**DOI: 10.32347/2412-9933.2021.45.102-106**
УДК 69:002;69.059

**Терентьєв Олександр Олександрович**
Доктор технічних наук, професор, професор кафедри інформаційних технологій проєктування та прикладної математики, *orcid.org/0000-0001-6995-1419*
*Київський національний університет будівництва і архітектури, Київ*
**Горбатюк Євгеній Володимирович**
Кандидат технічних наук, доцент кафедри будівельних машин, *orcid.org/0000-0002-8148-5323*
*Київський національний університет будівництва і архітектури, Київ*
**Лященко Тамара Олексіївна**
Старший викладач кафедри інформаційних технологій, *orcid.org/0000-0001-9092-0297*
*Київський національний університет будівництва і архітектури, Київ*
**Кузьмінський Олег Вікторович**
Студент, *orcid.org/0000-0002-4528-9210*
*Київський національний університет будівництва і архітектури, Київ*

# БРАНДМАУЕРИ НОВОГО ПОКОЛІННЯ: ДОСЛІДЖЕННЯ ІСТОРІЇ РОЗВИТКУ

***Анотація.*** *Спроби несанкціонованого вторгнення відбуваються доволі часто, навіть після прийняття необхідних політик та практик безпеки для інформаційної мережі. Це атаки, при яких зловмисник отримує доступ до системи за допомогою різних технік зламу. Брандмауер – це мережева система безпеки, заснована на апаратному та програмному забезпеченні, яка використовує певні правила для управління вхідними та вихідними мережевими пакетами. Брандмауер контролює доступ до ресурсів мережі за допомогою позитивної моделі управління. Існують різні традиційні брандмауери, такі як фільтри пакетів, шлюзи на рівні програми та шлюзи рівня мікросхеми, які мають свої плюси і мінуси. Щоб подолати недоліки традиційного брандмауера, вводяться брандмауери нового покоління. Наведено вивчення традиційних брандмауерів та їх еволюції до брандмауера нового покоління та його переваг. Нові брандмауери все ще належать до третього покоління, однак їх часто називають «наступним поколінням» або NGFW. Цей вид поєднує всі раніше використані підходи з поглибленим оглядом відфільтрованого контенту та його порівнянням з базою даних для виявлення потенційно небезпечного трафіку. Сучасні брандмауери часто мають вбудовані додаткові системи безпеки: віртуальні приватні мережі (VPN), системи запобігання та виявлення вторгнень (IPS/IDS), управління ідентифікацією, управління додатками та вебфільтрація. Їхня сучасна технологія може фільтрувати вихідний трафік. Це допомагає зменшити ймовірність викрадення даних зловмисниками. Крім цього, важлива функція брандмауера полягає у зменшенні ризику пристроїв стати частиною ботнету (шкідлива мережа з великою групою пристроїв, що керується кіберзлочинцями).*

***Ключові слова: брандмауер; UTM; фільтрування пакетів; мережева безпека інформаційних систем; брандмауер нового покоління***

## Вступ

Комп'ютерна мережа складається з двох або більше комп’ютерів, які підключені до обміну ресурсами, такими як принтери, сканер, бази даних, файли, програми. Комп'ютери в комп'ютерній мережі можуть бути підключені за допомогою коаксіальних кабелів, крученої пари, волоконної оптики, супутників або інфрачервоних променів світла. Коли комп'ютерна мережа підключена до Інтернету, навіть окремий комп’ютер може стати ціллю хакерів та шкідливого програмного забезпечення. Брандмауер може забезпечити достатню безпеку, яка допоможе уникнути загрози або мати засоби для боротьби з мережевими атаками. Брандмауер – це перешкода чи гарантія, яка призначена для захисту вашого ПК, планшета чи телефону від зловмисного програмного забезпечення, яке існує в Інтернеті. Брандмауер має гарантувати, що тільки авторизований користувач має доступ до операційної системи або до комп'ютера, підключеного до мережі, захищаючи приватну інформацію і захищаючи користувачів комп'ютерів від крадіжок особи. У більшості випадків брандмауери блокують несанкціонований доступ, про який користувачі комп'ютерів не знають [2]. Дані обмінюються між вашим комп’ютером, серверами та маршрутизаторами в мережі,

 

і між-мережеві вузли відстежують ці дані (що надсилаються в пакетах), щоб перевірити, чи безпечні вони чи ні.

