УДК 004.056.55

Фернега Є.І.
Салієва О.В.

АНАЛІЗ ТЕХНОЛОГІЙ ЗАХИСТУ ТРАНСПОРТУВАННЯ ДАНИХ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто технології захисту транспортування даних в комп'ютерних мережах. Наведено їх особливості, переваги та недоліки. Описано відмінності між технологіями SSL і TLS, NAT і PAT.

Ключові слова: Захист, інформація, транспортування, комп'ютерна мережа.

Abstract

This article discusses the technologies for protecting data transport in computer networks. Their features, advantages and disadvantages are given. The differences between SSL and TLS, NAT and PAT technologies are described.

Key words: Protection, information, transportation, computer network.

Вступ

Актуальність проблеми захисту транспортування даних безпосередньо залежить від рівня розвитку цифрових технологій. Оскільки в сучасному світі спостерігається збільшення кількості та якості нових технологій, то відповідно стає нагальною потреба в захисті інформації в комунікаційних мережах. Таким чином ще від початку створення комп'ютерів та до сьогодні, було створено багато технологій захисту транспортування даних. В цій статті розглядаються основні з них, їх особливості, переваги та недоліки.

Дослідження

Транспортний рівень призначений для передачі даних між прикладними процесами. Він забезпечує єдиний інтерфейс між ними. В залежності від вимог, які висуваються до якості передачі, технології транспортного рівня можуть забезпечувати доставку даних дейтаграмним способом або з використанням механізмів надійної доставки. Таким чином, аби захистити збережені дані, компанії можуть шифрувати або конфіденційні файли перед зберіганням, або сам накопичувач.

Проблематика стандартних технологій транспортного рівня закладена у відсутності перевірки вхідних адресантів, що в свою чергу спричиняє перехоплення та/або витік інформації, в окремих випадках підключення до відкритих портів протоколів даного рівня.

Серед усіх технологій захисту інформації на транспортному рівні, найвідомішою є SSL (Secure Socket Layer), що являє собою технологію захищених сокетів. Однак остання версія TLS (Transport Layer Security) була прийнята як стандарт, після чого технологія почала називатись SSL/TLS.

Дана технологія має наступні властивості [1]:

– Цілісність. Кожне повідомлення містить код, який дозволяє користувачеві перевірити, чи були дані змінені або втрачені під час передачі;

– Безпека. Інформація захищена за допомогою симетричного шифрування;

– Автентифікація. Асиметричне шифрування дозволяє ідентифікувати власника з'єднання.

Загалом TLS і SSL забезпечують безпечну автентифікацію та передачу даних через Інтернет, проте варто розуміти певну різницю між ними, яка перш за все, полягає у:

– Шифрованих комплектах;

– Протоколах запису;

– Автентифікації повідомлень;

– Тривожних повідомленнях.

За для більш інформативно-зрозумілого подання, відобразимо загальні відмінності у таблиці 1.

Таблиця 1 − Відмінності між SSL та TLS

SSL (Secure Socket Layer)	TLS (Transport Layer Security)
Створено компанією Netscape в 1995 році.	Створено інженерною групою IETF в 1999 році.
Існує 3 версії: – SSL 1.0 – SSL 2.0 – SSL 3.0	Існує 4 версії: – TLS 1.0 – TLS 1.1 – TLS 1.2 – TLS 1.3
Уразливості були виявлені у всіх версіях SSL, всі з яких були застарілими.	TLS 1.0 та TLS 1.1 з березня 2020 більше не підтримуються. На даний момент TLS 1.2 найбільш використовувана версія.
Веб-сервер і клієнт безпечно взаємодіють за допомогою SSL - криптографічної технології, яка забезпечує явне з'єднання.	TLS дозволяє веб-серверам і клієнтам безпечно взаємодіяти через неявне з'єднання і є альтернативою SSL.

Наступна, не менш відома технологія ACL (Access Control List) – набір правил, які забороняють або дозволяють використання мережевих ресурсів: доступу до мережі Інтернет, телефонії, відеозв'язку і т.д..

ACL працюють з IP-пакетами, але можуть також аналізувати порти протоколів керування передачею (TCP) і протоколів користувацьких дейтаграм (UDP).

Перелік функцій ACL полягає у класифікації трафіку, спочатку його потрібно перевірити, а потім виконувати дії над ним залежно від того, де ACL застосовується, наприклад [2]:

– На інтерфейсі – пакетна фільтрація;

– На лінії Telnet – обмеження доступу до маршрутизатора;

– VPN – який трафік потрібно шифрувати;

– QoS – який трафік обробляти пріорітетніше;

– NAT – які адреси транслювати.

Загалом використання списків доступу здійснюється з метою фільтрації пакетів, яка необхідна у ситуаціях, коли обладнання розташоване на межі Інтернету й приватних мереж, та небажаний трафік необхідно відфільтрувати.

