УДК 004:656.13
DOI: 10.31673/2412-9070.2021.050310

В. В. ХАРЧЕНКО, студент;
О. В. БОНДАРЕНКО, студент;
Н. В. КАСИНЕЦЬ, студентка;
В. В. ЛЯШЕНКО, студент;
А. В. ЛЕМЕШКО, доктор філософії,
Державний університет телекомунікацій, Київ

АНАЛІЗ НАЯВНИХ VPN-ВИРІШЕНЬ ДЛЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ПЕРЕДАВАННЯ ДАНИХ

Швидкий розвиток мережі «Інтернет» зумовив появу нової тенденції в побудові глобальних корпоративних зв'язків дешевшого і доступнішого транспорту пакетних мереж загального користування. Але таке привабливе і маловартісне вирішення — передавання корпоративних даних через загальнодоступну мережу, створює велику загрозу для безпеки мережі підприємства, що особливо важливо для банківських інформаційних систем. Крім того, для корпоративних мереж важливе значення має якість обслуговування користувачів, надання заданого набору послуг і гарантій, яких не завжди можна забезпечити в публічних мережах.

Ключові слова: VPN; тунелювання; автентифікація; шифрування; OpenVPN; L2TP; IPSec; GRE; PPTP; WireGuard.

ВСТУП

Як відомо, створювати і прокладати особистий канал зв'язку — процес не дуже швидкий, оскільки практичне виконання робіт (а саме прокладання кабелю) становить, зазвичай, не більш ніж 20% усього проєкту, тоді як понад 80% припадають на підготовчі процеси:

- етап створення необхідної документації;
- узгодження робіт;
- отримання різноманітних дозволів на будівництво [1].

Для вирішення цих проблем може бути використана технологія віртуальних приватних мереж **VPN**. *Virtual Private Network* — віртуальна приватна мережа, котра формується поверх інших мереж із меншим рівнем довіри. Безпека передавання інформації через загальнодоступні мережі реалізується завдяки шифруванню, а отже, створюється закритий для сторонніх канал обміну інформацією. Технологія дає можливість перетворити з'єднання в пакетних мережах загального користування в захищені канали з гарантованою смугою пропускання, забезпечуючи безпеку і широкий спектр сервісів із прийнятною вартістю встановлюваних з'єднань. Тому така технологія затребувана багатьма підприємствами й організаціями, що не мають власних мережних ресурсів.

ОСНОВНА ЧАСТИНА

Різновид архітектури VPN

Технологія VPN пов'язує мережі в єдину мережу із застосуванням непідконтрольних каналів. Провайдери пропонують власні послуги для розгортання своєї VPN-мережі. VPN вважається клієнт-серверною технологією [2]. Сучасні технології для оброблення, передавання та збору інформації сприяють розвитку загроз, зокрема можливості втрати, модифікації та розкриття даних, котрі направляються кінцевим користувачам. Забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з перспективних напрямків розвитку комп'ютерних інформаційних технологій. Інформація була і буде товаром, який можна придбати, продати, обміняти, а вартість інформації завжди перевищуватиме вартість купівлі та обслуговування [2]. Інформація, що передається через корпоративні канали зв'язку, має бути конфіденційною та недоступною для третіх осіб. Безпека є надважливою, тому ця тематика надзвичайно актуальна.

Залежно від розташування програмного забезпечення захищеного каналу розрізняють дві схеми організації каналу зв'язку:

1) схема з кінцевими вузлами, що взаємодіють через публічну мережу (рис. 1);

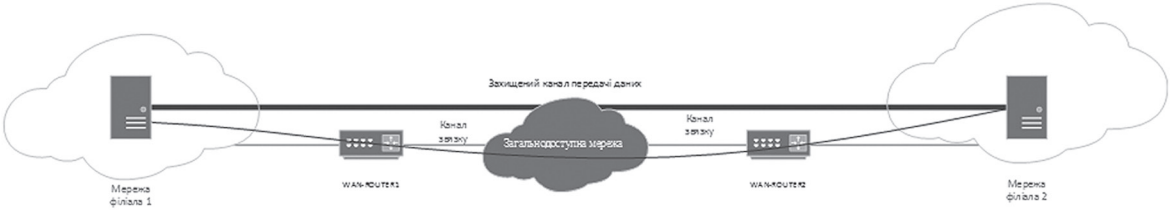

Рис. 1. Схема з кінцевими вузлами, що взаємодіють через публічну мережу

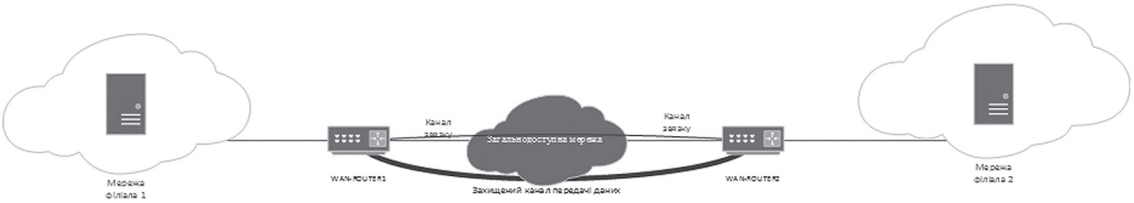

Рис. 2. Схема з розташованим на межі мережним обладнанням, підімкненим до публічної мережі

2) схема з підімкненим до публічної мережі мережним обладнанням, розташованим на межі (рис. 2).

