Міністерство освіти і науки України
Харківський національний університет ім. В. Н. Каразіна
Факультет комп'ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

«Допущено до захисту»
В.о. завідувача кафедри БІСТ
Мелкозьорова О.М.

_____

« » 2024 р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
на тему: «Аналіз технологій міжмережевого екранування та дослідження можливостей рішень покоління NG (Next-Generation)»

оцінка « »

Голова ЕК
Лемешко О.В._____

Керівник к.т.н. Малахов С.В.

Рецензент Гостєв О. Л.

Виконавець: студент групи КБ-42

Січкар М.В

Харків – 2024

РЕФЕРАТ

Пояснювальна записка містить: 54 сторінок, 3 рисунка, 2 таблиці та 20 використаних джерел.

Мета роботи: - аналіз принципів функціонування та можливостей засобів міжмережевого екранування покоління Next-Generation (NG).

Об’єкт дослідження: - сучасні технології міжмережевого екранування (ММЕ) для корпоративного та приватного сегментів користувачів.

Предмет дослідження: - особливості розміщення, налаштування і використання засобів ММЕ від різних розробників та порівняння їх можливостей з рішеннями покоління NG (NG firewalls, NGFW).

Основними методами досліджень є: - аналіз, комп’ютерне моделювання та порівняльне тестування програмного забезпечення (ПЗ).

В роботі виконано аналіз розвитку технологій міжмережевого екранування, встановлені характерні відмінності між засобами ММЕ для корпоративного і приватного сегменту користувачів. В межах досліджень проведено узагальнення основних функції і особливостей використання сучасних засобів ММЕ. Розглянуто концепцію активного мережевого захисту та досліджено можливості і принцип дії ММЕ покоління NG. Запропоновано огляд сучасного стану розробок рівня NGFW та проведено дослідне тестування програмних рішень ММЕ для приватного сегменту користувачів. Сформульовано перспективи розвитку технологій ММЕ, зокрема в контексті використання хмарних рішень та інтеграції FWNG до складу комплексних систем безпеки.

Результати роботи можуть бути використані в освітніх цілях та, як допоміжний матеріал для розширення рівня компетенцій персоналу підрозділів з інформаційної безпеки (ІБ), стосовно особливостей сучасних засобів ММЕ та можливостей з подальшої інтеграції FWNG до складу комплексних систем ІБ.

Ключові слова: МІЖМЕРЕЖЕВЕ ЕКРАНУВАННЯ, NEXT-GENERATION FIREWALL, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, ТРАФІК, ПЕРИМЕТР БЕЗПЕКИ, МЕРЕЖЕВІ АТАКИ, АКТИВИНИЙ ЗАХИСТ.

ABSTRACT

The explanatory note includes: 54 pages, 3 figures, 2 tables, and 20 references.

Objective of the work: To analyze the principles of operation and capabilities of Next-Generation (NG) firewall technologies.

Object of the study: Modern firewall technologies (FW) for corporate and private user segments.

Subject of the study: Features of deployment, configuration, and use of firewall technologies from various developers and comparison of their capabilities with NG solutions (NG firewalls, NGFW).

The main research methods are: Analysis, computer modeling, and comparative testing of software (SW).

This work analyzes the development of firewall technologies and identifies characteristic differences between firewall solutions for corporate and private user segments. The study summarizes the main functions and features of modern firewall technologies. The concept of active network protection is considered, and the capabilities and principles of NG firewall operation are investigated. An overview of the current state of NGFW development is provided, and experimental testing of firewall software solutions for the private user segment is conducted. The prospects for the development of firewall technologies are formulated, particularly in the context of using cloud solutions and integrating NGFW into comprehensive security systems.

The results of the work can be used for educational purposes and as auxiliary material to enhance the competencies of information security (IS) department personnel regarding the features of modern firewall technologies and the possibilities of further integrating NGFW into comprehensive IS systems.

Keywords: FIREWALL, NEXT-GENERATION FIREWALL, INFORMATION SECURITY, CYBER THREATS, TRAFFIC, SECURITY PERIMETER, NETWORK ATTACKS, ACTIVE PROTECTION.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

ІБ - Інформаційна безпека

ІКС - Інформаційно-комунікаційні системи

ММЕ – Міжмережеве екранування

ACL – Access Control List

AI – Artificial intelligence

ASR – Attack Surface Reduction

CASB – Cloud Access Security Broker

FTP – File Transfer Protocol

HTTP – Hypertext Transfer Protocol

IAM – Identity and Access Management

ICMP – Internet Control Message Protocol

IDS – Intrusion Detection System

IP – Internet Protocol

IPS – Intrusion Prevention System

LM – Language Model

ML – Machine Learning

NG – Next-Generation

NGFW – Next-Generation Firewall

SIEM – Security Information and Event Management

SOCKS – Socket Secure

SWG – Secure Web Gateway

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

ВСТУП

Сучасний світ стає все більш залежним від інформаційних технологій, тому зростає важливість забезпечення надійного захисту сучасних інформаційно-комунікаційних систем (ІКС) від нових та/чи вже відомих, але модифікованих загроз безпеки. Одним із ключових елементів в загальному арсеналі сучасних засобів забезпечення інформаційної безпеки (ІБ) є міжмережеві екрани (*англ., firewalls*), які в своєму розвитку еволюціонували від «простих» засобів фільтрації трафіку до комплексних рішень мережевої безпеки нового покоління – *Next Generation Firewalls* (або, *NGFW*). Технологія ММЕ рівня *Next Generation*, надають їх користувачам розширені можливості для виявлення та блокування загроз, зокрема завдяки інспекції трафіку на прикладному рівні, аналізу поведінки користувачів та інтеграції з іншими системами/засобами ІБ. Враховуючи те, що рішення рівня NGFW, втилюють концепцію «активного» захисту, особливу увагу необхідно приділити порівнянню «традиційних» *firewalls (тобто технологій і засобів ММЕ, попередніх етапів їх розвитку)* з NGFW, а також вивченню їх переваг та обмежень у контексті захисту сучасних ІКС.

Враховуючи те, що *firewalls* рівня *NG*, на теперішній час є найбільш вдосконалою реалізацією технологій ММЕ, то в роботі буде проведено детальний аналіз архітектури, функціональних можливостей та механізмів роботи відповідних рішень. Крім того, розглянути особливості застосування NGFW в корпоративних та приватних мережевих середовищах. Вочевидь, що впровадженя в практику мережевого захисту, відповідних рішень покоління NG, є важливим кроком у посиленні функціоналу міжмережевого екранування. Застосування засобів рівня NGFW дозволяє значно підвищити рівень ІБ та забезпечити більш ефективний захист інформаційних ресурсів *(мережевого остаткування та безпосередньо інформації, що циркулює*). Дослідження можливостей впровадження NGFW є необхідним для розробки оптимальних стратегій забезпечення мережевої безпеки, що відповідають вимогам сучасного бізнесу та приватних користувачів.

У процесі виконання досліджень використано різноманітні методи, включаючи аналіз профільних джерел інформації, порівняння технічних характеристик різних рішень, а також практичні експерименти з впровадження та налаштування NGFW у різних середовищах. В цілому дана робота спрямована на всебічне вивчення технологій міжмережевого екранування та оцінку можливостей NGFW, що дозволяє сформувати рекомендації щодо їх ефективного застосування для підвищення загального рівня ІБ в сучасних ІКС.

1. АНАЛІЗ РОЗВИТКУ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАСОБІВ МІЖМЕРЕЖЕВОГО ЕКРАНУВАННЯ РІЗНИХ ПОКОЛІНЬ

1.1 Аналіз основних етапів розвитку технологій ММЕ

Брандмауер (чи firewall) - це апаратне або програмне рішення, яке здійснює контроль мережевого трафіку між двома чи більше мережами. Воно використовує набір правил для дозволу або заборони передачі певних пакетів даних між мережами [1,5]. Зазвичай брандмауери розміщуються між внутрішньою локальною мережею організації та Інтернетом, що сприяє захисту внутрішньої мережі від шкідливих програм та інших загроз ззовні. Проте брандмауери також можуть використовуватися для моніторингу та обмеження трафіку всередині локальної мережі, наприклад, блокуючи доступ до певних вебсайтів або додатків.

Брандмауер функціонує, пропускаючи весь мережевий трафік через себе. Кожен пакет даних перевіряється на відповідність заданим правилам: якщо пакет відповідає правилам, він проходить далі, якщо ні – блокується [1]. Правила брандмауера можуть бути налаштовані відповідно до потреб організації. Наприклад, можна дозволити доступ до Інтернету лише для певних комп’ютерів або програм, або заборонити доступ до конкретних вебсайтів чи додатків.

Брандмауери відіграють важливу роль у забезпеченні безпеки мережі. Вони захищають мережу від шкідливого ПЗ, атак та інших загроз. Для розуміння принципів функціонування різних типів брандмауерів необхідно враховувати їх роль на відповідних рівнях моделі OSI (*Open Systems Interconnection Basic Reference Model*).

Модель OSI [5] описує стек мережевих протоколів, який дає змогу різним мережевим пристроям взаємодіяти між собою. У цій моделі визначено кілька рівнів, кожен з яких виконує конкретні функції під час обміну даними.

У таблиці 1.1 представлено структуру стека протоколів OSI.

Таблиця 1.1 – Представлено структуру стека протоколів OSI

Модель				
Рівень (layer)		Тип даних (PDU)	Функції	Приклади
Host layer	7 Прикладний (application)	Дані	Доступ до мережевих служб	HTTP, FTP, POP3, SMTP, WebSocket
	6 Представлення (presentation)		Представлення та шифрування даних	ASCII, EBCDIC, SSL, gzip
	5 Сеансовий (session)		Управління сеансом зв'язку	RPC, PAP, L2TP, gRPC
	4 Транспортний (transport)	Сегменти (segment)/Датаграми(datagram)	Прямий зв'язок між кінцевими пунктами та надійність	TCP, UDP, SCTP, Порти
Media layers	3 Мережевий (network)	Пакети (packet)	Визначення маршруту та логічна адресація	IPv4, IPv6, IPsec, AppleTalk, ICMP
	2 Канальний (data link)	Біти (bit) / Кадри (frame)	Фізична адресація	PPP, IEEE 802.22, Ethernet, DSL, ARP, сетевая карта.
	1 Фізичний (physical)	Біти (bit)	Робота із середовищем передавання, сигналами та двійковими даними	USB, RJ («кручена пара», коаксіальний, оптоволоконний), радіоканал

Фундаментом мережевого світу слугує фізичний рівень моделі OSI. Саме він відповідає за транспортування даних у вигляді двійкових сигналів між мережевими пристроями. Цей рівень є основою для роботи таких компонентів, як повторювачі сигналів, концентратори та медіаконвертери, хоча його функціонал реалізований у будь-якому пристрої, що підтримує мережеве підключення. Наприклад, на автоматизованому робочому місці дані передаються через послідовний порт або

мережевий адаптер, використовуючи стандартні інтерфейси, такі як RJ-11, RJ-45 або RS-232.

Канальний рівень відповідає за встановлення з'єднання між вузлами в межах одного локального сегмента мережі. На цьому рівні дані передаються у вигляді кадрів, які містять заголовки з MAC-адресами відправника та одержувача. Це дозволяє розпізнавати пристрої, що беруть участь у передачі даних. Кожен мережевий інтерфейс має унікальну MAC-адресу, що дозволяє канальному рівню виконувати функції адресації та ідентифікації мережевих пристроїв. Пристрої, такі як мости та комутатори, працюють на цьому рівні. Прикладами протоколів цього рівня є Point-to-Point Protocol (PPP) та Ethernet.

На мережевому рівні моделі OSI визначається найкращий маршрут для передачі даних, здійснюється перетворення логічних імен та адрес у фізичні, а також виконується маршрутизація і комутація. Цей рівень охоплює роботу маршрутизаторів, а в Інтернеті адреси цього рівня відомі як IP-адреси.

