УДК 004.056.5(045) **І.І. Пархоменко, В.В. Галкін**

СПОСОБИ ЗАХИСТУ КАНАЛІВ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ VPN-РІШЕНЬ

В статті розглянуто методи та способи реалізації захищених каналів VPN, їх переваги та недоліки, розглянуто принципи роботи та призначення технології VPN передані в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу.

Ключові слова: vpn, корпоративна мережа, internet, безпека інформації, тунелювання, маршрутизатор, загроза, аутентифікація.

Постановка проблеми

Сучасний розвиток інформаційних технологій і, зокрема, мережі Internet, приводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу. VPN - це технологія, яка поєднує довірені мережі, вузли й користувачів через відкриті мережі і тим самим вирішує питання захисту інформації, що циркулює між довіреними мережами, вузлами, користувачами, його технічної та економічної сторони.

Мета статті

Дослідження використання VPN-технологій та процесу захисту інформації переданої в рамках розподіленої корпоративної мережі, яка використовує мережі відкритого доступу, з використанням технології VPN-з'єднань.

Основні матеріали дослідження

Корпоративна мережа - взаємозалежна сукупність мереж, служб передачі даних і телеслужб, призначена для надання єдиного захищеного мережного простору обмеженому рамками корпорації колу користувачів.

До загального виду корпоративної мережі можемо віднести наступне:

1. Корпоративний сервер баз даних;
2. Електронний документообіг;
3. Доступ в мережу Інтернет;
4. Апаратний та програмний захист інформації;
5. Відеоконференцзв'язок;
6. Корпоративна електронна пошта;
7. Корпоративна IP-телефонія.

Основними особливостями корпоративних мереж(КМ) є:

1. Використання того ж інструментарію, що й при роботі з мережею передачі даних загального користування.

2. Доступ до інформації надається тільки обмеженій групі клієнтів у внутрішній мережі організації. Внутрішня мережа представляє із себе локальну мережу, відділену від глобальних мереж міжмережевими екранами (МЕ).

3. Циркуляція інформації трьох типів: офіційна (поширення якої офіційно санкціонується й заохочується на рівні організації), проектна або групова (призначена для використання окремою групою співробітників, як правило, підлягає захисту) і неофіційна (особиста папка або каталог на сервері, що слугують сховищем статей, заміток і ідей, з якими можна поділитися з іншими співробітниками підприємства в спільних інтересах для обміну зауваженнями або якихось інших цілей).

4. Наявність централізованої системи керування корпоративною мережею.

Корпоративна мережа дозволяє ефективно об'єднати територіально вилучені підрозділи компанії. Єдина мережа забезпечує широкий спектр можливостей:

- охоплення всіх робочих місць підприємства в on-line режимі;
- віддалений доступ до ресурсів корпоративної мережі;
- доступ в Інтернет;
- розсилання великих обсягів даних по одному або багатьом адресам та ін.

Так само, що немаловажне, корпоративна мережа дозволяє одержувати доступ до Інтернет з єдиного сервера й розділяти канали по точках усередині компанії, що може суттєво знизити витрати на Інтернет для компанії в цілому.

Класифікаційні ознаки корпоративних мереж

Відповідно до введеного визначення корпоративної мережі її склад у загальному випадку утворюють наступні функціональні елементи:

Робочі місця (абоненти) корпорації, які можуть бути:

- зосередженими, або розташовуватися в рамках одного будинку;
- розподіленими на якійсь в загальному випадку необмежено великій території.

Інформаційні сервери корпорації, призначені для зберігання й обробки інформаційних масивів (баз даних) різного функціонального призначення. Вони також можуть бути *розподіленими* на великій території корпорації.

Засоби телекомунікації, що забезпечують взаємодію між собою робочих станцій і їх взаємодія з інформаційним серверами. Засоби телекомунікації в рамках корпорації можуть бути:

- виділеними (або орендованими), що є приналежністю корпорації;
- загального призначення (існуючі поза корпорацією мережі зв'язку, засоби яких використовуються корпорацією). Це, як правило, засоби існуючих мереж загального користування.

Телеслужби**.** У рамках корпорації інформаційний вплив може бути реалізовано в рамках однієї (телефонія, телетекст, відеотекст, телефакс); або декількох служб (інтеграція служб), що повинне забезпечуватися відповідними засобами телекомунікації й абонентських кінцевих точок.