Зазначимо переваги та недоліки застосування даної технології [3]:

– Основною перевагою ACL є їхня простота. ACL чітко визначає рівні доступу та дозволи, які кожен користувач, група або пристрій має в конкретній мережі. Це полегшує визначення та інтерпретацію ACL. Оскільки ці списки можна зробити зрозумілими для людини, адміністратор може з легкістю визначити поточні дозволи та елементи керування доступом, розміщені в мережі, внести зміни та відкликати дозволи за потреби;

– З іншого боку, ACL також мають ряд недоліків. Не вистачає ефективності, оскільки вони підтримують лише явно оголошені елементи захисту мережі. Зі збільшеням кількості користувачів, груп і ресурсів зростає довжина ACL і час, необхідний для визначення рівня доступу, наданого конкретному користувачеві.

– Окрім того, ACL не видно, оскільки дозволи та рівні доступу користувача можуть бути розкидані по кількох окремих списках. Аудит, зміна або скасування доступу вимагає перегляду кожного списку у середовищі організації, щоб застосувати нові дозволи.

Також варто проаналізувати такі механізми захисту мережі, як є NAT (Network Address Translation) та PAT (Port Address Translation). Дані технології використовуються для відображення незареєстрованої приватної адреси внутрішньої мережі із зареєстрованою публічною адресою зовнішньої мережі перед відправленням пакету [4].

Користувачі внутрішньої мережі з приватною (незареєстрованою) IP-адресою не можуть підключатися до Інтернету або зовнішніх мереж, оскільки кожен пристрій у мережі повинен мати унікальну IP-адресу. NAT працює з маршрутизатором, який з'єднує дві мережі і перетворює приватну адресу на публічну адресу.

Поміж того, дані технології були розроблені для зберігання IP-адрес. Це пов'язано з тим, що користувачі Інтернету зіткнулися з проблемою нестачі IP-адрес, коли кількість користувачів перевищує обмежений діапазон IP-адрес. З тієї чи іншої причини з'явилися протоколи NAT і PAT [5].

Однак варто зазначити певні розбіжності поміж даних технологій (таблиця 2).

Таблиця 2 − Розбіжності між NAT та PAT

	NAT (Network Address Translation)	PAT (Port Address Translation)
Принцип роботи	Перетворює приватну локальну IP-адресу на публічну глобальну IP-адресу.	Переводить приватні IP-адреси внутрішньої мережі у публічні IP-адреси за номерами портів.
Види	– Статичний – Динамічний	– Статичний – Перевантажений
Відносини	Над множина PAT	Форма динамічного NAT
Використовується	Адреса IPv4	IPv4 адреси разом з номером порту

Проаналізовані технології захисту інформації відповідають сучасним вимогам. Використання застарілих технологій є небезпечним. Саме тому варто звертати увагу, щодо мережевого обладнання для спеціалізованих рішень, що вирішують завдання комплексного захисту мереж.

Висновок

Підводячи підсумки даного дослідження, варто відмітити, що завдання захисту комп'ютерної мережі на транспортному рівні може бути вирішено шляхом об'єднання розглянутих технологій. Крім того, при виборі та впровадженні технологій захисту для конкретної мережі слід враховувати її структуру, спеціалізацію компанії та ймовірність конкретних атак. Налаштовуючи мережеве обладнання із застосуванням відповідних технологій, можна керувати дотриманням мережевої безпеки та реалізовувати захист якомога ближче до джерела можливого порушення, тим самим мінімізуючи негативний вплив на комп’ютерну мережу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. SSL Support Team. Pros And Cons Of SSL / HTTPS / TLS [Електронний ресурс] / SSL Support Team // SSL.COM. – 2020. – Режим доступу до ресурсу: https://www.ssl.com/article/pros-and-cons-of-ssl-https-tls/.
2. Обискалов Е. А. Забезпечення безпеки комп'ютерної мережі, побудованої на комутаторах D-Link / Е. А. Обискалов., 2019. – 86 с. – (Allbest).
3. Anna Hofman. Understanding the Pros and Cons of Access Control Lists [Електронний ресурс] / Anna Hofman // Dandelife. – 2020. – Режим доступу до ресурсу: https://dandelife.com/understanding-the-pros-and-cons-of-access-control-lists/.
4. Stanley Avery. Difference Between Network Address Translation (NAT) and Port Address Translation (PAT) [Електронний ресурс] / Stanley Avery // Javatpoint. – 2019. – Режим доступу до ресурсу: https://www.javatpoint.com/network-address-translation-vs-port-address-translation.
5. Indeed Editorial Team. NAT vs. PAT: What's the Difference? (Plus FAQ and Answers) [Електронний ресурс] / Indeed Editorial Team // Indeed. – 2021. – Режим доступу до ресурсу: https://www.indeed.com/career-advice/career-development/nat-vs-pat.

Фернега Євгеній Іванович – студент групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: evgeniyfernega@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», старший викладач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Fernega Yevheniy I. – student of KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail evgeniyfernega@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in 125 "Cybersecurity", Senior Lecturer, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com