УДК 004.77

БраіловськийМ. М., к.т.н.; **Погребна Т. В.**,студентка; **Пташок О. В.,** студентка
(Державний університет телекомунікацій, м. Київ. +380 (67) 4292056. bk1972@bk.ru, Tanya31-91@mail.ru)

МЕРЕЖІ VPN ТА ПРОБЛЕМИ ЇХ ЗАХИСТУ

Браіловський М. М., Погребна Т. В., Пташок О. В. Мережі VPN та проблеми їх захисту. Розглянуто переваги та недоліки VPN мережі. Описано технологію VPN та її протокол PPTP. Розглянуто захищений віддалений доступ до мережі, за допомогою якого здійснюється віртуальний локальний зв'язок між розподіленими мережами. Одним з найважливіших завдань технології VPN є захист потоків корпоративних даних, що передаються по відкритих мережах. Відкриті канали можуть бути надійно захищені лише одним методом – криптографічним.
Ключові слова: VPN, інтернет, Centrex, безпека, криптографія, тунелювання, аутентифікація

Браиловский Н. Н., Погребная Т. В., Пташок Е. В. Сети VPN и проблемы их защиты. Рассмотрены преимущества и недостатки VPN сети. Описана технология VPN и ее протокол PPTP. Рассмотрен защищенный удаленный доступ к сети, с помощью которого осуществляется виртуальный локальный связь между распределенными сетями. Одной из важнейших задач технологии VPN является защита потоков корпоративных данных, передаваемых по открытым сетям. Открытые каналы могут быть надежно защищены лишь одним методом – криптографическим.
Ключевые слова: VPN, Интернет,Centrex, безопасность, криптография, туннелирование, аутентификация

Brailovskyy M. M., Pogrebna T. V., Ptashok O. V. VPN networks and problems of their defence. Advantages and disadvantages of VPN networks are considered. VPN technology and its Protocol PPTP is described . It is considered secure remote access to the network through which the virtual link between local distributed networks. One of the most important tasks of VPN technology is to protect corporate data streams transmitted over public networks. Open channels can be protected by only one method – cryptographic.
Keywords: VPN, Internet, Centrex, network security, cryptography, tunnelings, authentification

Вступ. Дуже часто сучасній людині, розвиваючи свій бізнес, доводиться багато подорожувати. Це можуть бути поїздки у віддалені куточки нашої країни або до країн зарубіжжя. Нерідко людям потрібен доступ до своєї інформації, що зберігається на їх домашньому комп'ютері або на комп'ютері фірми. Цю проблему можна вирішити, організувавши віддалений доступ до нього за допомогою модему і телефонної лінії. Використання телефонної лінії має свої особливості. Недоліки цього рішення в тому, що дзвінок з іншої країни коштує чималих грошей. Є й інше рішення під назвою VPN (VirtualPrivateNetwork– віртуальна приватна мережа). Переваги технології VPN в тому, що організація віддаленого доступу робиться не через телефонну лінію, а через Інтернет, що набагато дешевше і краще. Для організації віддаленого доступу до приватної мережі за допомогою технології VPN знадобиться лише Інтернет і реально діюча IP адреса. І будь-який користувач з будь-якого куточка земної кулі зможе зайти в мережу, якщо він знає IP адресу, логін і пароль [1].

Технологія VPN. Сьогодні будь-який адміністратор вважає своїм обов'язком організувати VPN-канали для співробітників, що працюють поза офісом (Рис. 1).

VPN (Рис. 2) представляє собою об'єднання окремих машин або локальних мереж у віртуальну мережу, яка забезпечує цілісність та безпеку переданих даних. Вона має властивості виділеної приватної мережі й дозволяє передавати дані між двома комп'ютерами через проміжну мережу, наприклад Internet [2].

VPN відрізняється рядом економічних переваг у порівнянні з іншими методами дистанційного доступу. Маючи доступ в Інтернет, будь-який користувач може без проблем підключитися до мережі офісу своєї фірми. Слід зауважити, що загальнодоступність даних зовсім не означає їхню незахищеність. Система безпеки VPN – це броня, яка захищає всю корпоративну інформацію від несанкціонованого доступу.

