Міністерство освіти і науки України
Чорноморський національний університет
імені Петра Могили

НАУКОВІ ПРАЦІ

Видається з грудня 2001 року
Періодичність – двічі на рік

Науковий журнал

Т. 307. Вип. 295
Серія «Комп'ютерні технології»

Миколаїв
Вид-во ЧНУ імені Петра Могили
2017

ЗМІСТ

УДК 004.056.5

Ситніков В. С.,
професор,
e-mail: *sitnvs@gmail.com*
Ніконенко О. В.,
магістрант,
e-mail: *steam1994@gmail.com*
Одеський національній політехнічний університет, м.Одеса, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАПОБІГАННЯ РОЗКРИТТЯ IP-АДРЕСИ ПРИ АКТИВНОМУ VPN-З'ЄДНАННІ

Для захищеної роботи в мережі інтернет можна застосовувати різні типи підключення. Одним з типів таких підключень є VPN-з'єднання. Воно дозволяє тунелювати весь вхідний/вихідний трафік, шифрувати його. Але в моменти відключення або втрати VPN-з'єднання може статися витік реальної IP-адреси користувача. Це дозволить ідентифікувати користувача і перехопити його дані. Відомі методи захисту не дозволяють вирішити цю проблему. В роботі розглянуто основні методи запобігання розкриття реальної IP-адреси при використанні активного з'єднання у VPN мережі, проведено аналіз та запропоновано методи запобігання витоків у різних операційних системах, відтворено метод захисту на прикладі операційної системи macOS 10.13. В результаті реалізації методу отримали можливість VPN-з'єднання, яке має більш високий ступінь захищеності.

Ключові слова: *VPN (Virtual Private Network – віртуальна приватна мережа); операційна система; таблиці адрес; методи запобігання розкриття IP-адреси; захист з'єднання; розрив з'єднання; фільтр пакетів.*

Вступ

В наш час інтернет поширюється на всі сфери нашого життя, але користування ним досі має певні ризики. Багато інтернет-користувачів вже помітили потенційні ризики розкриття даних інтернет-провайдерами, державними установами або кібер-злочинцями. Для збереження своєї конфіденційності та безпеки в мережі існують VPN сервіси.

VPN (скорочення від англ. Virtual Private Network – віртуальна приватна мережа) – загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу інтернет [1].

Нажаль, навіть найстабільніше і найнадійніше VPN-з'єднання може іноді перериватися. Коли це відбувається, користувач за замовчуванням встановлює з'єднання з інтернетом через звичайне підключення, що надається його інтернет-провайдером, внаслідок цього реальна IP-адреса та географічне положення користувача може бути розкрито. Така ситуація може бути особливо ризикованою для політичних активістів, журналістів і блогерів, які живуть і працюють в країнах з авторитарними режимами і високим рівнем стеження і цензури в інтернеті. У таких випадках їх можна легко ідентифікувати і відстежувати, при цьому вони навіть не будуть знати, що VPN-з'єднання було перервано.

Безпека та конфіденційність при використанні VPN-з'єднання є вкрай важливою проблемою.

Аналіз останніх досліджень і публікацій.

Проблеми безпеки віртуальних приватних мереж розглядають у своїх дослідженнях І. І. Пархоменко, В. В. Галкін [2], К. В. Мілян, Ю. І. Грицюк [3], О. О. Квачук [4], T. Berger [13], Jung-Tae Kim [14]. А саме розгляд, визначення і обґрунтування переваг впровадження і використання технологій VPN в корпоративних мережах. Дослідження використання VPN-технологій та процесу захисту інформації переданої в рамках розподіленої корпоративної мережі, яка використовує мережі відкритого доступу, з використанням технології VPN-з'єднань.

Постановка завдання

Метою статті є розгляд методів запобігання розкриття IP-адреси за умови використання активного

з'єднання у VPN-мережі. Розгляд можливих методів реалізації захисту та поліпшення безпеки VPN-з'єднання у операційних системах Android, Windows. macOS, iOS, Linux. Пропозиція щодо конкретної реалізації захисту на прикладі операційної системи macOS.

1. Аналітичний розгляд методів реалізації захисту у ОС Android, Windows, iOS, Linux

На **iOS** всі реалізації запобігання розкриття IP-адреси зводяться до функції Always On VPN (Завжди увімкнений VPN) – якщо VPN не підключено, але пристрій запрошує доступ до мережі інтернет, автоматично встановлюється з'єднання VPN. Реалізувати захист іншими способами неможливо через обмеження системи [12].

