УДК 005.95/.96

І. П. Кулібабчук
А. О. Азарова

ПОРІВНЯННЯ МОЖЛИВОСТЕЙ ТА ПРОДУКТИВНОСТІ VPN-ПРОТОКОЛІВ

Вінницький національний технічний університет

Анотація

Досліджено доцільність використання різних VPN-протоколів у корпоративній мережі IT-компанії. Здійснено порівняльну характеристику певних протоколів та вивчено їх взаємодію між собою у мережі підприємства. Розроблено модель застосування на пристроях CISCO та pfSense ПЗ.

Ключові слова: VPN, CISCO, Pfsense, корпоративна мережа.

Abstract

The expediency of using different VPN protocols in the corporate network of an IT company has been studied. The comparative characteristics of certain protocols are carried out and their interaction with each other in the enterprise network is studied. An application model has been developed on CISCO and pfSense software devices.

Keywords: VPN, CISCO, pfSense, corporate network.

Вступ

Проблематика захисту інформації та передавання її у шифрованому вигляді залишається актуальною для ведення будь-якого бізнесу, особливо IT. Відомо, що існують багато рекомендацій про налаштування корпоративної мережі, але кожен випадок унікальний і залежить від масштабів підприємства.

Отже, метою дослідження є порівняння та оцінювання доцільності використання певних VPN-протоколів порівняно з іншими під час побудови корпоративної мережі.

Результати дослідження

Сценарії використання VPN можуть бути різними, найпопулярніші серед них такі:

– побудова захищеного каналу між двома або більше віддаленими сегментами мережі (наприклад, між офісами у Києві та Львові);

– підключення віддаленого працівника до корпоративної мережі;

– віртуальна зміна розташування за допомогою послуг VPN Providers (вимагає найменших витрат часу для налаштування, проте весь трафік відбувається засобами «чужого» сервера).

Для реалізації цих сценаріїв існують різні види протоколів VPN – для зв'язку, для шифрування трафіку та ін. Отже, на підставі відповідного протоколу можна проєктувати своє рішення.

Найчастіше застосовуваними для вирішення задач дослідження є два протоколи — OpenVPN і IPSec, також нещодавно з'явився протокол WireGuard, який став неоднозначним щодо доцільності застосування. Є й інші альтернативи, які вже застарілі, але цілком здатні вирішувати певні завдання. Перевага того чи іншого протоколу VPN залежить від низки чинників та умов використання. Розглянемо основні з них:

– пристрої – різні пристрої підтримують різні протоколи;

– мережа – якщо певні послуги не доступні у вашій локації, деякі протоколи можуть не підійти;

– продуктивність – деякі протоколи мають більшу продуктивність, особливо на мобільних пристроях, інші – зручніші для використання у великих мережах.

– модель загроз – деякі протоколи менш безпечні, ніж інші, тому зловмисники можуть впливати на них по-різному.

Розглянемо більш детально базові протоколи та порівняємо їх за вище викладеними критеріями.

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 з багатьма операційними системами, що дозволяє застосовувати його без сторонніх програм (на відміну від OpenVPN).

Internet Key Exchange version 2 (IKEv2) є протоколом IPsec, що використовується для виконання взаємної аутентифікації, створення та обслуговування Security Associations (SA), стандартизований у RFC 7296. Він є захищеним, як і L2TP, що може говорити про їх однаковий рівень безпеки. IKEv2 було розроблено Microsoft спільно з Cisco, існують реалізації протоколу з відкритим вихідним кодом (наприклад, OpenIKEv2, Openswan та strongSwan).

