УДК 004.56.5

АНАЛІЗ МЕТОДІВ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ НА ОСНОВІ *VPN*-ТЕХНОЛОГІЙ

Нестеренко М.М., Саєнко Б.В., Кукліна А.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nesterenko_nik@ukr.net , saienko.bohdan@gmail.com, kuklina_anna1995@mail.ru

Analysis methods of construction corporate networks VPN-based technologies

Modern technology VPN occupy a leading position in creating a secure corporate network. The most promising technology for current time OpenVPN technology is supported by virtually all operating systems and has a robust and flexible mechanisms to organize secure tunnel.

На теперішній час, технологія *Virtual Private Network* (*VPN*) набула широкого використання, постійно вдосконалюється та являється актуальною системою інформаційної безпеки для розгортання захищених корпоративних мереж. Основним завданням при адмініструванні даного типу мереж є організація захищеного тунелю між локальними мережами віддалених філій корпорації (захищене підключення користувачів *VPN*), через загальнодоступні канали (наприклад Internet), всередині якого в передається інформація зашифрованому вигляді [1].

Розглянемо існуючі технологій організації віртуальних приватних мереж. Один з перших протоколів *VPN* – це протокол тунелювання „точка-точка” *Point-to-Point Tunneling Protocol* (*PPTP*). Однак, на даний час *PPTP* вважається недостатньо безпечним, так як використовує слабкі механізми аутентифікації, більшість *PPTP* реалізацій базується на основі протоколу *MS-CHAP*v*2* для шифрування паролів що вважається умовно надійним, не всі клієнти *PPTP* підтримують *EAP-TLS* для використання сертифікатів X.509 [2].

Технологія *IPSec* є офіційним стандартом *IEEE/IETF* для захисту *IP*-мереж та працює на рівнях 2 і 3 моделі OSI. *IPSec* може бути налаштований на використання загальних ключів або сертифікатів X.509 для захисту з’єднання *VPN*. Крім того, він використовує сертифікати X.509, одноразові паролі або протоколи (ім'я користувача/пароль) для аунтентифікації *VPN*-з’єднання. Цілісність пакетів *IPSec* забезпечується за допомогою хеш-кодів *Hash-based Message Authentication Code* (*HMAC*), умовно цифровий підпис пакетів. Одним з головних недоліків *IPSec* є те, що багато виробників реалізували власні розширення до цього стандарту, що ускладнює конфігурування (або призводить до не сумісності) мережевого обладнання різних вендорів, при встановленні *VPN*-тунелю.

Також необхідно відмітити, що однією з сучасних технологій віртуальних приватних мереж є *Secure Sockets Layer* (*SSL*), тобто захист на рівні сокетів. Вона заснована на протоколі *SSL* (криптографічний протокол, що забезпечує встановлення безпечного з’єднання між клієнтом і сервером за

рахунок асиметричного шифрування і використання сертифікатів X.509) та протокол *Transport Layer Security* (*TLS*), який усуває недоліки *SSL* та прийнятий як стандарт *RFC*. *SSL* розташований між транспортним рівнем і рівнем додатків та здійснює шифрування на рівні додатків рис. 1.

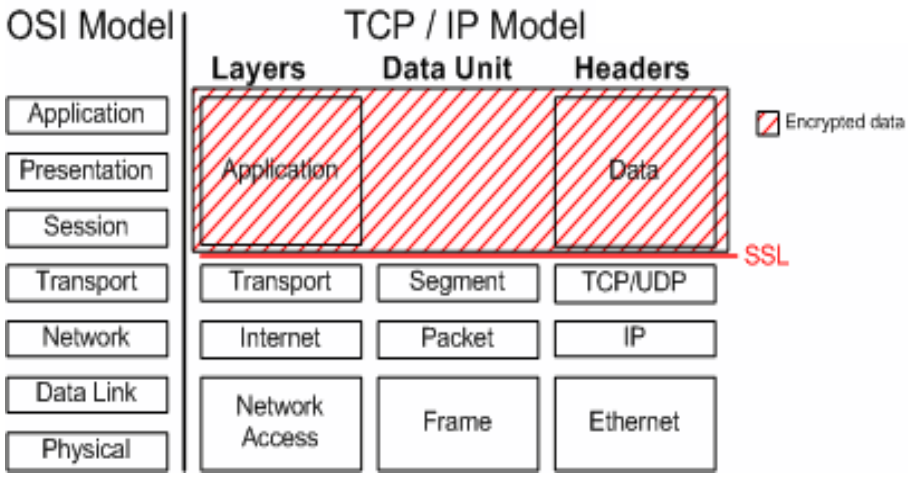

Рис. 1. Принцип роботи протоколу *SSL* та його відповідність стеку *TCP/IP*.

Але немає чітко визначеного стандарту для побудови *VPN* на основі *SSL* та більшість програмних рішень використовують протокол *SSL/TLS*, лише для захисту при встановленні з'єднання [3].

Однією з перспективних *SSL*-подібних захищених приватних мереж є технологія *Open VPN*. *OpenVPN* – інструмент з відкритим вихідним кодом, що дозволяє шифрувати *TCP* або *UDP* тунелі в мережах типу *site-to-site* та клієнт/сервер. Особливістю даної технології полягає в тому, що *OpenVPN* має власний формат для шифрування і підписування трафіку даних, а саме *HMAC* (алгоритм цифрового підпису пакету) в поєднанні з алгоритмом дайджест (або хешування) за необхідності налаштований на використання загальних (*pre-shared*) ключів, а також сертифікатів X.509. Також вона дозволяє встановлювати *VPN*-з'єднання між комп'ютерами, що знаходяться за *NAT* і мережевим екраном, без необхідності зміни їх налаштувань.