На **Windows** для реалізації захисту можна використовувати Windows Firewall, який доступний на Windows Vista та вище. Для роботи з фаєрволом потрібно використовувати WinAPI [5]. Принцип реалізації: додавання спеціального правила в фаєрвол, який перериває усі з'єднання не через VPN. В версії 10, існує проблема розкриття IP-адреси через DNS [6].

На **Linux** ми маємо можливість заборонити весь доступ до мережі всім додаткам з двома винятками: дозволити доступ через мережевий інтерфейс VPN; дозволити процесу OpenVPN доступ в інтернет безпосередньо, щоб той міг встановити VPN-підключення. Зробити це можна за допомогою iptables [7].

У системі **Android** захист від розкриття IP-адреси доступний тільки починаючи з Android 8 в системних налаштуваннях під назвою «Always-ON VPN» (Завжди увімкнений VPN). Також можлива реалізація як в ОС Linux, але для цього потрібно мати root привілеї в пристрої, а це загрожує вразливістю безпеки [11].

2. Загальне рішення

Розглянувши можливі рішення, приведемо їх до одного універсального методу запобігання розкриття IP-адреси.

Увесь трафік прилада користувача потрібно передавати в інтернет через VPN-сервер, а інший вихідний трафік заборонити – це зображено на рисунку 1. Дозволити отримання конфігураційних файлів для VPN – клієнта, для можливості його підключення до VPN сервера. Потрібно знати його IP-адресу та параметри для авторизації.

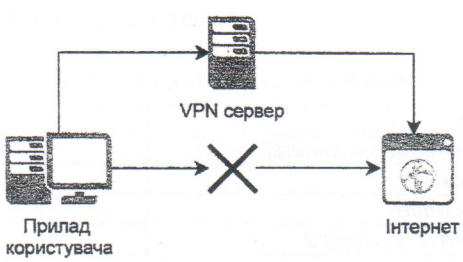

Рис 1. Загальне рішення

Реалізувавши або використовуючи системний фільтр пакетів з'явиться можливість відокремити увесь інтернет-трафік, та переправити його до VPN серверу. Ідея нового методу полягає у тому, що через мережу інтернет прилад користувача буде мати доступ тільки до отримання конфігурації. При умові, якщо активне VPN-з'єднання обірветься, інтернет-трафік буде зупинено до моменту відновлення. При активному VPN-з'єднанні у прилада буде доступ до усієї інтернет-мережі. Можливі шляхи для інтернет трафіку при використанні такого методу захисту зображено на рисунку 2.

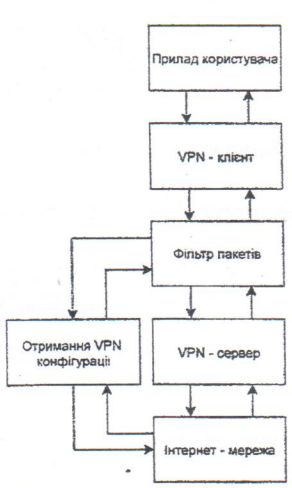

Рис 2. Шляхи для інтернет трафіку.

3. Реалізація методу захисту від розкриття IP-адреси на прикладі системи macOS

На основі загального рішення реалізуємо захист від відкриття IP-адреси в операційній системі macOS.

В операційній системі macOS заради безпеки програми повинні працювати у App Sandbox (з англ. пісочниця) – це технологія керування доступом, що входить у macOS, яка застосовується на рівні ядра. Вона призначена для захисту системи та даних користувача, якщо програма стає скомпрометованою. Додатки, що розповсюджуються через Mac App Store, повинні працювати у пісочниці. Додатки, підписані та розповсюджені за межами магазину Mac App Store з ідентифікатором розробника, можуть (і в більшості випадків повинні) також використовувати пісочницю [8]. У порівнянні з іншими системами це накладає певні обмеження в привілеях програми.

Ми маємо можливість використовувати системний механізм Packet Filter (пакетний фільтр) – це система OpenBSD для фільтрації трафіку TCP/IP та перекладу мережевих адрес. Він за допомогою конфігураційного файла буде блокувати доступ до мережі інтернет, у випадку якщо VPN з'єднання розірвано, та пропускати пакети тільки через VPN з'єднання. Для цього для програми потрібні привілеї root користувача [9].

Для отримання цих привілей визначимо привілейовані операції поза програмою та будемо передавати команди в привілейований допоміжний інструмент, який запускається сервісом launchd. Він використовує сучасні технології, а саме: SMJobBless, представлений в 10.6, і NSXPCConnection, представлений в 10.8 – допоможе радикально скоротити код, необхідний для підтримки привілейованих допоміжних інструментів, у порівнянні з старшими зразками [10].