Завдяки підтримці Mobility and Multi-homing Protocol (MOBIKE) IKEv2 є дуже стійким до зміни мереж. Це робить IKEv2 отимальним вибором для користувачів смартфонів, які регулярно перемикаються між домашнім Wi-Fi та мобільним з'єднанням або переміщуються між точками доступу. IKEv2/IPsec може використовувати низку різних криптографічних алгоритмів, включаючи AES, Blowfish та Camellia, у тому числі з 256-бітними ключами. IKEv2 підтримує Perfect Forward Secrecy. У багатьох випадках IKEv2 є швидшим за OpenVPN, оскільки є менш ресурсоємний. За критерієм продуктивності IKEv2 є найкращим варіантом для мобільних користувачів, тому що він добре встановлює з'єднання. IKEv2 підтримується ОС Windows 7+, Mac OS 10.11+, iOS, а також деякими Android-пристроями.

OpenVPN — це універсальний протокол VPN із відкритим вихідним кодом, розроблений компанією OpenVPN Technologies. Він є найпопулярнішим протоколом VPN. Як відкритий стандарт, він пройшов не одну незалежну експертизу безпеки.

Для роботи OpenVPN потрібне спеціальне клієнтське програмне забезпечення. Більшість сервісів VPN створюють свої програми для роботи з OpenVPN, які можна використовувати в різних операційних системах та пристроях. Протокол може працювати на будь-якому з портів TCP та UPD і може використовуватися на всіх основних платформах: Windows, Mac OS, Linux, Apple iOS, Android через сторонніх клієнтів.

Найновішим є протокол VPN WireGuard. Позиціонується розробниками як заміна IPsec і OpenVPN для більшості випадків їх використання. Він є більш безпечним, продуктивним і простим у використанні.

Код WireGuard виглядає набагато скромніше і простіше, ніж код OpenVPN, внаслідок чого його простіше досліджувати на вразливості (4 тисяч рядків коду проти кількох сотень тисяч). Також багато хто зазначає, що його набагато легше розгорнути та налаштувати.

Розглянемо переваги та недоліки протоколів, що надано у табл. [1 – 3].

Аналіз вищевикладених переваг та недоліків описаних протоколів дозволяє дійти висновку, що для корпоративної мережі з пристроями CISCO та Pfsense ПЗ, розгорнутому на відповідній платформі, доцільно використовувати два VPN-протоколи: OpenVPN та IKEv2/IPsec.

CISCO роутери можна використовувати для маршрутизації трафіку між філіалами компанії, таке з’єднання називається SITE-TO-SITE. Це забезпечує високу швидкість оброблення та передавання даних між офісами та їх надійний захист.

Завдяки PFsense ПЗ можна створити з потужного сервера надійний firewall з можливістю підключення на його основі до корпоративної мережі ззовні співробітників із застосуванням протоколу OpenVPN, який є дуже зручним для швидкого налаштування мобільного додатку OpenVPN на пристрої співробтника. Підключення відбувається завдяки імпорту профіля налаштування. Крім того, підключення між сервером та клієнтом OpenVPN можна робити на основі pre-shared key. OpenVPN має багато можливостей налаштування під різні потреби користувача.

Нещодавно було представлено WireGuard 1.0.0, який засвідчив собою постачання компонентів WireGuard в основному складі ядра Linux 5.6.

Включений до складу ядра Linux, код пройшов додатковий аудит безпеки, виконаний незалежною фірмою, який не виявив жодних проблем.

Досвід у застосуванні та дослідження безпеки на основі такого протоколу дозволять довести доцільність використання WireGuard порівняно з IPsec та OpenVPN.

Висновки

VPN настільки поширена технологія, що давно вже ввійшла до користувацького сегмента. Вона надійна, захищена потужними криптографічними протоколами шифрування. У цьому полягає головне питання захищеності створених підключень на базі цієї технології. Адже стійкість визначається саме криптографічним алгоритмом, оскільки зламаний шифр свідчить про велику вразливість віртуальних приватних мереж.

