УДК 004.007

АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ МЕРЕЖ VPN

Корман Н.А, Могилевич Д.І.
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського
E-mail:kormannatasha21292@gmail.com

Проаналізовано основні принципи побудови віртуальних приватних мереж, досліджено основні методи захисту інформації від несанкціонованого доступу, що можуть бути реалізовані впливом природного або штучного характеру у VPN мережах.

Analysis of technologies for building virtual secure VPN networks

Korman N.A., Mogilevich D.I.

The basic principles of building virtual private networks are analyzed, the basic methods of protection of information against unauthorized access are investigated, which can be realized by influence of natural or artificial nature in VPN networks.

У загальному випадку VPN (англ. VirtualPrivateNetwork – віртуальна приватна мережа) – технологія, що дозволяє забезпечити одне або кілька мережевих з’єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Суть технології віртуальних приватних мереж полягає в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже створеному з'єднанні організується зашифрований канал, що забезпечує високий рівень захисту каналу інформації від небажаного втручання. Таким чином, створюється "тунель" між персональним комп'ютером і сервером, в якому всі дані зашифровані, і провайдер не розуміє, з яким сайтом працює користувач.

З'єднання з сервером через VPN має ряд переваг:

1. Створення WAN-з’єднання дуже дороге і може бути недоцільним для окремих користувачів. Дані, що передаються між двома кінцевими точками VPN, зашифрована, таким чином, жодне несанкціоноване втручання неможливе, коли інформація передається мережею загального користування.
2. Приховування конфіденційності, маскування дійсної IP-адреси.
3. Обходження географічних обмежень.

Недоліком використання VPN є збільшення кількості інформації, що передається в мережах. Це пов’язано із застосуванням спеціальних методів для шифрування даних, що призводить до підвищення навантажень на мережу [1].

Класифікувати рішення VPN можна за призначенням:

- Intranet VPN;
- Remote Access VPN;
- Extranet VPN;

- Client / Server VPN;
- Internet VPN.

Intranet VPN дозволяє створити надійні з'єднання між внутрішніми підрозділами розподіленої компанії. Для такої мережі маються на увазі: криптографічні засоби захисту інформації, надійність роботи важливих додатків, електронної пошти, швидкість і продуктивність передачі.

Remote Access VPN дозволяє створити захищений канал між сегментом корпоративної мережі (центральним офісом або філією) і єдиними користувачами, що мають доступ до корпоративного ресурсу за допомогою персонального комп'ютера.

Extranet VPN дозволяє створити захищену від несанкціонованого доступу корпоративну мережу, що використовує Інтернет-технології для внутрішньо-корпоративних цілей.

Client / Server VPN технологія надає захист даних, що передаються між двома вузлами корпоративної мережі. Особливість полягає в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером.

Internet VPN технологія дозволяє створити «тунель» для передачі даних, що дозволить зберегти цілісність та автентичність інформації.[2].

Фундаментом VPN на основі Internet є дві основні технології:

1. Технологія «Тунелю», що дозволяє створювати віртуальні канали
2. Методи забезпечення конфіденційності і цілісності інформації, що передається, а також автентифікації та авторизації користувачів які мають до неї доступ.

Розглянемо технологію тунелювання (tunneling) або інкапсуляція (encapsulation) - це спосіб передачі даних через проміжну мережу. Технологія «Тунелю» використовується не тільки для забезпечення конфіденційності внутрішнього пакета даних, але і для його цілісності.

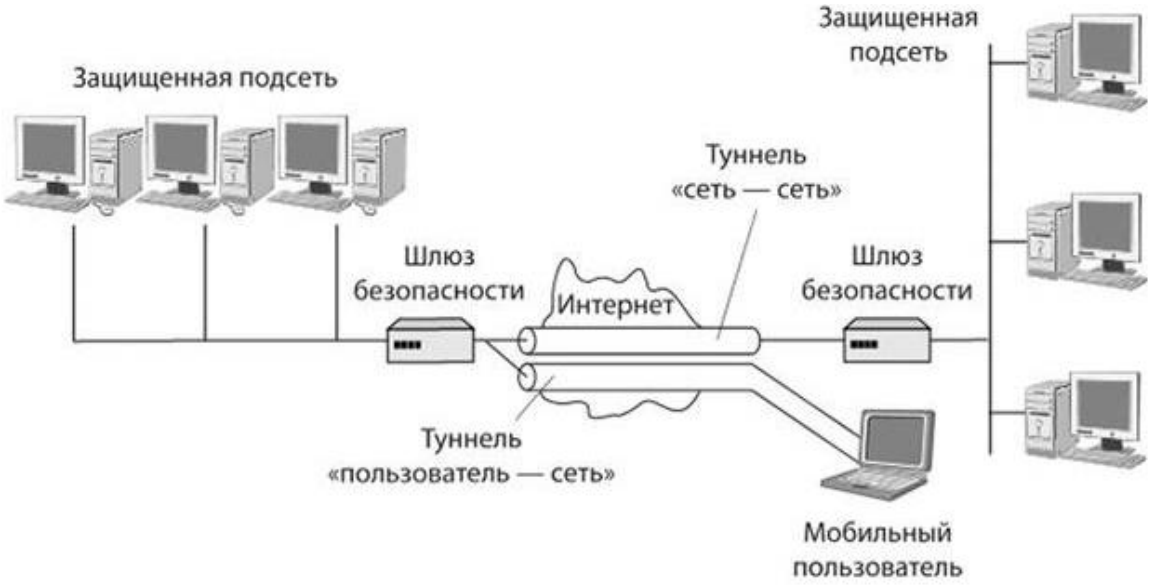

Рис. 1. Тунельна схема організації VPN-мережі

В процесі тунелювання дані розбиваються на більш дрібні пакети, які потім будуть переміщатися по "тунелю" для транспортування до кінцевого пункту призначення.Перш ніж потрапити в Internet-тунель дані шифруються, що забезпечує їх додатковий захист та надійність. [3]

Протоколи тунелювання *VPN* пропонують різні функції і рівні безпеки, і кожен з них має переваги і недоліки.