У першому випадку захищений канал утворюється програмними засобами, встановленими на двох віддалених комп'ютерах або серверах, що належать двом різним локальним мережам одного підприємства та пов'язаних між собою через публічну мережу. Перевагою цього підходу є повна захищеність усього каналу проходження, а також можливість використання будь-яких протоколів для каналу за умови, що на кінцевих точках каналу підтримується ідентичний протокол. До недоліків належать надмірність та децентралізованість вирішення. Надмірність полягає в тому, що навряд чи варто створювати захищений канал на всьому шляху проходження даних: адже зазвичай вразливими для зловмисників є мережі з комутацією пакетів, а не канали телефонної мережі або виділені канали, чи локальні мережі підімкнені до територіальної мережі. Тому захист каналів доступу до публічної мережі вважається надмірним. Децентралізація полягає в тому, що для кожного комп'ютера, якому потрібно надати послуги захищеного каналу, необхідно окремо встановлювати, конфігурувати та адмініструвати програмні засоби захисту даних.

Підімкнення кожного нового комп'ютера до захищеного каналу потребує повторного виконання цих трудомістких операцій.

У другому випадку клієнти та сервери не беруть участі у створенні захищеного каналу. Канал прокладається лише всередині публічної мережі з комутацією пакетів, наприклад, такий захищений канал може бути прокладено між двома чи більше маршрутизаторами. Це масштабоване вирішення, що керується централізовано адміністраторами корпоративних мереж. Такий гнучкий підхід дає можливість легко сформовувати нові захищені канали між комп'ютерами незалежно від місця їх розташування. Реалізація цього підходу складніша, оскільки потрібний стандартний протокол для створення захищеного каналу [3].

Захищений канал має дотримуватися таких основних функцій:

♦ взаємної автентифікації абонентів під час установлення з'єднання, яка може бути виконана, наприклад через обмін паролями;

♦ захисту повідомлень, що передаються по каналу зв'язку, від несанкціонованого доступу, наприклад шифруванням;

♦ підтвердження цілісності повідомлень, які передаються по каналу зв'язку, наприклад одночасним передаванням із повідомленням його дайджесту.

VPN базується на трьох методах забезпечення безпеки в мережах:

1) тунелювання;

2) автентифікація;

3) шифрування.

За допомогою методики ***тунелювання*** пакети даних транслюються через загальнодоступну мережу, як за звичайним з'єднанням. Між кожною парою відправника та одержувача встановлюється своєрідний тунель — безпечне логічне з'єднання, що дає змогу інкапсулювати дані одного протоколу в пакети другого. Тунелювання здатне організувати передавання пакетів одного протоколу в логічному середовищі, яке використовує інший протокол. Автентифікація забезпечить перевірку доступу між вузлами та дозволить або заборонить з'єднання між ними. Шифрування гарантує, що в разі отримання доступу до інформації її ніхто не зможе розшифрувати.

Автентифікація — це процедура доведення особою того, що вона є тією, за кого себе видає. Розрізняють автентифікацію на основі пароля і на основі сертифіката. На основі пароля користувач або ж адміністратор створює символьний пароль, який зберігається в базі даних зашифрованим, і в разі правильного введення користувачем пароля він порівнюється і доступ дозволяється. На основі сертифіката паролі не застосовуються, в центрі сертифікації створюється сертифікат і передається користувачу. Зазвичай автентифікацію на основі сертифіката використовують великі підприємства та корпорації.

Шифрування — це засіб забезпечення конфіденційності даних, що зберігаються в пам'яті комп'ютера або передаються по проводових і безпроводових мережах.

Шифрування поділяють на симетричні та асиметричні алгоритми шифрування. Симетричний метод шифрування застосовує для шифрування і розшифрування даних один ключ, прикладом є алгоритм DES та AES. Асиметричний метод використовує два ключі — один публічний, а дру-

гий секретний. Публічним ключем послуговуються для шифрування, а секретним для розшифрування, прикладом алгоритму є RSA та diffie-Hellman [3].

Отже, тунелювання, автентифікація та шифрування забезпечують передавання даних між двома вузлами, модулюючи роботу локальної мережі.

