УДК 621.396:004.056.5

# ДОСЛІДЖЕННЯ ЗАХИСТУ VPN З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ KILL SWITCH

Юркевич М.О.
Науковий керівник – к.т.н., ст. викл. Марчук А.В
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
e-mail: maksym.iurkevych@nure.ua

This research investigates the effectiveness and implications of VPN protection augmented by Kill Switch technology, exploring its capacity to fortify digital privacy, prevent data exposure, and bolster overall cybersecurity in an increasingly interconnected digital landscape.

Технологія віртуальних приватних мереж VPN створює захищений від зовнішних впливів тунель для передачі інформації [1]. Збільшується рівень безпеки та конфіденційності. Інтернет-трафік спрямовується через віддалений сервер. Це маскує IP-адресу користувача та його місцезнаходження, що ускладнює відстеження його активності в Інтернеті для інтернет-провайдера або інших осіб. Як правило трафік, що передається шифрується, однак іноді деякі провайдери VPN іноді цим нехтують. VPN технологія особливо корисна для обходу географічних обмежень, захисту даних від прослуховування в незахищених мережах, покращення конфіденційності.

Одним з недоліків технології VPN є залежність від стабільності інтернет-з'єднання. Низький рівень сигналу, пропадання сигналу, не якісне конфігурування маршрутизаторів або брандмауерів, атаки на канал, що призводять до втрати зв’язку.

Для вирішення цієї проблеми в багатьох VPN вбудовуються програми вимикачі Kill Switch [2].

Якщо VPN-з'єднання несподівано розривається, Kill Switch негайно відключає інтернет-з'єднання. Це дуже важливо, тому що розрив VPN-з'єднання без "вимикача" може розкрити справжню IP-адресу користувача та активність в Інтернеті, що зводить нанівець сенс використання VPN. Цей додатковий рівень захисту гарантує, що навіть якщо основне VPN-з'єднання на мить обірветься, конфіденційні дані залишаться захищеними.

Однак важливо враховувати обмеження використання інтегрованого VPN з Kill Switch:

- потенційний вплив на продуктивність. Шифрування і маршрутизація через віддалений сервер можуть сповільнити швидкість інтернет-з'єднання;
- не є надійним рішенням, тому що, як правило, Kill Switch є частиною VPN, що надаються як комплексне рішення окремими провайдерами.

Надавачі послуг іноді можуть використовувати своє програмне забезпечення для вбудовування реклами, збору інформації про користувачів і інформації, що передається.

Тому актуальною є задача усунення існуючих недоліків системи VPN з Kill Switch.

Використовується два типи Kill Switch: вимикач на системному рівні і на рівні додатків.

Аварійний вимикач на системному рівні блокує всі вхідні та вихідні з'єднання для всієї системи, гарантуючи, що жодна програма або процес не зможе вийти в Інтернет.

Аварійний вимикач на рівні додатків працює так само, але тільки з додатками, які вибирає користувач у меню «Налаштування». Якщо VPN-з'єднання обривається, всі вхідні та вихідні з'єднання відключаються тільки для цих додатків, у той час як всі інші програми, як і раніше, можуть без проблем виходити в Інтернет.

Пропонується відокремити Kill Switch від інтегрованого VPN і зменшити залежність від надавача послуг. Для вирішення цієї задачі можно побудувати вимикач Kill Switch на основі відомої технології iptables [3]. Iptables є функцією ядра і не залежить від служби VPN.

Основні вимоги до впровадження цього рішення: машина з Linux з правами root і встановленим iptables.

Був проведений пошук можливих програмних рішень iptables в якості вимикача Kill Switch. Для перевірки працездатності рішення по використанню вимикача на базі iptables були проведені експериментальні дослідження таких програм. Було дві групи досліджень: для безпроводового і проводового доступу в Інтернет. Отримані результати показали на можливість використання вимикача Kill Switch при спеціальному налаштуванні iptables.

Список використаних джерел

1. If you're using a VPN without a kill switch, you're putting your privacy at risk. CNET. URL: https://www.cnet.com/tech/services-and-software/vpn-kill-switch-what-is-it-and-should-you-enable-it/ (дата звернення: 27.02.2024).

2. VPN kill switch – protected at all times. NordVPN. URL: https://nordvpn.com/features/vpn-kill-switch/ (дата звернення: 01.03.2024).

3. How To Create A VPN Killswitch Using Iptables on Linux. URL: https://linuxconfig.org/how-to-create-a-vpn-killswitch-using-iptables-on-linux (дата звернення: 01.03.2024).