## Архітектура брандмауера

На рисунку наведена архітектура брандмауера. Брандмауер є важливим компонентом архітектури безпеки комп'ютерної мережі. Брандмауер – це програмне забезпечення або апаратний пристрій, який фільтрує інформацію (пакети), що надходить через Інтернет до вашого персонального комп'ютера або комп'ютерної мережі. Брандмауери можуть вирішити чи дозволити, чи заблокувати мережевий трафік між пристроями на основі правил, попередньо налаштованих або встановлених адміністратором брандмауера.

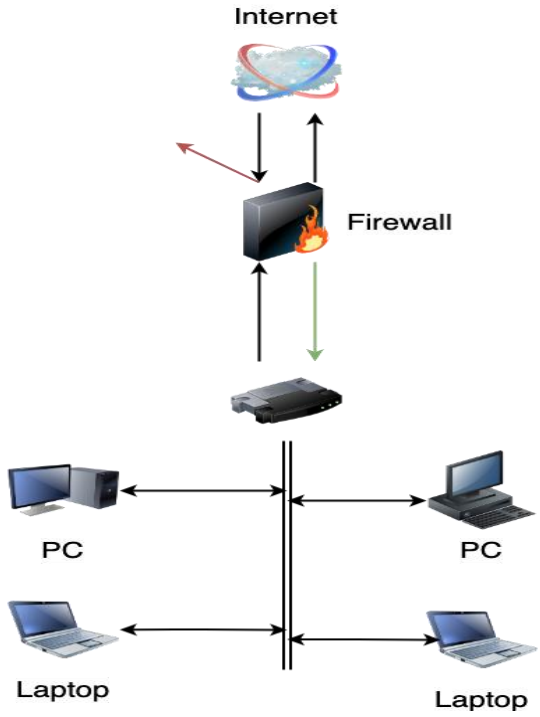


*Рисунок – Архітектура брандмауера*

## Актуальність та аналіз проблеми

З кожним роком обсяг інтернет-трафіку та пристроїв, підключених до мережі збільшується. Відповідно зростає необхідність у мережевій безпеці як персональних пристроїв, так і великих розгалужених інформаційних мереж. Брандмауер це один з основних інструментів, які використовуються для захисту мереж від несанкціонованих спроб доступу. Проте брандмауери сучасного покоління вже не здатні самостійно (без додаткових та постійних налаштувань) забезпечувати достатній рівень безпеки [1]. На заміну приходять брандмауери нового покоління.

## Мета статті

Мета активного дослідження полягає в тому, щоб узагальнити еволюцію традиційного брандмауера, в результаті чого зроблено висновок про те, що традиційний брандмауер має певні обмеження. У статті розглядаються особливості та переваги брандмауерів нового покоління.

## Виклад основного матеріалу

Брандмауер захищає комп'ютер / мережу користувача від несанкціонованого віддаленого доступу. Він може блокувати повідомлення, що посилаються на небажаний контент, і відстежує та контролює мережевий трафік всередині мережі. Відповідно до визначених політик безпеки, брандмауер – апаратний або програмний пристрій дає змогу множині мереж спілкуватися між собою. Брандмауер застосовується, коли є потреба в мережах різного рівня влади для спілкування один з одним. Програмне забезпечення брандмауера працює на хості, який підключений як до надійних, так і ненадійних мереж. Хост-операційна система відповідає за виконання функцій маршрутизації, які здатні виконувати багато операційних систем. Операційна система хоста має бути максимально захищеною до встановлення програмного забезпечення брандмауера [2].

