УДК 004.056.5(045) **Пархоменко І.І., Квачук О.О., Воскобойніков А.О., Попов Г.В.**

ТУНЕЛЮВАННЯ, ЯК СПОСІБ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

В статті розглянуті принципи побудови і функціонування механізмів захисту інформації в корпоративних мережах на базі VPN-технологій. Детально розглянуто та проаналізовано модель функціонування процесу тунелювання, наведено спосіб за якого він забезпечує конфіденційність, цілісність та автентичність інформації. Також представлено опис протоколу IPSec, його переваги, недоліки, компоненти та технологічну базу.

Ключові слова**:** корпоративні мережі, VPN-тунелі, протокол IPSec, захищена передача даних, шифрування.

Корпоративні мережі відносяться до розподілених комп'ютерних систем, що здійснюють автоматизовану обробку інформації. Проблема забезпечення інформаційної безпеки є центральною для таких комп'ютерних систем. Забезпечення безпеки КМ передбачає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування КМ, а також спробам модифікації, розкрадання, виходу з ладу або руйнування її компонентів, тобто захист усіх компонентів КМ - апаратних засобів, програмного забезпечення, даних і персоналу.

Стрімкий розвиток інформаційних технологій відкрив нові можливості для бізнесу, однак це призвело й до появи нових загроз.

Таким чином першочерговим завданням є створення та опис моделі загрози, визначення її цілей та способів протидії їй.

Під загрозою безпеці [3] розуміється можлива небезпека (потенційна або реально існуюча) здійснення якого-небудь діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), що завдає збиток власникові або користувачеві і проявляється в небезпеці викривлення, розкриття або втрати інформації. Реалізацію загрози надалі будемо називати атакою.

Реалізація тієї або іншої загрози безпеки може переслідувати наступні цілі:

- порушення конфіденційності інформації. Інформація, збережена й оброблювана в корпоративній мережі, може мати велику цінність для її власника. Її використання іншими особами завдає значної шкоди інтересам власника;
- порушення цілісності інформації. Втрата цілісності інформації (повна або часткова, компрометація, дезінформація) - загроза близька до її розкриття. Цінна інформація може бути втрачена або знецінена шляхом її несанкціонованого видалення або модифікації. Збиток від таких дій може бути набагато більшим, ніж при порушенні конфіденційності;
- порушення (часткове або повне) працездатності корпоративної мережі (порушення доступності). Вихід з ладу або некоректна зміна режимів роботи компонентів КМ, їх модифікація або підміна можуть привести до одержання неправильних результатів, відмови КМ від потоку інформації або відмов при обслуговуванні. Відмова від потоку інформації означає невизнання однієї із взаємодіючих сторін факту передачі або приймання повідомлень. Якщо такі повідомлення містять важливі дані: замовлення, фінансові узгодження й т.п., збиток у цьому випадку може бути досить значним.

Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним із провідних напрямків розвитку інформаційних технологій.

Наступним важливим завданням є визначення моделі захищеного каналу зв’язку, в якому ми і будемо впроваджувати тунелювання, його властивостей та технологічної бази.

Тунелювання. Захист інформації в процесі її передачі по відкритих каналах заснований на побудові захищених віртуальних каналів зв'язку, що називаються криптозахищеними тунелями. Кожний такий тунель являє собою з'єднання, проведене через відкриту мережу, по якому передаються криптографічно захищені пакети повідомлень [1].

Створення захищеного тунелю виконують компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати ініціатором і термінатором тунелю [2]. Ініціатор тунелю інкапсулює (вбудовує) пакети в

новий пакет, що містить поряд з вихідними даними новий заголовок з інформацією про відправника й одержувача. Хоча всі передані по тунелю пакети є пакетами IP, пакети, що інкапсулюються, можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, що не маршрутизуються, таких, як Netbeui. Маршрут між ініціатором і термінатором тунелю визначає звичайна мережа IP, що маршрутизується, яка може бути й мережею відмінною від Інтернет. Термінатор тунелю виконує процес зворотний інкапсуляції – він видаляє нові заголовки й направляє кожний вихідний пакет у локальний стек протоколів або адресатові в локальної мережі.

Сама по собі інкапсуляція ніяк не впливає на захищеність пакетів повідомлень, переданих по тунелю. Але завдяки інкапсуляції з'являється можливість повного криптографічного захисту пакетів. Конфіденційність таких пакетів забезпечується шляхом їх криптографічного закриття, тобто зашифровування, а цілісність і автентичність – шляхом формування цифрового підпису. Оскільки існує велика безліч методів криптозахисту даних, дуже важливо, щоб ініціатор і термінатор тунелю використовували одні й ті ж методи й могли погоджувати один з одним цю інформацію.

Крім того, для можливості розшифровування даних і перевірки цифрового підпису при прийманні ініціатор і термінатор тунелю повинні підтримувати функції безпечного обміну ключами. Ну й нарешті, щоб тунелі створювалися тільки між уповноваженими користувачами, кінцеві сторони взаємодії потрібно аутентифікувати.

Для побудови VPN-тунеля використовуються наступні протоколи: PPTP, L2TP, IPSec, SSL [4].

Протокол IPSec. Основне призначення протоколів IPSec — забезпечення безпечної передачі даних по мережах IP.

Застосування IPSec гарантує [4]:

- цілісність переданих даних (тобто дані при передачі не перекручені, не загублені й не продубльовані);
- автентичність відправника (тобто дані передані саме тим відправником, який довів, що він той, за кого себе видає);
- конфіденційність переданих даних (тобто дані передаються у формі, що запобігає їхньому несанкціонованому перегляду).

