

ОРГАНІЗАЦІЯ КОНТРОЛЮ ОБМІНУ ІНФОРМАЦІЄЮ МІЖ ДВОМА ОФІСАМИ

Одним із пріоритетів при побудуванні мережі, слугує захищеність файлів, що передаються і приймаються. Для цих цілей під час організації мережі дуже добре підходить, з моєї точки зору, використання VPN- доступу. Розглянемо більше детально його побудову та використання. VPN ((англ. Virtual Private Network - віртуальна приватна мережа) – ця технологія забезпечує зашифроване з'єднання між двома мережами або окремим користувачем та мережею, за її допомоги всі дані користувача при підключенні до Інтернету зашифровуються. Дана технологія дуже популярна, адже перш за все вона економічно вигідна. Розглянемо, наприклад, два офіси в різних точках міста. Для того, щоб об'єднати всі дані, що передаються між ними, ми можемо взяти та придбати персональну лінію, яка буде сполучати дані офіси, Але якщо взяти до уваги випадок, коли офіси знаходяться в різних містах, чи коли більшість співробітників працюють з дому у зв'язку з карантинном, то дана технологія буде занадто дорогою і невигідною. Тому для збереження часу і грошей простіше організувати VPN- доступ для всіх співробітників, що працюють в офісі та за його межами наступним чином (рис.1). На рис. 1 зображено підключення до мережі двома способами: клієнт - мережа - віддалений доступ окремо взятих співробітників до корпоративної мережі організації через модем або загальнодоступну мережу. (Мережа – мережа- це об'єднання двох і більше офісів в єдину захищену віртуальну мережу за допомогою інтернет [1] озглянемо приклад підключення за допомогою OpenVPN (рис.2).



Рисунок 1– Приклад організації VPN- доступу для двох офісів з можливістю підключення співробітників, що працюють вдома.

Ця додаткова програма, яка встановлюється на робоче місце користувача (ноутбук/ комп'ютер) і забезпечує шифрування каналів типу « точка- точка» або « сервер- клієнт», була створена Джеймсом Йонаном у 2002 році. Вона підходить для багатьох ОС, таких як : [Solaris](#), [Open BSD](#), [Free BSD](#), [Net BSD](#), [GNU](#) / [Linux](#), [Apple Mac OS X](#), [QNX](#), [Microsoft Windows](#), [Android](#), [iOS](#) [2]. Для шифрування і аутентифікації використовують бібліотеку OpenSSL, а також для передачі даних можуть використовувати UDP чи TCP. Зазвичай використовують TCP, бо він вважається стабільнішим тому, що пропонує функцію виправлення помилок (після відправлення мережевого пакета TCP очікує підтвердження перед його повторною відправкою чи відправленням нового пакета). UDP виправляє помилки, що робить його менш стабільним, але набагато швидшим. В даній програмі перш за все використовують UDP, спочатку йде з'єднання, але, якщо його встановити неможливо, тоді сервер переналаштовується на TCP.[3]. Без VPN-доступу співробітники не мають можливості приступити до роботи. Після встановлення програми користувач вводить свій логін і пароль, і цим самим забезпечує доступ до VPN. Переваги даного методу в його анонімності в мережі, шифруванні даних, можливості співробітникам працювати віддалено, маючи доступ до корпоративної інформації. На які умови варто звернути увагу при виборі VPN : для шифрування інформації варто вибирати рівень, який максимально захистить ваші приватні дані від сторонніх, дуже чудово може підійти – 256- бітове шифрування. Екстремне відімкнення від мережі: за допомогою цієї функції відбувається переривання мережі VPN , щоб запобігти витоку даних. (Захист від витоків DNS і IPv6).

Для тих, хто збирається працювати не тільки вдома, краще за все використовувати VPN - сервіс з серверами, що розташовані в усіх куточках планети. Це дає можливість відкрити доступ до різного виду контенту з будь – яких країн світу.

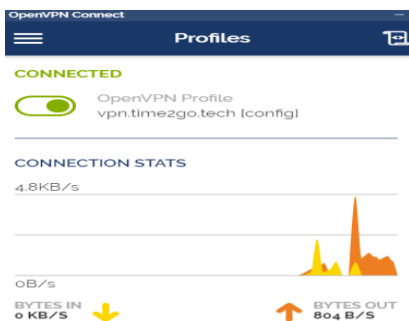


Рисунок 2– Підключення додатку VPN.

Якщо виникає потреба в VPN - захисту для декількох пристроїв, то варто звернути увагу на функцію «Одночасної підтримки відразу декількох підключень»

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. <https://justrust.ru/uk/vpn-cherez-set-obshchego-polzovaniya-cto-takoe-vpn-ili-kak-zashchitit-set/>
2. <https://ru.wikipedia.org/wiki/OpenVPN>
3. <https://www.cactusvpn.com/ru/beginners-guide-to-vpn/what-is-openvpn/#definition>