Система керування ефективністю функціонування корпоративної мережі. Залежно від реалізованого набору служб у корпоративній мережі повинні використовуватися свої засоби керування мережею, зокрема засоби маршрутизації й комутації; засоби адміністрування, реалізовані з метою ефективного використання мережних ресурсів. По можливості керування елементами корпоративної мережі можна виділити:

- керовані в рамках корпорації функціональні елементи (це власні, або, що додатково вводяться в рамках корпоративної мережі засобу);
- некеровані в рамках корпорації функціональні елементи, (зокрема, маршрутизатори й комутатори), що є приналежністю використовуваних корпорацією підмереж загального призначення.

Система керування безпекою функціонування корпоративної мережі. У корпоративній мережі повинні бути реалізовані необхідні мережні служби безпеки, повинні використовуватися відповідні засоби безпеки.

Система забезпечення надійності корпоративної мережі**.** Повинні бути передбачені засоби забезпечення працездатності всієї мережі або її фрагментів при відмовах елементів мережі. [1]

Система діагностики й контролю**.** У рамках корпоративної мережі повинні бути передбачені засоби контролю працездатності окремих функціональних елементів, система збору інформації про відмови й збої та надання її системам забезпечення живучості; керування ефективністю функціонування; керування безпекою. Для корпоративної мережі повинні бути розроблені засоби діагностики, реалізовані як у процесі функціонування мережі, так і профілактично.

Система експлуатації**.** Крім перерахованих функціональних елементів, корпоративні мережі зв'язку повинні мати план процесу розвитку, що визначає функціональні можливості, що закладаються в неї, зокрема на рівні протоколів взаємодії мережних компонентів і можливості їх інтеграції.

Узагальнюючи введені ознаки корпоративних мереж, одержимо можливу їхню класифікацію:

- по набору функціональних елементів;
- по ієрархії керування;
- по набору (типу й кількості) поєднуваних у рамках корпоративної мережі підмереж загального користування;
- по набору (типу й кількості) реалізованих у рамках корпоративної мережі телеслужб.

Безпека корпоративної мережі є вкрай важливим моментом для успіху будь-якої компанії.

Провідні підприємства середнього бізнесу опираються на свої комп'ютерні мережі для надання безпечного постійного доступу до даних компанії, додаткам і електронній пошті. Повний розв'язок для захисту мережі дозволить організації зберігати стійкість до атак, захищати конфіденційність даних компанії й забезпечувати безперервний цілодобовий доступ до них.

Завдання створення комп'ютерної мережі підприємства в межах однієї будівлі може бути вирішене відносно легко. Однак сучасна інфраструктура корпорацій включає в собі географічно розподілені підрозділи самої корпорації, її партнерів, клієнтів і постачальників. Тому створення корпоративної мережі стало істотно більш складним завданням.

З бурхливим розвитком Internet і мереж колективного доступу стався якісний стрибок у поширенні й доступності інформації. Користувачі отримали дешеві й доступні канали Internet. Підприємства прагнуть використовувати такі канали для передачі критичної комерційної та управлінської інформації. [2]

Функції й компоненти мережі VPN

Захищеною віртуальною мережею VPN називають об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних.

При підключенні корпоративної локальної мережі до відкритої мережі виникають загрози безпеці двох основних типів:

- несанкціонований доступ до корпоративних даних в процесі їх передачі по відкритій мережі;
- несанкціонований доступ до внутрішніх ресурсів корпоративної локальної мережі, одержуваний зловмисником в результаті несанкціонованого входу в цю мережу.

Виявлення структури і основних властивостей незахищеної мережі

Сучасні обчислювальні мережі організацій представляють собою складні системи, які складаються з декількох компонентів. Серед цих компонентів можливо виділити різні комп’ютери, системне і прикладне програмне забезпечення цих комп’ютери, мережеві адаптери, комутатори, маршрутизатори і з’єднання (кабельні) системи. Широке використанні Інтернету та інтернет-технологій призвело до якісної зміни обчислювальних мереж. Якщо раніше Інтернет використовувався в цілому як середовище передачі, то в даний час Інтернет стає не тільки засобом інтерактивної взаємодії людей, а також засобом ведення ділових операції організацій, реальним засобом проведенні бізнес-операції.