Таблиця – Порівняльна характеристика VPN-протоколів

Критерії порівняння	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Компанія-розробник	Microsoft	Microsoft	L2TP – спільна розробка Cisco та Microsoft, IPsec – The Internet Engineering Task Force	IKEv2 – спільна розробка Cisco та Microsoft, IPsec – The Internet Engineering Task Force	OpenVPN Technologies	Jason A. Donenfeld
Ліцензія	Proprietary	Proprietary	Proprietary	Proprietary	GNU GPL	GNU GPL
Розгортання	Windows, MacOS, iOS, деякий час GNU/Linux. Працює з коробки, не вимагаючи установки додаткового ПЗ	Windows. Працює з коробки, не вимагаючи установки додаткового ПЗ	Windows, Mac OS X, Linux, iOS, Android. Багато ОС (включно з Windows 2000/XP+, Mac OS 10.3+) мають вбудовану підтримку	Windows 7+, macOS 10.11+ та більшість мобільних ОС мають вбудовану підтримку	Windows, Mac OS, GNU/Linux, Apple iOS, Android та маршрутизатори. Необхідна установка спеціалізованого ПЗ, що підтримує роботу з цим протоколом	Windows, Mac OS, GNU/Linux, Apple iOS, Android.
Шифрування	Використовує Microsoft Point-to-Point Encryption (MPPE), який реалізує RSA RC4 з максимум 128-розрядними сеансовими ключами	SSL (шифруються всі частини, крім TCP- та SSL-заголовків)	3DES або AES	Реалізує велику кількість криптографічних алгоритмів, включаючи AES, Blowfish, Camellia	Використовує бібліотеку OpenSSL (реалізує більшість популярних криптографічних стандартів)	Обмін ключами по 1-RTT, Curve25519 для ECDH, RFC7539 для ChaCha20 та Poly1305 для автентифікаційного шифрування, та BLAKE2s для хешування
Порти	TCP-порт 1723	TCP-порт 443	UDP-порт 500 для первонач. обміну ключами та UDP-порт 1701	UDP-порт 500 для первинного обміну ключами, а UDP-порт 4500 для обходу NAT	Будь-який UDP- або TCP-порт	Будь-який UDP-порт
Недоліки безпеки	Має серйозні вразливості. MSCHAP-v2 вразливий для атаки за словником, а алгоритм RC4 піддається атаці Bit-flipping	Серйозних недоліків безпеки не було виявлено	3DES вразливий для Meet-in-the-middle та Sweet32, але AES не має відомих вразливостей. Проте є думка, що стандарт IPsec	Не вдалося знайти інформації про наявні недоліки безпеки, крім інциденту з витоком доповідей АНБ щодо IPsec	Серйозних недоліків безпеки не було виявлено	Серйозних недоліків безпеки не було виявлено

СПИСОК ЛІТЕРАТУРИ

1. Кузнецов О. О., Мордвинов Р. І., Колованова Є. П., Самойлова А. В. Методика статистичного тестування криптографічних алгоритмів. *Спеціальні телекомунікаційні системи та захист інформації*. Київ. 2014. №1(25). С.54 – 61.
2. Горбенко Ю. І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За заг. ред. д.т.н., професора І.Д. Горбенка / Ю.І. Горбенко. Харків : Видавництво «Форт», 2016. 960 с.
3. Attacks On Cryptosystems. 2015. URL : https://www.tutorialspoint.com/cryptography/attacks_on_cryptosystems.html (Дата звернення 10.04.22 р.)

Кулібабчук Іван Павлович – студент групи КІТС-18б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: ivanp8577gmail.com.

Kulibabchuk Ivan P. – Department of Management and security information systems, Vinnytsia National Technical University, Vinnytsia, e-mail : ivanp8577@gmail.com.

Азарова Анжеліка Олексіївна – к.т.н., професор кафедри МБІС Вінницького національного технічного університету, м. Вінниця.

Azarova Anzhelika O. **–** PhD in technique, Professor of Management and security information systems department of Vinnytsia National Technical University, Vinnytsia.