УДК 004.738

В. В. Шульга, Д. С. Комін, О. В. Першин

ЕКСПЕРИМЕНТАЛЬНА МЕТОДИКА ОЦІНЮВАННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ SITE-TO-SITE VPN-КАНАЛІВ ЗА УМОВ МЕРЕЖЕВИХ ЗАТРИМОК І БАГАТОПОТОКОВОГО TCP-НАВАНТАЖЕННЯ

Анотація. *Розглянуто проблему оцінювання фактичної пропускної спроможності захищених каналів Site-to-Site VPN за умов мережевих затримок і паралельного передавання даних. На основі попередніх досліджень впливу затримок на VPN-протоколи та багатопотоковість TCP обґрунтовано експериментальну методику, що передбачає порівняння каналу без VPN і захищених тунелів за однакових умов. Запропоновано план експериментів із використанням реальних маршрутизаторів, Linux-вузла для емуляції мережевого середовища та iPerf3 для вимірювання пропускної спроможності. Визначено основні фактори експерименту, контрольовані параметри та підхід до оцінювання похибки прогнозної моделі. Очікуваним результатом є методика, придатна для експериментальної перевірки й подальшого застосування під час планування пропускної спроможності захищених інформаційних напрямків.*

Ключові слова: *Site-to-Site VPN, пропускна спроможність, TCP, затримка, багатопотоковість.*

Abstract. *The paper addresses the assessment of effective throughput in Site-to-Site VPN tunnels under network delay and concurrent TCP traffic. Building on prior studies of VPN performance under delay and TCP parallelism, an experimental methodology is proposed to compare unprotected links and VPN tunnels under equivalent conditions. The testbed combines physical routers, a Linux node for controlled network emulation, and iPerf3 for throughput measurements. The experimental factors, control parameters, and an approach to evaluating prediction error are defined. The expected outcome is a methodology suitable for empirical validation and subsequent use when planning the capacity of protected information links.*

Keywords: *Site-to-Site VPN, throughput, TCP, latency, parallel streams.*

Актуальність дослідження зумовлена тим, що номінальна швидкість фізичного каналу не відображає повною мірою обсяг корисних даних, який може бути переданий через захищене з'єднання. На фактичний результат впливають затримка та втрати пакетів у мережевому середовищі, механізми керування перевантаженням TCP, службові витрати інкапсуляції й криптографічної обробки, а також обчислювальні можливості маршрутизатора. Тому використання лише паспортної швидкості інтерфейсу може призводити до неточного планування пропускної спроможності інформаційного напрямку.

У дослідженні Site-to-Site VPN [1] порівнювалися протоколи SSTP, L2TP/IPsec, OpenVPN і WireGuard за умов різних затримок та використання маршрутизаторів із різними технічними характеристиками. В іншій роботі [2] встановлено залежність пропускної спроможності TCP від мережевої затримки та кількості паралельних потоків, а також запропоновано коефіцієнт зниження пропускної спроможності. Водночас результати, одержані для каналу без VPN, не можна без додаткової перевірки безпосередньо застосувати до захищеного тунелю. Це обґрунтовує необхідність дослідження спільного впливу мережевих і апаратно-програмних чинників.

Мета роботи – розробити експериментальну методику оцінювання пропускної спроможності Site-to-Site VPN-каналів залежно від затримки, кількості паралельних TCP-потоків, типу VPN-протоколу та продуктивності мережевого обладнання, а також визначити підхід до перевірки точності моделі, побудованої за результатами вимірювань.

Для проведення дослідження пропонується стенд із двох кінцевих комп'ютерів, двох VPN-шлюзів і проміжного вузла на базі Linux. На кінцевих комп'ютерах запускається iPerf3 у режимах клієнта й сервера, а Linux-вузол використовується для контрольованої емуляції мережевих умов засобом tc netem. Затримка вноситься на визначеному інтерфейсі; за потреби окремо задаються втрати пакетів. До початку вимірювань необхідно перевірити маршрутизацію, підтвердити

проходження тестового трафіку саме через VPN-тунель і зафіксувати номінальну швидкість фізичних інтерфейсів.

Експеримент доцільно проводити у кілька етапів. Спочатку вимірюється контрольний канал без VPN. Надалі за аналогічних умов досліджуються тунелі WireGuard, L2TP/IPsec, OpenVPN і SSTP. Для початкової серії пропонується використати затримки 0, 10, 20, 30, 50, 100 і 200 мс та кількість паралельних TCP-потоків 1, 2, 4, 8 і 15. Також передбачається перевірка щонайменше двох апаратних конфігурацій маршрутизаторів, що дасть змогу оцінити вплив продуктивності обладнання. Остаточну матрицю дослідів слід уточнити з урахуванням доступних пристроїв і часу, потрібного для повторних вимірювань.

У кожній комбінації факторів потрібно реєструвати сумарну пропускну спроможність TCP, фактичну затримку, втрати пакетів та завантаження центрального процесора VPN-шлюзу. Кожний режим варто повторювати не менше трьох разів із фіксованою тривалістю тесту. Порядок тестування різних конфігурацій доцільно змінювати, а перед запуском кожного нового досліду перевіряти, що фонова передача даних відсутня або контрольовано врахована. RTT слід фіксувати окремо від штучно внесеної односторонньої чи двосторонньої затримки.