Насамперед, інформація передається в зашифрованому виді. Прочитати отримані дані може лише власник ключа до шифру. Підтвердження справжності містить у собі перевірку цілісності даних і ідентифікацію користувачів, задіяних в VPN. Перша гарантує, що дані дійшли до адресата саме в тому виді, у якому послані. Самі популярні алгоритми перевірки

цілісності даних – MD5 і SHA1. Побудова VPN припускає створення захищених від стороннього доступу тунелів між декількома локальними мережами або користувачами.

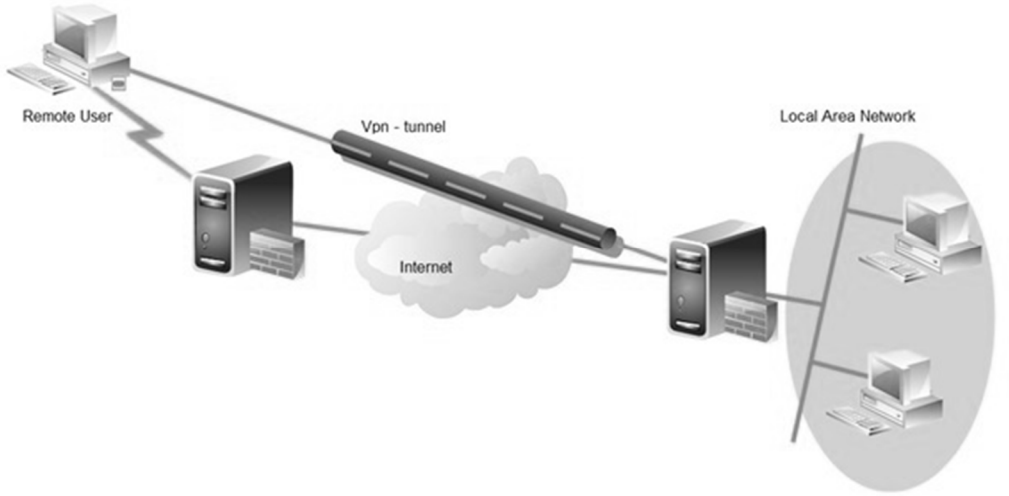

Рис. 1. VPN для віддалених користувачів

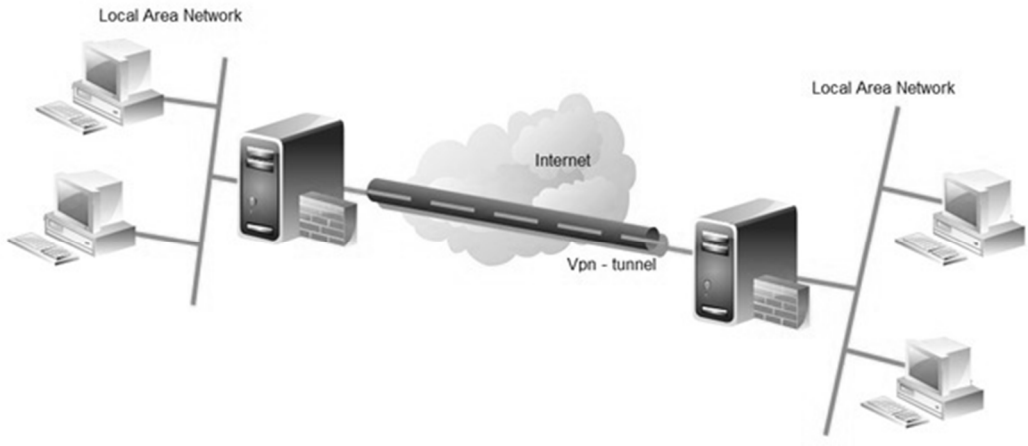

Рис. 2. VPN для двох офісних мереж

Для побудови VPN необхідно мати на обох кінцях лінії зв'язку програми шифрування вихідного й дешифрування вхідного трафіків. Вони можуть працювати як на спеціалізованих апаратних обладнаннях, так і на ПК із такими операційними системами як Windows, Linux або Netware [3]. Керування доступом, аутентифікація й шифрування – найважливіші елементи захищеного з'єднання.

