УДК 004.77 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.034

ОГЛЯД ТЕХНОЛОГІЇ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У МІКСОВАНИХ VPN-ЛАНЦЮГАХ

Міхнов Є.Д.
Науковий керівник – к. т. н., доц. Ткачов В.М.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
e-mail: yevhen.mikhnov@nure.ua

In this paper, the most common load balancing technologies in mixed VPN chains are considered. A critical analysis of these technologies has been conducted, including scenarios of their use, potential drawbacks, and implementation challenges. This publication serves as a review and is intended to summarize known methods.

З метою побудови високозахищених систем віддаленого доступу застосовується складні багатошарові або міксовані VPN-тунелі [1]. Такі рішення, як правило, мають місце в організації бізнес-процесів з використанням гібридних хмарних рішень або багатошарових схем віртуалізації на рівні приватних хмар.

Інша сфера застосування може мати місце при вирішенні задач, пов'язаних з досягненням високого рівня анонімності при роботі у мережі Інтернет [2].

Однак, у підходах щодо створення міксованих VPN-ланцюгів виникає проблема ефективного розподілу мережного трафіку між VPN-серверами, VPN-оптимізаторами та іншими підсистемами, які відповідають за маршрутизацію захищеного трафіку. Найчастіше дана задача пов'язана з перевантаженням каналів зв'язку, які представлені у вигляді віртуальних тунелів або шифрованих каналів (рис. 1).

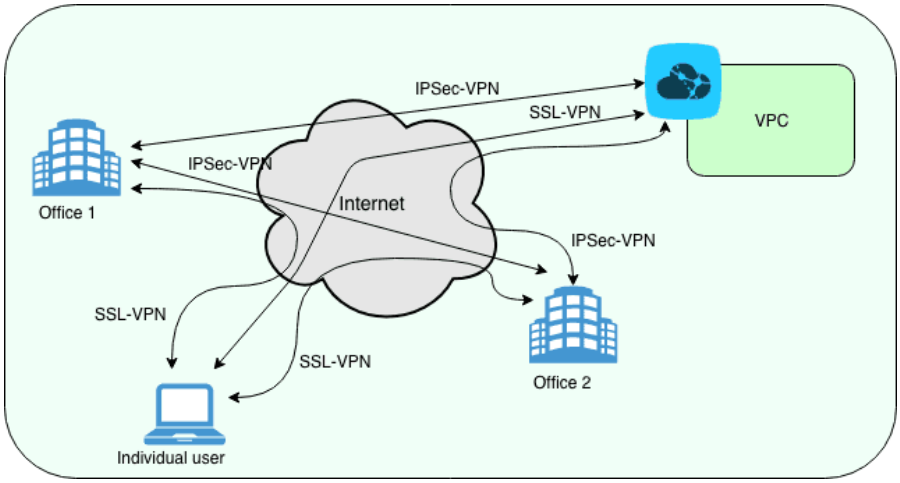

Рисунок 1 – Приклад мульти-VPN архітектури

Метою даної роботи є огляд та критичний аналіз існуючих технологічних рішень щодо вирішення вказаної задачі. В теорії комп'ютерної інженерії цю задачу можна класифікувати як задачу балансування мережного навантаження [3].

Одним із ефективних рішень є класичні мережні балансувальники, наприклад Load Balancer, Finagle та інші. Однак, недоліком даних рішень є недостатній рівень захищеності вхідних та вихідних інтерфейсів міжмережної взаємодії. Таким чином, доцільно розглянути рішення, які побудовані на принципах Round Robin [4]. Його суть полягає у способі балансування мережного навантаження, при якому запити або потоки даних розподіляються між кількома вузлами (у даному випадку, VPN-серверами) у порядку черги. Відповідно, кожен вузол мережі, який задіяний у функціонуванні VPN-ланцюга, отримує запити від спеціального вузла або підсистеми, яка реалізує даний підхід. Ці запити, незалежно від складності, розподіляються за принципом першого-ліпшого вузла. Наприклад, якщо у комунікаційному середовищі VPN-серверів існує три сервери, а четвертий вузол реалізує функцію Round Robin, то перший запит від користувача, який хоче здійснити передачу даних через цю систему, буде оброблятися першим VPN-сервером, який, у свою чергу, буде мати мінімальний час затримки на передачу даних у віртуальному тунелі між цим користувачем та, власне, VPN-сервером. Час буде визначатися сукупністю часових значень затримки передачі тестового повідомлення між задіяними вузлами (користувач та перший VPN-сервер), часом побудови VPN-тунелю та часом передачі тестового повідомлення у тунелі. Відповідно, процес тестування часових затримок між околом вузлів, які є потенційними першими VPN-серверами та користувачем, може також займати певний час. У такому випадку, вузлом, який реалізує функцію Round Robin, здійснюється вирішення додаткових задач побудови першого VPN-тунелю у ланцюгу. Якщо часові затримки даного етапу перевищують допустимі, то користувач може отримати відмову у обслуговуванні або мати значні часові затримки в обслуговуванні.

Аналогічним чином може бути створений маршрут до другого та інших VPN-серверів, таким чином, будуючи VPN-ланцюг (рис. 2).

Наведений алгоритм не враховує ряд інших аспектів, які мають специфіку та певні особливості мережного середовища, в якому здійснюється реалізація даного підходу. Також відомі інші рішення, які дозволяють встановити значення ваги як для кожного VPN-сервера, так і до їх груп [4].