Далі розглянемо кілька основних протоколів VPN, серед яких PPTP, OpenVPN, L2TP/IPSec, IKE, WireGuard.

Протоколи PPTP

PPTP — протокол тунелювання «точка-точка» — один із найстаріших протоколів VPN, що існують. Створений у середині 90-х Microsoft, PPTP було інтегровано в Windows 95 і спеціально розроблено для комутованих комунікацій. PPTP використовує протокол автентифікації MS-CHAPv2, і все ще вважається основним механізмом автентифікації для більшості клієнтів віртуальної приватної мережі. За допомогою ChapCrack можна приймати захоплений мережний трафік, який містить рукостискання MS-CHAPv2 (підтвердження PPTP VPN або WPA2 Enterprise), зменшуючи безпеку рукостискання до одного ключа DES.

Потім цей ключ DES можна надіслати на CloudCracker.com — комерційну онлайн-службу злому паролів, де його буде розшифровано менш ніж за добу. Вихідні дані CloudCracker можна використовувати разом із ChapCrack для розшифрування всього сеансу, записаного за допомогою WireShark або інших подібних інструментів для виявлення мережі [4]. Однак оскільки йому не вистачає багатьох функцій безпеки, притаманних іншим сучасним протоколам, він може забезпечити найкращі швидкості з'єднання для користувачів, яким, можливо, не потрібне сильне шифрування.

Протокол PPTP все ще використовується в певних застосунках, хоча більшість провайдерів з того часу оновили його до більш швидких і надійних протоколів. Протокол має слабке шифрування і може бути зламаний як спецслужбами, так і кваліфікованими зловмисниками. З переваг варто зазначити відсутність потреби в установленні додаткового програмного забезпечення і швидкості роботи.

Отже, переваги протоколу PPTP:

- висока швидкість передавання даних;
- легке налаштування;
- вбудований у всі платформи.

Його недоліки:

- не гарантує високу захищеність.

Протоколи OpenVPN

OpenVPN — безплатне вирішення з відкритим вихідним кодом, яке, за визнанням більшості фахівців, є найкращим сьогодні для створення приватної віртуальної мережі. Модель безпеки OpenVPN заснована на SSL, галузевому стандарті для безпечного зв'язку через інтернет. OpenVPN реалізує надійне розширення мережі OSI рівня 2 або 3 за допомогою протоколу SSL/TLS, підтримує гнучкі методи автентифікації клієнта на основі сертифікатів, смарт-карт і двофакторної автентифікації, а також дає змогу керувати доступом для користувачів або груп за допомогою правил брандмауера. Застосовується до віртуального інтерфейсу VPN. OpenVPN не є проксі-сервером вебзастосунків і не працює через веббраузер.

OpenVPN має такі режими автентифікації:

- ♦ статичний ключ — використовується попередньо спільний статичний ключ;
- ♦ TLS — застосовуються сертифікати SSL/TLS для автентифікації та обміну ключами.

У режимі статичного ключа попередньо спільний ключ генерується і поширюється між обома одноранговими OpenVPN перед запуском тунелю. Цей статичний ключ містить чотири незалежних ключі: HMAC send, HMAC receive, encrypt та decrypt. За замовчуванням у режимі статичного ключа обидва хости будуть використовувати один і той самий ключ HMAC, а також той самий ключ шифрування та дешифрування. Однак, застосовуючи параметр direction для --secret, можна використовувати всі чотири клавіші незалежно.

У режимі SSL/TLS сеанс SSL установлюється з двонапрямленою автентифікацією (тобто кожний бік з'єднання має надати свій власний сертифікат). Якщо автентифікація SSL/TLS проходить успішно, шифрування/дешифрування та вихідний матеріал ключа HMAC випадковим чином генеруються функцією RAND_bytes OpenSSL і обмінюються через з'єднання SSL/TLS. Обидва боки з'єднання вносять випадковий вихідний матеріал. У цьому режимі ніколи не використовується жоден ключ двонапрямлено, тому кожен одноранговий партнер має окремий ключ HMAC для відправлення, HMAC приймання, шифрування пакетів і ключ дешифрування пакетів [5].

OpenVPN не входить до складу стандартних дистрибутивів сучасних операційних систем, тому потребує встановлення додаткового програмного забезпечення. У разі правильного налаштування його не зможуть розшифрувати ані спецслужби, ані зловмисники, а під час нестандартних налаштувань його складно блокувати. Захоплення пакетів програмою Wireshark зображено на рис. 3, на якому можна побачити, що між сервером і клієнтом передається тільки UDP-трафік.

Цей протокол набув популярності завдяки використанню (практично непорушного) шифрування ключів AES-256 з 2048-розрядною автентифікацією RSA та 160-бітовим алгоритмом хешу SHA1. OpenVPN працює на всіх сучасних операційних системах: Linux, Android, Windows, macOS, iOS.