Транспортний рівень моделі OSI впевнено поєднує кінцеві точки мережі, гарантуючи чітку та безпечну передачу даних. Цей рівень бере на себе відповідальність за розбивку даних на зручні для транспортування пакети, забезпечуючи їхню цілісність та виправляючи можливі помилки. Транспортний рівень також виступає в ролі диспетчера, розпізнаючи різні мережеві додатки та сесії. Для цього він використовує порти як унікальні адреси, що чітко окреслюють початок і кінець кожної комунікаційної взаємодії. Завдяки своїм функціям, транспортний рівень гарантує безперебійну та надійну доставку даних, немов досвідчений експедитор, що доставляє вантаж від пункту відправлення до пункту призначення.

Сеансовий рівень моделі OSI відповідає за управління комунікаційними сеансами між додатками. Його головна функція - забезпечення тривалої взаємодії між додатками. На цьому рівні здійснюється обмін інформацією, встановлення прав доступу до передачі даних, а також створення та завершення сеансів зв'язку. Сеансовий рівень також забезпечує синхронізацію робочих завдань між додатками та підтримку сеансів під час їхньої неактивності. Важливим аспектом цього рівня є

визначення контрольних точок, які вставляються в потік даних для синхронізації передачі. У разі переривання зв'язку або сеансу, процес можна відновити з останньої контрольної точки. Таким чином, сеансовий рівень моделі OSI забезпечує надійну та стабільну взаємодію між додатками протягом усього часу сеансу зв'язку.

Прикладами протоколів, що працюють на п'ятому рівні моделі OSI, є netBIOS і H.245.

На рівні Представлення моделі OSI здійснюється перетворення даних у формат, зрозумілий для кінцевих систем. Основна мета цього рівня - забезпечити стандартизоване представлення даних, незалежно від характеристик кінцевих систем. Основними функціями цього рівня є компресія даних для зменшення їх обсягу та підвищення ефективності передачі, а також шифрування та розшифрування для забезпечення конфіденційності. Крім того, на цьому рівні відбувається конвертація форматів даних між різними системами, наприклад, між ASCII та Unicode, щоб забезпечити коректне розуміння даних на обох кінцях зв'язку. Таким чином, рівень Представлення моделі OSI забезпечує взаємодію між різними системами, стандартизуючи формати даних і гарантувавши їх конфіденційність та цілісність під час передачі через мережу.

Сьомий, найвищий рівень моделі OSI, забезпечує взаємодію між користувачем і мережею. Прикладний рівень дозволяє кінцевим додаткам доступ до файлів, мережевих сервісів, електронної пошти та інформації про помилки при передачі даних. На цьому рівні працюють різноманітні протоколи, такі як HTTP, FTP, DNS, SMTP, POP3.

Перші брандмауери з'явилися в 1988 році і були відомі як фільтруючі пакети. Працювали на третьому рівні OSI, також відомому як мережевий рівень [2]. Вони аналізували пакети даних, що переміщалися між комп'ютерами в мережі, і дозволяли або відхиляли їх на основі встановлених правил. Цей тип брандмауера, який не зберігав стан з'єднань, часто називали "Stateless Firewall" або "брандмауер рівня мереж" [3].

У 1989 році з'явилося друге покоління брандмауерів, відоме як "Stateful Firewall". Ці пристрої враховували стан з'єднання, що дозволяло забезпечувати більш точний контроль трафіку [4].

У 1991 році Digital Equipment Corporation (DEC) випустила третє покоління брандмауерів, що стало відомим як "брандмауер прикладного рівня". Такі брандмауери, як Gauntlet від Trusted Information Systems та FireWall-1 від Check Point, керували трафіком на рівні застосунків. Вони забезпечували захист від шкідливого програмного забезпечення і регулювали доступ до Інтернету через протоколи, такі як FTP, Telnet і HTTP [4,5].

У 2004 році термін "Unified Threat Management" (UTM) був вперше використаний IDC (Міжнародною корпорацією з обробки даних). UTM поєднує кілька технологій безпеки, таких як мережевий брандмауер, фільтрація веб-сторінок, антивірусна шлюзова захист, система запобігання вторгненням (IPS), антиспам та VPN, у єдине комплексне рішення для захисту мережі [4,5].

У 2009 році компанія Gartner ввела термін "Next-Generation Firewall" (NGFW), який об'єднує функції традиційного брандмауера з новими технологіями, такими як глибока інспекція пакетів (DPI), управління застосунками, фільтрація URL-адрес, захист від складних шкідливих програм, профілювання мережі, ідентифікація користувачів, VPN та інші. Основною відмінністю NGFW є використання DPI на рівні застосунків, що значно покращує захист порівняно з попередніми рішеннями, які обмежувалися інспекцією портів і протоколів [4,6].

Таким чином, сучасні NGFW об'єднують функції традиційних брандмауерів та систем запобігання вторгненням, значно підвищуючи рівень безпеки мережевого трафіку [5].

1.2 Основні відмінності засобів MME для корпоративного та приватного сегменту користувачів.

Брандмауери, призначені для захисту приватних та корпоративних мереж, мають суттєві відмінності як за функціональністю, так і за спрямованістю застосування.

У сегменті приватного користування, брандмауери класу споживача, часто відомі як SOHO (Small Office/Home Office), зазвичай призначені для простих домашніх мереж або невеликих офісних середовищ з обмеженими потребами в безпеці. Такі засоби забезпечують базовий рівень захисту, виявляючи та блокуючи загрози, які можуть виникати в невеликих мережах з обмеженим трафіком. Однак їхня функціональність зазвичай обмежена, а їхні можливості оновлення та масштабування обмежені. Вони часто не забезпечують активного моніторингу, і їхні можливості реакції на загрози обмежені.

У суперечність з цим, брандмауери корпоративного класу, відомі також як Enterprise Firewalls, розроблені для використання в складних корпоративних мережах з великим обсягом трафіку та великою кількістю пристроїв. Їхня функціональність значно розширена, щоб забезпечити ефективний захист від різноманітних кіберзагроз, включаючи атаки, що стають все більш складними та витонченими [7]. Брандмауери корпоративного класу надають можливості для активного моніторингу та виявлення вразливостей, інтеграції з іншими системами безпеки та забезпечення високої доступності та надійності. Вони також можуть підтримувати велику кількість одночасних з'єднань та масштабуватися з ростом мережі.

Крім того, брандмауери корпоративного класу часто мають вбудовану підтримку для додаткових функцій та сервісів, таких як VPN (Virtual Private Network), IDS/IPS (Intrusion Detection System/Intrusion Prevention System), а також інтеграцію з системами керування інцидентами та аналізу безпеки [8].

Отже, відмінності між брандмауерами приватного та корпоративного класу полягають не лише у їхній функціональності та ціні, але й у спрямованості застосування та здатності забезпечити необхідний рівень захисту від сучасних кіберзагроз.

2. ОСНОВНІ ФУНКЦІЇ ТА ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ ЗАСОБІВ ММЕ

2.1 Огляд та узагальнення основних функцій сучасних засобів ММЕ

Існує кілька різних типів брандмауерів, які можуть бути використані в залежності від ситуації [1-2, 5].

1) Proxy Firewall

Брандмауер-проксі, відомий як один з найефективніших методів захисту мережі, діє на прикладному рівні, ретельно фільтруючи всі вхідні та вихідні повідомлення. Цей тип брандмауера виступає в ролі надійного охоронця, що пильно стежить за всіма даними, які проходять через мережу.

Однак, подібна ретельність має й свою ціну. Брандмауер-проксі обмежує кількість програм, які може підтримувати мережа, що може потенційно вплинути на її швидкість та функціональність.

Переваги:

- Неперевершена безпека: Фільтрація на прикладному рівні забезпечує найвищий рівень захисту від кіберзагроз.
- Захист від несанкціонованого доступу: Брандмауер-проксі блокує доступ до несанкціонованих програм та веб-сайтів.
- Контроль трафіку: Ви можете чітко контролювати, які програми та дані мають доступ до мережі.

Недоліки:

- Обмежена підтримка програм: Кількість програм, що можуть працювати в мережі, може бути обмеженою.
- Вплив на швидкість: Фільтрація даних може призвести до незначного зниження швидкості роботи.
- Можливі проблеми з функціональністю: Деякі програми можуть працювати некоректно через обмеження брандмауера.

Отже: Брандмауер-проксі пропонує безпрецедентний рівень безпеки мережі, але його використання може мати певні компроміси. Перед впровадженням цього типу брандмауера важливо ретельно оцінити всі його переваги та недоліки, щоб прийняти обґрунтоване рішення, яке відповідатиме вашим потребам.

2) Unified Threat Management (UTM) Firewall [7];

Брандмауер Уніфікованого управління загрозами (UTM) виступає як центр кібербезпеки вашої мережі, поєднуючи в собі комплексні функції захисту, такі як антивірусне програмне забезпечення, фільтрування контенту, захист від вторгнень та багато іншого. Це рішення, яке охоплює широкий спектр загроз, забезпечуючи надійний захист вашої мережі та даних.

Переваги UTM:

- Економія коштів: Замість того, щоб купувати та обслуговувати окремі рішення для кожної загрози, UTM пропонує комплексне рішення, економлячи ваші ресурси.
- Спрощене управління: Завдяки централізованому інтерфейсу керування UTM, ви легко можете контролювати та налаштовувати всі аспекти кібербезпеки вашої мережі.
- Підвищена ефективність: UTM поєднує в собі функції захисту, що синхронно працюють together, забезпечуючи більш швидке та ефективне виявлення та блокування загроз.
- Покращена видимість: UTM надає детальну інформацію про всі аспекти кібербезпеки вашої мережі, даючи вам чітке розуміння загроз та їх впливу.

Підходить для:

- Компаній та організацій будь-якого розміру: UTM пропонує масштабовані рішення, які підходять для потреб як малого, так і великого бізнесу.
- Підприємств, які потребують надійного захисту: UTM ідеально підходить для організацій, які працюють з чутливою інформацією та потребують високого рівня кібербезпеки.
- Тих, хто прагне спростити управління: UTM економить час та ресурси, надаючи централізоване рішення для кібербезпеки.

Підсумок:

Брандмауер UTM - це інвестиція в безпеку вашого бізнесу. Він пропонує комплексний захист, економить кошти та полегшує управління кібербезпекою вашої мережі.

3) Stateful Inspection Firewall

Брандмауер з перевіркою стану - це тип брандмауера, який моніторить стан активних мережевих з'єднань і одночасно аналізує вхідний трафік на предмет потенційних ризиків та загроз. Брандмауери із перевіркою стану розташовані на 3 і 4 рівнях моделі OSI.

Перевірка пакетів зі збереженням стану використовується брандмауерами зі збереженням стану для аналізу того, які пакети можуть пройти через брандмауер. Брандмауери з перевіркою стану працюють, переглядаючи вміст пакету даних через мережу, а потім порівнюючи його з пакетами даних, які вже пройшли через брандмауер.

Брандмауери з перевіркою стану (Stateful Firewalls) - це потужний тип брандмауера, який поєднує в собі динамічний контроль та аналіз трафіку для забезпечення всебічного захисту мережі. Ці брандмауери діють на 3-му та 4-му рівнях моделі OSI, що дозволяє їм глибоко аналізувати вміст пакетів даних та приймати рішення про дозвол або блокування трафіку на основі його історії та контексту.

Суть роботи брандмауера з перевіркою стану:

- Моніторинг активних з'єднань: Брандмауер постійно відстежує всі активні з'єднання в мережі, створюючи "карту" поточного трафіку.
- Аналіз вхідного трафіку: Кожен вхідний пакет даних ретельно аналізується на предмет потенційних загроз, таких як віруси, трояни, програмне забезпечення для вимагання та інші кібератаки.
- Перевірка пакетів зі збереженням стану: Брандмауер порівнює вміст нового пакету з інформацією про попередні пакети в тому ж з'єднанні. Це дозволяє йому виявляти аномальні або підозрілі дії, які можуть бути ознакою кібератаки.

- Гнучкий контроль: На основі результатів аналізу, брандмауер може дозволити, блокувати або перенаправляти трафік.

