ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2024, № 1 (25)

COMPUTER SCIENCE AND CYBERSECURITY, 2024, Iss. 1 (25)

DOI: https://doi.org/10.26565/2519-2310-2024-1-05
УДК 004.056.5

ФУНКЦІОНАЛЬНІ ОСОБЛИВОСТІ ВІДОМИХ ЗАСОБІВ МІЖМЕРЕЖЕВОГО ЕКРАНУВАННЯ

Михайло Січкар[1], студент бакалавр спеціальності «Комп'ютерні системи та мережі», кафедра захисту інформаційних систем та технологій, e-mail: sichkar2020kb13@student.karazin.ua
Миколай Карпінський[2], професор, e-mail: mikolaj.karpinski@up.krakow.pl,
ORCID: https://orcid.org/0000-0002-8846-332X
Сергій Малахов[1], доктор філософії, старший науковий співробітник, кафедра комп'ютерних наук, e-mail: malakhov@karazin.ua, ORCID: https://orcid.org/0000-0001-8826-1616
[1]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна*
[2]*Інститут безпеки та комп'ютерних наук, Університет комісії національної освіти, 30-084 Краків, Польща*
Рукопис надійшов 2 квітня 2024 р. Отримано після рецензування 2 травня 2024 р.
Прийнято 3 червня 2024 р.

Анотація: В роботі коротко розглядається історія, типи та можливості основних типів фаєрволів (FW). Міжмережеві екрани є важливим засобом захисту мережевих ресурсів від різноманітних загроз інформаційній безпеці. З розвитком технологій і зміною характеру атак, особливо тих, що включають штучний інтелект (AI), брандмауери також еволюціонували, набуваючи нових функцій і можливостей. У цій роботі наведено короткий огляд основних типів та можливостей міжмережевих екранів, що забезпечують вирішення питань комплексного захисту мережевого обладнання та їх інформаційних ресурсів від сучасних загроз безпеки. Різні типи фаєрволів знаходять своє застосування в залежності від умов функціонування і призначення базової інформаційно-комунікаційної системи (ІКС), а також від місця їх (фаєрволів) інтеграції в мережеву чи віртуальну інфраструктуру сучасних інформаційних систем. Для інтегрованих мереж, що вимагають високого рівня їх безпеки, продуктивності і гнучкості, брандмауери бізнес-сегменту покоління Next-generation та Threat-focused NGFW, безумовно є кращим вибором. Звернено увагу на те, що мобільні фаєрволи повинні всіляко сприяти підтримці ресурсного консенсусу та усувати можливий диспаритет в продуктивності мережевих мобільних застосунків. Адаптивність до мобільності сучасних систем зв'язку (Wi-Fi, GSM та інші) визначає специфічність загроз безпеки для мобільних пристроїв та зумовлює їх ключову особливість. Ця особливість базується на перманентній готовності до безшовних переходів (перепідключень) між різними мережами в умовах постійного енергодефіциту та обмеженості наявних обчислювальних ресурсів (мається на увазі гаджетів). Висвітлено основні тенденції, перспективи розвитку та впровадження різних типів міжмережевих екранів, включаючи вплив штучного інтелекту, машинного навчання, хмарних технологій та Інтернету речей (IoT), а також важливі аспекти сфери їх (фаєрволів) застосування. Підкреслено, що впровадження FW не підміняє собою інших технологій і інструментів безпеки, а лише ефективно розширює наявний арсенал протидії новим загрозам безпеки (як інструмент проактивної протидії та швидкого реагування на складні мережеві інциденти). Стаття може

бути корисною для студентів, науковців та фахівців з інформаційної безпеки, які прагнуть розширити рівень своїх компетенцій, пов’язаних з розробкою і експлуатацією сучасних технологій міжмережевого захисту.

Ключові слова: *FW, фаєрвол, інформаційна безпека, загрози безпеки, зловмисне програмне забезпечення*

Як цитувати: Січкар М., Карпінський М., Малахов С.. Функціональні особливості відомих засобів міжмережевого екранування. *Комп’ютерні науки та кібербезпека.* 2024; № 1(25): С. 53–65. https://doi.org/10.26565/2519-2310-2024-1-05

In cites: Sichkar M., Karpinski M., Malakhov S. (2024). Functional features of well-known means of network shielding. *Computer Science and Cybersecurity.* 1(25): 53–65. https://doi.org/10.26565/2519-2310-2024-1-05 (in Ukrainian)

1. Вступ

У сучасному світі інформація є найціннішим ресурсом, тому питання безпеки функціонування сучасних інформаційно-комунікаційних систем (ІКС) стають критично важливим напрямом діяльності, оскільки масштаби та складність нових кіберзагроз дедалі тільки зростають. В рамках заходів з протидії сучасним мережевим атакам, важливу роль незмінно продовжують відіграють міжмережеві екрани (*фаєрволи, від англ. Firewall*). Ці засоби, безперечно, є одними з найефективніших та найпоширеніших інструментів захисту інформаційних ресурсів сучасних інформаційних систем та/чи окремих мобільних гаджетів пересічних користувачів, від різноманітних типів мережевих загроз [1-7]. Вони надають можливість управління доступом до різних сегментів мережі (*безвідносно цілей їх утворення*), аналізуючи циркуляцію мережевого трафіку, мережеву поведінку користувачів та мережеву активність відповідних додатків, завчасно виявляючи й блокуючи потенційно небезпечну (недекларовану) мережеву активність [3-8]. Враховуючи неперервний розвиток загроз безпеки і еволюцію технологій та засобів їх парирування, вочевидь, що розгляд питань, щодо узагальнення основних функціональних особливостей, та практики використання відомих рішень міжмережевого екранування, є безумовно актуальним.

