УДК 004

АНАЛІЗ ПРОБЛЕМ ПРИ ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ МІЖ ПРИВАТНИМИ МЕРЕЖАМИ

Кудінов Є.О.

Харківський національний автомобільно-дорожній університет, Харків

Надійний зв'язок між окремими сегментами мережі через інтернет завжди був важливим як для приватних осіб, так і для організацій. Такі сегменти можуть бути розкидані по всьому світу. Незалежно від того, яким чином і де вони були організовані, чи локально в якомусь офісі, чи на обладнанні якогось хмарного провайдера, їх потрібно зв'язати надійним захищеним тунелем, виходячи з своїх потреб та ресурсів.

На даний час для зв'язку між сегментами мережі існує величезна кількість апаратних маршрутизаторів (роутерів) з підтримкою сервера та клієнта віртуальних приватних мереж (VPN). А також, програмні у ролі яких зазвичай виступають операційні системи (Microsoft Windows, Linux, *BSD) з встановленими або налаштованими засобами тунелювання та маршрутизації. Наприклад, Kerio Control для Windows. Апаратні маршрутизатори виробляються безліччю фірм, наприклад, Cisco , Mikrotik , Juniper та інші.

Вибір того або іншого маршрутизатора здійснюється виходячи з того, якими протоколами ми будемо користуватися для створення тунелю, необхідної продуктивності, а також вартості обладнання.

Одним з варіантів організації тунелю є IPsec . IPsec (IP Security) – це набір протоколів для забезпечення захисту даних, що передаються міжмережевим протоколом IP. Він дозволяє здійснювати підтвердження автентичності (автентифікацію), перевірку цілісності та/або шифрування IP-пакетів. IPsec також включає протоколи для захищеного обміну ключами в інтернеті. Завдяки тому, що ipsec розташовується на мережному рівні моделі OSI , він дуже гнучкий і може захищати будь-які протоколи, що базуються на IP , наприклад, TCP і UDP [1].

Але у нього є і недоліки. Для роботи ipsec повинні бути доступні UDP порти 500, 4500, а також як мінімум протокол ESP (він може виконувати функції AH). Кінцеві та проміжні інтернет-провайдери можуть заблокувати будь-який з цих портів і протоколів випадково або маючи намір. У моїй практиці найчастіше це відбувалося під час заміни магістральних маршрутизаторів у проміжних провайдерів. Також ipsec чутливий до маршрутизації пакетів. Якщо від одного маршрутизатора до іншого пакети йдуть по одному маршруту, а повертаються по іншому маршруту, то ipsec тунель не встановиться. Вимагає білу ip -адресу з кожної сторони з'єднання. Однак, не дивлячись на наведений недолік, ipsec є швидким і достатньо безпечним варіантом зв'язку, що має підтримку практично в будь-якому апаратному або програмному маршрутизаторі, а також у всіх популярних операційних системах. Також, зазвичай, апаратний роутер має так звану «апаратну» підтримку цього протоколу у вигляді спеціальних інструкцій у процесорі, що дозволяє значно підвищити швидкість.

Протокол тунелювання L2TP забезпечує лише тунелювання , тобто групування даних у пакети для їх конфіденційної передачі через загальнодоступні мережі. Для шифрування та конфіденційності він використовує ipsec , за допомогою якого «домовляється» про використання певних інструментів захисту та шифрування даних. Після цього пристрої на обох кінцях каналу зв'язку, використовуючи ESP, пізнають один одного. І вже потім L2TP встановлює тунель . В результаті відбувається подвійна інкапсуляція пакетів, через що страждає швидкість [2]. Всі недоліки та переваги ті ж самі як у ipsec . L2TP використовує для роботи порт UDP 1701, але в поєднанні з ipsec його не потрібно додатково відкривати для зовнішнього доступу, так як він застосовується всередині шифрованого каналу зв'язку.

SSTP (Secure Socket Tunneling Protocol) – VPN протокол прикладного рівня, заснований на SSL. Завдяки цьому дані шифруються. Аутентифікація здійснюється за допомогою PPP та SSL . З'єднання зазвичай проходить по 443 порту TCP , але порт можна змінити. Все шифрування даних здійснюється протоколом SSL. Усі пакети протоколів SSTP, PPP і вище передаються лише у зашифрованому вигляді[4].

