УДК 004.056
А. Космина
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВІДМОВОСТІЙКЕ З'ЄДНАННЯ OPENVPN

UDC 004.89
A. Kosmyna

FAULT-TOLERANT CONNECTION OPENVPN

Мережа Інтернет не є тим середовищем передачі інформації, де забезпечується достатній рівень захищеності даних, що передаються. Тому виникає потреба у використанні засобів, що роблять з'єднання безпечним для циркуляції конфіденційної інформації. Одним з таких засобів є організація віртуальних приватних мереж (VPN), які являють собою відокремлену підмножину реальної мережі, що моделюється реальними каналами. Популяризація технології призводить до напливу великої кількості користувачів, які намагаються підключитися до сервера VPN, але внаслідок технічної обмеженості бувають випадки, коли не вдається встановити з'єднання чи постійно виникають обриви з'єднання, що змушує користувача проводити повторне підключення чи обирати інший сервер.

З метою забезпечення неперервності бізнес-процесів та сталого з'єднання або розподілу навантаження між серверами здійснюється організація VPN на основі OpenVPN з функцією автоматичної зміни сервера. Існує декілька варіантів реалізації VPN в залежності від рівня моделі OSI. Технологія OpenVPN має переваги, що виявляються у гнучкому налаштуванні сервера, завдяки чому він підлаштовується під конкретні завдання та вимоги.[1]

Гнучкі налаштування OpenVPN пропонують на вибір достатню кількість алгоритмів шифрування. В сучасних бізнес процесах циркулює великий обсяг інформації, саме тому окрім надійності алгоритму важливу роль відіграє швидкість шифрування та передачі такої інформації. При виборі алгоритму шифрування для реалізації VPN-з'єднання, окрім ступеню захищеності, потрібно звертати увагу на його продуктивність та пропускну здатність. [2]

Саме тому було проведено дослідження продуктивності основних алгоритмів шифрування, що підтримуються OpenVPN. На основі програмної реалізації алгоритмів з використанням бібліотеки Crypto++ Library 8.6 виявлено максимальну швидкість обчислення невеликих блоків випадково згенерованих даних для кожного з алгоритмів.

Реалізація відбувається на основі декількох серверів та клієнтів з відповідними налаштуваннями для автоматизації процесу перепідключення та перенаправлення користувачів у разі втрати з'єднання з одним із серверів.

Основним результатом є розгляд організації та переваг VPN на основі OpenVPN з налаштуванням автоматичної зміни сервера, вибір найбільш оптимального алгоритму шифрування на основі захищеності та продуктивності.

Реалізація VPN на основі OpenVPN з автоматичною зміною сервера дозволяє впроваджувати гнучкі налаштування відповідно до поставлених задач та забезпечувати усім користувачам стале й якісне швидкісне з'єднання шляхом унеможливлення обриву з'єднання окрім випадків, коли усі сервери будуть недоступні, а також достатню захищеність мережі передачі інформації.

Література.

1. Електронний ресурс https://sites.google.com/site/ponatievpn/home/klassifikacia-vpn. Last accessed: 27.11.2021
2. OpenVPN 2 Cookbook 2nd Edition «100 simple and incredibly effective recipes for harnessing the power of the OpenVPN 2 network», Jan Just Keijser, Packt Publishing-2017.-400 с.