2. Основна частина

В загальному випадку, фаєрвол - це фізичний пристрій або спеціалізоване програмне забезпечення, що контролює мережевий трафік між двома чи більше мережами та/або різними сегментами однієї і тієї ж мережі, згідно з встановлених для неї (*мережі чи сегменту мережі*) набором правил безпеки. Іншими словами, *Firewalls* використовують відповідні правила, щоб дозволити чи заборонити певним пакетам даних циркулювати між різними мережами та/чи різними сегментами однієї мережі. Як правило, файрволи встановлюють між локальною/внутрішньою мережею підприємства та Інтернет. Таке розміщення *Firewalls* покликане захистити внутрішні інформаційні ресурси корпоративної ІКС від шкідливого програмного забезпечення (ПЗ) та інших − «зовнішніх» загроз з Інтернету. Крім того, фаєрволи активно використовуються для контролю циркуляції трафіку всередині периметру безпеки корпоративної ІКС (*тобто за 1-м, вхідним Firewall*), наприклад: - для контролю мережевої активності на всіх внутрішніх шлюзах–мостах і блокування доступу внутрішніх користувачів до певних веб-сайтів та/або додатків.

В межах своїх функціональних задач, фаєрвол аналізує весь мережевий трафік, що циркулює в місті його інтеграції, де для кожного пакету даних здійснюється їх верифікація на відповідність наперед заданим правилам. Так, якщо пакет відповідає дозволеним − легітимним правилам мережевої активності, то фаєрвол транслює його далі. В іншому випадку, мережева активність припиняється у відповідності із заданими сценарієм поточних налаштувань кожного окремого *Firewalls* (*наприклад, блокування назавжди чи тимчасово (на певний час) або перенаправлення пакетів к іншому узлу/маршруту тощо*).

В цілому, правила функціонування *Firewalls* налаштовуються відповідно до потреб організації. Наприклад, корпоративною політикою інформаційної безпеки (ПІБ), може передбачатися доступ до Інтернету лише певним користувачам, комп'ютерам та/або програмам. Крім того, може бути заборонений доступ до певних зовнішніх інформаційних ресурсів (*веб-сайтів і онлайн сервісів*), так й деяких внутрішніх функцій (*наприклад, доступ до корпоративних принтерів для певної групи користувачів та ін.*).

Таким чином міжмережеві екрани є вкрай важливим елементом в загальній системі безпеки інформаційних ресурсів сучасних ІКС та забезпечують адаптивний захист мережевого устаткування від деструктивного впливу шкідливого ПЗ в дуже широкому спектрі загроз, причому, як зовнішнього, так і внутрішнього походження [4-5, 9]. Для цілісного розуміння принципів функціонування *різних* типів фаєрволів, важливо усвідомлювати їх «місце» і роль на відповідних рівнях моделі *OSI* та виокремлювати *основні етапи* розвитку технологій міжмережевого екранування, як окремої складової загального процесу еволюції інформаційних технологій.

Етапи еволюції засобів міжмережевого екранування та їх особливості.

У 1988 році компанія *«Digital Equipment Corporation»* (DEC) запропонувала перше покоління засобів міжмережевої фільтрації трафіку, відомих як «*Packet-Filter Firewall*» чи фаєрвол з фільтрацією пакетів [11]. У 1989 році з'явилось друге покоління, відоме як «*Stateful Firewall*». Третє покоління фаєрволів прикладного рівня, було визначено в 1991 році. У 2004 році «Міжнародна корпорація з обробки даних» (*IDC*) вперше використала термін «Об'єднаний брандмауер загроз» (*UTM - Unified Threat Management*). У 2009 році компанія *Gartner* запропонувала концепцію фаєрволу нового покоління, визначив її як «*Next-Generation Firewall*» (*NGFW*) [5, 10].

Фаєрволи 1-го покоління проводили аналіз пакетів інформації, які циркулювали між комп'ютерами в мережі. Правила фільтрації базувалися на різних параметрах, таких як адреси джерела та вузлу призначення, використовувані протоколи та номери портів на обох сторонах взаємодіючих комп'ютерів. При цьому, цей тип фаєрволів не враховував стан з'єднання пакету та не зберігав його стан. Тому його часто називали «брандмауерами без стану» (*Stateless Firewalls*). Вони операційно працювали на мережевому рівні моделі *OSI* [7] та були відомі, як фаєрволи «рівня мереж» (*Network Layer Firewalls*) [12].

У 1991 році, DEC представила рішення 3-го покоління (*SEAL - Secure External Access Link*), яке отримало назву «Брандмауер на рівні застосунків». Брандмауери на рівні застосунків (наприклад, *Gauntlet* від *Trusted Information Systems* та *FireWall-1* від *компанії Check Point*, у 1994 р.) керували трафіком застосунків, які підключалися до Інтернет та/чи інших «зовнішніх мереж» і адміністрували трафік на протоколах *FTP*, *Telnet* та *HTTP* [4, 10].