Віртуальні приватні мережі мають кілька переваг над традиційними приватними мережами [4]. Головні з них – економічність, гнучкість і зручність використання. За допомогою VPN-мереж підприємствам вдається хоча б частково обмежити зростання числа модемів, серверів доступу, комутаційних ліній і інших технічних засобів, які організація змушена впроваджувати, щоб забезпечити віддаленим користувачам доступ до своїх мереж.

Особливо вигідні віртуальні приватні мережі в тих випадках, коли користувачі віддалені на великі відстані й тому орендовані лінії обходяться дуже дорого, а також коли таких користувачів багато, у зв'язку із чим їм потрібна велика кількість орендованих ліній. Однак ці переваги можуть зійти на ні, якщо обсяг трафіка в VPN-мережі настільки великий, що система не встигає зашифровувати й розшифровувати пакети даних[3]. Щоб уникнути виникнення таких вузьких місць, підприємство змушено купувати додаткове устаткування.

Необхідно відзначити, що рівень безпеки і анонімності мереж VPN залежить від того, яким чином вона реалізована і налаштована. Високого рівня конфіденційності можна домогтися за допомогою спеціального програмного забезпечення та правильної його реалізації. Тонкі налаштування мереж VPN дозволяють користувачам досягти повної анонімності в віртуальному просторі.

Структура VPN складається з двох рівнів. Перший рівень називається "внутрішня мережа". Таких мереж може бути декілька. Другий рівень – це "зовнішня мережа". Як правило, для з'єднання використовується інтернет. Для підключення віддаленого користувача до віртуальної мережі використовується спеціальний сервер, який підключений як до внутрішньої , так і до зовнішньої мереж. Для того щоб підключитися до віртуальної мережі, комп'ютера необхідно пройти декілька процесів. Тільки після успішного завершення процесів ідентифікації і аутентифікації користувач зможе пройти процес авторизації. Авторизація, в свою чергу, дозволяє отримати повний доступ до можливостей мережі [5].

Споживча сутність VPN – віртуальний захищений тунель, або шлях, за допомогою якого можна організувати віддалений захищений доступ через відкриті канали Інтернету до серверів баз даних, FTP і поштових серверів. Фізична сутність технології VPN полягає в здатності захистити трафік будь-яких інформаційних інтранет- і екстранет-систем, аудіовідеоконференцій , систем електронної комерції і т. п.

Захист інформації в мережах VPN. Віртуальна приватна мережа базується на трьох методах, які застосовуються при реалізації заходів безпеки в інформаційних мережах: тунелювання, аутентифікація, шифрування.

Тунелювання забезпечує передачу даних між двома точками – закінченнями тунелю – таким чином, що для джерела і приймача даних виявляється прихованою вся мережева інфраструктура, що лежить між ними. Транспортна середовище тунелю підхоплює пакети використовуваного мережного протоколу біля входу в тунель і без змін доставляє їх до виходу. Побудови тунелю достатньо для того, щоб з'єднати два мережевих вузла так, що з точки зору працюючого на них програмного забезпечення вони виглядають підключеними до однієї (локальної) мережі.

Такий стан справ таїть в собі дві проблеми. Перша полягає в тому, що передається через тунель інформація може бути перехоплена зловмисниками. Якщо вона конфіденційна (номери банківських карток, фінансові звіти, відомості особистого характеру), то цілком реальна загроза її компрометації. Крім того, зловмисники мають можливість модифікувати дані так, що одержувач не зможе перевірити їх достовірність. Враховуючи сказане, приходимо до висновку, що тунель в чистому вигляді придатний хіба що для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації. Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Суть методу полягає в тому, що кожен переданий пакет забезпечується додатковим блоком інформації, який виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для вмісту пакета і секретного ключа ЕЦП відправника. Цей блок інформації є ЕЦП пакета і дозволяє виконати аутентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання сильних алгоритмів шифрування.