Переваги брандмауерів з перевіркою стану:

- Підвищений рівень безпеки: Завдяки динамічному аналізу та контролю, брандмауери з перевіркою стану забезпечують кращий захист від нових та складних кіберзагроз.
- Ефективне управління трафіком: Ці брандмауери можуть чітко контролювати, які типи трафіку дозволені в мережі, що допомагає оптимізувати її пропускну здатність та продуктивність.
- Гнучкість: Firewalls з перевіркою стану можна налаштувати відповідно до потреб конкретної мережі, враховуючи її розмір, тип даних, що передаються, та рівень ризику.

Брандмауери з перевіркою стану - це важливий компонент комплексної стратегії кібербезпеки, який може значно підвищити стійкість мережі до кібератак.

4) Next-generation Firewall (NGFW)

Брандмауери нового покоління (NGFW) – це еволюційний крок у розвитку мережевої безпеки, що поєднує в собі можливості традиційних брандмауерів з інноваційними функціями для протистояння сучасним кіберзагрозам. Ці брандмауери, які належать до третього покоління, пропонують розширений спектр інструментів, таких як системи запобігання вторгненням (IPS) та глибокий інспектування пакетів (DPI), забезпечуючи комплексний захист мережі.

Відмінні риси NGFW:

- Детальний аналіз трафіку: NGFW не лише контролюють порти та адреси, як традиційні брандмауери, але й глибоко аналізують вміст пакетів даних. Це дозволяє їм виявляти загрози, що ховаються в зашифрованому трафіку, атаках типу "людина посередині" та інших складних кібератаках.
- Системи запобігання вторгненням (IPS): NGFW вбудовані IPS, які в режимі реального часу сканують мережевий трафік на наявність шкідливих дій та атак. Це дозволяє їм блокувати загрози ще до того, як вони завдадуть шкоди [5,7].

- Гнучкість та контроль: NGFW пропонують широкий спектр налаштувань та політик, що дає адміністраторам мережі гнучкість у контролі того, які типи трафіку дозволені, а які блокуються. Це дозволяє їм створювати персоналізовані правила безпеки, що відповідають потребам конкретної мережі.
- Підвищена обізнаність: NGFW збирають детальну інформацію про мережевий трафік, надаючи адміністраторам цінні дані для аналізу та аудиту. Це допомагає їм краще розуміти, як використовується мережа, та виявляти потенційні проблеми безпеки.

Переваги NGFW [7,20]:

- Більш ефективний захист від кіберзагроз: NGFW забезпечують комплексний захист від широкого спектра кіберзагроз, включаючи зловмисне програмне забезпечення, фішингові атаки, вторгнення та багато іншого.
- Зниження ризику втрати даних: Завдяки кращому захисту від кібератак, NGFW допомагають зберегти конфіденційність та цілісність даних, що
- Зменшення навантаження на інші мережеві пристрої: NGFW можуть обробляти багато функцій безпеки, які раніше виконували інші пристрої, такі як IPS та системи захисту від вірусів. Це може зменшити навантаження на мережу та покращити її загальну продуктивність.

5) Брандмауери нового покоління – Threat-focused NGFW

NGFW з фокусом на загрози - це еволюційна категорія брандмауерів нового покоління, які спеціально розроблені для захисту від сучасних кіберзагроз, таких як зловмисне програмне забезпечення, атаки на прикладному рівні та інші цілеспрямовані атаки. Ці брандмауери виступають як щит, який нещадно бореться з кіберзлочинцями, забезпечуючи комплексний захист вашої мережі.

Основні характеристики NGFW з фокусом на загрози:

- Виявлення та блокування відомих загроз: Ці брандмауери володіють обширними базами даних з сигнатурами шкідливого програмного забезпечення, атак на прикладному рівні та інших відомих загроз. Завдяки цьому вони можуть негайно блокувати ці загрози, не даючи їм шансу завдати шкоди.

- Захист від невідомих загроз: NGFW з фокусом на загрози використовують передові аналітичні методи, такі як машинне навчання та поведінковий аналіз, для виявлення та блокування нових, невідомих загроз. Це дозволяє їм йти на крок попереду кіберзлочинців, які постійно шукають нові шляхи для проникнення в мережі.
- Відстеження та аналіз атак: Ці firewalls ретельно відстежують всі атаки, що відбуваються, збираючи детальну інформацію про їх характер та джерело. Ці дані можуть бути використані для аналізу та покращення стратегії кібербезпеки.
- Протидія цілеспрямованим атакам: NGFW з акцентом на загрози спеціально розроблені для протидії складним цілеспрямованим атакам, які часто використовуються хакерськими угрупованнями та державними органами. Вони можуть виявляти та блокувати ці атаки, навіть якщо вони використовують нові та невідомі методи.

Переваги NGFW з фокусом на загрози:

- Більш ефективний захист від кіберзагроз: Ці брандмауери забезпечують безпрецедентний рівень захисту від широкого спектра кіберзагроз, як відомих, так і невідомих.
- Зниження ризику втрати даних: Завдяки кращому захисту від кібератак, NGFW з фокусом на загрози допомагають зберегти конфіденційність та цілісність даних, що
- Зменшення навантаження на інші мережеві пристрої: Ці брандмауери можуть обробляти багато функцій безпеки, які раніше виконували інші пристрої, такі як IPS та системи захисту від вірусів. Це може зменшити навантаження на мережу та покращити її загальну продуктивність.

NGFW з фокусом на загрози – це незамінний інструмент для забезпечення кібербезпеки сучасних мереж, який надійно захистить вашу мережу від кіберзлочинців.

6) Virtual Firewall

Віртуальний брандмауер, також відомий як хмарний брандмауер, стає все більш популярним рішенням для забезпечення кібербезпеки в динамічному

середовищі хмарних технологій. Цей тип firewalls пропонує гнучкість та масштабованість, які ідеально підходять для сценаріїв, де розгортання апаратних брандмауерів є складним або неможливим [7,9,20].

Основні характеристики віртуальних брандмауерів:

- Простота розгортання: Віртуальні брандмауери легко встановлюються та налаштовуються у віртуальних середовищах, таких як публічні та приватні хмари, а також SDN (програмно-визначені мережі). Це робить їх ідеальним вибором для організацій, які потребують швидкого та гнучкого захисту своїх мереж.
- Масштабованість: Віртуальні брандмауери легко масштабуються відповідно до мінливих потреб вашої мережі. Ви можете динамічно додавати або видаляти екземпляри віртуальних брандмауерів, щоб гарантувати оптимальний захист у міру зростання або зменшення вашого трафіку.
- Економічність: Віртуальні брандмауери зазвичай пропонують значну економію коштів у порівнянні з апаратними брандмауерами, оскільки не потребують додаткового обладнання або фізичного простору. Ви платите лише за ресурси, які використовуєте, що робить це рішення дуже вигідним.
- Централізоване управління: Віртуальні брандмауери можна централізовано управляти з єдиної консолі, що спрощує адміністрування та контроль над мережевою безпекою. Це дозволяє вам легко створювати та застосовувати політики безпеки до всіх ваших віртуальних брандмауерів, незалежно від їх розташування.

Переваги віртуальних брандмауерів:

- Гнучкість: Віртуальні брандмауери адаптуються до будь-якої хмарної інфраструктури, SDN або віртуального середовища.
- Масштабованість: Легко масштабуються відповідно до потреб вашої мережі.
- Економічність: Пропонують значну економію коштів у порівнянні з апаратними брандмауерами.

- Централізоване управління: Спрощують адміністрування та контроль над мережевою безпекою.
- Підвищена доступність: Забезпечують високий рівень доступності та стійкості до відмов.

Віртуальні брандмауери стають незамінним інструментом для забезпечення кібербезпеки в сучасних динамічних мережах, пропонуючи гнучкість, масштабованість та економічність, що робить їх ідеальним вибором для організацій, які переходять до хмарних технологій. В таблиці 2.2 наведено порівняння функціоналу популярних брандмауерів [5,7,20].

Таблиця 2.2 – Узагальнене порівняння функціоналу брандмауерів

Параметри	Proxy Firewall	UTM	Stateful Inspection Firewall	NGFW	Threat-focused NGFW	Virtual Firewall
Антивірус та антиспам	Ні	Так	Ні	Так	Так	Так
Безпека електронної пошти	Ні	Так	Ні	Так	Так	Так
Видимість додатків та керування додатками	Ні	Так	Ні	Так	Так	Так
Звітність	Ні	Так	Так	Так	Так	Так
Послуги з управління репутацією та ідентифікацією	Ні	Так	Ні	Так	Так	Так
Рівень на моделі OSI	7	7	3-4	2-7	2-7	3-4
Управління пропускною здатністю	Ні	Так	Ні	Так	Так	Так
Фільтрація контенту/веб-сторінок	Ні	Так	Ні	Так	Так	Так
Фільтрація трафіку (на основі портів, IP-адрес та протоколів)	Так	Так	Так	Так	Так	Так
DLP	Ні	Так	Ні	Так	Так	Так

Продовження таблиці 2.2

IDS (Система виявлення вторгнень)	Ні	Так	Ні	Так	Так	Так
IPS (Система запобігання вторгненням)	Ні	Так	Ні	Так	Так	Так
NAT	Ні	Так	Так	Так	Так	Так
VPN	Ні	Так	Ні	Так	Так	Так

Ця таблиця є узагальненою. Можливості систем можуть відрізнятися в залежності від конкретного продукту та версії файрволу [20].

Підсумовуючи всю інформацію можна зробити висновок, що Firewall потрібно обирати під конкретну задачу.

Продукти UTM стають все більш схожими по функціоналу на NGFW. Для більшої безпеки можна звернути увагу на технологію яка розвивається а саме Threat-focused NGFW.

2.2 Особливості розгортання (розміщення) та використання сучасних засобів MME

Сучасні засоби мережевої безпеки (MME) відіграють ключову роль у забезпеченні безпеки та захисту інформаційних активів в корпоративних та приватних мережах. Однак, їх ефективне розгортання та використання вимагає уважного аналізу і підходу до кожного етапу впровадження.

Вибір правильної архітектури: Перший крок у розгортанні засобів MME - це вибір оптимальної архітектурної конфігурації. Під час цього етапу важливо враховувати різноманітні аспекти, такі як розмір та склад мережі, типи загроз, якими вона потенційно може зіткнутися, та потреби в доступності та масштабованості.

Наприклад, для великих корпоративних мереж може бути виправданим розгортання внутрішніх брандмауерів що фільтрують весь трафік тоді як для

менших організацій може бути доцільним використання периметральних брандмауерів.

Периметральні рішення безпеки мережі використовують різноманітні методи та типи firewalls для забезпечення захисту мережевих ресурсів На рисунку 2.1 зображено приклад архітектрури розгортання firewall периметру. Ось деякі з них:

Статична фільтрація пакетів: Цей метод передбачає фільтрацію трафіку на основі параметрів пакетів та правил, встановлених адміністратором мережі. Брандмауер порівнює кожен пакет зі списками керування доступом (ACL) та відповідно до цього дозволяє або блокує його.

Проксі-брандмауери: Ці брандмауери діють як проміжники між внутрішніми та зовнішніми мережами, перешкоджаючи прямій передачі пакетів та ускладнюючи виявлення мережі зловмисниками.

Перевірка пакетів зі збереженням стану: Цей метод, відомий також як динамічна фільтрація пакетів, відстежує стан вхідного та вихідного трафіку та дозволяє проходження лише тих пакетів, які відповідають попереднім запитам.

MME наступного покоління NG: Ці firewalls поєднують у собі різні методи безпеки, такі як статична фільтрація пакетів та перевірка стану, а також розширені функції, включаючи глибоку перевірку пакетів (DPI) та системи мережевої безпеки (IDS та IPS) [5], що забезпечує комплексний захист мережі.