Як вже було зазначено вище, у 2004 році *IDC* запроваджує новий концепт мережевої безпеки - *UTM*, в межах якої еволюція «традиційних» брандмауерів (*контроль портів та протоколів*) трансформується у спробу створення комплексного рішення мережевої безпеки. *UTM* передбачає інтегроване використання різноманітних інструментів/засобів, таких як: − мережевий *FW*, фільтрація web-сторінок, шлюзовий антивірус, антиспам, *VPN* та ін. [7, 10].

У 2009 році Gartner® представляє нову концепцію - *Next-Generation FW*, яка в рамках одного рішення поєднує ідеї «традиційного» фаєрволу та нові технології, такі як: − системи виявлення і запобігання вторгненням (*IDS/IPS*); − глибока інспекція пакетів (*DPI*); − «пісочниця»; − управління застосунками; − фільтрація *URL*-адрес; − захист від поліморфного шкідливого ПЗ; − профілювання мережі; − політика ідентифікації; − *VPN* та ін. Головною особливістю *NGFW* є використання *DPI* на рівні застосунків, що відрізняє його від усіх попередніх рішень *FW*, які обмежувались моніторингом портів і протоколів [4-5, 7, 10, 12-13]. Комплексування в межах *NGFW* зазначених властивостей і функціоналу в значній мірі сприяє підвищенню загального рівня мережевої безпеки сучасних ІКС.

Цілком очевидно, що різні типи фаєрволів знаходять свою нішу застосування в залежності від умов функціонування й призначення базової ІКС [3, 7-8, 13-18] та місця їх (*FW*) інтеграції в мережевої чи віртуальної [1, 5-6] інфраструктурі сучасних інформаційних систем. Стисло розглянемо основні властивості зазначених різновидів *FW* [3-4, 7-18].

1. Proxy FW.

Проксі (*proxy*) фаєрвол вважається найбезпечнішим і найнадійнішим типом фаєрволів, який аналізує повідомлення на прикладному рівні, намагаючись захистити ресурси мережі. *FW* цього типу обмежують кількість програм, які здійснюють мережеву активність, що сприяє підвищенню безпеки, однак процес фільтрації потенційно може вплинути на швидкість і в деякій мірі на функціональність інформаційних систем, що захищаються.

2. UTM FW.

UTM фаєрволи є реалізацією комплексного рішення, котре поєднує функції антивірусного ПЗ і розширеної фільтрації контенту, що, вкупі, забезпечує протидію несанкціонованому витоку даних (тобто, функції *DLP*). В даному разі важливим є те, що з’являється можливість заощадити на витратах і технічному обслуговуванні такої системи, оскільки в цьому разі потрібно подбати лише про єдине рішення для управління загрозами.

3. Stateful Inspection FW.

Фаєрволи з перевіркою стану - це варіант захисту, який контролює стан активних мережевих з'єднань і одночасно аналізує вхідний трафік на предмет потенційних ризиків та загроз. Брандмауери із перевіркою стану функціонують на 3-му та 4-му рівнях моделі *OSI*, «переглядаючи» вміст пакетів даних і порівнюючи його з пакетами даних, які вже успішно пройшли через процес аналізу й фільтрації.

4. Next-generation FW.

Фаєрволи цього типу створені шляхом об'єднання функцій традиційних брандмауерів з різними мережевими засобами безпеки, перш за все системи запобігання вторгненням (*IPS*) та глибинний інспектування пакетів (*DPI*). *NGFW*, порівняно з іншими типами файрволів, зазвичай, використовують більш ретельний механізм перевірок, оцінюючи вміст пакетів і збігаючи їх сигнатури з відомими шкідливими зразками (*в т.ч. зловмисного ПЗ*). *FW* покоління *Next-generation* надають адміністраторам безпеки, кращу обізнаність і контроль над використовуваним ПЗ, а також більш глибші можливості, щодо спостереження поточної мережевої активності в тому числі за рахунок широкого залучення можливостей штучного інтелекту і машинного навчання (*AI/LM*) [19].

5. Threat-focused NG FW.

Ці фаєрволи є специфічною категорією *NGFWs*, які мають своїм основним завданням,

протидію впливу зловмисного ПЗ, атак на прикладному рівні та таргетованих атак. Крім того до сфери впливу *Threat-focused FW*, слід віднести протидію всім видам загроз, в тому числі й раніше невідомим.

6. Virtual FW.

Віртуальний або «хмарний» фаєрвол, це тип міжмережевого екрану, що призначений лише для сценаріїв, де розгортання апаратних брандмауерів є складним чи навіть неможливим завданням. Наприклад, у публічних/приватних хмарних середовищах чи *SDN* (*програмно-визначених мережах*). Також, вони можуть бути впроваджені, як віртуалізовані демони [1] для *NGFW* релізів.

Результати узагальнення основної функціональності, що притаманна для різних типів міжмережевих екранів, представлені в Табл.1 [4]. Вочевидь, така компіляція даних має вербальний характер, так як можливості різних релізів одного і того ж *FW*, можуть помітно відрізнятися між собою, в залежності від ступеню поточної актуалізації відомих загроз (*тобто, врахування їх механізмів й принципів дії*) [2, 15] та специфіки роботи ІКС (*топології, інтерфейсів, ступеню критичності основних процесів, швидкодії і типу використовуваних каналів передачі даних та ін.*) [4 ,7-8, 19]. Проте, вона надає кумульоване уявлення про загальний розподіл функціональних можливостей для основних різновидів засобів міжмережевого екранування та висвітлює найбільш показові відмінності у їх властивостях та комплектації відповідних продуктів.