Так як цей протокол був створений у компанії Microsoft , її операційні системи мають повну підтримку SSTP починаючи з Windows Vista SP 1 та Windows Server

2008. Переважно він був розрахований для роботи в Windows, але сьогодні має підтримку для Linux , RouterOS . Клієнт SSTP існує для більшого списку операційних систем. SSTP показує добру продуктивність, на нього не впливають на налаштування NAT. Провайдери зазвичай не блокують 443 TCP порт, тому ви можете без проблем з'єднатися з сервером VPN. Рівень безпеки досить високий. З мінусів, з погляду підбору маршрутизатора, для доброї швидкості вимагає продуктивного апаратного забезпечення.

Одним із варіантів SSL VPN є OpenVPN. Для шифрування керуючого каналу та потоку даних OpenVPN використовує бібліотеку OpenSSL. Завдяки цьому це дозволяє використовувати всі алгоритми шифрування доступні у цій бібліотеці. На сьогоднішній день OpenVPN має підтримку у всіх популярних операційних системах, таких як Solaris , OpenBSD , FreeBSD , NetBSD , GNU/ Linux , macOS , QNX, Microsoft Windows , Android , iOS. OpenVPN може використовувати як TCP, так і UDP протоколи. Офіційно порт 1194(TCP,UDP) виділено організацією IANA для роботи цієї програми, але у реальному сценарії використання його часто змінюють [5]. Зазвичай переважним є UDP з тієї причини, що показує більшу швидкість у звичайних обставинах. Через тунель проходить трафік мережного рівня і вище з OSI, якщо використовується TUN-з'єднання, або трафік канального рівня і вище, якщо використовується TAP . TAP використовується для передачі кадрів Ethernet та для мостового з'єднання, а TUN використовується для передачі IP-пакетів (маршрутизація). OpenVPN є швидким та надійним рішенням, але, у разі апаратного маршрутизатора, швидкість залежить від потужності заліза та реалізації самого OpenVPN.

Одним з найшвидших поширених протоколів є WireGuard. Це комунікаційний протокол та безкоштовне програмне забезпечення з відкритим вихідним кодом, який реалізує зашифровані VPN. Він був розроблений для простого використання VPN , високої продуктивності та низькою кількістю можливих уразливих місць. Він має більш високу продуктивність ніж OpenVPN і набагато вищу ніж ipsec . Також WireGuard використовує стійкі ключі шифрування - Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF [6]. На даний момент підтримка цього VPN протоколу

реалізована в Microsoft Windows , Linux , Android , IOS , RouterOS , pfSence , OpenBSD , FreeBSD , NetBSD та інших. На жаль, якщо інтернет-провайдер блокує UDP -трафік, WireGuard працювати не буде, оскільки функціонує тільки за протоколом UDP . Також він підтримує лише третій рівень мережевої моделі OSI (маршрутизація).

Протокол PPTP - тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартної, незахищеної мережі [3]. На даний момент він застарів і є небезпечним, хоч і підтримується більшістю маршрутизаторів та операційних систем. Але, наприклад, компанія Apple відмовилася від його підтримки у своїх мобільних телефонах та планшетах.

Після розгляду всього вище переліченого, можна сказати, що немає єдиного сценарію зв'язку між приватними сегментами мережи. У більшості випадків доводиться враховувати обставини: можливість використовування певних протоколів та портів для зв'язку через мережи провайдерів, виділений бюджет на придбання роутерів та їх фунціонал для зв'язку між собою. Наведу підсумкову порівняльну таблицю швидкості та шифрування VPN без урахування зовнішніх факторів (Табл. 1).

Таблиця 1 – Порівняння протоколів тунелювання

	IPsec	L2TP/IPsec	PPTP	SSTP	OpenVPN	Wireguard
Швидкість	++	+	++	++*	+++*	++++
Шифрування	+	+	-	+	++	++

*- істотно залежить від реалізації та можливостей «заліза» апаратних маршрутизаторів

Література:

1. Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2005). Guide to IPsec VPNs:.
2. Patel, B., Aboba, B., Dixon, W., Zorn, G., & Booth, S. (2001). *Securing L2TP using IPsec* (No. rfc3193).
3. Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., & Zorn, G. (1999). *Point-to-point tunneling protocol (PPTP)* (No. rfc2637).

4. Rajamohan, P. (2014). An overview of remote access VPNs: Architecture and efficient installation. *Ipasj International Journal of Information Technology (Iijit)*.
5. Crist, E. F., & Keijser, J. J. (2015). *Mastering OpenVPN*. Packt Publishing Ltd.
6. Donenfeld, J. A. (2017, February). Wireguard: next generation kernel network tunnel. In *NDSS* (pp. 1-12).