УДК 004.007

АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В КОРПОРАТИВНИХ МЕРЕЖАХ

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

ANALYSIS OF THE USE OF IPSEC AND SSL PROTOCOLS IN CORPORATE NETWORKS

The use of IPsec and SSL protocols to increase the level of information security in corporate networks is analyzed, the main advantages and disadvantages of these protocols are investigated the analysis of the main problems of network information security in building a virtual network is analyzed.

Проаналізовано використання протоколів IPsec та SSL для підвищення рівня інформаційної безпеки в корпоративних мережах, досліджено основні проблеми мережевої інформаційної безпеки при побудові віртуальної корпоративної мережі.

Реалізувати віртуальну приватну мережу можна різними методами. Головною метою вибору способу побудови є її продуктивність та швидкість, сумісність між сайтами і компаніями, а також необхідність підтримувати багато типів мережевих профілів зв'язку, адже неправильна побудова може зупинити роботу мережі, через малопотужність маршрутизаторів, технічні конфлікти, політичні проблеми і проблема технічного досвіду, пов'язаними з будь-яким рішенням тому найкраще використовувати спеціалізоване обладнання або програмне рішення.

Основними способами реалізації VPN є:

1. Remote access VPN
2. Site-to-site VPN

Саме реалізація за допомогою VPN з мережею "мережа - віддалений користувач" відповідає за криптографічний захист, шифрування та дешифрування даних, що передаються.

З точки зору використовуваних протоколів можна виділити кілька типів Remote Access VPN:

- використовують протоколи сімейства IPSec / IKE;
- використовують протоколи сімейства SSL / TLS;
- використовують неліцензійні та незареєстровані протоколи, що несумісні з іншими рішеннями.

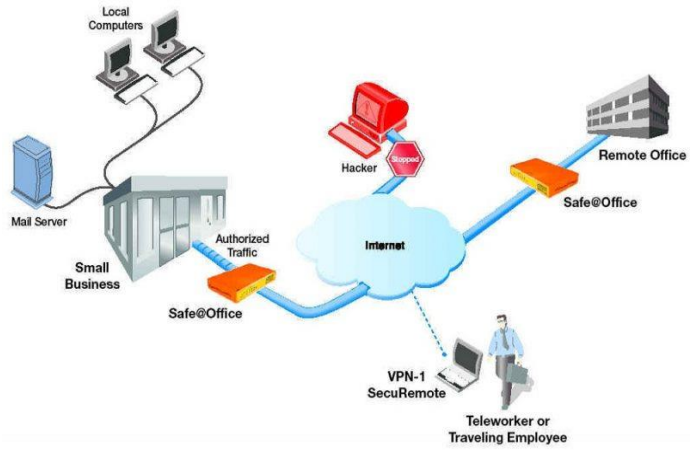

Рис. 1. Загальна схема підключення Remote access VPN.

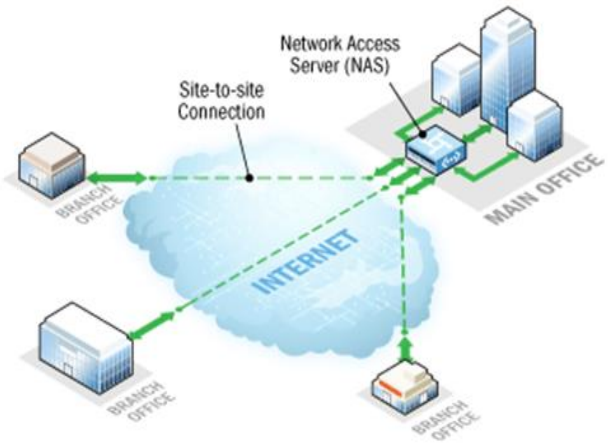

Рис. 2. Технічна реалізація VPN site-to-site.

Дані, що передаються спочатку переобразуються та шифруються VPN з віддаленим доступом, а вже тоді преедається на шлюз, що розташований поза локальною мережею. Після надходження даних до шлюзу, вони підлягаються дешифруванню і ретрансляції в локальну мережу.

Site-to-site VPN – реалізація в локальних мережах захищеного тунелю за допомогою двух маршрутизаторів для передачі даних без використання програмного забезпечення.

Існує два поширені типи VPN від сайту до сайту: інтранет та екстранет. VPN, що базуються на екстранеті, дозволяють компанії використовувати загальнодоступний Інтернет для підключення своєї локальної мережі до мереж інших фірм. Це надає змогу пересилати дані з інших будівель, зберігаючи свою локальну мережу (intranet).

Домогтися високого ступеня захищеності можна тільки при використанні передових технологій захисту мережі передачі даних. На даний час одним із засобів забезпечення безпеки в мережі Інтернет є використання протоколів захищеної передачі даних, а саме:

SSL (**S**ecure **S**ockets **L**ayer – рівень захищених сокетів)

IPSec (IP Security — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP).

Розглянемо детальніше можливості, переваги та недоліки цих протоколів.

SSL - це протокол забезпечення безпеки, який використовує сучасний метод шифрування для отримання і відправки конфіденційної інформації через Інтернет. Він працює шляхом створення захищеного каналу між браузером користувача та сайтом, який користувач збирається відвідати. Будь-яка інформація відправлена по цьому каналу шифрується з одного боку і розшифровується одержувачем на іншій стороні.

