

ДОСЛІДЖЕННЯ ПРИНЦИПІВ РОБОТИ VPN МЕРЕЖІ

VPN (Віртуальна приватна мережа, англ. Virtual Private Network) – технологія, яка дозволяє встановити віртуальний канал між двома чи більше локальними мережами через мережу загального користування, якою зазвичай виступає інтернет.

VPN складається із «внутрішньої» та «зовнішньої» мереж. Під «внутрішньою» мережею слід розуміти всі ті мережі, між якими потрібно встановити з'єднання, тобто локальні мережі компанії. «Зовнішня» мережа – та, через яку проходять дані (інтернет).

З'єднання між мережами у VPN здійснюється за принципом точка-точка. Тобто, між двома мережами створюється захищений канал (тунель), через який йде передача даних. Для захисту інформації яка передається є декілька протоколів:

1. Протокол PPTP (Point-to-Point Tunneling Protocol) – тунельний протокол, який за допомогою захищеного тунелю створює з'єднання з сервером. Принцип його роботи полягає у тому, що один мережевий протокол інкапсулюється (вставляється) в інший, причому інкапсульований протокол відноситься до того ж або більш низького рівня, ніж той, яким користуються в якості тунелю. Призначення тунелю полягає в тому, щоб "упакувати" передану порцію даних разом зі службовими полями в новий "конверт".

2. IPsec (скорочення від IP Security) – набір протоколів для забезпечення захисту даних, які передають за допомогою протоколу IP, який не є надійним і дозволяє реалізувати тільки негарантовану доставку даних. Протокол IPsec працює на мережевому рівні, що робить його дуже гнучким [2].

3. OpenVPN – програмне забезпечення для створення з'єднання між двома клієнтськими машинами або забезпечення роботи централізованого VPN-сервера для одночасної роботи декількох клієнтів. Перевагами даної технології є її відкритий код та можливість створення з'єднань між комп'ютерами, які перебувають за NAT-екраном. OpenSSL (універсальна бібліотека для криптографії) використовується для забезпечення безпеки керуючого каналу та потоку даних [1].

Також важливою складовою безпеки мережі VPN є сервер доступу, який підключається як до внутрішньої, так і до зовнішньої мережі. Сервер доступу вимагає у всіх віддалених користувачів, які намагаються підключитись до мережі, пройти процес авторизації і тільки тоді їм надається доступ до мережі.

За функціональність VPN відповідає комплекс, який також вирішує завдання фільтрації мережевого трафіку, забезпечує якість обслуговування та організацію мережевого екрану.

Концепція таких мереж дозволяє організовувати такий необхідний обмін інформацією усередині компанії і з клієнтами при оптимальному поєднанні продуктивності, оперативності, захищеності і вартості. Такі технології, як VPN, активно розвиваються, вдосконалюються і все більше поширюються.

Література

1. Eric F Crist. Mastering OpenVPN 1st Edition. – Birmingham: Packt Publishing, 2015. – 366 p.
2. Henry James. IPsec Virtual Private Network Fundamentals. – Cisco Press book 2006. – 480 p.