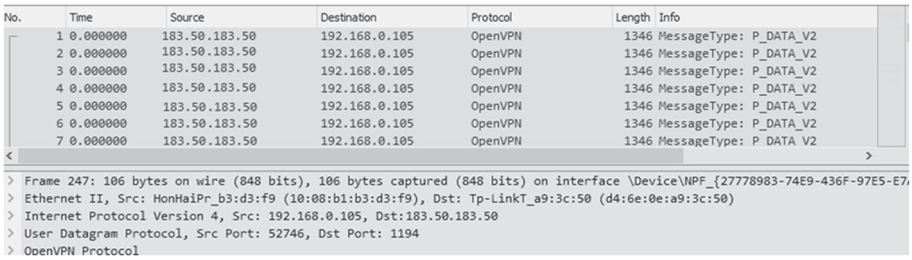

Рис. 3. Захоплення пакетів OpenVPN програмою Wireshark

Переваги протоколу OpenVPN:

- високий ступінь захищеності;
- легке налаштування;
- можливість підтримувати різні алгоритми шифрування;
- відкритий вихідний код;
- відсутність проблем із мережним екраном.

Його недоліки:

- потреба в установленні додаткового ПЗ.

Протоколи GRE, L2TP, IPSec, IKE

GRE і **L2TP** — це два загальновідомих протоколи тунелювання, і їх іноді можна сплутати. Тоді як GRE є абревіатурою від *Generic Routing Encapsulation*, L2TP означає *Layer 2 Tunneling Protocol*. Жоден із цих протоколів не шифрує трафік, щоб забезпечити захист даних, які тунелюються. Водночас, якщо ми хочемо захистити трафік, то IPsec потрібно запустити через L2TP або GRE. Хоча IP-тунель GRE використовується для передавання «іншого» типу трафіку, L2TP застосовується для мультиплексування кількох сеансів PPP між двома кінцевими точками IP. L2TP було розроблено на основі протоколу тунелювання *Microsoft Point-to-Point Tunneling Protocol* (PPTP) і технології пересилання рівня 2 (L2F) Cisco.

Internet Protocol Security **(IPSec)** є набором протоколів для забезпечення технології IP-комунікацій за допомогою автентифікації і шифрування кожного з IP-пакетів сеансу зв'язку. IPSec також містить протоколи для встановлення взаємної автентифікації між агентами на початку сесії і переговорів криптографічних ключів, які використовуватимуться під час сесії.

В основі IPSec є три протоколи:

♦ *Authentication Header* **(AH)** — забезпечує цілісність переданих даних, автентифікацію джерела інформації та функцію запобігання повторному передаванню пакетів;

♦ *Encapsulating Security Payload* **(ESP)** — забезпечує конфіденційність переданої інформації, обмежуючи потік конфіденційного трафіку. Водночас він може виконувати функції AH. Під час використання ESP потрібно мати зазначений набір служб безпеки, кожну його функцію може бути додатково активовано;

- *Internet Security Association and Key Management Protocol* **(ISAKMP)** — протокол, який використовують для початкового налаштування з'єднання, взаємної автентифікації кінцевими вузлами один одного та обміну секретними ключами. ISAKMP, також званий **IKE** (*Internet Key Exchange*), є протоколом узгодження (протоколом переговорів), який дає можливість двом хостам домовлятися про те, як створити забезпечення безпеки IPsec [5].

Узгодження ISAKMP передбачає його розбиття на два етапи: фазу 1 і фазу 2. Під час фази 1 (рис. 4) створюється перший тунель, який захищає наступні повідомлення узгодження ISAKMP. На етапі фази 2 (рис. 5) формується тунель, який захищає дані. Потім у гру вступає IPSec для шифрування даних із використанням алгоритмів шифрування та надає автентифікацію, шифрування та захист від повторного відтворення.

AH і **ESP** — це протоколи безпосереднього захисту даних. Роль IKE зовсім інша — він не здійснює безпосередній захист даних користувача, але забезпечує AH та ESP автентифікованими ключами.