Підсумовуючи відомості табл.1, можна зробити висновок, що засоби міжмережевого екранування потрібно обирати виключно під конкретну задачу та властивості базової ІКС. В рамках такого цілепокладання слід враховувати, що *UTM* рішення наближаються за своїми можливостями до *NGFW*, а для створення надійного безпекового базису для критично важливих ІКС, безумовно потрібно звернути увагу на технології *NGFW* та *Threat-focused NGFW*, які продовжують стрімко еволюціонувати.

Вочевидь, що торкаючись проблематики розвитку технологій і засобів міжмережевого екранування, ми неодмінно торкаємося питань, що стосуються функціональних особливостей *FW*, котрі мають різну цільову аудиторію, а саме: − рішення для корпоративного сегменту (*бізнес-клас*); − для приватних користувачів (*споживчій клас*).

Зрозуміло, що брандмауер споживчого класу реалізує більш простий користувальницький інтерфейс та має декілька звужений набір можливостей й налаштувань, що зумовлено необхідністю захисту лише декількох користувачів та/чи пристроїв з відносно простою топологією локальної мережі, якщо така взагалі є (*безвідносно інтерфейсів утворення цих мереж*). Інакше кажучи, для фаєрволів споживчого класу безумовними пріоритетами є їх швидкість і зручність використання (*Usability*), особливо з огляду на некомпетентність більшості кінцевих користувачів з питань забезпечення ІБ.

В загальному випадку *FW споживчого класу* призначені для «простої» домашньої мережі, з набагато меншим обсягом циркулюючих даних і меншим різновидом мережевих взаємодій та використовуваних протоколів. Ці фаєрволи в своєї переважній більшості є втіленням «реактивної» концепції мережевого захисту, що декілька знижує їх потенціал проти раніш невідомих загроз безпеки [2, 5, 15, 19]. Внаслідок власної функціональної обмеженості засоби міжмережевого екранування споживчого класу не можуть забезпечити виконання вимог з безпеки галузевих стандартів, що декларуються для відповідних бізнес-рішень (*наприклад, вимог стосовно обробки персоніфікованих даних*). При цьому, для фаєрволів бізнес-класу безумовними пріоритетами є безпека, котра включає в себе, в т.ч. таки можливості й якості, як віддалений доступ і масштабованість.

Таблиця 1 - Узагальнення функціоналу для основних типів фаєрволів
Table 1 - Generalization of functionality for the main types of firewalls

Підтримувані функції	**Тип реалізації FW**					
	Proxy FW	***UTM***	***Stateful Inspection FW***	***NGFW***	***Threat-focused NGFW***	***Virtual FW***
Антивірус та антиспам	-	+	-	+	+	+
Безпека *E-mail*	-	+	-	+	+	+
Управління додатками	-	+	-	+	+	+
Звітність	+	+	+	+	+	+
Управління репутацією та ідентифікацією	-	+	-	+	+	+
Рівень в моделі OSI	*7*	*7*	*3-4*	*2-7*	*2-7*	*3-4*
Управління пропускною здатністю	-	+	-	+	+	+
Фільтрація контенту *(web- сторінок)*	-	+	-	+	+	+
Фільтрація трафіку *(порти, IP/MAC - адреси, протоколи)*	+	+	+	+	+	+
DLP *(захист від витоку даних)*	-	+	-	+	+	+
IDS *(система виявлення вторгнень)*	-	+	-	+	+	+
IPS *(система запобігання вторгненням)*	-	+	-	+	+	+
NAT *(Network Address Translation)*	-	+	+	+	+	+
VPN *(Virtual Private Network)*	-	+	-	+	+	+

До основних складових захисту корпоративних FW слід віднести наступні [3-4, 7-14]:

- парирування загроз, в т.ч. за окремими векторами атак (*тобто, за конкретними вразливостями та/чи додатками*);
- поглиблений контроль поточних процесів для визначеного переліку ПЗ і використовуваного мережевого устаткування;
- перевірка *SSL* (*Secure Sockets Layer*);
- використання можливостей *AI* та *ML* для покращення процесу фільтрації та детектування ознак аномальної мережевої активності [1, 6, 19];
- аналіз з використанням репутаційних механізмів (*хмарних сервісів*);
- фільтрація трафіку на основі критеріїв геолокації і часових ознак;
- інтеграція з активним каталогом;
- фільтрація вмісту пакетів;
- антивірусні і антишпигунські функції;

- віддалена консоль безпеки/адміністрування;

- віртуальна кластеризація виконуваних модулів та динамічне балансування пропускної здатності (*тобто продуктивності фільтрації*);

- управління «активною» конфігурацією (*технологія програмних блейдів*).

Як слід з наведеного переліку складових, фаєрволи *бізнес-сегменту* розроблені з урахуванням набагато більш складних та декларованих умов їх подальшого застосування. Тому цілком зрозуміло, що корпоративні *FW* нового покоління в свої функціональній парадигмі орієнтуються на умови активного та адаптивного захисту критично важливих даних і мережевого устаткування від широкого спектру нових загроз [2, 15]. Для цього вони розробляються з набагато більш досконалим та різноманітним набором інструментів і функцій, зумовлених широким спектром нішевих інтересів, особливо в галузі високих технологій. До того ж фаєрволи *бізнес-класу* часто постачаються з постійною підтримкою, оновленнями та управлінням з боку фахівців розробника [4].

