втрати пакетів, якщо налаштувати експериментальну установку таким чином, щоб не розривати з’єднання при підвищених втратах.

Крім того, в тестах можна використовувати не тільки інші метрики, але й інші інструменти вимірювання, а потім порівняти отримані результаті з результатами тестів iPerf.

Надалі важливо протестувати рішення VPN з різними конфігураціями. У цьому дослідженні використовувались конфігурації за замовчуванням, але якщо застосувати інші налаштування для шифрування та решти параметрів, результати будуть відрізнятись. Було б корисно протестувати рішення VPN з уніфікованим набором криптографічних алгоритмів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] C. Scott, P. Wolfe and M. Erwin.*Virtual Private Networks.* O'Reilly, 1999.

[2] S. Brown. *Implementing Virtual Private Networks*McGraw.Hill, 1999.

[3] Network Performance Analysis of VPN Protocols: An Empirical Comparison on Different Operating Systems. [Online]. Available: www. URL: https://ieeexplore.ieee.org/document/4908347. Accessed on: 22.10.2022

[4] An Empirical Analysis of the Commercial VPN Ecosystem. [Online]. Available: www. URL: https://dl.acm.org/doi/pdf/10.1145/3278532.3278570. Accessed on: 22.10.2023

[5] Comparison of VPN Protocols at Network Layer Focusing on WireGuard Protocol. [Online]. Available: www. URL: https://www.researchgate.net/publication/345681297_Paper-Comparison_of_VPN-Protocols_at_Network_Layer_Focusing_on_Wire_Guard_Protocol_Comparison_of_VPN_Protocols_at_Network_Layer_Focusing_on_Wire_Guard_Protocol. Accessed on: 22.11.2022

[6] Performance Comparison of VPN Solutions. [Online]. Available: www. URL: https://core.ac.uk/download/pdf/322886318.pdf . Accessed on: 22.10.2022

[7] Improving VPN performance over multiple access links. [Online]. Available: www. URL: https://ieeexplore.ieee.org/document/4769158 . Accessed on: 22.10.2022

[8] A small network for modeling MPLS [Online]. Available: www. URL: https://ieeexplore.ieee.org/document/7506760. Accessed on: 22.10.2022
[9] Introduction – pfSense Documentation [Online]. Available: www. URL: https://docs.netgate.com/pfsense/en/latest/general/index.html. Accessed on: 14.10.2022

[10] Understanding Delay in Packet Voice Networks [Online]. Available: www. URL: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html. Accessed on: 09.10.2022

[11] Influence of packet loss on a speaker verification system over IP network [Online]. Available: www. URL: https://ieeexplore.ieee.org/document/7477365 Accessed on: 22.10.2022

Отримано 07.10.2022 р.

METHODOLOGY OF VPN PROTOCOLS CHOOSING FOR REMOTE ACCESS IN CORPORATE NETWORKS

Mykyta Kapustin,
lead computer systems engineer, Fozzy Group,
Zaporizhzhia, Ukraine

Abstract — The purpose of the work was to analyze and compare the performance of modern solutions of virtual private networks in conditions of stable and unreliable network connection, as well as to develop recommendations for choosing the best solution for organizing remote access in corporate networks.
For this, the problems of choosing a virtual private network protocol were investigated; a defined list of protocols for comparative analysis; defined metrics and tools for measuring performance; experimental performance studies were conducted, which allowed to compare the performance of different solutions, in different environments and application conditions, and to justify recommendations for choosing the best protocol.

***Keywords*—** IPERF, IPSEC, L2TP, OPENVPN, VPN, WIREGUARD, REMOTE ACCESS, RELIABILITY, PRODUCTIVITY, PROTOCOL**.**

Received 07.10.2022