УДК 004.7

Афанасьєв Д.С.
*Черкаський державний технологічний університет*

# Особливості застосування технології VPN

Віртуальна приватна мережа або просто VPN (Virtual Private Network) – це технологія, при якій відбувається обмін інформацією з віддаленою локальною мережею по віртуальному каналу через мережу загального користування з імітацією приватного підключення «Точка-точка» або «сервер-клієнт». Передана по цьому віртуальному каналу інформація зазвичай шифрується. Існує велика кількість варіантів програмного забезпечення, що дозволяє створювати віртуальні приватні мережі. Розглянемо один з варіантів – пакет «OpenVPN». «OpenVPN» - вільно поширювана програма для створення віртуальних приватних мереж (VPN). ПЗ «OpenVPN» передає дані по мережі за допомогою протоколів UDP або TCP із застосуванням драйвера TUN / TAP. Протокол UDP і драйвер TUN дозволяє підключатися до сервера «OpenVPN» клієнтам, розташованим за NAT (від англ. Network Address Translation — перетворення (трансляція) мережних адрес) – це механізм зміни мережної адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший.

Для «OpenVPN» можна вибрати довільний порт, що дозволяє долати обмеження брандмауера, через який здійснюється доступ з локальної мережі в Інтернет (якщо такі обмеження встановлені). Безпека і шифрування в «OpenVPN» забезпечується бібліотекою «OpenSSL» і протоколом транспортного рівня Transport Layer Security (TLS). Замість «OpenSSL» в нових версіях «OpenVPN» можна використовувати бібліотеку «PolarSSL». Протокол TLS – це засіб оптимізації протоколу захищеної передачі даних рівня захищених сокетів Secure Socket Layers (SSL). В «OpenSSL» може використовуватися симетрична і асиметрична криптографія. У першому випадку перед початком передачі даних на всі вузли мережі необхідно помістити однаковий секретний ключ. При цьому виникає проблема безпечної передачі цього ключа через небезпечний Інтернет. У другому випадку у кожного учасника обміну даними є два ключі - публічний (відкритий) і приватний (секретний). Для безпечної передачі даних необхідно ідентифікувати сторони, що беруть участь в обміні даними. В іншому випадку можна стати жертвою так званої "атаки посередника" (Man in the Middle, MITM). В ході такої атаки зловмисник підключається до каналу передачі даних і прослуховує його. Він також може втручатися, видаляти або змінювати дані. Щоб забезпечити аутентифікацію, протокол TLS використовує інфраструктуру публічних ключів (Public Key Infrastructure, PKI) і асиметричну криптографію. Віртуальна приватна мережа, побудована з використанням «OpenVPN», являє собою зашифрований канал зв'язку типу «точка-точка» або кілька зашифрованих каналів зв'язку між сервером і декількома клієнтами, що називається «сервер-клієнт» [1,2,3].

Основні переваги «OpenVPN»:

- Підтримка різноманітних операційних систем (Linux, FreeBSD, Windows, Solaris, Mac OS X, NetBSD і т.п.). Існує версія, портована на Windows Mobile.

- Робота за довільними TCP / UDP портами, а також через HTTP проксі-сервер. Доцільно використовувати, якщо існують обмеження по протоколам і портам, але також це вносить невелику кількість надлишкової інформації за рахунок заголовків TCP або UDP. На відміну від протоколу PPTP, використовується лише один виклик для передачі даних і керуючих команд. Рекомендується використовувати протокол

UDP, якщо це можливо.

- Підтримка різних режимів захисту каналу зв'язку (за загальним ключем - підтримує тільки канали точка-точка, простіше в налаштуванні, або за сертифікатом - підтримує підключення декількох клієнтів до сервера, складніше в налаштуванні), а також алгоритму шифрування. У режимі точка-точка шифрування може відключатися.

Приклад мереж, в яких може бути використана технологія «OpenVPN».

У розглянутому прикладі технологія VPN використовується для віддаленого доступу до ресурсів усередині мережі, а також для підключення дло Інтернету. Вона використовується для рішення трьох задач:

1. Доступ до файлів та інших ресурсів усередині локальної мережі, до якої підключений VPN-сервер.

2. Підключення до Інтернету через локальну мережу провайдера (вигідно, якщо трафік локальної мережі не тарифікується або коштує дешевше, ніж Інтернет-трафік). Потрібно, щоб сервер був підключений до локальної мережі того ж провайдера, що і клієнт. Може використовуватися з різними технологіями підключення, включаючи Ethernet, Wi-Fi і GPRS / EDGE / 3G.

3. Крім цього, можна знайти велику кількість застосувань для технології VPN, включаючи доступ до Інтернету на стороні провайдера, гра через Інтернету в локальній мережі, заміна зовнішньої IP-адреси (включаючи отримання зовнішньої IP-адреси, в тому випадку, якщо провайдер його не дає), обхід обмежень, встановлених в локальній мережі, об'єднання віддалених локальних мереж в одну мережу і т. д [4].