Відомий приклад адаптивного балансування, який використовує інформацію про поточне навантаження на кожному VPN-сервері для прийняття рішення вибору наступного вузла VPN-ланцюга. Однак, такий підхід передбачає наявність динамічно-змінюваних спеціалізованих баз даних із метаданими про стани таких вузлів. Це вимагає наявності певних

складнощів у забезпеченні окремого рівня безпеки для таких баз даних. Як приклад, хмарний балансувальник NaaS з елементами міксування функціонує за вказаним алгоритмом.

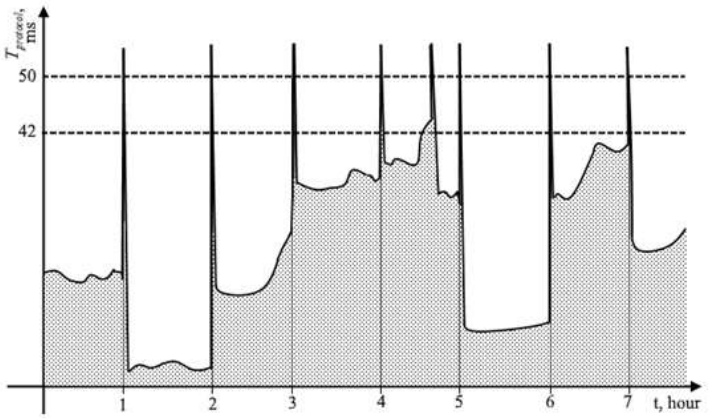

Рисунок 2 – Приклад часових затримок, які виникають при перебудові ланцюга

Окремою задачею, яка найчастіше виникає в оверлейних мережах, є визначення доступності VPN-вузлів перед запуском алгоритму пошуку вузлів при побудові ланцюга [3]. Цю задачу успішно вирішує відомий метод Health Check. Цей метод дозволяє уникати помилок, а також непередбачуваних часових затримок при побудові VPN-ланцюгів.

Інколи, додатковою задачею є побудова матриць пропускних здатностей та інших метрик, які визначають загальний стан пулу VPN-серверів, задіяних при побудові таких ланцюгів. Однак, складність обчислення таких значень напряму залежить від кількості вузлів у такому пулі та динаміки їх завантаженості.

У складних гетерогенних середовищах, де кількість VPN-серверів обчислюється сотнями, час на визначення оптимальних значень часових затримок між вузлом користувача та всіма VPN-вузлами може бути незадовільним. У таких випадках застосовується квазіоптимальні підходи, які дозволяють швидко створювати VPN-ланцюги з можливістю їх швидкої перебудови в залежності від мінливості метрик VPN-серверів мережі. В таких випадках має місце використання методу комівояжера з декількома активними пошукачами точок оптимуму [5].

Також складність задачі балансування навантаження у міксованих VPN-ланцюгах може визначатися кількістю вузлів у ланцюзі. Чим більша кількість, тим більша анонімність користувача, – але при цьому і менша швидкість доставки контенту від вузла, до якого надходить запит, до користувача. Проблема втрати службових даних цього запиту є найбільш критичною, так як у цьому випадку користувач має повторно їх генерувати, що може призвести до розкриття (деанонімізації) вузла користувача. У якості рішення цієї задачі може бути застосований асинхронний режим

обміну даними між користувачем та цільовим вузлом. Сутність цього рішення полягає у тому, що запит від користувача надходить через спрощену схему VPN-ланцюга, але з покращеною криптостійкістю, тоді як прикордонний VPN-сервер, який відповідає за пряме надсилання запиту до цільового вузла, перенаправляє отриману відповідь через повноцінний VPN-ланцюг до користувача [5].

Таким чином, проведений аналіз зазначених рішень дозволяє зробити висновок, про те, що використання міксованих VPN-ланцюгів забезпечує високий рівень анонімності в мережі Інтернет, однак, як і у будь-якій технології віртуалізації, відбувається втрата швидкості, що може бути критичним для передачі, наприклад, нееластичних даних, як-то голосовий, відеоконтент реального часу.

У якості напрямів подальших досліджень необхідно розглянути комбіновані схеми побудови VPN-ланцюгів з урахуванням регіональних особливостей постачальників віртуальних рішень, як-то VDS, VPS тощо.

Список використаних джерел

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, "Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.

2. V. Tkachov, M. Bondarenko, O. Ulyanov and O. Reznichenko, Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory, 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 161-165. DOI: 10.1109/ATIT49449.2019.9030494

3. Tkachov V. Architecture of overlay network with nested vpn tunneling / M. Hunko, V. Tkachov, M. Bondarenko // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 10-ї міжнар. наук.-техн. конф., 9-10 квітня 2020 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 1 : секції 1, 2 / Військ. акад. збройних сил Азербайджанської Республіки [та ін.]. – Харків : Петров В. В., 2020. – с. 36.

4. Kovalenko Andriy Метод забезпечення живучості комп’ютерної мережі на основі vpn-тунелювання / Andriy Kovalenko, Heorhii Kuchuk, Vitalii Tkachov // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:https://doi.org/10.26906/SUNZ.2021.1.090.

5. Tkachov, Vitalii & Tokariev, Volodymyr & Ilina, Iryna & Partyka, Stanislav. (2021). Modified Traveling Salesman Problem for a Group of Intelligent Mobile Objects and Method for Its Solving. International Journal of Electrical and Electronic Engineering & Telecommunications. 1-7. 10.18178/ijeetc.10.1.1-7.