УДК 004.771

ПОРІВНЯННЯ ПРОТОКОЛІВ ШИФРУВАННЯ У КОРПОРАТИВНІЙ МЕРЕЖІ

Мілєвський О.А., Міночкін Д.А.
Навчально-науковий Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: alexmillevs@gmail.com

COMPARISON OF ENCRYPTION PROCEDURES IN THE CORPORATE NETWORK

Due to the pandemic and the war, more and more people in the world are moving to a remote work format. The general principle of the process of connecting between remote computers is analyzed, comparable types of encryption are used in both small businesses and corporations.

У зв’язку з пандемією та війною у світі усе більше людей переходить до формату віддаленої праці. Проаналізовано загальний принцип роботи процесу з’єднання між віддаленими комп’ютерами, порівняні типи шифрування які використовують як в малому бізнесі, так і в корпораціях.

Етапи RDP з'єднання:

- установка з'єднання,
- узгодження параметрів шифрування,
- аутентифікація серверів,
- узгодження параметрів RDP сесії,
- аутентифікація клієнта,
- дані RDP сесії,
- розрив RDP сесії.

У корпоративній мережі найчастіше використовують такі типи шифрування як:

- SSTP,
- IPSec,
- L2TP/IPSec.

SSL (Secure Socket Layer) – протокол захищених сокетів, що забезпечує безпечну передачу даних через Інтернет. Під час його використання створюється захищене з'єднання між клієнтом та сервером.

Internet Protocol Security (IPsec) - це набір протоколів для забезпечення захисту даних, що передаються IP-мережею. На відміну від SSL, який працює на прикладному рівні, IPsec працює на мережному рівні і може використовуватися нативно з багатьма операційними системами, що дозволяє використовувати його без сторонніх додатків.

L2TP або Layer 2 - це протокол тунелювання, який є розширенням протоколу PPP та поєднує найкращі функції двох інших протоколів тунелювання PPTP та L2F. Протокол L2TP, хоч і використовується для VPN з'єднань, сам по собі не може забезпечити конфіденційність або аутентифікація, тому часто застосовується разом з протоколом IPSec, який

забезпечує захищене з'єднання. Комбінація цих двох протоколів відома як L2TP/IPsec.

За приклад було взято розроблену авторську структурну схему корпоративної мережі.(рис.1).

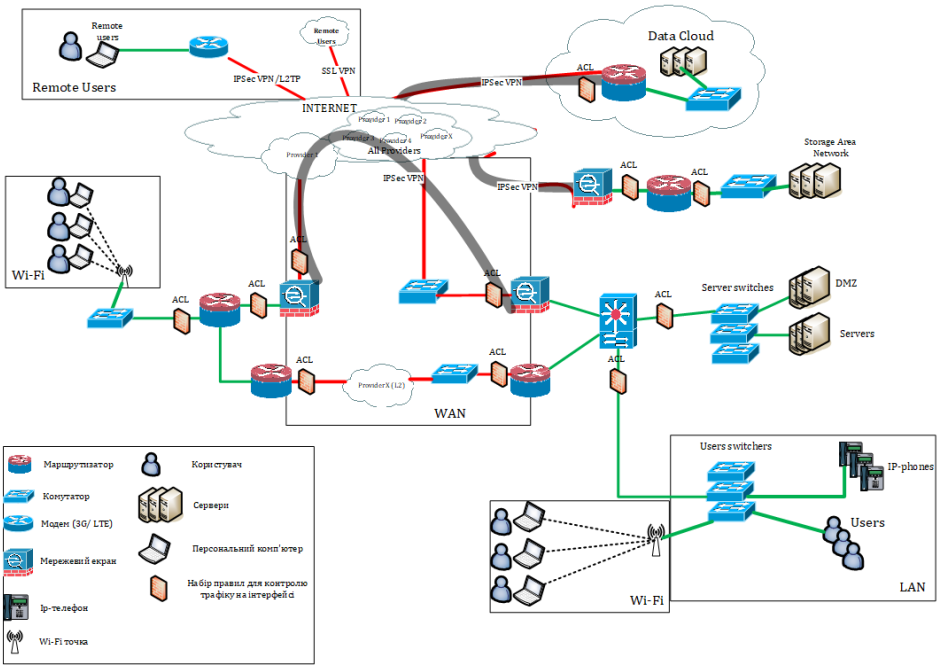

Рис.1. Структурна схема корпоративної мережі.

Таблиця 1. Порівняння протоколів шифрування.

	SSTP	**IPSec**	**L2TP/IPSec**
Компанія-розробник	Microsoft	група IP Security Protocol IETF	L2TP – спільна розробка Cisco та Microsoft, IPsec – The Internet Engineering Task Force
Розгортання	Windows. Працює з коробки, не вимагаючи установки додаткового ПЗ	Windows 7+, macOS 10.11+ та більшість мобільних ОС мають вбудовану підтримку	Windows, Mac OS X, Linux, iOS, Android. Багато ОС (включно з Windows 2000/XP+, Mac OS 10.3+) мають вбудовану підтримку, немає необхідності ставити додаткове ПЗ
Шифрування	SSL (шифруються всі частини, крім TCP- та SSL-заголовків)	Протокол AH (Authentication Header) та ESP (Encapsulated Security Payload)	3DES(Triple DES) або AES(Advanced Encryption Standard)

Таблиця 1 (продовження). Порівняння протоколів шифрування.

	SSTP	IPSec	L2TP/IPSec
Порти	TCP-порт 443	Чистий ipsec жодних портів не використовує. Він використовує протоколи. Порти використовують розширення ipsec на зразок IKE. Стандартні IKE-демони використовують udp/500.	UDP-порт 500 для первинного обміну ключами та UDP-порт 1701 для початкової конфігурації L2TP, UDP-порт 5500 для обходу NAT
Недоліки безпеки	Серйозних недоліків безпеки не було виявлено	Серйозних недоліків безпеки не було виявлено	3DES вразливий для Meet-in-the-middle та Sweet32, але AES не має відомих вразливостей.

У сьогоднішньому світі витоків даних і зламів, як ніколи важливо вжити заходів для забезпечення вашої безпеки в Інтернеті. Більшість збереження конфіденційності в Інтернеті полягає в тому, щоб ваші дані проходили безпечними каналами.

В роботі показано, що деякі протоколи застаріли, в той час, як інші все ще розвиваються. Намагаючись порівняти різні VPN-рішення, доступні на ринку, обов'язково вивчіть технології та протоколи, які використовує кожне з них, та шукайте інструмент VPN, який поєднує в собі швидкість, надійність та безпеку.

Література

1. Which Is the Best VPN Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpipsec-vs.-sstp/.
2. VPN Protocols [Електронний ресурс] – Режим доступу до ресурсу: https://blog.flashrouters.com/2021/08/30/vpn-protocols-from-l2tp-to-wireguard-to-openvpn-to-lightway/.
3. Олифер В. Г. Компьютерные сети [Принципы, технологии, протоколы. 5-е издание] [Електронний ресурс] / В. Г. Олифер, Н. А. Олифер – Режим доступу до ресурсу: https://www.rulit.me/books/kompyuternye-seti-principy-tehnologii-protokoly-5-e-izdanie-get-475363.html.