КОНФІГУРАЦІЯ VPN ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ ДАНИХ

Богдан Цибуляк
Львівський державний університет безпеки життєдіяльності,
вул. Клепарівська, 35, м. Львів, 79007, Україна, bohdan_ts@yahoo.com

За останні десятиліття світ став свідком інтенсивного розвитку Інтернету та передачі даних. Цілком очевидно, що такий прогрес, підтриманий безпрецедентним розвитком технологій, не буде припинятися і надалі. Спостерігається не просто щоденне, чи навіть щогодинне збільшення чисельності спільноти користувачів Інтернету, але його проникнення практично у всі сфери людської діяльності, що змушує переосмислювати пріоритети в бізнесі, споживчі вимоги та комерційні потреби сучасного суспільства.

Значний рівень інформативності сучасного суспільства характеризується можливістю володіння певною інформацією чи знаннями. Тому забезпечення їх швидкої та безперешкодної передачі з дотриманням основних властивостей інформації: конфіденційності, цілісності, достовірності, юридичної значущості інформації, оперативності доступу до неї, а також дотримання цілісності й доступності інформаційних ресурсів і компонентів наявних систем чи мереж є актуальною проблемою сьогодення.

Захист інформації в процесі передачі по відкритих каналах зв'язку заснований на виконанні наступних основних функцій: автентифікації взаємодіючих сторін; криптографічному закритті (шифруванні) даних, що передаються; перевірці достовірності та цілісності доставленої інформації. Для цих функцій характерний взаємозв'язок "один до одного". Його реалізація заснована на застосуванні криптографічних методів захисту інформації, ефективність якої забезпечується за рахунок спільного використовування симетричних і асиметричних криптографічних систем.

Постійна потреба у безпечній та дешевій передачі даних через відносно "небезпечні" засоби загального користування, зокрема й такі, як Інтернет, дали поштовх до розробки дуже актуального нині альтернативного варіанту – використання для цієї цілі VPN (virtual private networks – віртуальних приватних мереж) [1]. Завдяки тим незаперечним перевагам, які мають сьогодні VPN, вони стали об’єктом підвищеного інтересу в колах працівників сфери інформаційних технологій. Ефективність віртуальної приватної мережі визначається ступенем захищеності інформації, що циркулює відкритими каналами зв'язку [2]. Захист даних у процесі їх передачі базується на побудові захищених віртуальних каналів зв'язку, які називають тунелями VPN.

Суть тунелювання полягає в тому, щоб "запакувати" порцію даних (разом із службовими полями) у новий "конверт". При цьому пакет протоколу нижчого рівня розміщується в полі даних пакету протоколу вищого або такого ж рівня [3]. Тунелювання саме по собі не захищає дані від несанкціонованого доступу або спотворення, але забезпечує можливість повного криптографічного захисту початкових пакетів, що інкапсулюються. Щоб забезпечити конфіденційність передачі даних, відправник шифрує початкові пакети, запаковує їх у зовнішній пакет з новим IP-заголовком і відправляє транзитною мережею (Рис. 1).

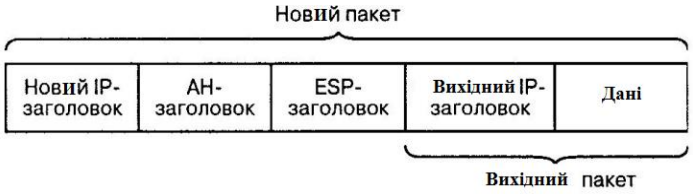

Рис. 1. Приклад пакету, підготовленого для тунелювання

Після прибуття в кінцеву точку захищеного каналу із зовнішнього пакету вилучають і розшифровують внутрішній початковий пакет і використовують його відновлений заголовок для подальшої передачі по внутрішній мережі. Тунелювання може бути використане для забезпечення не тільки конфіденційності вмісту пакету, але і його цілісності й автентичності, при цьому на всі поля пакету можна розповсюдити електронний цифровий підпис. Воно також вирішує проблеми переходів між мережами з різними протоколами, наприклад, IPv4 і IPv6, дозволяючи організувати передачу пакетів одного протоколу в логічному середовищі, що використовує інший протокол. Завдяки цьому з'являється можливість організувати взаємодію декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності й конфіденційності даних, що передаються, і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації. Для тунелювання можна використовувати протоколи канального рівня PPTP і L2TP, а також протокол мережевого рівня IPSec [4, 5].

Безпеку інформаційного обміну необхідно забезпечувати як у разі об'єднання локальних мереж, так і у разі доступу до локальних мереж виділених або мобільних користувачів. При проектуванні VPN зазвичай розглядаються дві основні схеми: захищений віртуальний канал між локальними мережами ("мережа-мережа"); захищений віртуальний канал між вузлом і локальною мережею ("користувач-мережа").