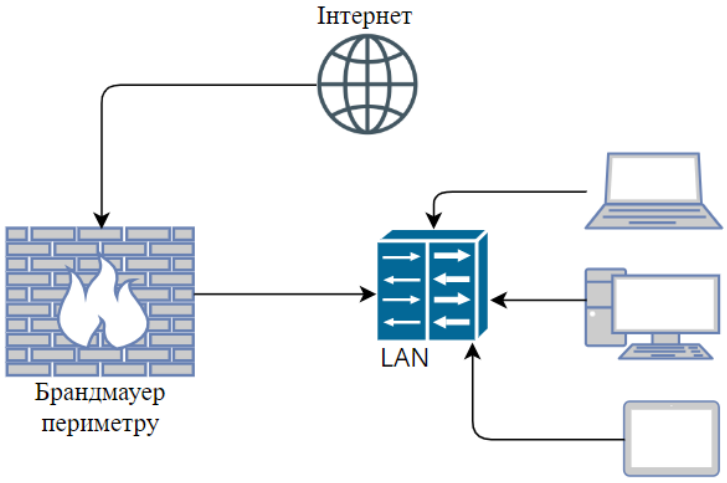

Рисунок 2.1 – Архітектрура розгортання Брандмауер периметру.

Внутрішні брандмауери є важливим рішенням для забезпечення безпеки мережі, оскільки вони працюють на внутрішній лінії оборони, контролюючи трафік між внутрішніми пристроями, такими як сервери та робочі станції, та запобігаючи атакам, які можуть проникнути через зовнішній периметр. Це більш складне застосування брандмауера, яке використовується для моніторингу трафіку та запобігання несанкціонованому доступу всередині мережі. Розташований стратегічно всередині мережі, внутрішній брандмауер використовує концепцію забезпечення доступу до мережі з нульовою довірою (ZTNA), щоб уникнути інсайдерських загроз та мінімізувати можливі наслідки.

Внутрішні брандмауери використовують дві основні стратегії для забезпечення безпеки мережі (рис. 2.2):

1) Мікросегментація: Цей підхід передбачає поділ мережі на дрібні, ізольовані зони, кожна з яких захищена окремо. Це дозволяє значно зменшити можливість атак і збільшити рівень захисту мережі.

2) Інтелектуальна автоматизація: Цей метод використовується для автоматичного застосування та оновлення політик безпеки на основі аналізу "відомої хорошої" поведінки мережевого трафіку. Такий підхід дозволяє ефективно виявляти та запобігати потенційним загрозам безпеки.

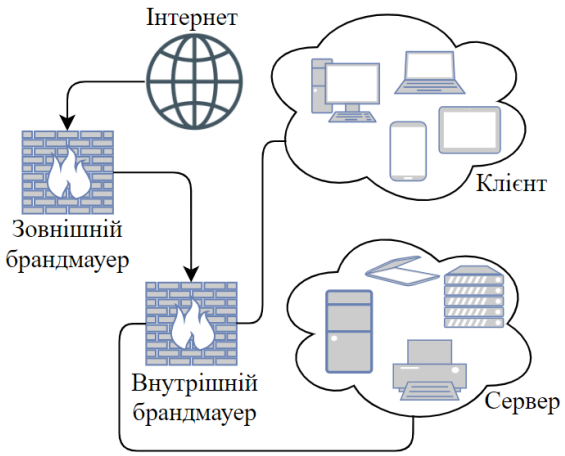

Рисунок 2.2 – Архітектура розгортання Внутрішнього брандмауера.

Стратегії розгортання: Після вибору архітектури необхідно розробити стратегію розгортання засобів MME. Це включає в себе визначення оптимального місця розташування засобів, обрання типу розгортання (апаратне, програмне або хмарне) та розробку плану міграції.

Інтеграція та сумісність: Важливим аспектом є забезпечення сумісності та інтеграції засобів MME з існуючою інфраструктурою та застосунками. Це може включати налаштування мережевих протоколів, встановлення спеціальних інтеграційних модулів та взаємодію з іншими системами безпеки.

Налаштування та управління: Після розгортання необхідно належним чином налаштувати та управляти засобами MME. Це включає в себе налаштування правил безпеки, моніторинг активності, вчасне виявлення та реагування на загрози, а також регулярне оновлення програмного забезпечення.

Оцінка ефективності: Не менш важливим етапом є оцінка ефективності розгорнутих засобів MME. Це дозволяє виявити слабкі місця в системі захисту та прийняти відповідні заходи для їх вдосконалення.

2.3 Узагальнення питань організації користувальницького інтерфейсу MME для приватного сегменту користувачів

Користувальницький інтерфейс засобів мережевої безпеки (MME) для приватного сегменту користувачів відіграє критичну роль у забезпеченні ефективного та зручного управління безпекою мережі. Організація інтерфейсу вимагає уважного узгодження з потребами та рівнем експертизи користувачів, щоб забезпечити їм зручний доступ до функцій безпеки та ефективне взаємодію з системою.

Першим аспектом, який потрібно враховувати при організації користувальницького інтерфейсу, є його зрозумілість та простота використання. Для багатьох приватних користувачів, які не мають спеціалізованої освіти в галузі інформаційної безпеки, важливо, щоб інтерфейс був інтуїтивно зрозумілим і не викликав плутанини. Це може включати в себе наявність зрозумілих підказок, інструкцій та графічних елементів.

Другим важливим аспектом є налаштування інтерфейсу з урахуванням потреб та можливостей користувачів. Наприклад, деякі користувачі можуть бути зацікавлені в простих, базових налаштуваннях безпеки, тоді як інші можуть вимагати розширених функцій і деталізації. Тому важливо надати можливість персоналізації інтерфейсу, щоб кожен користувач міг вибрати ті налаштування, які відповідають його потребам.

Третім аспектом є забезпечення візуалізації даних та статистики. Під час використання засобів MME, користувачам може бути важливо мати доступ до інформації про активність мережі, загрози та заходи, які були вжиті для їх запобігання. Тому інтерфейс повинен забезпечувати зручний доступ до цієї інформації через графіки, діаграми та інші візуальні елементи.

Четвертим аспектом є конфіденційність та безпека. MME-послуги повинні відповідати всім вимогам щодо конфіденційності та безпеки. Користувачі повинні мати можливість контролювати свою особисту інформацію та те, як вона використовується. Інтерфейс користувача повинен бути захищений від несанкціонованого доступу та атак.

П’ятим аспектом є підтримка. Користувачі повинні мати доступ до чіткої та лаконічної документації, яка допоможе їм користуватися MME-послугами. Повинна бути доступна служба підтримки користувачів, яка може допомогти користувачам вирішити проблеми та відповісти на їхні запитання.

Крім того, важливою складовою є підтримка мобільних пристроїв. З огляду на зростання використання смартфонів та планшетів, багато користувачів можуть вимагати можливості управління безпекою своєї мережі зі своїх мобільних пристроїв. Тому важливо, щоб користувальницький інтерфейс MME був адаптований для використання на різних типах пристроїв та мав зручний мобільний додаток. Розглянемо інтерфейс FW від лідерів на ринку. А саме: Fortinet, Cisco, Palo Alto, Checkpoint. Узагальнюючи, організація користувальницького інтерфейсу MME для приватного сегменту користувачів, він повинен бути зрозумілим, налаштованим під конкретних користувачів, містити візуальнізацію даних та бути підтриманим на різних типах пристроїв.

3. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ММЕ ПОКОЛІННЯ NEXT-GENERATION.

3.1 Принцип дії та основні можливості FWNG

Брандмауер покоління *NG*, одночасно використовує концепції традиційного брандмауера, а деякі нові технології: - *IPS*, глибока інспекція пакетів (*DPI*), пісочниця, управління застосунками, фільтрація URL-адрес, захист від складних/інтегрованих шкідливих програм, профілювання мережі, політика ідентифікації, *VPN* тощо. При цьому, головна відмінність *NGFW*, це перш за все, функція *DPI* на рівні застосунків, а не тільки в рамках інспекції портів і протоколів, що було притаманно для попередніх рішень [4,6-7] також більш новіші моделі підтримують штучний інтелект (AI).

Таким чином програмно-апаратні *NGFW* поєднують у собі функції традиційного брандмауера та системи запобігання вторгнення [5]. Використання таких програмно-апаратних *NGFW* сприяє підвищенню рівня безпеки мережевого трафіку.

Розглянемо ключові можливості й переваги рішень NGFW.

Можливості.

1) Аналіз і фільтрація трафіку на рівні додатків, а не лише за портами.

2) Реалізація IPS, що дозволяє своєчасно блокувати небажаний трафік або відключає частину мережі для парирування розповсюдження загрози.

4) DPI, яка аналізує найдрібніші деталі пакетів даних, включаючи відправника та отримувача даних.

5) Підтримка списків управління трафіком додатків.

6) Впровадження консолі централізованого управління мережею, що спрощує налаштування і моніторинг мережі.

Переваги.

1) Підвищення продуктивності: досягається шляхом використання *DPI*, що дозволяє ідентифікувати та керувати програмами, незалежно від їх IP-порту.

2) Багатофункціональність: є результатом інтеграції системи *IDS* та IPS, які виявляють атаки на основі аналізу поведінки мережі (*NBA*), сигнатур загроз та аномальної активності, зберігаючи при цьому, всі функції традиційних брандмауерів. Це забезпечує глибоку перевірку мережевого трафіку та покращує фільтрацію вмісту пакетів на рівні застосунків [20].

3) Фільтрування вмісту: можливість фільтрування вмісту є дуже корисною для запобігання несанкціонованого витоку даних в реальному часі.

4) Видимість і керованість: дозволяє адміністраторам з ІБ контролювати мережу та ідентифікувати користувачів. Інтеграція зі сторонніми каталогами користувачів полегшує контроль та ідентифікацію користувачів й груп.

5) Запобігання та «пом'якшення» наслідків загроз безпеки: - реалізують захист від вірусів і шкідливого програмного забезпечення, який автоматично оновлюється щоразу, коли з'являються нові загрози безпеки [11]. Вони також обмежують додатки, що працюють на них, перевіряючи їх на наявність потенційних вразливостей [12,13].

6) Розширений контроль політики безпеки: - надають детальний рівень контролю над додатками, блокуючи негативні аспекти їх роботи (*наприклад, надмірний трафік в моменти пікових навантажень*).

7) Низька вартість: є слідством глибокої інтеграції відразу декількох рішень під управлінням єдиної консолі управління [14].

Рішення на базі технології *NGFW* пропонує більшість великих компаній, наприклад, такі як: *Palo Alto Networks Fortinet, Cisco* та інші [13,6], де кожна з них пропонує широкий спектр функцій та можливостей для захисту від різних загроз (*мережеві шлюзи безпеки*) . Загальні для них функції безпеки, це [5,6,13,15,16]: *– мережевий захист; – IPS; – URL фільтрація; – захист від шкідливого коду; – DLP; – збіг ідентифікаторів (IDP); – управління доступом на основі ролей (RBAC); – контроль вмісту*. Взагалі такі рішення знаходять своє використання в таких сферах, як: – великі організації і державні установи; – малі і середні підприємства; – банки й фінансові установи; – рядові організації та підприємства. На рисунку 3.1 зображена узагальнена інтерпретація концепції NGFW.