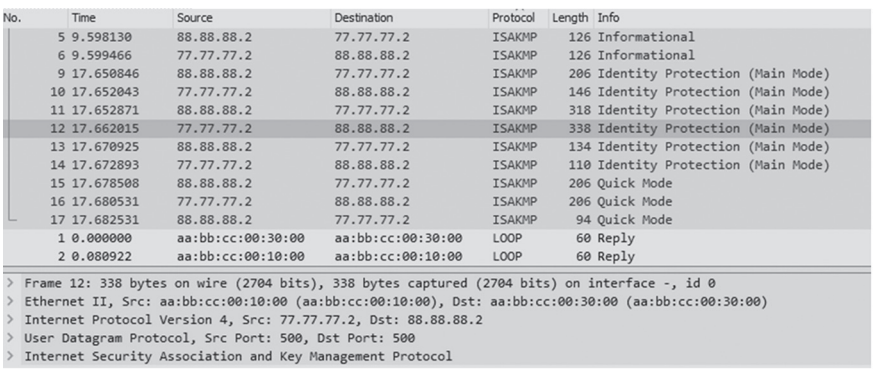

Рис. 4. Захоплення пакетів першої фази IPSec

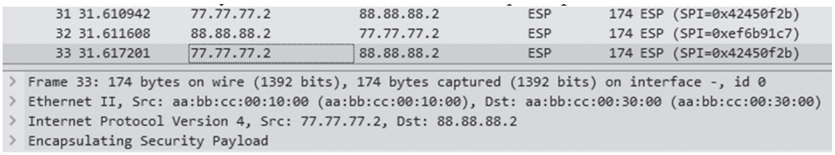

Рис. 5. Захоплення пакетів другої фази IPSec

Для демонстрації було встановлено з'єднання «Site-to-site» у віртуальному середовищі «EVE-NG», де налаштовано GRE/IPSec. У даних, отриманих із демонстрації, видно тільки зовнішні IP-адреси, а дані, що передаються в середині каналу, зашифровано протоколом ESP. На зображені передавались ICMP пакети канальних IP-адрес. Для прикладу захоплення пакетів тунелю, який створено протоколом GRE, зображено на рис. 6.

Основний режим потрібно застосовувати, коли однорангові VPN використовують статичні IP-адреси. Якщо один або другий одноранговий VPN не використовує IP-адресу як ідентифікатор цього однорангового вузла, то основний режим можна застосовувати лише за наявності сертифікатів.

IKE SA використовуються для захисту переговорів щодо безпеки [7].

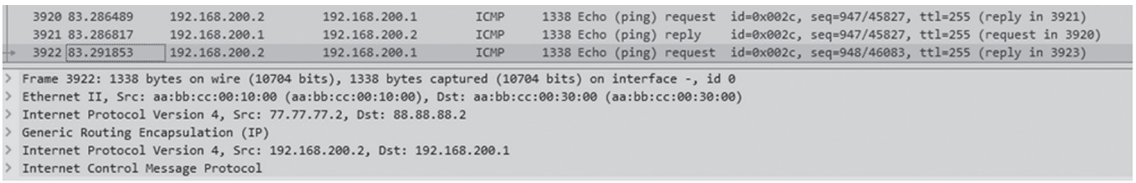

Рис. 6. Захоплення пакетів тунелю GRE

З рис. 6 випливає, що дані ніяким чином не шифруються, а лише інкапсулюються в GRE протокол і відправляються у відкритому вигляді.

Асоціацію безпеки можна досягти двома способами: використовуючи або основний режим, або агресивний режим. Метою основного режиму (або фази 1) є налаштування безпечного каналу, в якому можна узгоджувати швидкий режим (або фазу 2). Обидва пристрої в переговорах обмінюються обліковими даними один з одним, в яких вони мають збігатися, аби успішно авторизуватися, щоб мати можливість установити VPN-з'єднання. Це досягається обміном однаковими загальними ключами обох однорангових партнерів або використанням цифрових сертифікатів. Однак обидва пристрої мають застосовувати ту чи іншу форму ідентифікації. Отже, якщо один пристрій використовує попередній спільний ключ для підтвердження своєї ідентичності, то другий пристрій також має використовувати ідентичний попередній спільний ключ. Те саме стосується і цифрових сертифікатів: якщо один пристрій використовує цифрові сертифікати, то обидва боки мають використовувати цифрові сертифікати. Коли обидва користувачі успішно досягли цього, можна вважати, що вони вдало ідентифікували себе один перед одним.

У фазі 1 застосовується основний режим і досягається двосторонній обмін між ініціатором і приймачем тунелю. Основний режим забезпечує захист ідентифікації завдяки автентифікації однорангових ідентифікаторів, коли використовуються попередні спільні ключі, і зазвичай застосовується для тунелів «сайт-сайт».

IKE має дві версії — IKEv1 і IKEv2. Асоціації безпеки в IKEv2 називаються дочірніми SA і можуть створюватися, змінюватися та видалятися незалежно в будь-який час протягом життя тунелю VPN. Далі наведено деякі відмінності цих протоколів.

