УДК 004.7(043)

ТЕХНОЛОГІЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Дар'я Чижиченко, Дарина Кухарець

Національний авіаційній університет, Київ

Науковий керівник – Савченко Аліна Станіславівна, д.т.н.,доц.

Ключові слова: VPN, мережа, кібербезпека, особисті дані, шифрування.

VPN (Virtual Private Network) - це технологія, яка дозволяє створити безпечне, зашифроване з'єднання між двома вузлами мережі через Інтернет. Сьогодні VPN є актуальною з кількох причин. Одна з них - це збільшення кількості віртуальних загроз у Інтернет, таких як крадіжка особистої інформації, шпигунство, віруси та інші види кібератак. Використання VPN дозволяє захистити приватність, шифруючи всі дані, які відправляються та отримуються через Інтернет. Крім того, у зв'язку зі збільшенням кількості людей, які працюють з віддаленої локації, VPN стає важливим інструментом для забезпечення безпеки та захисту корпоративних даних під час роботи з віддалених місць.

VPN класифікують за потребами користувачів:

- VPN з віддаленим доступом (Remote Access VPN) - дозволяють індивідуальним користувачам організувати безпечний доступ до корпоративних ресурсів через публічні мережі.
- Внутрішньокорпоративні VPN (Intranet VPN) - ще називаються "точка-точка" - використовується для об'єднання в єдину захищену структуру декількох територіально-розподілених комп'ютерних мереж (приміром, зв'язок центрального офісу компанії з її регіональними відділеннями).
- Міжкорпоративні VPN (Extranet VPN) - дають можливість підключення до корпоративної мережі "зовнішніх" користувачів (наприклад, замовники або клієнти).

Безпека VPN передбачає весь набір атрибутів захищеної мережі - конфіденційність, цілісність і доступність інформації при передачі через загальнодоступну мережу, а також захищеність внутрішніх ресурсів мереж споживача і постачальника від зовнішніх атак. Ступінь безпеки VPN варіюється в широких межах залежно від застосовуваних засобів захисту: шифрування трафіку, аутентифікації користувачів і пристроїв ізоляції адресних просторів (наприклад, на основі техніки NAT), використання віртуальних каналів і двоточкових тунелів, що ускладнюють підключення до них несанкціонованих

користувачів. Так як ні один спосіб захисту не дає абсолютних гарантій, то засоби безпеки можуть комбінуватися для створення ешелонованої оборони.

Сервіси VPN наближаються до сервісів приватної мережі за якістю обслуговування. Якість транспортного обслуговування має на увазі, в першу чергу, гарантії пропускної здатності для трафіку клієнта, до яких можуть додаватися й інші параметри - максимальні затримки і відсоток втрачених даних. У пакетних мережах пульсації трафіку, змінні затримки і втрати пакетів - неминуче зло, тому ступінь наближення віртуальних каналів до каналів TDM завжди неповна і імовірнісна (в середньому, але ніяких гарантій для окремо взятого пакета). Вважається, що безпека - обов'язкова властивість VPN, а якість транспортного обслуговування - тільки бажана.

Мережа VPN наближається до реальної приватної мережі, якщо вона забезпечує для клієнта незалежність адресного простору. Це дає клієнтові одночасно і зручність конфігурації, і спосіб підтримки безпеки. Причому бажано, щоб не тільки клієнти нічого не знали про адресні простори один одного, але і магістраль постачальника мала власний адресний простір, невідомий користувачам. В цьому випадку мережа постачальника послуг буде надійніше захищена від навмисних атак або ненавмисних дій своїх клієнтів, а значить, більш високою буде якість послуг, що надаються VPN.

Основні переваги використання VPN:

1. Захист від прослуховування - VPN забезпечує шифрування трафіку між користувачем та сервером VPN, що зменшує ризик його прослуховування сторонніми особами.
2. Анонімність - VPN дозволяє приховати реальну IP-адресу користувача від сервера, що забезпечує більшу анонімність в Інтернеті.
3. Доступ до заблокованого контенту - з допомогою VPN можна обходити блокування веб-сайтів, які заборонені в певних країнах або мережах.
4. Захист від кібератак - VPN може забезпечити захист від різних видів кібератак, таких як DDoS-атаки, мережеві атаки та інші, оскільки весь трафік пересилається в зашифрованому вигляді.
5. Захист від реклами та трекінгу - VPN дозволяє блокувати рекламу та трекінг користувачів в Інтернеті.
6. Розширення мережі - VPN може дозволити користувачеві підключатись до мережі з будь-якого місця в світі та працювати з віддаленими серверами або робочими станціями.

VPN є потужним інструментом для захисту даних та приватності в Інтернет. Однак, існує кілька сучасних проблем, пов'язаних з використанням VPN:

1. Недостатня безпека: Багато безкоштовних VPN-сервісів можуть збирати та продавати дані користувачів своїм партнерам та рекламодавцям. Це може призвести до витоку особистої інформації користувачів, такої як логіни, паролі, веб-історія, IP-адреса та інші конфіденційні дані.
2. Обмеження швидкості: під час використання VPN трафік маршрутизується через сервери, що може призвести до зменшення швидкості Інтернет-з'єднання через додатковий шар шифрування і тунелювання даних. Це може стати проблемою для користувачів, які потребують великої швидкості з'єднання для роботи чи потокової передачі відео.
3. Нестабільність з'єднання: Деякі VPN-провайдери можуть працювати ненадійно, особливо при високих навантаженнях на сервери або якщо їх сервери розташовані далеко від місця знаходження користувача.
4. Блокування VPN: Деякі додатки та веб-сайти блокують доступ через VPN. Це може стати проблемою для користувачів, які намагаються отримати доступ до вмісту, який обмежується географічно.

Ці проблеми необхідно враховувати при використанні VPN, тому важливо вибирати надійних VPN-провайдерів та дотримуватися кращих практик щодо кібербезпеки.

Висновок

Використання VPN забезпечує безпеку під час роботи з віддаленими серверами та забезпечує захист від кібератак. Використання VPN забезпечує безпеку від несанкціонованого доступу до відкритих мереж, які можуть бути не захищені. Використання VPN дозволяє зберегти приватність та анонімність в Інтернеті, забезпечуючи захист від відстеження активності в мережі.

Список використаних джерел:

1. Послуга віртуальних приватних мереж. URL http://um.co.ua/1/1-8/1-82951.html (Last accessed: 24.03.2023).
2. Віртуальні приватні мережі. URL: https://www.untc.ua/ua/business/datatransfer/vpn/ (Last accessed: 24.03.2023).
3. Wikipedia. https://uk.wikipedia.org/wiki/VPN (Last accessed: 24.03.2023).