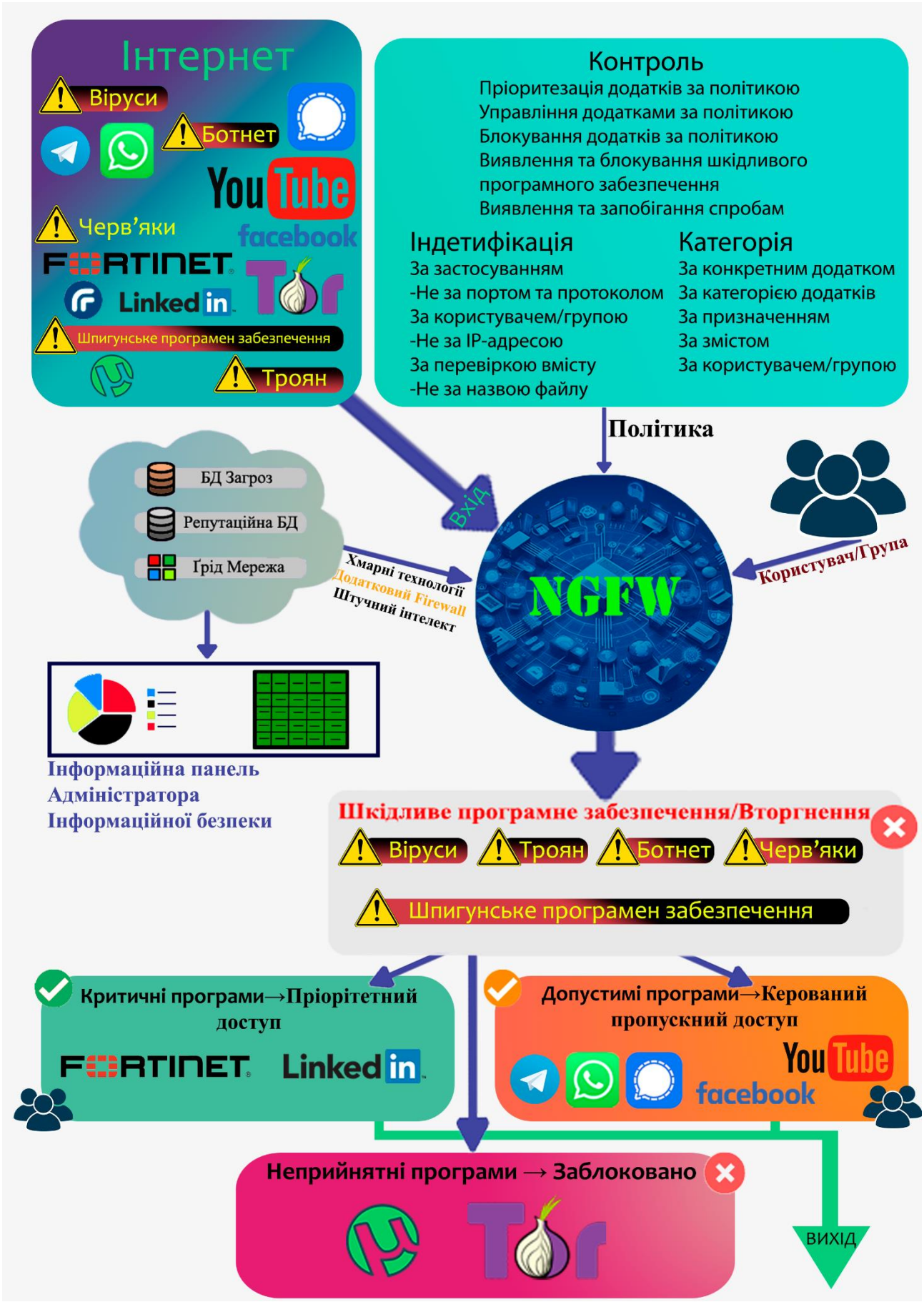

Рисунок 3.1 – Узагальнена інтерпретація концепції *NGFW*

3.2 Огляд сучасного стану ринку засобів MME, покоління NG

Palo Alto Networks пропонує широкий спектр NGFW, які відповідають потребам будь-якого корпоративного середовища. Доступні три типи firewall:

- Фізичні: Ці апаратні пристрої встановлюються безпосередньо в центрі обробки даних або в офісі, забезпечуючи надійний захист мережі.
- Віртуальні: Ці програмні продукти запускаються на віртуальних машинах, пропонуючи гнучкість та масштабованість для хмарних середовищ.
- Для контейнерів: Ці спеціально розроблені рішення забезпечують комплексний захист контейнерних середовищ, стаючи ідеальним вибором для сучасних динамічних додатків.

Panorama: Централізоване управління для кращої ефективності

Для покращення експлуатаційних характеристик та спрощення адміністрування, Palo Alto Networks пропонує Panorama. Це централізована платформа управління, яка дозволяє адміністраторам мережевої безпеки:

- Контролювати всі брандмауери Palo Alto: Незалежно від типу та розташування firewall (фізичні, віртуальні, для контейнерів), Panorama дає можливість керувати ними з єдиної консолі.
- Створювати та редагувати політики безпеки: Panorama спрощує процес створення та застосування комплексних політик безпеки, що охоплюють всі мережеві ресурси.
- Моніторити та аналізувати трафік: Panorama надає детальну інформацію про мережевий трафік, дозволяючи виявляти аномалії та потенційні загрози.
- Автоматизувати завдання: Panorama пропонує широкий спектр функцій автоматизації, які допомагають зменшити час, витрачений на рутинні завдання, та підвищити загальну ефективність роботи.

Переваги Palo Alto Networks:

- Широкий спектр NGFW: Різноманітні типи брандмауерів Palo Alto Networks дозволяють вибрати рішення, яке ідеально підходить для ваших потреб, будь то традиційні мережі, хмарні середовища або контейнерні платформи.
- Централізоване управління: Panorama забезпечує зручне та ефективне керування всіма брандмауерами Palo Alto, економлячи час та ресурси.
- Комплексний захист: NGFW Palo Alto Networks пропонують багаторівневий захист від широкого спектра кіберзагроз, включаючи зловмисне програмне забезпечення, атаки на прикладному рівні та цілеспрямовані атаки.
- Гнучкість та масштабованість: Рішення Palo Alto Networks легко масштабуються відповідно до ваших потреб, забезпечуючи захист мережі в міру її зростання.

Palo Alto Networks – пропонує комплексні рішення для кібербезпеки, що допомагають захистити ваші дані та інфраструктуру від сучасних кіберзагроз [12].

FortiNet пропонує широкий спектр NGFW під брендом FortiGate, які підходять для підприємств будь-якого розміру та потреб. Рішення FortiGate доступні в трьох основних форматах:

- Фізичні: Ці апаратні пристрої ідеально підходять для центрів обробки даних та офісів з високими вимогами до продуктивності та масштабованості.
- Віртуальні: Ці програмні рішення запускаються на віртуальних машинах, забезпечуючи гнучкість та економічність для хмарних середовищ [8,15].
- Для контейнерів: Ці спеціально розроблені брандмауери захищають контейнерні середовища, стаючи ідеальним вибором для сучасних динамічних додатків.

Уніфіковане управління та розширений захист:

Всі NGFW FortiGate працюють під керуванням власної операційної системи FortiOS, яка забезпечує уніфіковану конфігурацію та управління політиками безпеки. Це дозволяє адміністраторам з безпеки створювати та застосовувати комплексні правила, включаючи політики доступу до мереж з нульовою довірою (ZTNA) [12].

FortiGuard Labs:

Користувачі FortiGate отримують доступ до служб безпеки FortiGuard Labs, які пропонують широкий спектр функцій, таких як:

- IP-геотрекінг: Відстежує джерело мережевого трафіку для виявлення потенційних загроз.
- Виявлення пристроїв IoT: Ідентифікує та моніторить пристрої Інтернету речей (IoT) в мережі.
- Хмарна "пісочниця": Ізолює та аналізує підозрілий трафік, щоб запобігти зараженню шкідливим програмним забезпеченням.
- IPS з підтримкою AI/ML: Використовує штучний інтелект та машинне навчання для виявлення та блокування нових, невідомих загроз.

Універсальність та масштабованість:

FortiGate - це універсальне рішення NGFW, яке підходить як для великих підприємств з кількома центрами обробки даних, так і для невеликих офісів з одним філіалом. Завдяки своїй модульній конструкції та широкому спектру варіантів розгортання, FortiGate може легко масштабуватися відповідно до ваших потреб.

Ключові переваги FortiGate:

- Широкий спектр варіантів розгортання та пропускної здатності брандмауерів.
- Хмарний сандбокс для захисту від невідомих загроз.
- Власна операційна система FortiOS для уніфікованого управління політиками безпеки.
- Розширені функції безпеки FortiGuard Labs.
- Масштабованість для підприємств будь-якого розміру.

FortiGate - це надійне та гнучке рішення NGFW, яке забезпечує комплексний захист вашої мережі від сучасних кіберзагроз [12-14].

Cisco Secure Firewall (CSF) – це потужний NGFW (брандмауер нового покоління), який фокусується на розширеному застосуванні політик безпеки для всіх розподілених додатків у вашій мережі. Його мета – зробити мережеву інфраструктуру невід'ємною частиною системи безпеки брандмауера.

Різноманітні варіанти розгортання [14]:

- Апаратні firewall: Cisco пропонує широкий спектр апаратних брандмауерів, таких як серії Firepower та Meraki MX, які підходять для різних потреб та середовищ.
- Віртуальне рішення: CSF доступний як віртуальне рішення для приватних хмар, забезпечуючи захист у середовищах VMware ESXi, Microsoft Hyper-V та KVM (Kernel-based Virtual Machine).
- Рішення для публічних хмар: Cisco також пропонує CSF як рішення для публічних хмар, гарантуючи безпеку даних та додатків на платформах Azure та AWS (Amazon Web Services).

Функціональні можливості CSF:

- Поведінкова аналітика [5,15]: CSF використовує поведінкову аналітику для швидкого виявлення та реагування на кіберзагрози, що робить його більш ефективним у порівнянні з традиційними методами.
- Централізоване управління журналами: CSF збирає та аналізує дані з усіх firewall CSF у вашій організації, навіть з географічно розподілених локацій, забезпечуючи адміністраторам мережі чітку картину всієї мережевої активності.
- Підтримка TLS 1.3: CSF інтегрує Cisco Transport Layer Security (TLS) Server Identity and Discovery, що дозволяє застосовувати політики безпеки OSI 7-го рівня до зашифрованого трафіку (TLS 1.3). Це дає адміністраторам видимість трафіку, навіть якщо він не розшифровується, при цьому політики безпеки 7-го рівня залишаються незмінними.

Переваги CSF:

- Комплексний захист: CSF забезпечує всебічний захист вашої мережі від широкого спектра кіберзагроз, включаючи зловмисне програмне забезпечення, атаки на прикладному рівні та цілеспрямовані атаки.
- Гнучкість: Різноманітні варіанти розгортання CSF дозволяють легко адаптувати його до будь-яких потреб та середовищ.

- Централізоване управління: CSF пропонує централізовану платформу управління, яка спрощує адміністрування та контроль над усіма вашими брандмауерами.
- Покращена видимість та аналітика: CSF збирає та аналізує дані з усіх брандмауерів, надаючи адміністраторам мережі чітку картину всієї мережевої активності.
- Підтримка TLS 1.3: CSF забезпечує розширений захист зашифрованого трафіку, не жертвуючи видимістю та контролем.

Cisco Secure Firewall – це надійне та гнучке рішення NGFW, яке допоможе вам захистити ваші дані та додатки від сучасних кіберзагроз.

4. УЗАГАЛЬНЕННЯ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ПРОГРАМНИХ ММЕ ПРИВАТНОГО СЕГМЕНТУ КОРИСТУВАЧІВ.

4.1 Визначення умов тестування та узагальнення результатів

Регулярне проведення тестування безпеки брандмауера є важливим для забезпечення та підтримки безпеки організації. Тестування на проникність можна мати наступні переваги [18]:

1) Виявлення заздалегідь:

- Оцінка та виявлення проблем на ранніх стадіях: Проактивний підхід до кібербезпеки [5,13,15] передбачає регулярне тестування та оцінку ваших систем, щоб виявити потенційні загрози та вразливості до їх використання зловмисниками. Це дозволяє вжити заходів для усунення цих проблем до того, як вони призведуть до серйозних інцидентів.
- Прийняття проактивної, а не реактивної стратегії: Замість того, щоб реагувати на вже відбулі кібератаки, проактивний підхід зосереджується на запобіганні їм. Це може заощадити час, гроші та ресурси, а також мінімізувати шкоду для репутації та даних.