*Традиційні типи брандмауерів*: Брандмауери можна класифікувати на три типи:

1. *Фільтри пакетів*. Набір правил застосовується на основі відповідності полів у заголовку IP або TCP до кожного вхідного пакету IP, після чого вирішується, пересилати чи відкидати його.

2. *Шлюзи рівня додатків*. Його також називають проксі-сервером, який діє як ретрансляція трафіку на рівні додатків. Використовуючи шлюзи контактів користувачів програми, запит надається лише автентичним користувачам. Шлюз додатків – це специфічні послуги, такі як: FTP, TELNET, SMTP або HTTP.

3. *Шлюзи рівня ланцюга*. Шлюз рівня ланцюга може бути окремим або спеціалізованою системою. Шлюз встановлює два TCP-з'єднання, оскільки він не дозволяє кінцеві TCP-з'єднання. Після встановлення з'єднань TCP шлюз ретранслює сегменти TCP від одного з'єднання до іншого без вивчення вмісту. Функція захисту визначає, які з'єднання будуть дозволені, а які заборонено.

Незважаючи на те, що брандмауер забезпечує безпеку для користувачів, усі вищезазначені типи брандмауера мають певні обмеження, що наведені нижче.

– Брандмауер не може сканувати кожен вхідний пакет на вміст вірусу. Отже, він не може

захистити внутрішню мережу від вірусної загрози.

– Брандмауер не забезпечує систему виявлення вторгнень (IDS).

– Брандмауер не може ефективно (швидко) обробляти Інтернет-трафік.

– Брандмауер не може захистити від будь-яких атак, які обходять брандмауер.

– Відповідно, це не захищає від внутрішніх загроз зсередини (man-in-the-middle attack).

– Брандмауери не можуть захистити від тунелю більшість протоколів програми.

Брандмауер нового покоління повинен містити:

– стандартні можливості брандмауера, такі як державна повна інспекція;

– комплексна профілактика вторгнень;

– поінформованість програми і контроль необхідний для визначення та блокування ризикованих програм;

– оновлені шляхи для включення майбутніх інформаційних каналів;

– методи вирішення проблем інформаційних загроз, що тільки розвиваються [1-3].

Розвиток традиційного брандмауера до *брандмауера нового покоління*

1. *Брандмауер єдиного управління загрозами* (UTM).

Брандмауер UTM – це лише брандмауер, який вставляє особу користувача у відповідність критеріям брандмауера, дозволяючи підприємствам налаштовувати політики та ідентифікувати користувачів безпосередньо за ім'ям користувача, а не через IP-адреси. Це потужний апаратний брандмауер, який забезпечує стаціонарний і глибокий огляд пакетів, тим самим захищаючи підприємства від атак підробки IP, контролю доступу, автентифікації користувачів, захисту мережі та рівня додатків. У цій роботі вивчено розробку критеріїв, функцій UTM та показано, наскільки UTM краще у порівнянні зі звичайним брандмауером та VPN [3].

Брандмауери UTM приносять передові технології мережевої безпеки для малого та середнього бізнесу та віддалених офісів / філій. Традиційні брандмауери можуть блокувати / приймати трафік лише на основі IP-адрес та портів і забезпечувати невеликий захист поза цим. Такий підхід швидко застаріває в сьогоднішньому Інтернеті, де багато додатків надсилають / отримують трафік через порти, які зазвичай дозволені традиційними брандмауерами.

Особливості UMTS:

– єдина апаратна платформа;

– уніфікований інтерфейс управління;

– contract Один договір / контакт постачальника;

– зниження площі центру опрацювання даних;

– зниження споживання електроенергії;

– мінімізована точка відмови / затримки;

– спрощена архітектура мережевої безпеки;

– змішаний захист від загрози.

Переваги UTM:

– зменшена складність;

– Легкість розвитку Інтеграція;

– Легка зйомка неполадок.