Таким чином, можна стверджувати, що фаєрволи споживчого класу, в своєї переважній більшості, надають їх користувачам базові функції (*такі як контроль портів/протоколів, захист від несанкціонованого доступу тощо*), а рішення бізнес-класу пропонують «агресивно» проактивний набір функцій, наприклад: - виявляють і блокують складні атаки та спроби ведення мережевої розвідки, забезпечують детальний контроль пакетів (*DPI*), підтримують функції *DLP* та *IPS* тощо. Крім того для рішень корпоративного сегменту більш виражена можливість оперативних оновлень діючих алгоритмів та процедурних блоків для ефективної протидії до змінних (поліморфних) загроз. На їх фоні фаєрволи споживчого рівня в більшої мірі сфокусовані на питаннях простоти використання, швидкодії та низької вартості підписки, а склад їх функціоналу орієнтований на забезпечення безпеки невеликих мереж з низьким рівнем ризиків. При цьому для складних, інтегрованих ІКС, котрі вимагають високого рівня їх безпеки, продуктивності і гнучкості (масштабованості), брандмауери бізнес-рівня покоління *Next-generation* та *Threat-focused NGFW*, безумовно є кращим вибором. В разі необхідності захисту і моніторингу програмно емульованих [1, 19] середовищ з глибоким рівнем вкладеності й кластеризації відповідних віртуалізованих платформ, слід звернути увагу на рішення рівня *Virtual FW*.

Специфіка реалізацій фаєрволів для мобільних платформ.

Мобільний фаєрвол - це програмний засіб безпеки, що протидіє мережевим загрозам, які притаманні для мобільних пристроїв, працюючи згідно принципів «традиційних» *FW*, однак на відміну від них, розроблений спеціально для умов користування саме мобільних гаджетів. До таких умов насамперед слід віднести наступні:

- високий ступінь мобільності гаджетів по відношенню до комунікаційних шлюзів верхнього рівня ієрархії (*провайдерів послуг*);

- обмеженість бортових обчислювальних можливостей (*перш за все, процесор та оперативна пам'ять*);

- обмеженість ємності *вбудованого* джерела електроживлення;

- необхідність адміністрування та врахування поточних параметрів енергоспоживання для «активних» додатків та резидентних процесів;

- переривчастість сеансів зв’язку;

- обмеженість і нестабільність у часі доступної смуги пропускання та необхідність буферизації даних для «вирівнювання» трафіку;

- яскраво виражена асиметричність трафіку (вгору/вниз) для більшості програмних додатків;

- можливість існування великої кількості проміжних репітерів та зростання пінг-таймінгу;

- необхідність підтримки режиму реального часу, для певного числа додатків (наприклад, *Skype*);

- можливість роботи пристрою, як вхідний proxy або шлюз для сукупності інших пристроїв (в т.ч. обслуговування скаттернет (*Scatternet*));

- висока динамічність мережевого оточення в рамках підтримуваної *Scatternet* (*в т.ч. в межах реалізації технології Інтернету речей - IoT*);

- робота через велику кількість випадкових точок доступу (шлюзів) з неконтрольованою на них ПІБ та фільтрації трафіку;

- різноманіття стандартів передачі та порядку їх використання в рамках однієї сесії (*в тому числі супутниковий канал зв’язку*) та ін..

В загальному випадку мобільний фаєрвол контролює обмін даними та забезпечує безпеку підключень до мережі (*в т.ч. через віртуальні приватні мережі - VPN*), цілеспрямовано оптимізуючі параметри використання наявних ресурсів і циркуляцію трафіку за всіма інтерфейсами (протоколами) взаємодії. Адміністрування ресурсами гаджету підтримується, завдяки здатності контролювати використання апаратних ресурсів з боку додатків, що здійснюють мережеву взаємодію та параметри обробки самих даних (*наприклад, за рахунок зміни бітрейту мультимедійного контенту для відповідного мережевого застосунку, в залежності від параметрів наявної смуги частот (вільного канального ресурсу)*). Таким чином мобільні фаєрволи повинні всіляко сприяти підтримці ресурсного консенсусу та усувати можливий диспаритет в продуктивності мобільних застосунків. В межах виконання зазначених вище завдань, мобільний *FW* на базовому рівні захисту повинен запобігати мережеву взаємодію з небажаними ресурсами, протидіяти підміні IP-адрес й спуфінгу, контролювати перелік додатків, які здійснюють мережеву взаємодію та не дозволяти пакетам даних, що містять шкідливе навантаження, перетинати умовний «периметр безпеки» гаджету. Це стає особливо актуально, як превентивний захід для забезпечення безпеки корпоративного трафіку даних в разі використання гаджетів, як віддаленого терміналу/консолі співробітників компанії (установи).