Аутентифікація.Забезпечення безпеки є основною функцією VPN. Всі дані від комп'ютерів-клієнтів проходять через Internet до VPN-сервера. Такий сервер може знаходитися на великій відстані від клієнтського комп'ютера, і дані на шляху до мережі організації проходять через обладнання багатьох провайдерів. Для захисту даних від спотворення та несанкціонованого доступу різні методи аутентифікації і шифрування.

Для аутентифікації користувачів PPTP може задіяти будь-який з протоколів, що застосовуються для PPP: EAP (Extensible Authentication Protocol);MSCHAP (Microsoft Challenge Handshake Authentication Protocol), версії 1 і 2; CHAP (Challenge Handshake

Authentication Protocol); SPAP (Shiva Password Authentication Protocol); PAP (Password Authentication Protocol). Кращими вважаються протоколи MSCHAP версії 2 і EAP-TLS (Transport Layer Security), оскільки вони забезпечують взаємну аутентифікацію, тобто VPN-сервер і клієнт ідентифікують один одного. У всіх інших протоколах тільки сервер проводить аутентифікацію клієнтів.

Аутентифікація здійснюється або відритим тестом (clear text password), або за схемою запит / відгук (challenge / response).

При відкритій аутентифікації клієнт посилає серверу пароль, де він порівнюється з еталоном. На основі цього порівняння робиться висновок щодо дозволу або заборони доступу. Відкрита аутентифікація практично не зустрічається.

Схема запит / відгук набагато більш застосована. В загальному вигляді вона виглядає наступним чином. Клієнт посилає серверу запит (request) на аутентифікацію, на що сервер повертає випадковий відгук (challenge). Клієнт знімає зі свого пароля хеш (хешем називається результат хеш-функції, яка перетворює вхідний масив даних довільної довжини в вихідну бітову рядок фіксованої довжини), шифрує їм відгук і передає його серверу.

Те ж саме проробляє і сервер, порівнюючи отриманий результат з відповіддю клієнта: якщо зашифрований відгук збігається, аутентифікація вважається успішною.

На першому етапі аутентифікації клієнтів і серверів VPN, L2TP поверх IPSec використовує локальні сертифікати, отримані від служби сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють захищене з'єднання ESP SA (security association). Після того як L2TP (поверх IPSec) завершує процес аутентифікації комп'ютера, виконується аутентифікація на рівні користувача. Для аутентифікації можна задіяти будь-який протокол, навіть PAP, що передає ім'я користувача та пароль у відкритому вигляді. Це цілком безпечно, так як L2TP поверх IPSec шифрує всю сесію. Проте проведення аутентифікації користувача при допомоїі MSCHAP, що застосовує різні ключі шифрування для аутентифікації комп'ютера і користувача, може посилити захист.

Шифрування за допомогою PPTP гарантує, що ніхто не зможе отримати доступ до даних при пересиланні через Internet. В даний час підтримуються два методи шифрування:

• Протокол шифрування MPPE (Microsoft Point-to-Point Encryption), сумісний тільки з MSCHAP (версії 1 і 2);

• Протокол EAP-TLS,який може автоматично вибирати довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером.

MPPE підтримує роботу з ключами довжиною 40, 56 або 128 біт. Старі операційні системи Windows підтримують шифрування з довжиною ключа тільки 40 біт, тому в змішаному середовищі Windows слід вибирати мінімальну довжину ключа.

PPTP змінює значення ключа шифрування після кожного прийнятого пакета. Протокол MMPE розроблявся для каналів зв'язку точка-точка, в яких пакети передаються послідовно, і втрата даних дуже мала. У цій ситуації значення ключа для чергового пакета залежить від результатів дешифрування попереднього пакета. При побудові віртуальних мереж через мережі загального доступу цих умов дотримуватися неможливо, так як пакети даних часто приходять до одержувача не в тій послідовності, в якій були відправлені. Тому PPTP використовує для зміни ключа шифрування порядкові номери пакетів. Це дозволяє виконувати дешифрацію незалежно від попередніх прийнятих пакетів.

Таким чином, зв'язка «тунелювання + аутентифікація + шифрування» дозволяє передавати дані між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) мережі.