2) Підвищення загального рівня безпеки:

- Покращення загального рівня безпеки організації: Впровадження проактивних заходів кібербезпеки, таких як регулярне тестування брандмауерів, сприяє загальному підвищенню рівня захисту організації.
- Забезпечення надійного захисту firewall: Брандмауери є умовною «першою лінією оборони» любої мережі, тому їх надійний захист має вирішальне значення. Регулярне тестування брандмауерів гарантує, що вони правильно налаштовані та оновлені, щоб блокувати найновіші кіберзагрози.
- Захист мережевих ресурсів: Брандмауери захищають не лише інформацію, що циркулює в рамках периметру безпеки мережи, але й усі наявні ресурси, такі як комп'ютери, сервери, мережеве устаткування та мобільні гаджети,

що взаємодіють з мережею [5]. Це допомагає запобігти крадіжці даних, фінансовим втратам та іншим серйозним наслідкам кіберзлочинів.

3) Зменшення витрат:

- Уникнення витрат на відновлення після інцидентів: Реакція на кіберінцидент може бути дуже дорогою, адже вона включає витрати на відновлення даних, ремонт систем, юридичні послуги та компенсації постраждалим. Проактивний підхід, який передбачає регулярне тестування брандмауерів, значно знижує ризик виникнення таких інцидентів, економлячи кошти.
- Зниження ризику штрафів за невідповідність: Багато галузей мають суворі нормативні вимоги щодо кібербезпеки. Невідповідність цим вимогам може призвести до штрафів та інших санкцій. Проактивний підхід до кібербезпеки допомагає гарантувати відповідність усім чинним нормам, економлячи кошти та захищаючи репутацію.

Інвестування в проактивний підхід до кібербезпеки – це розумне рішення, яке може заощадити час, гроші та ресурси, а також мінімізувати ризик серйозних кіберінцидентів.

Існує 13 кроків у тестуванні брандмауера, а саме:

Крок 1. Першим кроком є вибір брандмауера, який тестуватиметься. Це може бути фізичний брандмауер, віртуальний брандмауер або програмне брандмауерне рішення. Важливо вибрати брандмауер, який відповідатиме потребам.

Після вибору брандмауера потрібно буде його розгорнути. Це може включати установку апаратного забезпечення, налаштування програмного забезпечення та підключення брандмауера до мережі.

Для створення IP-пакетів з TCP, UDP або ICMP навантаженням знадобиться спеціальне програмне забезпечення для створення пакетів. Два популярних інструменти для цього: Hping та Nmap. Nmap може сканувати цілий діапазон IP-адрес, що робить його кращим для загального сканування мережі. Hping може сканувати лише одну IP-адресу за раз, але здатний генерувати більш детальні пакети та кращий контроль над трафіком, що робить його кращим для виявлення незвичайної активності. Окрім Hping та Nmap, можуть бути й інші інструменти, які

можуть бути корисними для тестування брандмауера. Деякі з цих інструментів можуть включати сканери вразливостей, інструменти для перехоплення мережевого трафіку та інструменти для аналізу журналів.

Важливо зазначити, що перед тестуванням будь-якого брандмауера тестувальник завжди повинен отримати дозвіл від власника або адміністратора брандмауера.

Крок 2. Використання команди traceroute на брандмауері дозволяє визначити маршрут, яким пакети проходять через мережу. Цей крок надає корисну інформацію про:

- Маршрутизатори та пристрої: Можна побачити всі маршрутизатори та пристрої, які беруть участь у встановленні з'єднання між комп'ютером та брандмауером.
- Фільтрація трафіку: Traceroute може допомогти визначити, які протоколи та порти блокуються брандмауером.

Хоча ping та traceroute виконують схожу функцію - перевіряють з'єднання між двома вузлами - вони мають ключові відмінності:

- Деталізація маршруту: Traceroute показує кожен етап шляху, яким йде пакет, тоді як ping просто повідомляє, чи вдалося встановити з'єднання.
- Протоколи та порти: Ping та traceroute використовують різні протоколи та порти, тому одна команда може дати результат, а інша - ні.

Команда traceroute може відрізнятися залежно від операційної системи. Наприклад, у Windows використовується команда tracert. При виконанні команди traceroute виводить список доменних імен та IP-адрес, через які проходить пакет. Можна проаналізувати цей список, щоб визначити маршрут пакетів та будь-які потенційні проблеми з фільтрацією трафіку.

Приклад команди traceroute:

tracert google.com

Ця команда покаже вам маршрут пакетів до веб-сайту Google.

Крок 3. Сканування портів за допомогою Nmap [5]. Nmap - це популярний інструмент сканування портів, який використовується завдяки своїй гнучкості та

можливостям детального налаштування. Він дозволяє не лише виявляти відкриті порти, але й ідентифікувати сервіси, які працюють на цих портах. Виконання сканування Nmap:

- Nmap пропонує широкий спектр опцій для налаштування сканування.
- Можна вказати тип сканування, діапазон портів, інтенсивність сканування та багато іншого.

Приклад команди Nmap яка виконує агресивне сканування SYN перших 1024 портів на IP-адресі x.x.x.x: *nmap -sS -p 0-1024 x.x.x.x -T4*

Nmap може експортувати результати сканування в різних форматах, таких як CSV, XML та HTML. Можливо проаналізувати ці результати, щоб визначити:

- Відкриті порти: Nmap покаже, які порти відкриті на брандмауері.
- Закриті порти: Nmap також покаже, які порти закриті.
- Відфільтровані порти: Nmap може допомогти визначити, які порти фільтруються брандмауером.
- Сервіси: Nmap може ідентифікувати сервіси, які працюють на відкритих портах.

Важливо розуміти різницю між закритими та відфільтрованими портами. На закритий порт комп'ютер не відповідає на запити. У випадку з відфільтрованими портами, брандмауер блокує запити, тому комп'ютер навіть не має можливості відповісти.

Nmap може використовувати різні методи для ідентифікації сервісів, які працюють на відкритих портах. Ці методи включають аналіз відповідей на запити, відбитків пальців TCP/IP та базу даних сервісів Nmap.

Крок 4. Захоплення банерів. Захоплення банерів - це процес отримання інформації про систему та сервіси, які працюють на її відкритих портах. Це може бути корисно для адміністраторів мережі, які хочуть повністю інвентаризувати свої системи та сервіси.

Захоплення банерів з брандмауера може розкрити версію використовуваного firewall, що може бути використано для пошуку вразливостей та експлойтів [12], які можуть бути використані для обходу його захисту.

Існує два основних методи захоплення банерів:

- Активне захоплення банерів: Цей метод передбачає надсилання пакетів на віддалений хост та аналіз отриманих відповідей. Тестувальник може створювати або змінювати пакети відповідно до своїх потреб.
- Пасивне захоплення банерів: Цей метод є менш ризикованим, оскільки він не потребує прямого з'єднання з віддаленим хостом. Замість цього він використовує інші програми або системи як шлюзи для з'єднання.

Існує багато різних інструментів, які можна використовувати для захоплення банерів. Деякі з найпопулярніших інструментів включають:

- Telnet: Telnet - це мережевий протокол, який можна використовувати для підключення до віддалених систем та виконання команд.
- Wget: Wget - це інструмент командного рядка, який можна використовувати для завантаження файлів з веб-серверів. Wget також можна використовувати для захоплення банерів, надсилаючи запити на HTTP-сервери.
- cURL: cURL - це інструмент командного рядка, схожий на Wget. Його також можна використовувати для захоплення банерів.
- Nmap: Nmap - це сканер портів, який також можна використовувати для захоплення банерів.
- NetCat: NetCat - це мережевий інструмент, який можна використовувати для надсилання та отримання даних через мережу. NetCat також можна використовувати для захоплення банерів.
- ASR: ASR - це тип програмного забезпечення, яке використовується для зменшення атакованої поверхні системи. ASR може також використовуватися для захоплення банерів.

Важливо зазначити, що захоплення банерів може бути ризикованим. Активне захоплення банерів може бути виявлено системами виявлення вторгнень (IDS), а також може призвести до помилкових спрацьовувань. Пасивне захоплення банерів менш ризиковане, але воно може не збирати всю доступну інформацію.

Крок 5. Перерахування контролю доступу. Перерахування правил доступу - це процес активного з'єднання з цільовими хостами для виявлення потенційних векторів атаки, які можна використовувати для подальшого впливу на систему.

Брандмауери використовують ACL для визначення, який трафік з внутрішньої мережі дозволено або відхилено. ACL складаються з правил, які визначають, які типи трафіку дозволені, з яких джерел він може надходити та до яких пунктів призначення він може йти.

Тестувальники безпеки можуть перерахувати правила доступу, надсилаючи запити на брандмауер і аналізуючи відповіді. Вони можуть використовувати різні інструменти для цього, такі як Nmap або Wireshark. Результати перерахування правил доступу можуть показати тестувальнику безпеки, які порти відкриті, закриті або відфільтровані брандмауером. Ця інформація може бути використана для виявлення потенційних вразливостей у брандмауері.

Приклад команди Nmap для перерахування правил доступу:

nmap -sA 192.165.123.123

- Ця команда надсилає запити з прапорцем ACK на перші 1024 порти на IP-адресі 192.165.123.123.
- Результати можуть показати, які порти відкриті, закриті або відфільтровані.

Крок 6. Ідентифікація архітектури брандмауера. До основних архітектур брандмауерів які часто використовуються відносять: брандмауери з фільтрацією пакетів, брандмауери з екранованим хостом, брандмауери з двома хостами та брандмауери з екранованою підмережею.

Брандмауери з фільтрацією пакетів: Організації використовують маршрутизатори для підключення до Інтернету. Ці маршрутизатори встановлюються на межі між внутрішньою мережею підприємства та мережею провайдера. Вони можуть бути налаштовані для прийняття або відхилення пакетів відповідно до встановлених правил. Це один з найпростіших і найефективніших способів зменшити ризики з Інтернету для підприємства.

Брандмауери з екранованим хостом: Даний тип брандмауера поєднує в собі маршрутизатор з фільтрацією пакетів і окремий брандмауер, наприклад, проксі-брандмауер додатків. Маршрутизатор фільтрує пакети перед тим, як вони потрапляють у внутрішню мережу, зменшуючи навантаження на внутрішній проксі-сервер [18].

Брандмауери з двома хостами: Ця архітектура є більш складною версією брандмауерів з екранованим хостом. У цьому підході хост-бастіон має дві мережеві інтерфейсні карти (NIC). Одна карта підключена до зовнішньої мережі, а інша – до внутрішньої мережі, забезпечуючи додатковий рівень безпеки.

Брандмауери з екранованою підмережею (демілітаризована зона): Ця архітектура часто використовує трансляцію мережевих адрес (NAT). NAT дозволяє зіставляти зовнішні IP-адреси з внутрішніми, створюючи бар'єр для зовнішніх зловмисників

Брандмауер може видавати підроблені пакети, щоб надати список статусів портів, які були ідентифіковані. Інструменти, такі як Hping, Nmap або Hping2, можна використовувати для отримання відповідей на запити на певні порти та визначення реакції брандмауера, що дозволяє скласти карту відкритих портів [18].

Після сканування брандмауер повертає пакети дій, які показують, які з'єднання були відхилені, заблоковані або розірвані:

— Відповідь брандмауера пакетом SYN/ACK вказує на те, що порт відкритий.

— Повернення пакета RST/ACK свідчить про те, що підготовлений пакет був відхилений брандмауером.

— Повернення пакета ICMP типу 3 з кодом 13 означає, що з'єднання було розірвано.

— Відсутність відповіді означає, що підготовлений пакет був скинутий через фільтрацію порту.

Крок 7. Тестування політики брандмауера. Політика безпеки організації - це набір правил, призначених для захисту комп'ютерної мережі та даних, які нею

проходять. Брандмауер є ключовим компонентом цієї політики, оскільки він відхиляє всі пакети, які не мають явного дозволу.

Політики брандмауера визначають, які типи трафіку дозволені та заборонені в мережі. Вони ґрунтуються на таких факторах, як:

- Джерело та призначення пакета: Політика може дозволяти або забороняти трафік з певних IP-адрес або діапазонів IP-адрес.
- Порт TCP/IP або використовуваний протокол: Політика може дозволяти або забороняти трафік на певних портах або протоколах, таких як HTTP, FTP або SSH.
- Час доби: Політика може дозволяти або забороняти трафік у певний час доби.