Популярність IP-технологій пояснюється їх об'єктивними перевагами. До числа таких переваг можливо віднести відносну легкість принципів технології. Одним з таких принципів є відкритість, яка виражається вільним обговоренням, дослідженням і тестуванням нових протоколів стека TCP / IP в рамках не тільки робочих груп комітету Internet Engineering Task Force (IETF), але і усієї всесвітньої групи. Розробляються і пропонуються стандарти і специфікації доступу практично всім користувачам Інтернет. Відкритість технології дозволяє

забезпечити відносну легкість інтеграції в IP-мережі інших технологій, що значно збільшує область застосування Інтернету.[3]

Іншою перевагою IP-технологій є масштабність, яка була закладена вже при розробці Інтернету. Ієрархічно організований стек TCP / IP дозволяє нарощувати мережі організацій в достатньо більших межах.

Ці та інші переваги забезпечили на даний момент широке застосування IP-технологій. Технології, які привели до успіху Інтернету, виявитися дуже перспективними і для внутрішніх мереж організацій - мереж інтранет (intranet).

Корпоративну мережу (інтранет) - це мережа на рівня компанії, в якій використовують програмні кошти, підставу на стеку протоколів TCP / IP.

Під екстранет-мережами розуміється інтранет-мережу, підключену до Інтернету, тобто цю мережу типу інтранет, але доступ до її ресурсів конкретної категорії користувачів, яка наділена відповідними повноваженнями.

Оскільки надалі будуть розглядатися засоби захисту, то всі мережі представляються як локальні мережі, підключені до Інтернету. При цьому використовують в даній мережі Web-технологія, тому далі будемо називати такі мережі корпоративними.

Головними особливостями корпоративних мереж - глобальність зв'язків, масштабність і гетерогенність - представляють і підвищену небезпеку для виконання ними своїх функціональних завдань. Оскільки протоколи сімейства TCP / IP розроблені достатньо давно, коли проблеми безпеки ще не стояла так гостро, як зараз, то вони, в першу чергу, розроблялися як функціональні, які допомагали поширюватись стеку TCP / IP на декілька комп'ютерних платформ. Крім того, в даний час, при використанні Інтернету в розпорядженні зловмисників з'являються численні засоби і методи проникнення в корпоративні мережі.[4]

У зв'язку з гігантським ростом численності хостів, підключених до Інтернету, і ростом числа компаній, використовують технології Інтернету для ведення свого бізнесу, значно збільшилося число інцидентів, пов'язаних з інформаційною безпекою (ІБ). Дані CERT (Computer Emergency Response Team) показують, що число виявленних вразливостей і число зареєстрованих інцидентів постійно збільшуються.

Під вразливостями інформаційної системи розуміється будь-яка характеристика, використання якої порушником може привести до реалізації загрози.

Загрози (threat) інформаційної системи називається потенційно можливу подію, дія, процеси або явище, які можуть викликати заподіяння шкоди (матеріального, морального або іншого) ресурсів системи.

Види загроз - це параметр, який визначає цільову направленість захисту інформації.

Під випадковим розуміється таке походження загрози, яке обумовлює спонтанні і не залежні від волі людей події, які виникають в системі обробки даних в процесах її функціонування.

Методи реалізації VPN мереж

Віртуальна приватна мережа базується на трьох методах реалізації:

- Туннелювання;
- Шифрування;
- Аутентифікація

Туннелювання - 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.

Транспортне середовище тунелю, як паром, підхоплює пакети використовуваного мережевого протоколу біля входу в тунель і без змін доставляє їх до виходу. Побудови тунелю досить 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. Однак не можна забувати, що насправді «парою» з даними проходить через безліч проміжних вузлів (маршрутизаторів) відкритої публічної мережі.

Такий стан справ таїть в собі дві проблеми. Для аутентифікації користувачів PPTP може задіяти будь-який з протоколів. Кращими вважаються протоколи MSCHAP версії 2 і Transport Layer Security (EAP-TLS), оскільки вони забезпечують взаємну аутентифікацію, тобто VPN-сервер і клієнт ідентифікують один одного. У всіх інших протоколах тільки сервер проводить аутентифікацію клієнтів.[5]

Хоча PPTP забезпечує достатній рівень безпеки, але все ж L2TP поверх IPSec надійніше. L2TP поверх IPSec забезпечує аутентифікацію на рівнях «користувач» і «комп'ютер», а також виконує аутентифікацію і шифрування даних.