Розглянемо найпоширеніші протоколи тунелювання *VPN*: протокол тунелювання захищених сокетів (*SSTP*), протокол тунелювання «точка-точка» (*PPTP*), протокол тунелювання другого рівня (*L2TP*), *OpenVPN* і *Internet Key Exchange* версії 2 (*IKEv*2).

SSTP використовує протокол *HTTPS* для передачі трафіку через брандмауери і веб-проксі, які можуть блокувати інші протоколи. *SSTP* надає механізм для перенесення трафіку протоколу «точка-точка» (*PPP*) по каналу *SSL*. Використання *PPP* дозволяє підтримувати надійні методи аутентифікації, а *SSL* забезпечує безпеку на рівні транспорту з розширеним узгодженням ключів, перевіркою шифрування і цілісності.

OpenVPN - програмний додаток з відкритим вихідним кодом, яке реалізує методи *VPN* для створення безпечних з'єднань «точка-точка» або «сайт-сайт »в маршрутизованих або мостових конфігураціях і засобах віддаленого доступу. Він використовує власний протокол безпеки, який використовує *SSL / TLS* для обміну ключами.

*IKEv*2 – протокол тунелювання (протокол обміну ключами, версія 2), розроблений *Cisco* і *Microsoft*, він вбудований в *Windows* 7 і наступні версії. Протокол допускає модифікації з відкритим вихідним кодом, зокрема для *Linux* та інших платформ, також підтримуються пристрої *Blackberry*. *IKEv*2 особливо корисний при автоматичному відновленні *VPN*-з'єднання, коли користувачі тимчасово втрачають свої інтернет-з'єднання.

PPTP дозволяє шифрувати мультипротокольний трафік і потім обернути його в заголовок, який буде відправлений через мережу з використанням *IP*. *PPTP* можна використовувати для віддаленого доступу і *VPN*-з'єднань «точка-точка». При використанні *Internet PPTP*-сервер є *VPN*-сервером з підтримкою *PPTP* з одним інтерфейсом в *Internet* і другим інтерфейсом в корпоративній інтрамережі. *PPTP* використовує з'єднання протоколу управління передачею для управління тунелями та інкапсуляції загальної маршрутизації для перенесення кадрів PPP для даних, які передаються тунелем.

L2TP дозволяє зашифрувати мультипротокольний трафік, а потім використовувати будь-який носій, що підтримує доставку даних PPP, наприклад, IP або асинхронний режим передачі. L2TP це комбінація PPTP і Layer 2 Forwarding (L2F). L2TP представляє кращі функції PPTP і L2F. На відміну від PPTP, L2TP покладається на IP- безпеку (IPsec) в транспортному режимі для служб шифрування. комбінація L2TP і IPsec відома як L2TP / IPsec.

Обидва L2TP і IPsec повинні підтримуватися як VPN-клієнт, так і VPN-сервером.

Порівняльну характеристику протоколів шифрування наведено на Табл. 1.

Табл. 1. Характеристики протоколів шифрування.

	Шифрування	**Безпеки**	**Швидкість**
OpenVPN	256-біт	Найвище шифрування	Швидкий на високих латентних з'єднання
L2TP	256-біт	Найвище шифрування	Повільний і сильно процесорний
SSTP	256-біт	Найвище шифрування	Сповільнений
IKEv2	256-біт	Найвище шифрування	Швидкий
PPTP	128-біт	Мінімальна безпека	Швидкий

Висновки. Технологія VPN дозволяє ефективно вирішувати завдання щодо забезпечення безпеки інформаційних ресурсів, підтримати цілісність та конфіденційність інформації, що передається в локальних і глобальних інформаційних середовищах. Технологія VPN забезпечує зв'язок між мережами, а також між віддаленим користувачем і корпоративними мережами за допомогою захищеного каналу (тунелю), «прокладеного» в загальнодоступній мережі Internet.

Література

1. «VPN: плюси і мінуси, які ви повинні розглянути перед його використанням» - Електронний ресурс. – Режим доступу: https://uk.gadget-info.com/57085-vpn-pros-and-cons-you-should-consider-before-using-it.
2. «Концепція захищених віртуальних приватних мереж»- Електронний ресурс. – Режим доступу: https://stud.com.ua/97437.
3. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети - анализ технологий и синтез решений. М.: ДМК Пресс, 2004.
4. «Віртуальні захищені мережі VPN та антивірусні технології»: Електронний ресурс. – Режим доступу: https://studopedia.su/3_28437_kontseptsiya-pobudovi-virtualnih-zahishchenih-merezh-VPN.html.