УДК 004.72

І.А. Юзьків, І.О. Боднарчук канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПОРІВНЯЛЬНИЙ ОГЛЯД РЕАЛІЗАЦІЙ ТЕХНОЛОГІЇ VPN

I.A. Yuzkiv, I. O. Bodnarchuk Ph.D, Assoc. Prof.,

COMPARATIVE OVERVIEW OF VPN TECHNOLOGY IMPLEMENTATION

В галузі телекомунікацій спостерігається підвищена увага до віртуальних приватних мереж (Virtual Private Network – VPN). VPN – узагальнена назва технологій, що забезпечують одне або багато мережених з'єднань (логічну мережу) поверх іншої мережі з меншою довірою, наприклад Інтернет [1]. На даний час існує значна кількість реалізацій даних технологій, кожна з яких має свої переваги та недоліки. Крім цього існує багато застосувань VPN починаючи від окремих користувачів і аж до великих корпорацій. Тому питання порівняння реалізацій технології VPN є актуальним. VPN повинна вирішувати ряд завдань, пов'язаних з необхідністю аутентифікації користувачів та перевіркою джерел даних для захисту мережі від попадання до неї несанкціонованих вузлів та пакетів. З цією метою реалізовується маркування вузлів віртуальної мережі та відповідна адресація пакетів, призначених конкретним клієнтам. Також необхідно забезпечити ефективне, але не надто вимогливе до обчислювальних ресурсів, шифрування в реальному часі, а також повне блокування передачі будь-яких даних у відкритому вигляді. Для виконання цих завдань технологіями VPN використовуються різні протоколи та інструментальні засоби, а якість їх поєднання дозволяє виробити критерії оцінки ефективності певної реалізації. До цих критеріїв відносять показники безпеки, швидкодії та надійності роботи, а також мультиплатформенність і доступність [2].

Розглянемо основні реалізації:

- Протокол тунелювання точка-точка PPTP достатньо простий і стабільний, але не надто стійкий для сучасних інформаційних загроз.
- Протокол IPsec працює з великою кількість методів аутентифікації та алгоритмів шифрування для VPN і є базовою реалізацією для багатьох VPN.
- Протокол тунелювання другого рівня L2TP разом з IPsec має вискоий рівень безпеки і сумісний з багатьма ОС, але вимагає додаткового налаштування певних файєрволів на використання ним специфічних протоколів (UDP 1701, UDP 4500, UDP 500). Даний тунель має дещо сповільнену швидкодію, оскільки необхідно здійснювати подвійну інкапсуляцію.
- Протокол безпечного тунелювання SSTP легко налаштовується, має високі показники безпеки та достатньо стабільний, але надто прив'язаний до систем на базі рішень Microsoft. На інших платформах цей протокол є менш функціональним.
- Відкрита реалізація VPN – OpenVPN, яка забезпечує високу безпеку великим вибором інструментів шифрування (AES, Blowfish, Camelia, 3DES, CAST та ні.). Швидкодія залежить від вибраного алгоритму, та як правило більша ніж в L2TP/IPsec.

Отже, для задач об'єднання віддалених офісів малого та середнього масштабу доцільно використовувати OpenVPN, що забезпечить необхідний рівень безпеки даних на різних платформах.

Література.

1. VPN // [Електронний ресурс] – Режим доступу: URL: https://uk.wikipedia.org/wiki/VPN.
2. Protocol Compatibility // [Електронний ресурс] – Режим доступу: URL: https://openvpn.net/index.php/open-source/documentation/miscellaneous/protocol-compatibility.html