Перевага *OpenVPN* полягає в легкості інсталяції і конфігурування, надання широкого спектру алгоритмів шифрування (симетричні алгоритми: *Blowfish, DES, 3DES, AES*; сертифікати: x509; хеш-функції: *HMAC, MD5*) та аунтентифікації користувачів на основі інфраструктури відкритих ключів (*Public Key Infrastructure*) *PKI*. Це реалізовано за рахунок інтеграції *OpenSSL* до складу *OpenVPN*. Тобто для аутентифікації *VPN* вузлів перед тим як почати передавати зашифровані дані створюються ключі, здійснюється їх підпис, а також є можливість шифрування даних і тестування *SSL/TLS* з'єднань [4].

При чому на *OpenVPN* сервері один і той же порт може бути використаний для кількох тунелів. Принцип роботи *VPN*-тунелю для мережі *site-to-site* представлена на рис 2.

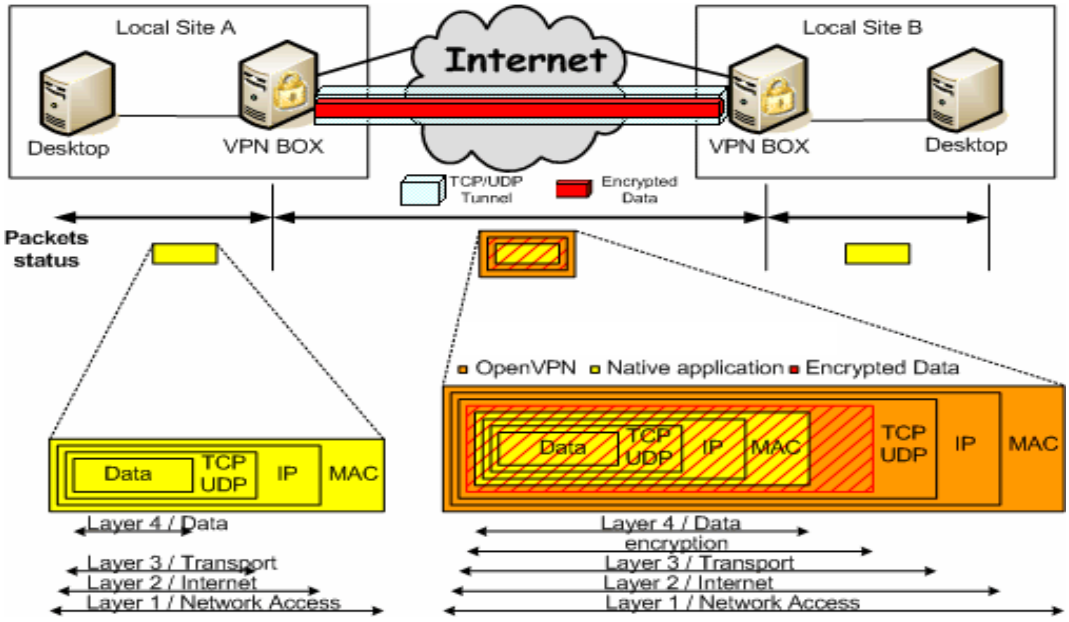

Рис. 2. Передача пакетів всередині локальної мережі і VPN.

При використанні *Open VPN* в мережі типу клієнт/сервер існує два режими: режим тунелювання і режим транспорту (*TUN/TAP*). У режимі *TUN* можливо маршрутизувати *IP*-трафік, *TAP* – можливо передавати *Ethernet*-трафік [5].

Для визначення продуктивності приватної мережі на основі *Open VPN* було здійснено оцінку пропускної спроможності каналу при використанні *VPN*-тунелю за допомогою утиліти *iperf* (рис. 3.).

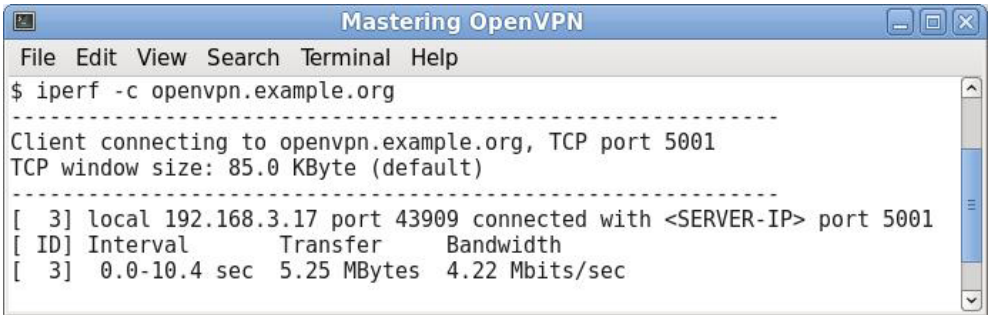

Рис. 3. Результати аналізу впливу тунелю на пропускну здатність каналу

При проведенні вимірювань при інших умовах спостерігається зниження пропускної здатності каналу приблизно 4.5%. Це пояснюється, тим що використання *VPN* вносить деякі накладні витрати для інкапсуляції, шифрування і аутентифікації (підписи) вихідних даних. Також істотний влив на ефективність роботи тунелю *OpenVPN* є апаратна платформа вузлів мережі та метод шифрування.

Література

1. Eric F Crist Jan Just Keijser Master building and integrating secure private networks using OpenVPN, 2015 341 pages.
2. https://www.schneier.com/paper-pptpv2.html.
3. Marcus Fellner OpenVPN Building and Integrating Virtual Private Networks 272 pages.
4. http://www.linuxsecurity.com/content/view/117363/49/
5. http://adsabs.harvard.edu/abs/2005SPIE.6011..138H.