УДК 004.738.5

АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В КОРПОРАТИВНИХ МЕРЕЖАХ

Турчин Я. В., Кононова І.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: turchyn_v@ukr.net

Analysis of the use of IPSec and SSL in corporate networks

The analysis of the use of IPsec and SSL protocols to improve the level of information security in corporate networks is conducted. Based on the analysis, the main advantages and disadvantages of these protocols are identified, the main problems of providing information security of the network during the construction of the virtual network are identified.

Проблема захисту інформації в сучасних інформаційний системах від несанкціонованого доступу та спотворення на даний є актуальною проблемою. При появі загроз, пов'язаних з можливістю втрати, спотворення, розкриття конфіденційних даних і витоку стратегічно важливої інформації, організація або держава в цілому може втратити не тільки статки, але і репутацію на політичному та економічному рівні.

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 и відправки конфіденційної інформації по Інтернету. Він працює шляхом створення захисного каналу між браузером користувача і сайтом, який користувач збирається відвідати. Будь-яка інформація відправлена по цьому каналу шифрується з однієї сторони і розшифровується отримувачем з іншої сторони. Таким чином, якщо навіть хтось зможе заволодіти цією інформацією, він не зможе її розшифрувати [2].

Однак даний сертифікат передбачений тільки для обміну даними між користувачами, які дають підтвердження SSL сертифікатам, а самопідписані сертифікати забезпечують тільки безпечну передачу даних, однак не дають підтвердження про компанію. Також самопідписані сертифікати часто використовують хакери, здійснюючи фішингові атаки, перенаправляючи користувачів на сайт зі схожою адресою.

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 (рис. 1).

Технологія	IPSec	SSL
Апаратна залежність	Так	Так
Код	Не потребує змін для додатків. Може вимагати доступ 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

Рис. 1. Порівняльна характеристика IPsec та SSL.

Протокол IPSec - це набір протоколів Internet Engineering Task Force (IETF) між двома точками зв'язку в мережі IP, які забезпечують аутентифікацію даних, цілісність та конфіденційність. Він також визначає зашифровані, розшифровані та аутентифіковані пакети. У ньому визначені протоколи, необхідні для безпечного обміну та управління ключами.

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).

Тунельний режим несе в собі шифрування всього пакету, навіть включаючи заголовок мережевого рівня. Тунельний спосіб застосовують у випадку необхідності приховування обміну інформацією організації з навколишнім середовищем. При цьому, адресне поле заголовка мережевого рівня пакета, котрий використовує тунельний режим, заповнюються міжмережевим екраном організації і не несе в собі інформації про конкретного відправника пакета даних. При передачі даних із зовнішнього середовища у внутрішню мережу організації в якості кінцевої адреси використовується мережева адреса міжмережевого екрана. Після розшифрування екраном початкового заголовка мережевого рівня пакет відправляється отримувачу.

Особливістю IPsec є те, що він реалізується на мережевому (третьому) рівні, доповнюючи його таким чином, щоб для подальших рівнів все відбувалося непомітно. Але, основна складність полягає в тому, що в процесі встановлення з’єднання двом учасникам захищеного каналу необхідно узгодити досить велику кількість параметрів. І саме вони мають аутентифікувати один одного,

згенерувати і обмінятися ключами, а також домовитися, які протоколи вони будуть використовувати для подальшого шифрування даних.

Саме з цієї причини IPsec і складається зі стека протоколів, обов'язок, яких полягає в тому, щоб забезпечити встановлення захищеного з'єднання, його роботу та управління ним. IPsec підтримує два типи схем управління ключами, за допомогою яких учасники можуть узгодити параметри сеансу. Із версією IP, IPv4, можуть бути використані або ISAKMP, або ж Simple Key Management for Internet Protocol.

З погляду політики безпеки при VPN-з'єднання використання протоколу ISAKMP (Internet Security Association and Key Management Protocol) є надійнішим, це протокол узгоджує поновлення політик безпеки (SA) між учасниками віртуального з'єднання. Саме використання цього протоколу передбачає нова версія IP, IPv6, хоча не виключається можливість використання SKIP.

Необхідно зазначити, що прокол IPsec є безпечним протоколом при наданні захисту в мережах з пакетною передачею даних, але існує думка, що присутня складність роботи і надмірність протоколу ускладнює його масове використання та набір протоколів вимагає доопрацювання.

У цій статті було розглянуто деякі основні моменти, що стосуються протоколу мережевої безпеки IPsec. Можна зробити висновок, що протокол IPsec домінує в більшості реалізацій віртуальних приватних мереж.

Отже, на основі аналізу можна зробити висновок, що на сьогоднішній день найбільш надійними являються протоколи IPSec та SSL, але пріоритет їх використання для побудови VPN залежить від конкретних критеріїв (необхідний тип доступу для користувачів, рівень мережевої безпеки, рівень захист даних, необхідність масштабованості мережі в майбутньому). Розглянувши осноні моменти, які стосуються протоколу мережевої безпеки IPSec можна відмітити, що даний прокол домінує в більшості реалізацій віртуальних приватних мереж.

Метою подальших досліджень буде удосконалення методів побудови захищених з'єднань за допомогою протоколу IPSec за схемами "точка-точка" і "мережа-мережа".

Література

1. IPSec – протокол защиты сетевого трафика на IP-уровне. – IXBT.com. – Електронний ресурс. Режим доступу: https://www.ixbt.com/comm/ipsecure.shtml.
2. Почему SSL? Три преимущества использования SSL- сертификата. – HOSTINGER.com – Електронний ресурс. Режим доступу: https://www.hostinger.com.ua/rukovodstva/ssl-tri-preimuschestva-ispolzovania-ssl-certificata/
3. IP security (IPSec). – GEEKSFORGEEKS.org. – Електронний ресурс. Режим доступу: https://www.geeksforgeeks.org/ip-security-ipsec/
4. IPSec проткол. – CRIBS.me. – Електронний ресурс. Режим доступу: https://cribs.me/zashchita-informatsii-zi/ipsec-protokol.
5. IP security (IPSec). – BMSTU.wiki. – Електронний ресурс. Режим доступу: https://ru.bmstu.wiki/IPsec_(IP_Security).