- У IKEv2 кінцеві точки обмінюються меншою кількістю повідомлень, щоб створити тунель. IKEv2 використовує чотири повідомлення, IKEv1 використовує або шість повідомлень (в основному режимі), або три повідомлення (в агресивному режимі);
- IKEv2 має вбудовану функціональність NAT-T, яка покращує сумісність між постачальниками;
- IKEv2 підтримує автентифікацію EAP;
- IKEv2 має параметр Keep Alive, увімкнений за замовчуванням;
- IKEv2 підтримує мобільність і протокол Multihoming Protocol (MOBIKE), що робить його більш стабільним;
- протокол мобільності та багатоцільової переадресації (MOBIKE) для IKEv2 надає можливість підтримувати сеанс VPN, коли користувач переходить з однієї IP-адреси на другу, без потреби в повторному встановленні асоціацій безпеки IKE зі шлюзом. Наприклад, користувач може встановити тунель VPN, використовуючи фіксоване з'єднання Ethernet в офісі;
- IKEv2 зменшує кількість асоціацій безпеки, потрібних для кожного тунелю, зменшуючи в такий спосіб необхідну пропускну здатність, оскільки VPN зростають і вмикають дедалі більше тунелів між кількома вузлами або шлюзами;

• IKEv2 є більш надійним, оскільки всі типи повідомлень визначаються як пари запиту та відповіді;

• IKEv2 підтримує асиметричну автентифікацію [8].

MOBIKE дає можливість користувачеві вимкнути ноутбук і перейти до безпроводової локальної мережі офісу, не переривaючи сеанс VPN. Робота MOBIKE є прозорою і не потребує жодної додаткової конфігурації від вас або розгляду з боку користувачів [9].

L2TP/IPSec або **GRE/IPSec** повільніший за інші протоколи через подвійне інкапсулювання, використовує стандартні порти, через це його може легко заблокувати інтернет-провайдер або системний адміністратор. Операційні системи мають вбудовану підтримку цієї технології, тож ставити додаткове програмне забезпечення не потрібно. У разі правильного налаштування розшифрувати дані неможливо.

Після впровадження L2TP/IPSec або GRE/IPSec надзвичайно безпечний і не має відомих вразливих місць. Передавання даних здійснюється в тунелі, що забезпечує конфіденційність.

Переваги L2TP/IPSec або GRE/IPSec:

• легке налаштування;

• вбудований у всі платформи;

• висока швидкість;

• безпечність.

Недоліки:

• повільніший за OpenVPN;

• можливість легкого блокування мережним екраном.

Протокол WireGuard

WireGuard — це надзвичайно проста, але швидка й сучасна VPN, яка використовує найновітнішу криптографію. Протокол має на меті бути швидшим, простішим, компактнішим та кориснішим, ніж IPSec, уникаючи при цьому величезної кількості всіляких труднощів. Він має намір бути значно продуктивнішим, ніж OpenVPN. WireGuard розроблено як VPN загального призначення для роботи як на вбудованих інтерфейсах, так і на суперкомп'ютерах, що підходить для будь-яких обставин. Спочатку випущений для ядра Linux, тепер він є крос-платформним (Windows, macOS, BSD, iOS, Android) і широко розгортається. Нині WireGuard активно розробляється, але вже може вважатися найбезпечнішим, легким у використанні та найпростішим вирішенням VPN у галузі.

В основі WireGuard лежить концепція під назвою Cryptokey Routing, яка працює через пов'язування відкритих ключів зі списком тунельних IP-адрес, які дозволені всередині тунелю. Кожен мережний інтерфейс має приватний ключ і список одноранговых пристроїв. Кожен одноранговий партнер має відкритий ключ. Відкриті ключі короткі та прості і застосовуються користувачами для автентифікації один одного. Їх можна передавати для використання у файлах конфігурації будь-яким позасмуговим методом, подібно до того, як можна надіслати відкритий ключ SSH другу для доступу до сервера оболонки.

WireGuard використовує такі шифри:

• ChaCha20 — для симетричного шифрування (з Poly1305 для автентифікації та використання конструкції AEAD RFC7539;

• Curve25519 — еліптична крива для безпечного обміну ключами Діффі-Хеллмана;

• BLAKE2 — для звичайного хешування та хешування з ключем;

• SipHash24 — псевдовипадкова функція пошуку розшифрованих відкритих ключів ініціатора сесії встановлення зв'язку;

• HKDF — для отримання ключів.

Окрім симетричного ключа шифрування, WireGuard також підтримує додатковий попередньо спільний ключ, який можна змішати з криптографією з відкритим ключем [10].

Під час використання WireGuard сервер VPN не відповідає клієнту, який не був авторизований, щоб зменшити ризик DoS-атак. Перше повідомлення про рукостискання, яке надсилається на сервер, також містить позначку часу TAI64N для запобігання атак повторного відтворення.

WireGuard працює лише на UDP і офіційно не підтримує TCP (хоча є обхідні шляхи, розроблені програмістами GitHub і сторонніми службами). Він може вільно використовувати будь-який порт із діапазону високих портів. За замовчуванням порт UDP– 51820.