Додатковою перевагою VPN-з'єднання є можливість (і навіть необхідність) використання системи адресації, прийнятої в локальній мережі.

Реалізація віртуальної приватної мережі на практиці виглядає таким чином. У локальній обчислювальній мережі офісу фірми встановлюється сервер VPN. Віддалений користувач (або маршрутизатор, якщо здійснюється з'єднання двох офісів) з використанням клієнтського програмного забезпечення VPN ініціює процедуру з'єднання з сервером. Відбувається

аутентифікація користувача – перша фаза встановлення VPN-з'єднання. У разі підтвердження повноважень настає друга фаза – між клієнтом і сервером виконується узгодження деталей забезпечення безпеки з'єднання. Після цього організовується VPN-з'єднання, що забезпечує обмін інформацією між клієнтом і сервером у формі, коли кожен пакет з даними проходить через процедури шифрування/дешифрування та перевірки цілісності – аутентифікації даних.

Основною проблемою мереж VPN є відсутність установлених стандартів аутентифікації і обміну шифрованого інформацією. Ці стандарти все ще знаходяться в процесі розробки і тому продукти різних виробників не можуть встановлювати VPN-з'єднання і автоматично обмінюватися ключами. Дана проблема тягне за собою уповільнення розповсюдження VPN, так як важко змусити різні компанії користуватися продукцією одного виробника, а тому ускладнений процес об'єднання мереж компаній-партнерів в, так звані, extranet-мережі.

Зазвичай VPN розгортають на рівнях не вище мережевого. Застосування криптографії на цих рівнях дозволяє використовувати в незмінному вигляді транспортні протоколи (TCP, UDP).

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який-небудь інший протокол. Такий спосіб використовує реалізація PPTP (Point-to-Point Tunneling Protocol) або Ethernet (PPPoE) (хоча і вони мають відмінності). Технологія VPN останнім часом використовується не тільки для створення власне приватних мереж, але і деякими провайдерами "останньої милі" для надання виходу в Інтернет.

При належному рівні реалізації та використанні спеціального програмного забезпечення мережа VPN може забезпечити високий рівень шифрування переданої інформації. При правильному налаштуванні всіх компонентів технологія VPN забезпечує анонімність в мережі.

Висновки. Аналізуючи основні проблеми інформаційної безпеки в локальних чи глобальних мережах, якими є віртуальні приватні мережі, можна зробити висновок, що такі системи повинні забезпечувати виявлення внутрішніх і зовнішніх загроз і вторгнень, фільтрацію зовнішнього трафіку, контроль за використанням корпоративних мережевих ресурсів і запобігання витоків конфіденційної інформації. Вхідними даними при цьому є інформація про структуру і характеристиках трафіку (прецедентна інформація), що дозволяє побудувати набір правил, що класифікують нормальні або аномальні компоненти трафіку. У цьому напрямку слід очікувати істотне підвищення безпеки мереж за рахунок оперативного реагування на набір відомих загроз і на які раніше не зустрічалися аномальні ситуації, а також за рахунок ідентифікації реально функціонуючих мережевих додатків або процесів та управління ними для забезпечення доступності інформаційних сервісів необхідних мережному співтовариству.

Тому стає очевидним необхідність вирішення проблеми зв'язки «тунелювання + аутентифікація + шифрування», яка дозволяє побудувати захищену мережу VPN.

Література

1. Журнал Connect: технология VPN [Електронний ресурс] // – Режим доступу : http://www.connect.ru/article.asp?id=5343 -

2.Ситник В.О. Основи інформаційних систем / В. О. Ситник. – К.: КНЕУ, 1997. – 140 с.

3.Хетч Б. Linux: создание виртуальных частных сетей (VPN) / Б. Хетч, О. Колесников. – Москва : КУДИЦ-Образ, 2004. – 461 стр.

4. Браун С. Виртуальные частные сети / С. Браун. – Москва : Лори, 2001. – 503 с.

5. Росляков А. Виртуальные частные сети. Основы построения и применения / Александр Росляков. – Москва : Эко-Трендз, 2006 г. – 304 с.