Що стосується налаштування безпосередньо самого з'єднання, то із з'єднанням «точка-точка» ніяких проблем не виникає, а щодо з'єднання «сервер-клієнт», то викликає кілька проблем. Основна і мабуть найважливіша проблема, це питання безпеки і шифрування даних. Так як в цьому режимі необхідно замість ключів для аутентифікації і шифрування використовувати сертифікати. Сертифікат – це файл, який зберігає інформацію про джерело інформації і його відкритий ключ. Для визначення того, що він отриманий від того джерела, за яке себе видає, сертифікат підписується ключем сертифікаційного центру. Таким чином, для перевірки дійсності сертифіката необхідно перевірити його підпис з використанням сертифіката центру сертифікації (а також додаткові умови: термін дії, відсутність сертифіката в списку недійсних).

Зазвичай центрами сертифікації є компанії, що підписують сертифікати і відповідають за правильність представленої в сертифікаті інформації. При роботі з сертифікатами використовуються алгоритми асиметричного шифрування, на яких і ґрунтується метод електронного цифрового підпису - ЕЦП; він дозволяє встановити відсутність спотворення інформації в електронному документі з моменту формування ЕЦП і перевірити приналежність підпису власникові сертифіката ключа ЕЦП. Значення реквізиту формується за результатом криптографічного перетворення інформації з використанням закритого ключа ЕЦП. За допомогою такого алгоритму можна встановити, що інформація отримана від достовірного джерела. Для цього джерело формує документ, отримує від нього контрольну хеш-функцію і шифрує хеш за допомогою закритого (секретного) ключа. У цьому випадку говорять, що джерело підписує документ. Ключ розшифровки робиться відкритим (публічним). Для перевірки того, що документ був отриманий від довіреного джерела і не був змінений, одержувач розшифровує хеш за допомогою відкритого ключа та обчислює хеш-функцію документа. Якщо хеш-кодування збігаються, значить документу можна довіряти. Отримати закритий ключ на основі відкритого ключа практично неможливо [5, 6].

Основною проблемою при створенні з'єднання «сервер-клієнт» є як раз вище описана система сертифікатів. Це завдання і треба вирішити, для спрощення налаштування даного з'єднання за допомогою програмного забезпечення «OpenVPN».

Для вирішення даної проблеми, було проведено порівняння (табл. 1) різних способів створення і застосування сертифікатів для підписання програмного забезпечення.

Після порівняння способів створення сертифікатів, було вирішено використовувати створення власного центру сертифікації. Тому що даний спосіб має кілька незаперечних переваг: можна генерувати ключі самостійно; можна підписувати будь-яке ПЗ, де використовується серверна і клієнтська частина; можна створювати персональні сертифікати.

Таблиця 1 – Порівняння способів створення ключів і сертифікатів

| **Методи порівняння** | Замовлення сертифікату у «Засвідчуючого центру» | Використання Easy-RSA | Створення своїх сертифікатів |
|---|---|---|---|
| **Застосування ключів і сертифікатів** | Можна підписувати будь-яке ПЗ, де використовується серверна і клієнтська частина | Використовується тільки для підписання «OpenVPN» | Можна згенерувати ключі і підписувати будь-яке ПЗ, де використовується серверна і клієнтська частина |
| **Безпека** | Ключі генеруються в залежності від побажань замовника | Генерується ключ довжиною до 1024 біт | Можливість генерації ключів до 2048 біт. (Параметр вказується самостійно) |
| **Можливість розвитку організації** | Замовник замовляє обмежене число сертифікатів | Є можливість створення нових сертифікатів при збільшенні кількості клієнтів | Є можливість створення нових сертифікатів при збільшенні кількості клієнтів, а також можливе створення персональних сертифікатів співробітників |
| **Поширення** | Замовляється і купується у «Засвідчуючого центру». | Пакет безкоштовний | Пакет безкоштовний |
| **Основні недоліки** | Висока вартість даної послуги | Вузька спрямованість (тільки для «OpenVPN») | Вимагає великої роботи від адміністратора |

Для створення власного центру сертифікації, можна скористатися пакетом «OpenSSL» [7]. З його допомогою можна створювати ключі шифрування, сертифікати, а також підписувати сертифікати. Що стосується самого центру сертифікації, в який ми і будемо додавати створені сертифікати і ключі, то його необхідно створити самостійно.

В результаті проведених порівнянь ми можемо побачити що для методу "Власних сертефікатів" є недоліком великий обсяг роботи адміністратора, але в той же час він є найбільш функціональним (можливість генерувати ключі довжиною до 2048 біт, можливість установки самостійної довжини, підписувати будь-яке ПЗ), можливість створення додаткових і персональних сертефікатів.

**Список використаних джерел**

1. *Graf, Norbert Beginning OpenVPN 2.0.9/ Norbert Graf – Packt Publishing, 2009. – 356c.*
2. *Feilner, Markus OpenVPN: Building and Integrating Virtual Private Networks/ Markus Feilner – Packt Publishing, 2006. – 223c.*
3. *OpenVPN – «хмарний» сервіс VPN: [Електронний ресурс]. – Режим доступу: http://openvpn.net*
4. *OpenVPN – опис вільної реалізації технології: [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/OpenVPN*
5. *OpenVPN – методичні вказівки що до налаштування серверу: [Електронний ресурс]. – Режим доступу: https://help.ubuntu.com/community/OpenVPN*
6. *OpenVPN – методичні вказівки що до налаштування серверу: [Електронний ресурс]. – Режим доступу: http://wiki.kryukov.biz/wiki/Openvpn*
7. *OpenSSL – опис криптографічного пакету з відкритим кодом: [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/OpenSSL*