Таким чином, мобільні *FW* відрізняються від «традиційних» міжмережевих екранів завдяки всебічного врахування проблематики і умов функціонування мобільних пристроїв та мобільних мереж. Розробники відповідних рішень приділяють особливу увагу питанням економії заряду вбудованого акумулятора, використовуючи ресурсозберігаючі та обчислювально оптимізовані технології для мінімізації проявів й наслідків енергодефіциту при експлуатації мобільних платформ. При цьому, захист конфіденційності має першорядне значення, де основна увага приділяється контролю мережевої активності мобільних додатків для запобігання спробам несанкціонованого витоку даних і доступу до чутливої інформації чи окремим функціям самого гаджету. Усуваючи специфічні для мобільних гаджетів загрози безпеки, вони протидіють впливу шкідливого ПЗ та спробам реалізації найбільш поширених атак: – фішингу, спуфінгу (наприклад, *DNS Spoofing*) [15], таргетований спам та ін.

Адаптивність до мобільності сучасних мереж зв’язку, водночас, визначає специфічність загроз безпеки для мобільних пристроїв та зумовлює їх ключову особливість, яка базується на перманентній готовності до переходів (пере підключень) між різними мережами (*і цей процес значно складніший, ніж звичайний хендовер (handover) у рамках однієї мережі*). Зрозуміло, що зручні інтерфейси покращують *usability* мобільних *FW* завдяки сповіщенням у реальному часі та легким і «прозорим» налаштуванням. По суті, мобільні фаєрволи надають пріоритет безпеці, конфіденційності та забезпечення параметричного консенсусу для виконуваних процедур, з урахуванням унікальних характеристик і ризиків, що характерні для мобільних платформ. В рамках зазначеної цільової парадигми, мобільні *FW* в найбільшої мірі сфокусовані на виконанні наступних завдань [20-21]:

- Веб-фільтрація (*для блокування шкідливого вмісту*);
- Блокування небажаних web-джерел (*репутаційні хмарні сервіси, стоп-лист, батьківський контроль та ін.*);
- Впровадження політик/сценаріїв перегляду окремих *web*- сторінок;
- Контроль *Cookie* та скриптів;
- Усування передумов експлуатації вразливостей/експлойтів;
- VPN для безпечного підключення на «невідомих» точках доступу;
- Захист від відомих типів атак (*згідно відомих поведінкових сигнатур*);
- Блокування використання даних гаджету в межах задіяних обмежень;
- Підтримка правил контролю для різних типів трафіку і додатків;
- Управління напрямом трафіку додатків для блокування небажаних сеансів (*як функціонал DLP*);
- Блокування спаму і фішингових посилань в *E-mail* та *SMS* (*Smishing*);
- Нормування трафіку за типами інтерфейсів та звітування (*інколи логування*) про стан комунікаційної активності платформи.

3. Висновки

1. Міжмережеві екрани є вкрай важливою складовою в загальній системі безпеки інформаційних ресурсів сучасних ІКС та забезпечують адаптивний захист мережевого обладнання від деструктивного впливу широкого спектру загроз, як зовнішнього, так і внутрішнього походження.

2. Різні типи фаєрволів знаходять своє застосування в залежності від умов функціонування і призначення базової ІКС, а також від місця їх інтеграції в мережеву та/чи віртуальну інфраструктуру сучасних інформаційних систем.

3. Засоби міжмережевого екранування слід обирати виключно під конкретну задачу та властивості базової ІКС. В рамках такого цілепокладання слід враховувати, що *UTM* рішення наближаються за своїми можливостями до *NGFW*, а для створення надійного безпекового базису критично важливих ІКС, потрібно звернути увагу на технології *NGFW* та *Threat-focused NGFW*, які продовжують еволюціонувати.

4. Для інтегрованих ІКС, що вимагають високого рівня їх безпеки, продуктивності і гнучкості, брандмауери бізнес-сегменту покоління *Next-generation* та *Threat-focused NGFW*, безумовно є кращим вибором. При необхідності захисту та моніторингу програмно емульованих мережевих середовищ з глибоким рівнем кластеризації і відтворення відповідних віртуалізованих співтовариств, слід звернути увагу на рішення рівня *Virtual FW*.

5. Мобільні фаєрволи повинні всіляко сприяти підтримці ресурсного консенсусу та усувати можливий диспаритет в продуктивності мережевих мобільних застосунків. В рамках виконання цих завдань, мобільні *FW* повинні мати дружній *Usability*, запобігати мережеву взаємодію з небажаними ресурсами, протидіяти спуфінгу у всіх його проявах, контролювати перелік додатків, які здійснюють мережеву взаємодію та не дозволяти пакетам даних, що містять шкідливе навантаження, перетинати умовний «периметр безпеки» гаджету.

6. Адаптивність до мобільності сучасних мереж зв’язку (*Wi-Fi, GSM, CDMA, Bluetooth, супутникові канали зв’язку та ін.*), водночас, визначає й специфічність загроз безпеки для мобільних пристроїв та зумовлює їх ключову особливість, котра базується на перманентній готовності до «безшовних» переходів/перепідключень між різними мережами в умовах постійного енергодефіциту та обмеженості наявних обчислювальних ресурсів.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

Список літератури:

1. Азаров, С., Нємцев, М., & Малахов, С. Огляд аналогій та обґрунтування принципів створення демон юнітів відстеження мережевої активності користувачів. *Proceedings of the XX International Scientific and Practical Conference.* Graz, Austria. 2023. Pp. 447-453. https://doi.org/10.46299/ISG.2023.1.20
2. Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека*, (2), 35-40. https://periodicals.karazin.ua/cscs/article/view/21039/19745
3. Sichkar, M., & Pavlova, L. (2024). A short survey of the capabilities of Next Generation firewalls. *Computer Science and Cybersecurity*, (1), 28-33. https://periodicals.karazin.ua/cscs/article/view/23090
4. Січкар, М., & Малахов, С. Узагальнення особливостей відомих засобів міжмережевого екранування. *Proceedings of the XXI International Scientific and Practical Conference.* Sofia, Bulgaria. 2024. URL: https://isg-konf.com/category/archiv-conference-rub/
5. Кохановська, Т., Нарежний, О., & Дьяченко, О. (2020). Дослідження можливостей технології Honeypot. *Комп'ютерні науки та кібербезпека*, 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03
6. Михайленко Д., Нємцев М. Особливості технології мережевих пасток як інструменту активного захисту та аналізу дій атакуючої сторони. *Proceedings of the XXI International Scientific and Practical Conference.* Melbourne, Australia. 2023. Pp. 483-487. https://doi.org/10.46299/ISG.2023.1.21
7. Джон Маллери, & Джейсон Занн (2007). Безопасная сеть вашей компании. (Е. Линдеманн, пер. с англ.). – М.: НТ Пресс
8. Рондалєв, Д., Мелкозьорова, О., & Нарєжній, О. (2019). Особливості функціонування корпоративного міжмережевого екрану та питання взаємодії з системою IDS. *Комп'ютерні науки та кібербезпека*, (3), 11-21. URL: https://periodicals.karazin.ua/cscs/article/view/15614/14707
9. Брандмауер (FireWall). URL: http://surl.li/tuggo
10. Who Invented the Firewall? History, Types and Generations of Firewall. 28th September 2023 by Manish Sahay https://www.thepcinsider.com/who-invented-firewall-history-evolution-types-generations/
11. What Is a Firewall? URL: http://surl.li/fdtbp
12. Next-Generation Firewalls. URL: https://www.paloaltonetworks.com/network-security/next-generation-firewall
13. 8 Types of Firewalls: Know Which One Is Best for Your Network By John Villanueva / May 19, 2022. URL: https://techgenix.com/types-of-firewalls
14. Information Technology Gartner Glossary. URL: https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws
15. Яремчук, К., Воскобойников, Д., & Мелкозьорова, О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. *Комп'ютерні науки та кібербезпека*, (2), 28-34. https://periodicals.karazin.ua/cscs/article/view/21038/19744
16. What is a Next-Generation Firewall (NGFW)? URL: https://www.zenarmor.com/docs/network-security-tutorials/next-generation-firewall
17. Top Next-Generation Firewall (NGFW) Software By Jenna Phipps July 19, 2022. URL: https://www.cioinsight.com/security/ngfw-software/#What-is-a-next-generation-firewall
18. What are the Types of Firewalls? URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-firewall
19. Михайленко, Д., Чорна, Т. & Малахов, С. Використання можливостей AI при реалізації Static та Dynamic Honeypot для покращення параметрів захисту інформаційних ресурсів. *Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції*, (с. 54-57). 7.10.2022 р. Суми, Україна: МЦНД. https://doi.org/10.36074/mcnd-07.10.2022

20. How do firewalls for mobile devices differ from traditional firewalls? URL: https://www.xcel.com/how-do-firewalls-for-mobile-devices-differ-from-traditional-firewalls/
21. How mobile firewalls protect against unique threat vectors. URL: http://surl.li/tugix

FUNCTIONAL FEATURES OF WELL-KNOWN MEANS OF NETWORK SHIELDING

Mykhailo Sichkar[1], CSD Student (bachelor), Department of Security of Information Systems and Technologies; e-mail: sichkar2020kb13@student.karazin.ua;
Mikolaj Karpinski[2], Prof., DSc, Professor (Full); e-mail: mikolaj.karpinski@up.krakow.pl;
ORCID: https://orcid.org/0000-0002-9790-7260
Serhii Malakhov[1], Ph.D., Senior Researcher, Computer Science Department;
e-mail: malakhov@karazin.ua; ORCID: https://orcid.org/0000-0001-8826-1616
[1] *V. N. Karazin Kharkiv National University, Ukraine*
[2] *VInstitute of Security and Computer Science, University of the National Education Commission, Krakow, Poland*
Manuscript was received April 2, 2024; Received after review May 2, 2024; Accepted June 3, 2024

Abstract. The work briefly reviews the history, types, and capabilities of the main types of firewalls (*FW*). Firewalls are an important tool for protecting network resources from various information security threats. With the development of technology and the changing nature of attacks, especially those involving artificial intelligence (*IoT*), firewalls have also evolved, acquiring new functions and capabilities. This work provides a short survey of the main types, and capabilities of firewall technology, providing solutions to issues of comprehensive protection of network equipment and information resources from modern security threats. Different types of firewalls are used depending on the conditions of operation and purpose of the basic information and communication system (*ICS*), as well as on the place of their (*FW*) integration into the network or virtual infrastructure of modern information systems. For integrated networks that require a high level of their security, productivity and flexibility, firewalls of the business segment of generation *«Next-generation»* and *«Threat-focused NGFW»* are definitely the best choice. Attention was drawn to the fact that mobile firewalls should in every way contribute to the maintenance of resource consensus and eliminate a possible disparity in the performance of networked mobile applications. Adaptability to mobility of current communication systems (*Wi-Fi, GSM and others*) determines the specificity of security threats for mobile devices and It defines their key feature. This feature is based on permanent readiness for seamless transitions (reconnections) between different networks in conditions of constant energy shortage and limited available computing resources (meaning gadgets). Highlights the main trends, prospects for the development and implementation of different types of firewalls, including the impact of artificial intelligence, machine learning, cloud technologies and the Internet of Things as well as important aspects of their (*FW*) scope. It is emphasized that the introduction of *FW* does not replace other security technologies and tools, but effectively expands the existing arsenal of countering new security threats (primarily as an instrument of proactive countermeasures and rapid response to complex network incidents). The article may be useful for students, researchers, and information security professionals who seek to expand their competencies related to the development and operation of modern means of network protection.