У зв'язку з цим розробимо архітектуру рішення для захисту. VPNAntiIPLeakController – клас, який буде давати запит на встановку сервісу у систему, включати/виключати захист, перевіряти статус. VPNAntiIPLeakConfigGenerator – буде генерувати конфігурацію для фільтра пакетів, у шаблоні заміст {IP_LIST} встановлюємо IP – адреси VPN серверів, DNS серверів, у випадку якщо адреси VPN серверів представлені доменним ім'ям, а не IP-адресою. HelperTool – допоміжний XPC сервіс для зв'язку основної програми з сервісом та його встановлення. VPNService – сервіс який буде виконувати команди від основної програми які наведено у таблиці 1. На рисунку 2 зображена UML діаграма запропонованого рішення.

Таблиця 1

Команди для фільтру пакетів

Команди	Опис
/sbin/pfctl -f 'configPath'	Встановити вказаний конфігураційний файл
/sbin/pfctl –d	Вимкнути захист
/sbin/pfctl –e	Ввімкнути захист
/sbin/pfctl -si	Отримати поточний статус захисту

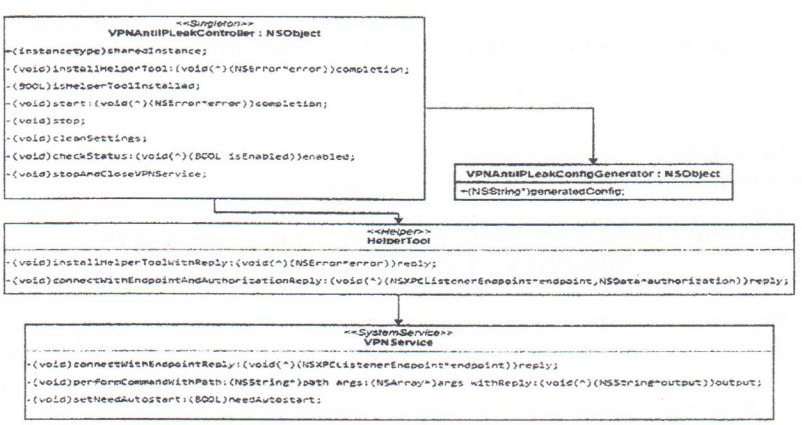

Рис 3. UML діаграма запропонованого рішення

Напишемо файл конфігурації для фільтру пакетів. Його структуру зображено на рисунку 3.

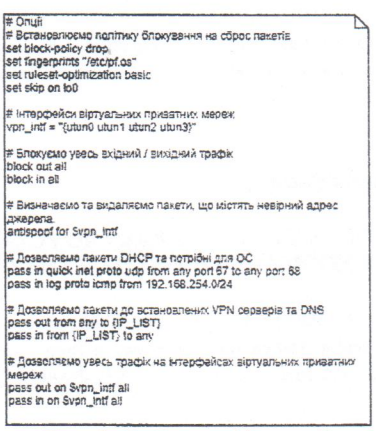

Рис 4. Файл конфігурації

Висновки

В результаті реалізації запропонованого методу захисту отримано безпечне від розкриття IP-адреси VPN-з'єднання, котре при перериванні блокує увесь інтернет трафік, до того моменту, коли з'єднання не відновиться.

В роботі розглянуто основні методи запобігання розкриття реальної IP-адреси під час використання активного з'єднання у VPN мережі, запропоновано та розроблено метод запобігання розкриття на прикладі ОС macOS. Перевага цього методу полягає в неможливості розкриття IP адреси, тому що інтернет трафік буде блокуватися, якщо він проходить не через VPN сервер. Недолік цього методу полягає в можливому збільшенні часу з'єднання і в можливості реалізації тільки в конкретній операційній системі.