Для порівняння результатів пропонується визначати коефіцієнт збереження пропускної спроможності під час використання VPN:

$$K_{VPN}(d, N, P, H) = G_{VPN}(d, N, P, H) / G_0(d, N, H)$$

Тут G_{VPN} – виміряна пропускна спроможність каналу з VPN; G_0 – пропускна спроможність того самого каналу без VPN; d – затримка в мережі; N – кількість паралельних TCP-потоків; P – тип VPN-протоколу; H – конфігурація апаратного обладнання. Вимірювання чисельника й знаменника мають виконуватися за однакових умов затримки, кількості потоків і конфігурації обладнання. Такий коефіцієнт дасть змогу відокремити втрати продуктивності, пов’язані з використанням VPN, від деградації, спричиненої самим мережевим середовищем.

За експериментальними даними передбачається побудувати модель оцінювання пропускної спроможності як функції затримки, числа TCP-потоків, типу VPN і характеристик маршрутизатора. При цьому необхідно перевірити не лише вплив кожного чинника окремо, а й наявність взаємодій між ними. Зокрема, додавання TCP-потоків може по-різному впливати на сумарну швидкість різних VPN-протоколів залежно від затримки й завантаження процесора.

Для забезпечення відтворюваності експерименту необхідно зафіксувати версії операційної системи, RouterOS, iPerf3 та параметри VPN-конфігурації. Упродовж основної серії слід підтримувати незмінними MTU, налаштування мережевих інтерфейсів, параметри TCP та тривалість тесту; усі відмінності конфігурацій потрібно реєструвати. Доцільно виконувати вимірювання в обох напрямках передавання, оскільки навантаження на VPN-шлюзи та характеристики мережевого маршруту можуть бути несиметричними. Перед кожною серією необхідно перевірити базову швидкість каналу й відсутність неконтрольованого фонового трафіку.

Під час обробки даних для кожної комбінації факторів слід обчислювати середнє значення, стандартне відхилення та довірчий інтервал. Значення, що суттєво відхиляються від інших вимірювань, не слід автоматично вилучати: спочатку потрібно перевірити журнали тесту, стан інтерфейсів і навантаження процесора. Для зіставлення різних пристроїв важливо порівнювати не тільки абсолютну швидкість, а й частку використання доступної смуги та завантаження CPU. Це допоможе визначити режими, у яких подальше збільшення кількості TCP-потоків уже не забезпечує істотного приросту продуктивності.

Для перевірки точності моделі частину експериментальних спостережень слід використати для її побудови, а іншу частину – для незалежної перевірки. Якість прогнозування можна оцінювати за середньою абсолютною похибкою, середньою абсолютною відносною похибкою та середньоквадратичною похибкою. Окремі UDP-тести з контрольованою інтенсивністю передавання та втратами пакетів можуть доповнити дослідження показниками втрат і джитера, однак результати UDP слід аналізувати окремо від TCP-пропускної спроможності.

Побудову моделі доцільно виконувати поетапно: спочатку оцінити базові залежності, а потім додати фактори, взаємодію яких підтверджено даними. До незалежної вибірки слід включати не лише повторні вимірювання відомих режимів, а й комбінації параметрів, які не

використовувалися для налаштування моделі. Якщо показники різних пристроїв суттєво відрізняються, апаратну конфігурацію потрібно враховувати як окремий фактор або будувати окремі моделі. Прогнозування за межами дослідженого діапазону затримок і кількості потоків слід позначати як неперевірене.

Очікуваним результатом є експериментально обґрунтована методика вимірювання й прогнозування пропускної спроможності захищених VPN-каналів за змінних мережевих умов. Її практичне застосування полягає в удосконаленні розрахунків потрібної пропускної спроможності інформаційних напрямків під час проєктування інформаційно-комунікаційних систем. До завершення вимірювань запропонована модель має розглядатися як гіпотеза, що потребує емпіричної перевірки; числові висновки про перевагу конкретного протоколу можна робити лише на підставі отриманих даних.

Список використаних джерел:

1. Комін Д. С., Шульга В. В., Лєбєдєв В. О., Коцюба В. П. Дослідження ефективності функціонування Site-to-Site VPN в умовах затримок в електронних комунікаційних мережах. *Системи обробки інформації*. 2024. № 1 (176). С. 52–62. https://doi.org/10.30748/soi.2024.176.07.
2. Комін Д., Шульга В., Хажанець Ю., Кириченко Д. Удосконалений метод розрахунку пропускної спроможності інформаційних напрямків з урахуванням затримок в мережі та багатопотоковості при обміні даними. *Системи обробки інформації*. 2026. № 3(186). С. 64–73. https://doi.org/10.30748/soi.2026.186.07.

Шульга Владислав Васильович *– старший викладач Харківського національного університету Повітряних Сил ім. І. Кожедуба, м. Харків, e-mail: v.shulha@m.hnups.mil.gov.ua, ORCID: https://orcid.org/0009-0008-8981-3214.*

Комін Дмитро Сергійович *– кандидат технічних наук, провідний науковий співробітник Харківського національного університету Повітряних Сил ім. І. Кожедуба, м. Харків, e-mail: d.komin@ps.mil.gov.ua, ORCID: https://orcid.org/0000-0003-4439-346X.*

Першин Олександр Васильович – *старший викладач Харківського національного університету Повітряних Сил ім. І. Кожедуба, м. Харків, e-mail: o.pershyn@m.hnups.mil.gov.ua, ORCID: https://orcid.org/0000-0003-0022-8972.*

Vladyslav Shulha *– Senior Lecturer at Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: v.shulha@m.hnups.mil.gov.ua, ORCID: https://orcid.org/0009-0008-8981-3214.*

Dmytro Komin *– PhD in Engineering, Leading Researcher at Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: d.komin@ps.mil.gov.ua, ORCID: https://orcid.org/0000-0003-4439-346X.*

Oleksandr Pershyn *– Senior Lecturer at Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: o.pershyn@m.hnups.mil.gov.ua, ORCID: https://orcid.org/0000-0003-0022-8972.*