Для підвищення захисту віртуальних приватних мереж на основі шифрування можна застосувати разом з технологіями VPN на основі розмежування трафіку. Технологія розмежування трафіку неодноразово

критикувалася за ненадійність безпеки, однак на сьогодні дана проблема має способи вирішення наприклад, за допомогою мережі VPN на основі протоколів IPSec и SSL.

Широкої популярності набуває побудова VPN на основі протоколу SSL(Secure Sockets Layer) та TLS(Transport Layer Security). SSL VPN будується за допомогою криптографічних методів шифрування інформації, що надає безпечний доступ з вашого персонального ПК до різних серверів Internet-додатків. Це відбувається завдяки тому, що веб-браузери вже інтегровані під SSL, такий захист даних має не тільки надійність, а й простоту реалізації, адже не потребує постійних налаштувань від користувача.

IPSec - це набір різних відкритих алгоритмів шифрування даних, що працюють поверх стека IP. Він надає служби аутентифікації і шифрування даних на мережевому рівні і може бути представлений на будь-якому пристрої, який працює по протоколу IP. Щоб домогтися конфіденційності передачі використовують два головних протоколи безпеки, такі як заголовок автентифікації (AH- Authentication Header) та інкапсуляції пакетів (ESP-Encapsulating Security Payload), та протоколів обміну криптографічними ключами через мережу Internet (IKE-Internet Key Exchange), що забезпечують режим роботи в захищеному вигляді. Існує два основних режими для передачі пакетів даних між двома різними мережами, з якими працює IPsec VPN. Режим транспортування та тунелювання. Саме в першому режимі усі дані підтягаються шифруванню та передаються параметри захисту у заголовку IP-протоколу , у режимі тунелювання інкапсулюється увесь пакет даних, який і є носієм параметрів захисту. Протокол IPsec надає можливість виконувати наступні дії:

- шифрування даних додаткового рівня;
- забезпечення безпеки маршрутизаторів, що надсилають дані про маршрутизацію через загальнодоступну мережу Інтернет;
- забезпечення аутентифікації без шифрування;
- захист мережевих даних, шляхом побудови схеми тунелю IPsec, в якому всі дані передаються між двома кінцевими точками, шифруються, як при підключенні до віртуальної приватної мережі (VPN).

Популярність даний протокол отримав через свою простоту використання, та максимальну надійність, адже він інкапсулює передані дані двічі, це суттєво зменшує його швидкодію, у порівнянні з SSL OpenVPN або SSTP.

Проаналізувавши сучасний стан захисту інформації за допомогою протоколу SSL та виділивши його основні недоліки переходимо до розгляду протоколу IPSec. При аналізі реалізації віртуальних приватних мереж протокол IPSec суттєво домінує та має ряд переваги у порівняння з SSL.

Розглядаючи деякі основні моменти, що стосуються протоколу мережевої безпеки IPsec, можна зробити висновок, що протокол IPsec домінує в більшості реалізацій віртуальних приватних мереж.

Таблиця 1. Порівняльна характеристика IPsec та SSL.

Технологія	IPSec	SSL
Апаратна залежність	Так	Так
Код	Не потребує змін для додатків. Може вимагати доступ до вихідного коду стека TCP/IP.	Потрібні зміни в додатках. Можуть знадобитися нові DLL або доступ до вихідного коду додатків.
Захист	IP-пакет цілком. Включає захист для протоколів верхніх рівнів.	Тільки рівень додатків.
Фільтрація пакетів	Заснований на автентифікованих заголовках, адреси відправника і одержувача, і т.д. Проста і дешева, підходить для маршрутизаторів.	Заснована на вмісті і семантиці високого рівня. Більш складна.
Платформи	Будь-які системи, включаючи маршрутизатори.	В основному, кінцеві системи (клієнти/сервери), а також брандмауери.
Firewall/VPN	Весь трафік захищений.	Захищений тільки трафік рівня додатків.
Прозорість	Для користувачів і додатків.	Тільки для користувачів.

Висновки. На сьогоднішній день найбільш надійними є протоколи IPSec та SSL, але пріоритетність використання даних протоколів для побудови VPN залежить від конкретних критеріїв (необхідний тип доступу для користувачів, рівень мережевої безпеки, рівень захисту даних, необхідність масштабованості мережі в майбутньому). Проаналізувавши основні моменти, що стосуються протоколу мережевої безпеки IPsec можна відзначити, що даний протокол домінує в більшості реалізацій віртуальних приватних мереж через подвійну інкапсуляцію даних. Отже, метою подальших досліджень є удосконалення методів побудови захищених з'єднань за допомогою протоколу IPSEC за схемами «точка-точка» і «мережа-мережа».

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 (дата звернення: 28.02.2021).
2. «Концепція захищених віртуальних приватних мереж»- Електронний ресурс. – Режим доступу: https://stud.com.ua/97437(дата звернення: 04.03.2021).
3. Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. / І.І. Маракова, А.І. Рибак, Ю.С. Ямпольський; Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с. (дата звернення: 01.03.2021).
4. Биячуев Т. БЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ / Т.А. Биячуев. – СПб: СПб ДУ ІТМО, 2004. – 161 с.(дата звернення: 04.03.2021).
5. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети - анализ технологий и синтез решений. М.: ДМК Пресс, 2004. (дата звернення: 04.02.2021).
6. «What is difference between SSL VPN and IPsec VPN» - Електронний ресурс. – Режим доступу: https://uk.gadget-info.com/57085-vpn-pros-and-cons-you-should-consider-before-using-it (дата звернення: 28.02.2021).