Тестування політик брандмауера є важливим кроком у забезпеченні безпеки вашої мережі. Існує два основних методи тестування:

- Аналіз конфігурації: Цей метод передбачає порівняння паперової копії конфігурації політики брандмауера з очікуваною конфігурацією. Це може допомогти виявити потенційні дірки в політиці.
- Тестування проникнення: Цей метод передбачає виконання дій на брандмауері, щоб підтвердити очікувану поведінку. Це може допомогти виявити будь-які проблеми з реалізацією політики.

Існує багато інструментів, які можна використовувати для тестування політик брандмауера. Деякі з найпоширеніших інструментів включають:

- Nmap: Nmap - це сканер портів, який можна використовувати для сканування брандмауера на наявність відкритих портів.
- Nessus: Nessus - це сканер вразливостей, який можна використовувати для сканування брандмауера на наявність відомих вразливостей.
- Wireshark: Wireshark - це інструмент перехоплення мережевого трафіку, який можна використовувати для аналізу трафіку, який проходить через брандмауер.

Крок 8. Firewalking. Методологія обхідного маневру базується на визначенні дозволених типів трафіку, а потім на використанні цих типів пакетів як основи для

додаткового сканування за типом трасування. Поширеною конфігурацією брандмауера може бути дозвіл лише на DNS-запити (UDP-порт 53). В результаті, якщо ми передамо трафік на UDP-порт 53 з наступним TTL-номером, він омине початковий брандмауер і поверне інформацію про наступний хост в черзі. Оскільки функція трасування заснована на обробці поля TTL на рівні IP, можна використовувати будь-який з різних транспортних механізмів (UDP, TCP або ICMP), а отже, будь-який сервіс, заснований на цих протоколах, може бути підроблений.

Інструмент Firewalk здатний виконувати розширене мережеве мапування і малювати зображення топології мережі. Зокрема, створюючи пакети з певними значеннями TTL, тестувальник може ідентифікувати відкриті порти, якщо відповідне повідомлення перевищило TTL [18]. Якщо відповіді немає, можна з упевненістю припустити, що брандмауер відфільтрував пакет і заблокував з'єднання.

Після того, як брандмауер буде знайдено на шляху до цільового хоста, використання процесу Firewalking для сканування цієї системи покаже будь-які відкриті порти. Навіть якщо наступна система в черзі відмовиться передавати інформацію про цільовий порт, ці порти будуть відомі. Ці дані можуть бути використані для складання загальних списків контролю доступу для кожного брандмауера на цьому шляху. Якщо не перевіряти кожен сайт на лінії, існує ризик шахрайського повідомлення про закриті порти, в той час як трафік насправді блокується проміжною системою [18].

Крок 9. Firewalking - це методика обходу брандмауерів та мережевих пристроїв безпеки. Вона ґрунтується на принципі аналізу дозволених типів трафіку та використання цих типів пакетів як основи для глибшого сканування за допомогою трасування.

Припустимо, що брандмауер дозволяє лише DNS-запити (UDP-порт 53). Firewalking може використовувати це знання для надсилання пакетів на UDP-порт 53 з нестандартним значенням TTL (Time-to-Live). TTL - це поле в заголовку IP-пакета, яке вказує, скільки разів пакет може бути перенаправлений, перш ніж буде

скинутий. Змінюючи значення TTL, Firewalking може змусити пакет перенаправлятися через брандмауер, а потім скидатися наступним пристроєм у мережі. Аналізуючи відповіді на ці пакети, Firewalking може отримати інформацію про топологію мережі та відкриті порти.

Існує кілька інструментів, які можна використовувати для Firewalking, наприклад:

- Nmap: Nmap має вбудовану функцію Firewalking, яка називається "traceroute".
- Hping: Hping - це інструмент з відкритим вихідним кодом, який можна використовувати для надсилання та аналізу IP-пакетів. Він має функцію Firewalking, схожу на Nmap.
- Angry IP Scanner: Angry IP Scanner - це інструмент сканування мережі, який також може виконувати Firewalking.

Переваги Firewalking:

- Firewalking може бути корисним для обходу брандмауерів та отримання інформації про мережі, які інакше були б недоступні.
- Він може допомогти виявити відкриті порти та інші вразливості.

Ризики Firewalking:

- Firewalking може бути незаконним без дозволу власника мережі.
- Він може бути виявлений системами виявлення вторгнень (IDS).
- Він може випадково пошкодити мережеві пристрої.

Приклад використання Firewalking:

Припустимо, що ви хочете сканувати хост за адресою 192.168.1.100, але перед ним стоїть брандмауер. Ви можете використовувати Firewalking, щоб обійти брандмауер і сканувати хост. Виконайте наступну команду Nmap:

1) nmap --traceroute 192.168.1.100
2) Nmap надішле пакети на UDP-порт 53 з різними значеннями TTL.
3) Nmap проаналізує відповіді на ці пакети та виведе інформацію про топологію мережі та відкриті порти.

Якщо тестеру вдалося скомпрометувати цільову систему і він бажає обійти брандмауер, він може встановити програмне забезпечення для перенаправлення портів, таке як Fpipe або Datapipe, і прослуховувати певні номери портів.

Крок 10. Важливість тестування на проникнення. Внутрішнє та зовнішнє тестування на проникнення не є обов'язковими для тестування брандмауера, але вони дають більш реалістичне уявлення про те, як зловмисник може атакувати системи. Зовнішнє тестування на проникнення призначене для оцінки ефективності політик безпеки периметра в запобіганні та виявленні атак. Воно також може допомогти виявити недоліки у веб-, поштових та FTP-серверах, які доступні з Інтернету.

Процес зовнішнього тестування на проникнення:

1) Розвідка: Тестувальник збирає інформацію про мережеві ресурси, включаючи відкриті порти, вразливості та інформацію про користувачів.

2) Експлуатація: Тестувальник використовує вразливості, знайдені під час розвідки, для отримання доступу до систем.

3) Підвищення привілеїв: Після отримання доступу тестувальник намагається отримати більш високі привілеї в системі.

4) Пост-експлуатація: Тестувальник використовує отримані привілеї для виконання зловмисних дій, таких як крадіжка даних або виведення з ладу систем.

Внутрішнє тестування на проникнення:

- Внутрішнє тестування на проникнення використовується для оцінки того, що зловмисник може зробити, якщо він вже має доступ до мережі.
- Воно може допомогти виявити вразливості у внутрішніх системах, а також недоліки у політиках та процедурах безпеки.

Процес внутрішнього тестування на проникнення:

1) Розміщення: Тестувальник отримує початковий доступ до вашої мережі, наприклад, через соціальну інженерію або експлуатацію вразливості.

2) Розвідка [5,15,19]: Тестувальник збирає інформацію про ваші внутрішні мережеві ресурси.

3) Експлуатація: Тестувальник використовує вразливості, знайдені під час розвідки, для отримання доступу до ваших систем [18].

4) Підвищення привілеїв: Тестувальник намагається отримати більш високі привілеї в системі.

5) Пост-експлуатація: Тестувальник використовує отримані привілеї для виконання зловмисних дій [18].

Переваги тестування на проникнення:

- Тестування на проникнення може допомогти вам виявити та виправити вразливості у ваших системах, перш ніж ними скористаються зловмисники.
- Воно також може допомогти вам покращити ваші політики та процедури безпеки.

Ризики тестування на проникнення:

- Існує ризик того, що тестування на проникнення може призвести до порушення безпеки ваших систем.
- Важливо вибрати надійного постачальника послуг тестування на проникнення та ретельно спланувати тестування.

Крок 11.

Прихований канал - це метод зв'язку, який використовується хакерами для обходу систем безпеки та залишатися непоміченими.

Приховані канали зазвичай створюються шляхом встановлення бекдору на скомпрометованому комп'ютері в мережі.

- Бекдор - це програма, яка надає хакеру віддалений доступ до комп'ютера.
- Після встановлення бекдору хакер може використовувати його для створення зворотного підключення до своєї власної системи [18].
- Це зворотне підключення може використовуватися для передачі даних, таких як викрадені файли або інформація про автентифікацію [18].

Приклади прихованих каналів:

Існує багато різних типів прихованих каналів. Деякі поширені приклади включають:

- Схований текст: Цей тип прихованого каналу використовує невидимі символи або символи Unicode для вбудовування повідомлень у файли зображень або інші типи даних [18].
- Стеганографія: Цей тип прихованого каналу використовує зміни в існуючих файлах, таких як зображення або аудіо, для приховування повідомлень.
- Команди DNS: Цей тип прихованого каналу використовує систему імен доменів (DNS) для передачі повідомлень [5,18].
- Протоколи обміну повідомленнями: Цей тип прихованого каналу використовує протоколи обміну повідомленнями, такі як IRC або XMPP, для передачі повідомлень.

Приховані канали небезпечні, тому що їх важко виявити.

- Вони можуть використовуватися для обходу систем безпеки та передачі даних без відома або дозволу власника мережі.

Існує багато способів захиститися від прихованих каналів. Деякі з них:

- Оновлення програмного забезпечення: Важливо регулярно оновлювати програмне забезпечення до останніх виправлень безпеки.
- Використання брандмауера: Брандмауер може допомогти заблокувати несанкціонований трафік у вашу мережу [18].
- Використання антивірусного програмного забезпечення: Антивірусне програмне забезпечення може допомогти виявити та видалити зловмисні програми з вашого комп'ютера [18].
- Навчання користувачів: Важливо навчити своїх користувачів про приховані канали та про те, як їх виявити та уникнути.

Інструменти для тестування на приховані канали:

Існує багато інструментів, які можна використовувати для тестування на приховані канали. Деякі з них:

- Netcat: Netcat - це мережевий інструмент, який можна використовувати для надсилання та отримання даних. Його можна використовувати для тестування на приховані канали, надсилаючи повідомлення на підозрілі порти.

- Wireshark: Wireshark - це інструмент перехоплення мережевого трафіку, який можна використовувати для аналізу трафіку на наявність прихованих каналів.
- Nmap: Nmap - це сканер портів, який можна використовувати для сканування мережі на наявність відкритих портів. Відкриті порти можуть використовуватися для прихованих каналів [5,18].
- Одним з найпоширінішим методів є використання відомої хакерської платформи Metasploit.

Крок 12. Нейтралізуйте приховані канали. HTTP-тунелювання. HTTP-тунелювання - це метод інкапсуляції трафіку за допомогою протоколу HTTP. Він часто використовується для обходу брандмауерів або проксі-серверів, які блокують доступ до певних веб-сайтів або служб [18]. При HTTP-тунелюванні клієнт встановлює з'єднання HTTP з сервером-прокси. Потім клієнт надсилає серверу-прокси запит HTTP, який містить інкапсульований трафік. Сервер-прокси перенаправляє інкапсульований трафік до кінцевого пункту призначення, а потім надсилає відповідь клієнту.

Переваги HTTP-тунелювання:

- HTTP-тунелювання може бути корисним для обходу брандмауерів або проксі-серверів, які блокують доступ до певних веб-сайтів або служб.
- Воно також може бути корисним для приховування трафіку від систем виявлення вторгнень (IDS) [5].

Ризики HTTP-тунелювання:

- HTTP-тунелювання може бути виявлено брандмауерами або проксі-серверами, які спеціально налаштовані для його виявлення [18].
- Воно також може бути повільнішим, ніж пряме з'єднання, оскільки трафік інкапсулюється та перенаправляється.

Існує багато інструментів, які можна використовувати для HTTP-тунелювання. Деякі з них:

- Proxifier: Proxifier - це комерційний інструмент, який дозволяє тунелювати будь-який трафік через проксі-сервер.

- GoProxy: GoProxy - це безкоштовний інструмент з відкритим вихідним кодом для тунелювання трафіку HTTP і SOCKS [18].
- Polipo: Polipo - це безкоштовний веб-прокси-сервер з відкритим вихідним кодом, який можна використовувати для HTTP-тунелювання.