Keywords: *FW, Firewall, Information Security, Security Threats, Malicious Software*

Conflicts of Interest: the authors declare no conflict of interest.

References

1. Azarov, S., Nemtsev, M., & Malakhov, S. Review of analogies and justification of the principles of creation of daemon units for tracking users' network activity. *Proceedings of the XX International Scientific and Practical Conference*. Graz, Austria. 2023. Pp. 447-453. Available at: https://doi.org/10.46299/ISG.2023.1.20 [In Ukrainian]
2. Bohdanova, E., Chorna, T., & Malakhov, S. (2022). Overview of the current state of threats caused by the influence of exploits. *Computer Science and Cybersecurity*, (2), 35-40. URL: https://periodicals.karazin.ua/cscs/article/view/21039/19745 [In Ukrainian]
3. Sichkar, M., & Pavlova, L. (2024). A short survey of the capabilities of Next Generation firewalls. *Computer Science and Cybersecurity*, (1), 28-33. Retrieved from https://periodicals.karazin.ua/cscs/article/view/23090
4. Sichkar, M., & Malakhov, S. Generalization of features of known means of network shielding. *Proceedings of the XXI International Scientific and Practical Conference*. Sofia, Bulgaria. 2024. https://isg-konf.com/category/archiv-conference-rub/ [In Ukrainian]
5. Kokhanovska, T., Narezhny, O., & Dyachenko, O. (2020). Exploring the capabilities of Honeypot technology. *Computer Science and Cybersecurity*, 1(1), 33-42 https://doi.org/10.26565/2519-2310-2020-1-03 [In Ukrainian]
6. Mykhaylenko D., Nemtsev M. Peculiarities of the technology of network traps as a tool of active protection and analysis of the actions of the attacking party. *Proceedings of the XXI International Scientific and Practical Conference*. Melbourne, Australia. 2023. Pp. 483-487. Available at: https://doi.org/10.46299/ISG.2023.1.21 [In Ukrainian]
7. John Mallery, & Jason Zann (2007). Your company's secure network. (E. Lindemann, translated from English). - M.: NT Press [In Ukrainian]
8. Rondalev, D., Melkozyorova, O., & Narezhniy, O. (2019). Peculiarities of the operation of the corporate inter-network screen and the issue of interaction with the IDS system. *Computer Science and Cyber Security*, (3), 11-21. https://periodicals.karazin.ua/cscs/article/view/15614/14707 [In Ukrainian]
9. FireWall. URL: http://surl.li/tuggo
10. Who Invented the Firewall? History, Types and Generations of Firewall. 28th September 2023 by Manish Sahay URL: https://www.thepcinsider.com/who-invented-firewall-history-evolution-types-generations/
11. What Is a Firewall? URL: http://surl.li/fdtbp
12. Next-Generation Firewalls. URL: https://www.paloaltonetworks.com/network-security/next-generation-firewall
13. Types of Firewalls: Know Which One Is Best for Your Network By John Villanueva / May 19, 2022. https://techgenix.com/types-of-firewalls
14. Information Technology Gartner Glossary. https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws
15. Yaremchuk, K., Voskoboynikov, D., & Melkozyorova, O. (2022). Modern threats and ways to secure web applications. *Computer Science and Cybersecurity*, (2), 28-34. https://periodicals.karazin.ua/cscs/article/view/21038/19744 [In Ukrainian]
16. What is a Next-Generation Firewall (NGFW)? Вилучено з URL: https://www.zenarmor.com/docs/network-security-tutorials/next-generation-firewall
17. Top Next-Generation Firewall (NGFW) Software By Jenna Phipps July 19, 2022. URL: https://www.cioinsight.com/security/ngfw-software/#What-is-a-next-generation-firewall
18. What are the Types of Firewalls? URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-firewall
19. Mykhaylenko, D., Chorna, T. & Malakhov, S. The use of AI capabilities in the implementation of Static and Dynamic Honeypot to improve the parameters of protection of information resources. *Technologies, tools and strategies for the implementation of scientific research: materials of the IV International Scientific Conference*, (p. 54-57). October 7, 2022. Sumy, Ukraine: MCND. https://doi.org/10.36074/mcnd-07.10.2022 [In Ukrainian]

20. How do firewalls for mobile devices differ from traditional firewalls? https://www.xcel.com/how-do-firewalls-for-mobile-devices-differ-from-traditional-firewalls/
21. How mobile firewalls protect against unique threat vectors. URL: http://surl.li/tugix