Аутентифікація здійснюється або відритим тестом (clear text password), або за схемою запит / відгук (challenge / response). З прямим текстом все ясно. Клієнт посилає серверу пароль. Сервер порівнює це з еталоном і або забороняє доступ, або говорить «ласкаво просимо». Відкрита аутентифікація практично не зустрічається.

Схема запит / відгук набагато більш просунута. У загальному вигляді вона виглядає так:

- клієнт посилає серверу запит (request) на аутентифікацію;
- 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 серверу та порівнює отриманий результат з відповіддю клієнта;
- якщо зашифрований відгук збігається, аутентифікація вважається успішною;[6]

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, передає ім'я користувача і пароль у відкритому вигляді. Це цілком безпечно, так як L2TP поверх IPSec шифрує всю сесію. Однак проведення аутентифікації користувача за допомогою 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 або Microsoft Point-to-Point Encryption сумісний тільки з MSCHAP (редакція 1 і 2); TLS і вміє автоматично вибирати довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером 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 та змінювати 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 пакету. При побудові віртуальних мереж через мережі загального доступу ці умови 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 «туннелювання + аутентифікація + шифрування» дозволяє передавати дані між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) мережі. Іншими словами, розглянуті засоби дозволяють побудувати віртуальну приватну мережу.[7]

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

Реалізація віртуальної приватної мережі на практиці виглядає наступним чином. У локальної обчислювальної 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 і перевірки цілісності - аутентифікації даних. Основною проблемою мереж VPN є відсутність усталених 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 поширення VPN, так як важко змусити різні компанії користуватися продукцією одного виробника, а тому утруднений процес об'єднання мереж компаній-партнерів в, так звані, extranet-мережі.

Висновки

Ідея побудови власних віртуальних мереж актуальна в тому випадку, коли поєднувати кілька локальних мереж у різних будинках або організаціях для створення власної мережі дорого або занадто довго, однак необхідно забезпечити захист переданих між сегментами мережі даних. Адже далеко не завжди дозволене передавати дані по загальнодоступних мережах у відкритому вигляді. Втім, можна захищати тільки зв'язки між окремими комп'ютерами з різних сегментів, але якщо корпоративна політика вимагає забезпечення безпеки більшої частини інформації, то захищати кожний окремий канал і комп'ютер стає досить складно. Крім того, при захисті окремих каналів інфраструктура корпоративної мережі залишається прозорою для зовнішнього спостерігача. Для розв'язку багатьох проблем застосовується архітектура VPN, при використанні якої весь потік інформації, переданий по загальнодоступних мережах, шифрується.

Література

1. Биячуев Т.А. / под ред. Л.Г.Осовецкого. Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

2. Олифер. В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.

3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределённых корпоративных сетях и системах, - М.:ДМК Пресс, 2002. – 626с.

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

5. С. В. Запечников, Н. Г. Милославская, А. И. Толстой. Основы построения виртуальных частных сетей. Для высших учебных заведений. СПб.: Питер, 2003. – 248 с.

6. Кулаков Ю.А., Луцкий Г.М. Локальные сети, - К.: Юниор, 2008. – 336с.

7. Компьютерные сети. Принципы, технологии, протоколы/ В.Г.Олифер, Н.А.Олифер. – СПб.: Питер, 2001. – 672с.

8. Пархоменко І.І., Галкін В.В., «Захист транзакцій в каналах корпоративних мереж за допомогою VPN-технологій» // Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні: матеріали наук.-техніч. конф.,(НУБіП, Київ, Україна, 23 – 24 червня 2016). – К.: НУБіП, 2016. – С.47 – 48.

9. Галкін В.В., Пархоменко І.І. «Використання VPN-технологій для захисту інформації в каналах корпоративних мереж» // Проблема кібербезпеки інформаційно-телекомунікаційних систем: матеріали наук.-техніч. конф.,(КНУ, Київ, Україна, 10 – 11 березня 2016). – К.: КНУ, 2016. – С. 66.

Надійшла 27.11.2016 р. Рецензент: д.т.н., проф. Дудикевич В.Б.