Перша схема з'єднання дозволяє замінити дорогі виділені лінії між окремими офісами і створити постійно доступні захищені канали між ними. В цьому випадку шлюз безпеки служить інтерфейсом між тунелем і локальною мережею; користувачі локальних мереж використовують тунель для спілкування один з одним. Багато компаній використовують даний вид VPN як заміну або доповнення до наявних з'єднань глобальної мережі, таких як Frame Relay.

Друга схема захищеного каналу VPN призначена для встановлення з'єднань з віддаленими або мобільними користувачами. Створення тунелю ініціює клієнт (віддалений користувач). Для зв'язку з шлюзом, що захищає віддалену мережу, він запускає на своєму комп'ютері спеціальне клієнтське програмне забезпечення. Цей вид VPN замінює собою комутовані з'єднання і може застосовуватися разом з традиційними методами віддаленого доступу.

Для забезпечення безпеки даних, що передаються у VPN, повинні бути вирішені наступні основні задачі мережевої безпеки: взаємна автентифікація абонентів при встановленні з'єднання; забезпечення конфіденційності, цілісності й автентичності інформації, що передається; авторизація та управління доступом.

У залежності від функцій мережі, які потрібні користувачам у той чи інший момент, VPN може будуватися по-різному, з використання всіх можливих рішень для забезпечення найкращого рівня захисту інформації з найменшими затратами. Перед керівниками IT-підрозділів часто постає запитання: який із протоколів обрати для оптимальної побудови такої мережі, адже кожний з підходів має як свої плюси, так і мінуси. Проведений у рамках дослідження аналіз дозволив порівняти ряд протоколів, визначити їхні переваги та недоліки та здійснити вибір найоптимальнішого рішення для побудови захищеної VPN мережі.

Порівняльний аналіз протоколів L2TP, IPSec та SSL [4-6], які претендують на розв'язання проблем безпеки в VPN показав наступне:

- переваги L2TP полягають у його незалежності від транспортного рівня, що дозволяє використовувати його в гетерогенних мережах, підтримці ОС Windows; проте через "канальну природу" даного протоколу важко гарантувати, що всі складові мережі та проміжні маршрутизатори зможуть його підтримувати;
- IPSec забезпечує автентифікацію, перевірку цілісності й шифрування повідомлень на рівні кожного пакету (з використанням протоколу IKE); VPN на його базі працюють повністю прозоро як для всіх без виключення додатків і мережевих сервісів, так і для мереж передачі даних канального рівня; робота між мережами з протоколами IPv4 і IPv6; проте необхідною є установка VPN-клієнта на робочу станцію користувача і пересилання досить великого об'єму службової інформації може істотно знизити швидкості обміну даними на низькошвидкісних каналах зв'язку;
- SSL забезпечує захист даних між сервісними протоколами (HTTP, NNTP, FTP тощо) та транспортними протоколами (TCP/IP), всі дані передаються у зашифрованому вигляді з використанням пари асиметричних ключів (публічного та приватного) для кодування/декодування інформації; протокол додатково проводить "розпізнавання" сервера та клієнта; характеризується відсутністю відчутного навантаження на сервер; замість VPN-клієнта використовується браузер, що вже є на станції.

Отже, не зважаючи на те, що IPSec цілком виправдано став основним протоколом, що забезпечує безпеку передачі даних між двома пристроями чи мережами, для гарантування безпеки інформації на канальному та мережевому рівнях одночасно доцільним є рішення використання протоколу L2TP поверх IPSec. Такий тип доступу для користувачів VPN варто використовувати у випадках повнофункціонального постійного підключення до корпоративної мережі, для забезпечення високого рівня безпеки даних керівництва компанії, між користувачем та співробітником за умови повного доступу до мережі. За умови швидкого розгортання VPN-мережі або створення тимчасового підключення (мобільний користувач, користувач з публічного комп'ютера, доступ до певних послуг тощо) з середнім рівнем безпеки даних варто застосовувати SSL протокол. Підвищення рівня безпеки у даному випадку досягається комбінуванням SSL та IPSec протоколів.

[1] Росляков А.В. Виртуальные частные сети. Основы построения и применения. Москва: Эко Трендз. (2006). 304 с.

[2] Василина А.В, Яловий М.М., Цибуляк Б.З. Захист цифрових каналів зв'язку за допомогою систем віртуальних приватних мереж. Міжнародна науково-практична конференція "Проблеми та перспективи забезпечення цивільного захисту". Збірник матеріалів. (Харків, 3-4 квітня 2013). Харків: Вид-во НУЦЗ України. (2013). С. 266-268.

[3] Построение защищенного узла доступа в интернет с применением технологии VPN и тунеллирования [Електронний ресурс]. Режим доступу: http://www.opennet.ru/docs/RUS/vpn_solution/.

[4] Bollapragada V., Mohamed Kh., Wainner S. IPSec VPN Design. Cisco Press. (2005). 384 p.

[5] IPSec – протокол защиты сетевого трафика на IP-уровне [Електронний ресурс]. Режим доступу: http://www.ixbt.com/comm/ipsecure.shtml.

[6] Что такое SSL? [Електронний ресурс]. Режим доступу: http://www.ods.com.ua/win/rus/security/ssl.html.