2. *Брандмауер нового покоління* (NGFW)

NGFW поєднує в собі функції традиційних брандмауерів, такі як фільтрація пакетів, трансляція мережевих адрес (NAT), блокування URL-адрес та віртуальних приватних мереж (VPN). Він також відповідає функціоналу якості обслуговування (QoS). Особливості містять запобігання вторгнень, перевірку SSL та SSH, глибоку перевірку пакетів та виявлення шкідливих програм на основі репутації, а також обізнаність із додатками. NGFW використовують більш ретельний стиль перевірки, перевіряючи корисні навантаження пакетів та узгоджуючи підписи на шкідливі дії, такі як експлуатовані атаки і зловмисне програмне забезпечення. Його мета – включити більше шарів моделі OSI.

Особливості:

– поінформованість додатків;

– державна інспекція;

– вбудована система захисту від втручання (IPS);

– поінформованість щодо ідентичності (користувач та група контролю);

– мостові та маршрутизовані режими;

– можливість використання зовнішніх джерел.

Переваги:

– NGFW поєднує традиційні функції брандмауера з профілактикою вторгнень, антивірусної та протокольної фільтрації;

– можливий для моніторингу та оновлення з однієї консолі;

– NGFW сканує вміст для запобігання витоку даних та зупинки загроз шляхом детальної перевірки руху в режимі реального часу;

– зменшує кількість необхідних приладів безпеки.

*3. NGFW, орієнтований на загрозу*

Ці брандмауери включають усі можливості традиційного NGFW, а також забезпечують розширене виявлення та усунення загроз.

Особливості:

– керована видимістю (аналіз загроз);

– сфокусований на загрозах;

– Установлений одразу на платформі.

Переваги:

– розуміння того, які активи найбільше ризикують;

– швидке реагування на атаки;

– краще виявляє ухильну або підозрілу активність;

– значно коротший час циклу виявлення реакції;

– легкість введення та зменшення складності.

## Висновок

У пропонованій статті подано короткий аналіз брандмауера нового покоління у порівнянні з традиційним брандмауером. Після короткого вивчення ми дійшли висновку, що брандмауер нового покоління поєднує в собі особливості традиційного брандмауера та має і свої особливості.

Система мережевої безпеки, заснована на апаратному та програмному забезпеченні, призначена для виявлення та блокування складних атак. Застосовуючи політику безпеки за допомогою спрощеного управління, вона знижує загальну вартість використання та захисту інформаційних систем.

## Список літератури

1. Гейр Е. Intro to Next Generation Firewalls // eSecurityPlanet. 2011. URL: https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html (дата звернення: 17.06.2019).
2. Гралла П. How the Internet Works. Інтіанаполіс: Que Pub, 1999. 340 с.
3. Імран М., Role of firewall Technology in Network Security. // International Journal of Innovations & Advancement in Computer Science, Том. 4, №. 12, Грудень 2015.
4. Microsoft Corporation. Improving Web Application Security: Threats and Countermeasures // Docs Microsoft. 2010. URL: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649432(v=pandp.10) (дата звернення: 18.06.2019).
5. Стварулакіс П., Штамп М. Phishing attacks and countermeasures. Кріт: Springer Science & Business Media, 2010. 867 с.
6. Канаван Дж. Fundamentals of Network Security. 1-е видання. Бостон: Artech House, 2001. 212 с.
7. Терентьєв О. О., Доля О. В., Лященко Т. О., Кузьмінський О. В. Діагностування та протидія мережевим загрозам. *Управління розвитком складних систем*. Київ, 2020. № 42. С. 125 – 131; dx.doi.org\10.32347/2412-9933.2020.42.125-131.