Порівнюючи WireGuard з IPsec та OpenVPN, швидкість передавання та надійність WireGuard значно більші. Крім того, час пінгу набагато нижчий із WireGuard (0,403 мс) відповідно до OpenVPN (1,541) (рис. 7).

WireGuard не використовує повторно одноразові номери (число, яке можна використовувати в криптографічних комунікаціях). Замість цього він спирається на 64-бітовий лічильник, який не можна повернути назад. Отже, атаки повторного відтворення є меншим ризиком, а пакети UDP не виходять з ладу (щось може статися з UDP).

WireGuard простіше у складанні, ніж більшість протоколів VPN — принаймні, з відкритим вихідним кодом (OpenVPN, SoftEther, IKEv2), де видно весь код. А загальна кількість рядків коду, застосовних у WireGuard, становить майже 4000.

Переваги протоколу WireGuard:

• використовує найсучаснішу криптографію для забезпечення високої безпеки;

• має легшу базу коду, ніж OpenVPN та IPSec, що полегшує її аудит;

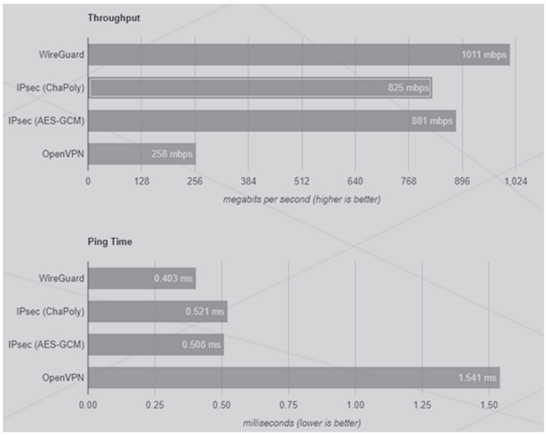

Рис. 7. Порівняння WireGuard з IPsec та OpenVPN

• пропонує дуже високі швидкості, перевершуючи майже всі протоколи на всіх платформах;

• має збільшену продуктивність, що може знизити споживання акумулятора та покращити підтримку роумінгу на мобільних пристроях;

• легкий у налаштуванні.

Його недоліки:

• WireGuard працює лише на UDP, тому ви не можете використовувати його через порт TCP 443;

• потрібно встановлювати додаткове ПЗ.

ВИСНОВКИ

Про вирішення PPTP у наш час практично не може і йтися. Хоча його легко налаштувати і він забезпечує швидке з'єднання, цей протокол пропонує дуже мало, коли йдеться про комплексну безпеку. Користувачі з підімкненням PPTP можуть бути без зусиль атаковані через численні вразливості, якими легко скористатися. Крім того, відновлення з'єднання PPTP може бути складним, особливо в нестабільних мережах. Загалом, користувачам слід уникати використання PPTP у будь-якому разі. Однак там, де платформи VPN недоступні або заборонені, застосування PPTP може бути кращим вирішенням, ніж взагалі нічого.

VPN-з'єднання L2TP/IPSec трохи повільніше, але безпечніше та надійніше, ніж PPTP. Цей протокол широко доступний на багатьох провідних платформах, і його складніше заблокувати, ніж PPTP. Крім того, використання пакета автентифікації IPSec ускладнює зловмисникам доступ до даних. Однак ефективне впровадження IPSec може бути складним, а незадовільне впровадження може призвести до зниження безпеки та частого вимикання мережі. До того ж, багато комерційних постачальників VPN повільно переходять від цього протоколу до новіших і більш просунутих протоколів, зокрема OpenVPN.

OpenVPN забезпечує швидкість і безпеку, але не є стандартною функцією в більшості операційних систем і є дещо складнішим у налаштуванні. Програму потрібно завантажити та налаштувати, а також забезпечити сумісність.

IKEv2/IPSec пропонує користувачам дивовижну швидкість, розширене шифрування та надзвичайну надійність. Однак він має відносно обмежене підтримання пристроїв і його легше заблокувати, ніж OpenVPN.

WireGuard блискавичний та дуже безпечний. WireGuard встановлює з'єднання набагато швидше, ніж інші протоколи. Але WireGuard працює тільки через UDP.

IKEv2/IPSec добре підійде для з'єднання двох маршрутизаторів типу «site to site», оскільки маршрутизатори мають підтримання даної технології апаратно і забезпечують високу швидкість передавання та шифрування, і після розриву VPN сесії між маршрутизаторами він швидко відновлюється. OpenVPN буде корисним для бізнес-користувачів, яким необхідний віддалений доступ до ресурсів компанії, що є власником конфіденціальної інформації, оскільки протокол може використовувати порт TCP 443. Це дає змогу обійти майже всі обмеження з боку міжмережного екрана.