Список використаних джерел

1. Компьютерные сети / Э. Таненбаум. – 5-е изд. – М. : Питер, 2012. – 992 с. : ил. – (Классика computer science).
2. Способи захисту каналів корпоративних мереж на базі VPN-рішень, І. І. Пархоменко, В. В. Галкін / Сучасний захист інформації – № 4, – 2016 [Електронний документ], Режим доступу : http://journals.dut.edu.ua/index.php/dataprotect/ article/viewFile/1245/1180
3. Особливості організації інформаційної безпеки корпоративної мережі промислової компанії, К. В. Мілян, Ю. І. Грищук / Науковий вісник НЛТУ України. – 2013. – Вип. 23.4 [Електронний документ]. – Режим доступу : http://nltu.edu.ua/ nv/Archive/ 2013/23_4/314_Mil.pdf
4. Переваги застосування технологій VPN в корпоративних мережах, І. І. Пархоменко, О. О. Квачук / Національний авіаційний університет України [Електронний документ], Режим доступу : http://avia.nau.edu.ua/doc/2011/2/ avia2011_2_22.pdf
5. Exercising the Firewall using C++ [Електронний ресурс], Режим доступу : https://msdn.microsoft.com/en-us/library/aa364726 (v=VS.85).aspx
6. Избавляемся от DNS Leak в Windows 10 [Електронний ресурс], Режим доступу : https://habrahabr.ru/post/268173/
7. Kill switch для OpenVPN на основе iptables [Електронний ресурс], Режим доступу : https://habrahabr.ru/post/274445/
8. About App Sandbox [Електронний ресурс], Режим доступу : https://developer.apple.com/library/content/documentation/ Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html
9. PF on Mac OSX [Електронний ресурс], Режим доступу : https://pleiades.ucsc.edu/hyades/PF_on_Mac_OS_X
10. EvenBetterAuthorizationSample. [Електронний ресурс], Режим доступу : https://developer.apple.com/library/content/samplecode/EvenBetterAuthorizationSample/Introduction/Intro.html#//apple_ref/doc/uid/DTS40013768-Intro-DontLinkElement ID_2
11. What's new in Android 8.0 [Електронний ресурс], Режим доступу : https://developer.android.com/work/versions/Android-8.0.html#behavior-changes
12. iOS Deployment Reference.Always-On-VPN [Електронний ресурс], Режим доступу : https://help.apple.com/deployment/ios/#/ iore8b083096
13. Analysis of current VPN technologies. T. Berger/ Availability, Reliability and Security. ARES. The First International Conference / ISBN : 0–7695–2567–9
14. Security issues in peer-to-peer systems. Jung-Tae Kim / Advanced Communication Technology, ICACT. The 7th International Conference.

О. В. Никоненко, В. С. Ситников,
Одесский национальный политехнический университет, г. Одесса, Украина

ИССЛЕДОВАНИЕ МЕТОДОВ ПРЕДОТВРАЩЕНИЯ РАСКРЫТИЯ IP-АДРЕСА ПРИ АКТИВНОМ VPN-СОЕДИНЕНИИ

Для защищенной работы в сети интернет можно применять различные типы подключения. Одним из типов таких подключений является VPN-соединение. Оно позволяет туннелировать весь входной / исходящий трафик, шифровать его. Но в моменты отключения или потери VPN-соединения может произойти утечка реального IP-адреса пользователя. Это позволит идентифицировать пользователя и перехватить его данные. Известные методы защиты не позволяют решить эту проблему. В работе рассмотрены основные методы предотвращения раскрытия реального IP-адреса при использовании активного соединения в VPN сети, проведен анализ и предложены методы предотвращения утечек в различных операционных системах, воспроизведен метод защиты на примере операционной системы

macOS 10.13. В результате реализации метода получили возможность установить VPN соединение, которое имеет более высокую степень защищенности.

Ключевые слова: *VPN (Virtual Private Network – виртуальная частная сеть); операционная система, таблицы адресов; методы предотвращения раскрытия IP-адреса; защиту соединения; разрыв соединения; фильтр пакетов.*

O. V. Nikonenko, V. S. Sytnikov,
Odessa National Polytechnic University, Odessa, Ukraine

INVESTIGATION OF METHODS OF PREVENTING THE DISCLOSURE OF AN IP-ADDRESS WITHAN ACTIVE VPN-CONNECTION

For secure operation on the Internet, you can use different types of connection. One type of such connections is VPN connections. It allows you to tunnel all incoming/outgoing traffic, encrypt it. However, when the VPN connection is disconnected or lost, the user's real IP address may be leaked. This will identify the user and intercept his data. Known methods of protection do not allow

solving this problem. The paper considers the basic methods of preventing the disclosure of a real IP address when using an active connection in a VPN network, an analysis and methods for preventing leakage in various operating systems are presented, a method of protection is exemplified using the example of the macOS 10.13 operating system. Based on the testing of the method, it was proved that it fully performs its functions to protect the user's device. The advantage of this method is the impossibility of disclosing the IP address, since Internet traffic will be blocked if it does not pass through the VPN server. The drawback of this method lies in the possible increase in connection time and in the possibility of implementation only in a specific operating system. As a result of the implementation of the method, they were able to establish a VPN connection, which has a higher degree of security.

Key words: *VPN (virtual private network); operating system; address tables; IP address disclosure prevention methods; connection protection; connection break; packet filter.*

Рецензенти: **Мусієнко М. П.,** д-р техн. наук, професор;
Журавська І. М., канд. техн. наук, доцент.

Дата надходження статті до редколегії 18.05.2017