*Стаття надійшла до редколегії 05.02.2021*

**Terentyev Alexander**
DSc (Eng.), Associate Professor, Department of Information Technology of Design and Applied Mathematics, *orcid.org/0000-0001-6995-1419*
*Kyiv National University of Construction and Architecture, Kyiv*
**Gorbatyuk Yevhenii**
PhD (Eng.), Associate Professor, Department of Construction Machinery, *orcid.org/0000-0002-8148-5323*
*Kyiv National University of Construction and Architecture, Kyiv*
**Lyashchenko Tamara**
Senior Lecturer of the Department of Information Technology, *orcid.org/0000-0001-9092-0297*
*Kyiv National University of Construction and Architecture, Kyiv*
**Kuzminskyi Oleh**
Student, *orcid.org/0000-0002-4528-9210*
*Kyiv National University of Construction and Architecture, Kyiv*

**NEW GENERATION FIREWORKS: A STUDY OF THE HISTORY OF DEVELOPMENT**

***Abstract.*** *Attempts at unauthorized intrusion occur quite often, even after the adoption of the necessary security policies and practices for the information network. These are attacks in which an attacker gains access to the system using various hacking techniques. A firewall is a hardware and software-based network security system that uses certain rules to manage incoming and outgoing network packets. The firewall controls access to network resources through a positive management model. There are various traditional firewalls, such as packet filters, program-level gateways, and chip-level gateways, which have their pros and cons. To overcome the shortcomings of the traditional firewall, a new generation of firewalls is introduced. The article presents the study of traditional firewalls and their evolution to a new generation firewall and its benefits. New firewalls still belong to the third generation, but are often referred to as the "next generation" or NGFW. This type combines all previously used approaches with an in-depth review of filtered content and its comparison with a database to identify potentially dangerous traffic. Modern firewalls often have built-in additional security systems: virtual private networks (VPNs), intrusion prevention and detection systems (IPS / IDS), authentication management, application management, and web filtering. Their state-of-the-art technology can filter outbound traffic. This helps reduce the likelihood of data theft by attackers. In addition, an important function of the firewall is to reduce the risk of devices becoming part of a botnet (a malicious network with a large group of devices controlled by cybercriminals).*

***Keywords: firewall; UTM; packet filtering; network security of information systems; new generation firewall***

**References**

1. Geier, E., (2019). Intro to Next Generation Firewalls // eSecurityPlanet. 2011. Access mode: https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html (access: 17.06.2019).
2. Gralla, P., (1999). How the Internet Works. Indianapolis: Que Pub, 340
3. Imran, M., (2015). Role of firewall Technology in Network Security. *International Journal of Innovations & Advancement in Computer Science*, 4, 12.
4. Microsoft Corporation. Improving Web Application Security: Threats and Countermeasures // Docs Microsoft. 2010. Access mode: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649432(v=pandp.10) (access: 18.06.2019).
5. Stavroulakis, P., Stamp, M., (2010). Phishing attacks and countermeasures. Crete: Springer Science & Business Media, 867.
6. Canavan, J. (2001). Fundamentals of Network Security. 1st ed. Boston: Artech House, 212.
7. Terentyev, Alexander, Dolya, Olena, Lyashchenko, Tamara & Kuzminskyi, Oleh, (2020). Diagnosing and counteracting network threats. *Management of Development of Complex Systems*, 42, 125–131, dx.doi.org\10.32347/2412-9933.2020.42.125-131.

---

**Посилання на публікацію**

APA Terentyev, Alexander, Gorbatyuk, Yevhenii, Lyashchenko, Tamara & Kuzminskyi, Oleh. (2021). New generation fireworks: a study of the history of development. *Management of Development of Complex Systems*, 45, 102 – 106, dx.doi.org\10.32347/2412-9933.2021.45.102-106.

ДСТУ Терентьєв О. О., Горбатюк Є. В., Лященко Т. О., Кузьмінський О. В. Брандмауери нового покоління: дослідження історії розвитку. *Управління розвитком складних систем*. Київ, 2021. № 45. С. 102 – 106; dx.doi.org\10.32347/2412-9933.2021.45.102-106.