Список використаної літератури

*1. **«Оптична пекарня»** або як інтернет потрапляє до вас у офіс — магія прокладки волоконно-оптичних кабелів [Електронний ресурс]. URL: https://gigatrans.ua/ua/news/opticheskaya-pekarnya-ili-kak-internet-popadaet-k-vam-ofis-magiya-prokladki-volokonno-opticheskih-kabeley*

*2. **Технічний** захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу [Електронний ресурс]. URL: http://www.dut.edu.ua/uploads/l_1036_36529430.pdf*

*3. **Комп'ютерні** мережі. Принципи, технології, протоколи. СПб.: Питер, 2020. 1008 с.*

*4. **Tools** released at Defcon can crack widely used PPTP encryption in under a day [Електронний ресурс]. URL: https://www.computerworld.com/article/2505117/tools-released-at-defcon-can-crack-widely-used-pptp-encryption-in-under-a-day.html*

*5. **Лужецький В. А., Кожухівський А. Д., Войтович О. П.** Основи інформаційної безпеки: навч. посіб. Вінниця: ВНТУ, 2013. 220 с.*

*6. **OpenVPN** cryptographic layer [Електронний ресурс]. URL: https://community.openvpn.net/openvpn/wiki/SecurityOverview*

*7. **Переваги** використання IPsec та IKEv2 у сучасних VPN/FW-рішеннях [Електронний ресурс]. URL:*

https://elvis.ru/upload/iblock/e78/IPsec_and_IKEv2_in_modern_vpn-fw-products.pdf

8. ***The Cisco*** *Learning Network [Електронний ресурс]. URL:*
https://learningnetwork.cisco.com/s/article/comparison-between-ikev1-and-ikev2

9. ***IKEv2*** *Mobility and Multihoming (mobike) [Електронний ресурс]. URL:*
https://datatracker.ietf.org/wg/mobike/about/

10. ***WireGuard*** *Protocol&Cryptography [Електронний ресурс]. URL:*
https://www.wireguard.com/protocol/

В. В. Харченко, О. В. Бондаренко, Н. В. Касинець, В. В. Ляшенко, А. В. Лемешко

АНАЛИЗ СУЩЕСТВУЮЩИХ VPN-РЕШЕНИЙ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ДАННЫХ

Быстрое развитие сети Интернет обусловило появление новой тенденции для построения глобальных корпоративных связей более дешевого и доступного транспорта пакетных сетей общего пользования. Но такое привлекательное и дешевое решение — передача корпоративных данных через общедоступную сеть, создает большую угрозу безопасности сети предприятия, что особенно важно для банковских информационных систем. Кроме того, для корпоративных сетей важно качество обслуживания пользователей, предоставление заданного набора услуг и гарантий, которые не всегда можно обеспечить в публичных сетях.

Ключевые слова: VPN; туннелирование; аутентификация; шифрование; OpenVPN; L2TP; IPSec; GRE; PPTP; WireGuard.

V. Kharchenko, O. Bondarenko, N. Kasynets, V. Liashenko, A. Lemeshko

ANALYSIS OF EXISTING VPN SOLUTIONS FOR ORGANIZATION OF SECURED DATA TRANSMISSION

The rapid development of the Internet has created a new trend for building global corporate connections of cheaper and affordable transport of public packet networks. But such an attractive and cheap solution — the transfer of corporate data over a public network, poses a great threat to the security of the enterprise network, which is especially important for banking information systems. In addition, for corporate networks, the quality of customer service, the provision of a given set of services and guarantees, which can't always be provided in public networks, is important.

For the help of the tunneling technique, the packets of data are transmitted through the globally accessible network, as if behind a great connection. Between the skin pair of the manager, that possessor becomes a kind of tunnel — a safer logical connection that allows you to encapsulate data from one protocol in packages of another. Tunneling allows you to organize the transmission of packets in one protocol in a logical middle, which is a different protocol. Authentication to ensure re-verification of access between nodes and allow or to block the data between them. Encryption guarantees that with limited access to information, nothing can be decrypted.

Authentication is the procedure for bringing an individual about those who won, who they think they are. Resolve authentication based on a password and based on a certificate. On the basis of the passwords user or the administrator creates a symbolic password which is saved in the database and encrypted with the correct input of the user password, it will be recognized and allowed access. On the basis of the certificate, we do not change passwords, but in the center of the certificate, the certificate is created and transferred to the correspondent. Call the authentication on the basis of the certificate of victorious great enterprises of that corporation.

Encryption - the purpose of ensuring the confidentiality of data that is stored in the computer's memory, or is transmitted over wired and wireless networks [3].

Also, tunneling, authentication and encryption secure the transfer of data between two nodes, modulating the local network robot.

Keywords: VPN; tunneling; authentication; encryption; OpenVPN; L2TP; IPSec; GRE; PPTP; WireGuard.