Слід зазначити, що звичайно в поняття безпеки даних включають ще одну вимогу — доступність даних, що в розглянутому контексті можна інтерпретувати як гарантію їх доставки. Протоколи IPSec не вирішують дане завдання, залишаючи його протоколу транспортного рівня TCP. Стек протоколів IPSec забезпечує захист інформації на мережному рівні, що робить цей захист невидимим для працюючих додатків.

Фундаментальною одиницею комунікації в IP-мережах є IP-пакет. IP-пакет містить S-адресу джерела й D-адресу одержувача повідомлення, транспортний заголовок, інформацію про тип даних, прийнятних у цьому пакеті, і самі дані.

Користувач сприймає мережу як надійно захищене середовище тільки в тому випадку, якщо він певен, що його партнер по обміну — саме той, за кого він себе видає (аутентифікація сторін), що передані пакети не проглядаються сторонніми особами (конфіденційність зв'язку) і що одержувані дані не піддалися зміні в процесі передачі (цілісність даних).

Для того щоб забезпечити аутентифікацію, конфіденційність і цілісність переданих даних стек протоколів IPSec побудований на базі стандартизованих криптографічних технологій:

- обміну ключами згідно з алгоритмом Діффі — Хеллмана для розподілу секретних ключів між користувачами у відкритій мережі;
- криптографії відкритих ключів для підписування обмінів Діффі — Хеллмана, щоб гарантувати справжність двох сторін і уникнути атак типу «man-in-the-middle»;
- цифрових сертифікатів для підтвердження справжності відкритих ключів;
- блокових симетричних алгоритмів шифрування даних;

- алгоритмів аутентифікації повідомлень на базі функцій хешування.

Протокол IPSec визначає стандартні способи захисту інформаційного обміну на мережному рівні моделі OSI для IP-мережі, що є основним видом відкритих мереж. Даний протокол входить до складу нової версії протоколу IP (IPv6) і застосовується також до його поточної версії (IPv4). Для протоколу IPv4 підтримка IPSec є бажаною, а для IPv6 — обов'язковою. Протокол IPSec являє собою систему відкритих стандартів, яка має чітко обкреслене ядро, і в той же час дозволяє доповнювати її новими протоколами, алгоритмами й функціями.

Стандартизованими функціями IPSec-захисту можуть користуватися протоколи більш високих рівнів, зокрема протоколи конфігурування, а також протоколи маршрутизації.

Основними завданнями встановлення й підтримки захищеного каналу є наступні [3]:

- аутентифікація користувачів або комп'ютерів при ініціації захищеного каналу;
- шифрування й аутентифікація переданих даних між кінцевими точками захищеного каналу;
- забезпечення кінцевих точок каналу секретними ключами, необхідними для роботи протоколів аутентифікації й шифрування даних.

Для розв'язку перерахованих завдань система IPSec використовує комплекс засобів безпеки інформаційного обміну.

Більшість реалізацій протоколу IPSec мають наступні компоненти [4].

Основний протокол IPSec. Цей компонент реалізує протоколи ESP і AH. Він обробляє заголовки, взаємодіє із БД SPD і SAD для визначення політики безпеки, застосовуваної до пакета.

Протокол керування обміном ключової інформації IKE (Internet Key Exchange). IKE звичайно представляється як процес користувацького рівня, за винятком реалізацій, вбудованих в ОС.

База даних політик безпеки SPD (Security Policy Database). Це один з найважливіших компонентів, оскільки він визначає політику безпеки, застосовувану до пакета. SPD використовується основним протоколом IPSec при обробці вхідних і вихідних пакетів.

База даних безпечних асоціацій SAD (Security Association Database). БД SAD зберігає список безпечних асоціацій SA (Security Association) для обробки вхідної й вихідної інформації. Вихідні SA використовуються для захисту вихідних пакетів, а вхідні SA використовуються для обробки пакетів із заголовками IPSec. БД SAD заповнюється SA вручну або за допомогою протоколу керування ключами IKE.

Керування політикою безпеки й безпечними асоціаціями SA. Це — додатки, які управляють політикою безпеки й SA.

Основний протокол IPSec (що реалізує ESP і AH) тісно взаємодіє із транспортним і мережним рівнем стека протоколів TCP/IP. Фактично протокол IPSec є частиною мережного рівня. Основний модуль протоколу IPSec забезпечує два інтерфейси: вхідний і вихідний. Вхідний інтерфейс використовується вхідними пакетами, а вихідний — вихідними. Реалізація IPSec не повинна залежати від інтерфейсу між транспортним і мережним рівнем стека протоколів TCP/IP.

БД SPD і SAD суттєво впливають на ефективність роботи IPSec. Вибір структури даних для зберігання SPD і SAD є критичним моментом, від якого залежить продуктивність IPSec. Особливості реалізації SPD і SAD залежать від вимог продуктивності й сумісності системи.

Отже, в ході роботи були досліджені загальні модель загрози в інформаційній безпеці та модель захищеної мережі. В статті представлено основний зміст впровадження та функціонування процесу тунелювання в комп’ютерній мережі. Наведено спосіб за якого тунелювання забезпечує конфіденційність, цілісність та автентичність інформації. Також було досліджено основний протокол, що використовується для побудови VPN-тунеля, наведено його переваги, недоліки, технологічну базу та основні компоненти, що лежать в основі протоколу.

ЛІТЕРАТУРА

1. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей. - Телеком 2003. – с.87-93.
2. Браун С. Виртуальные частные сети. – Лори 2001. – с.112-120.
3. Брэгг Р., Родс-Оусли М., Страссберг К. Безопастность сетей. Полное руководство. - Эком 2006. – с.96.
4. Bollapragada V., Khalid M. IPSec VPN Desighn. - Cisco Press 2005. c.157-178.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Юдін О.К.