Приклад використання HTTP-тунелювання:

Припустимо, що ви хочете отримати доступ до веб-сайту, який заблокований вашим брандмауером. Ви можете використовувати HTTP-тунелювання для обходу брандмауера та доступу до веб-сайту:

1) Встановіть інструмент HTTP-тунелювання, наприклад Proxifier.
2) Налаштуйте Proxifier на використання проксі-сервера, який дозволяє отримувати доступ до веб-сайту.
3) Запустіть браузер і перейдіть на веб-сайт, який ви хочете відвідати.

Крок 13. Виявлення вразливостей брандмауера. Вразливість брандмауера - це недолік у його дизайні, реалізації або конфігурації, який може бути використаний зловмисником для атаки на мережу. Існує багато різних типів вразливостей брандмауера. Ось деякі з найпоширеніших:

- Неправильна конфігурація: Це найпоширеніший тип вразливості брандмауера. Вона може бути викликана помилками в конфігурації брандмауера, наприклад, залишенням відкритими непотрібних портів або дозволом небажаного трафіку [18].
- Програмні помилки: Брандмауери, як і будь-яке програмне забезпечення, можуть містити програмні помилки, які можуть бути використані зловмисниками.
- Обхід: Зловмисники можуть використовувати різні методи для обходу брандмауерів, наприклад, тунелювання трафіку через інші протоколи або використання вразливостей у брандмауері [18].
- Соціальна інженерія [5,19]: Зловмисники можуть використовувати соціальну інженерію, щоб обдурити користувачів у розкриття інформації про брандмауер або для виконання дій, які дозволять їм обійти брандмауер.

Вразливості брандмауера можуть мати серйозні наслідки, включаючи:

- Несанкціонований доступ: Зловмисники можуть використовувати вразливості брандмауера для отримання несанкціонованого доступу до мережі.
- Витік даних: Зловмисники можуть використовувати вразливості брандмауера для крадіжки даних з мережі.
- Відмова в обслуговуванні: Зловмисники можуть використовувати вразливості брандмауера для відмови в обслуговуванні мережі.

Існує кілька способів виявити вразливості брандмауера. Ось деякі з них:

- Сканування вразливостей: Ви можете використовувати інструмент сканування вразливостей для сканування брандмауера на наявність відомих вразливостей.
- Тестування на проникнення: Ви можете найняти фахівців з тестування на проникнення, щоб провести тестування вашого брандмауера на наявність вразливостей.
- Самооцінка: Ви можете провести самооцінку своїх політик та процедур безпеки, щоб виявити потенційні вразливості.

Після виявлення вразливості брандмауера важливо вжити заходів для її виправлення. Це може включати [18]:

- Оновлення брандмауера: Переконайтеся, що на вашому брандмауері встановлено останні виправлення та оновлення.
- Зміна конфігурації брандмауера: Змініть конфігурацію брандмауера, щоб закрити вразливість.
- Встановлення оновлень програмного забезпечення: Встановіть оновлення програмного забезпечення для операційної системи та будь-яких інших програм, які працюють на брандмауері.

4.2 Формування рекомендацій, щодо налаштувань і особливостей використання сучасних ММЕ

Firewall є важливим компонентом будь-якої системи кібербезпеки [5,13,15], що захищає мережу від несанкціонованого доступу та кібератак. Коректне

налаштування та використання Firewall може значно підвищити рівень безпеки мережі [5,16]. Наведемо деякі основні рекомендації щодо інтеграції засобів MME:

Аналіз потреб: Перш ніж приступати до налаштування Firewall, важливо провести аналіз потреб вашої організації або індивідуального користувача. Це включає в себе визначення типів трафіку, які потрібно блокувати чи допускати, і встановлення рівня захисту відповідно до конкретних вимог безпеки.

Вибір типу Firewall: Існують різні типи Firewall, такі як програмні та апаратні. Вибір підходящого типу залежить від потреб вашої системи та фінансових можливостей. Наприклад, для великих корпоративних мереж може бути доцільніше використовувати апаратні Firewall для кращої продуктивності та безпеки.

Встановлення правил доступу: Одним з ключових аспектів налаштування Firewall є встановлення правил доступу. Це включає в себе визначення, який трафік дозволено, а який блокується. Рекомендується створювати детальні правила доступу з урахуванням потреб вашої мережі та забезпечення прозорості та безпеки.

Регулярне оновлення: Firewall потребує постійного оновлення для забезпечення ефективного захисту від нових загроз. Важливо регулярно оновлювати ядро програмного забезпечення та бази даних загроз для максимальної ефективності захисту.

Моніторинг та аналіз подій: Для ефективного використання Firewall необхідно проводити моніторинг та аналіз подій. Це допоможе вчасно виявляти потенційні загрози та вживати відповідних заходів для їх усунення.

Навчання користувачів: Нарешті, важливо навчати користувачів правильному використанню Firewall та свідомому ставленню до безпеки мережі. Регулярні навчальні заходи та інструкції допоможуть зменшити ризик виникнення безпекових проблем через некоректну діяльність користувачів.

Загалом, враховуючи ці рекомендації та особливості використання Firewall, можна забезпечити ефективний рівень захисту для вашої мережі та інформаційних ресурсів.

5. ВИЗНАЧЕННЯ ПЕРСПЕКТИВ ПОДАЛЬШОГО РОЗВИТКУ ММЕ ПОКОЛІННЯ NG

5.1 Особливості використання хмарних реалізацій ММЕ покоління NG

Хмарні рішення стають все більш популярними у різних сферах IT, включаючи кібербезпеку. Серед таких рішень особливу увагу привертають Next-Generation Firewalls (NGFW) — міжмережеві екрани нового покоління, які забезпечують більш високий рівень захисту порівняно з традиційними міжмережевими екранами. Хмарні NGFW поєднують переваги хмарної інфраструктури з розширеними можливостями захисту, що робить їх важливим елементом сучасних стратегій кібербезпеки.

NGFW — це більше, ніж просто фільтрація трафіку за IP-адресами, портами та протоколами. Вони включають такі функції, як:

1) Інспекція трафіку на прикладному рівні: NGFW аналізують трафік на рівні додатків, що дозволяє виявляти та блокувати загрози, які не можуть бути ідентифіковані на нижчих рівнях.

2) Ідентифікація користувачів: Замість роботи лише з IP-адресами, NGFW можуть ідентифікувати користувачів, що дозволяє застосовувати політики безпеки на основі ролей.

3) Інтеграція з іншими системами безпеки: NGFW можуть взаємодіяти з системами виявлення вторгнень (IDS), системами попередження про вторгнення (IPS) та іншими інструментами безпеки.

4) Захист від сучасних загроз: Включають функції для виявлення та блокування шкідливого ПЗ, атак нульового дня та інших новітніх загроз.

Використання хмарних рішень NGFW має низку переваг порівняно з традиційними, локально розгорнутими міжмережевими екранами:

1) Масштабованість: Хмарні NGFW легко масштабуються відповідно до потреб бізнесу. У випадку збільшення навантаження можна швидко додати ресурси без необхідності в апаратному забезпеченні.

2) Гнучкість та доступність: Вони забезпечують високу доступність і надійність завдяки розподіленій природі хмарних інфраструктур.

3) Зниження витрат: Використання хмарних NGFW може знизити загальні витрати на інфраструктуру та її обслуговування. Компанії не потрібно інвестувати в дороге апаратне забезпечення та витрачати ресурси на його підтримку.

4) Швидкість розгортання: Хмарні рішення можна розгорнути набагато швидше, ніж локальні. Це дозволяє організаціям оперативно реагувати на зміни в середовищі загроз.

5) Автоматичне оновлення: Хмарні NGFW отримують автоматичні оновлення без необхідності втручання користувачів, що забезпечує захист від нових загроз.

Попри численні переваги, використання хмарних NGFW має й певні виклики:

1) Проблеми з конфіденційністю: Дані, що проходять через хмарні NGFW, можуть бути піддані ризикам, пов’язаним з конфіденційністю та регуляторними вимогами.

2) Залежність від постачальника: Організації стають залежними від постачальника хмарних послуг, що може бути проблематичним у разі змін умов договору або технічних проблем на стороні постачальника.

3) Інтеграція з існуючими системами: Може виникати складність у інтеграції хмарних рішень NGFW з уже існуючими локальними системами безпеки.

Висновок

Хмарні рішення NGFW представляють собою потужний інструмент для захисту мережевих інфраструктур від сучасних кіберзагроз [11-13,19]. Вони поєднують в собі високу ефективність, гнучкість та масштабованість, що робить їх привабливим вибором для багатьох організацій. Проте, успішне впровадження хмарних NGFW вимагає ретельного планування та врахування можливих ризиків, щоб забезпечити максимальний рівень безпеки та відповідність регуляторним вимогам.

5.2 Питання інтеграції MME NG до складу комплексних систем захисту

Інтеграція міжмережевих екранів нового покоління (MME NG) до складу комплексних систем захисту є важливим аспектом забезпечення кібербезпеки сучасних організацій. Цей процес потребує ретельного планування та врахування багатьох факторів, щоб забезпечити ефективне та безперебійне функціонування всієї системи захисту.

5.2.1 Основні аспекти інтеграції MME NG

1) Сумісність з існуючими системами: MME NG повинні бути сумісними з уже наявними системами безпеки, такими як IDS/IPS, антивірусні програми, системи моніторингу трафіку та інші. Це забезпечує злагоджену роботу та мінімізує ризики конфліктів між різними компонентами системи. Для досягнення цього важливо використовувати стандартизовані протоколи та інтерфейси, такі як API та інтеграційні платформи, що дозволяють різним системам ефективно обмінюватися даними.

2) Централізоване управління: Інтеграція MME NG до комплексних систем захисту вимагає централізованого управління, яке дозволяє контролювати всі компоненти системи з єдиного інтерфейсу. Це спрощує адміністрування та забезпечує швидку реакцію на інциденти. Централізоване управління також сприяє кращій видимості мережевої активності та полегшує процес створення звітів і аналізу даних.

3) Кореляція даних та інцидентів: Ефективна інтеграція MME NG дозволяє корелювати дані з різних джерел для виявлення складних загроз та атак. Це включає поєднання інформації про мережевий трафік, активність користувачів, логів системи тощо. Використання засобів кореляції та аналітики дозволяє швидше і точніше ідентифікувати загрози, що сприяє своєчасному реагуванню та мінімізації можливих збитків.

5.2.2 Взаємодія з іншими системами та засобами безпеки

1) Інтеграція з SIEM-системами [13]: Системи управління подіями інформаційної безпеки (SIEM) є ключовими компонентами для збору, аналізу та зберігання даних про безпеку. MME NG повинні мати можливість інтеграції з SIEM для забезпечення ефективного моніторингу та аналізу подій. Це включає передачу логів та подій безпеки до SIEM-систем, що дозволяє аналітикам отримувати повну картину про стан мережі та швидко реагувати на загрози.

2) Інтеграція з системами управління ідентифікацією та доступом (IAM): MME NG можуть використовувати дані з систем IAM для ідентифікації користувачів та застосування політик доступу на основі ролей. Це забезпечує більш точний контроль доступу до ресурсів мережі та зменшує ризики несанкціонованого доступу. Зворотна інтеграція, коли дані про активність користувачів з MME NG передаються до IAM, дозволяє посилити політики безпеки та виявляти підозрілу активність.

3) Інтеграція з хмарними сервісами безпеки: Багато організацій використовують хмарні сервіси для розширення своїх можливостей у сфері безпеки. Інтеграція MME NG з такими сервісами, як безпечні веб-шлюзи (SWG), хмарні доступні безпекові брокери (CASB) та інші, забезпечує додатковий рівень захисту. Це дозволяє застосовувати політики безпеки незалежно від того, де знаходяться користувачі та ресурси, що є особливо важливим у сучасних гібридних та віддалених робочих середовищах.

5.2.3 Виклики інтеграції

1) Складність налаштування та управління: Інтеграція MME NG з іншими системами безпеки може бути складним та трудомістким процесом, що потребує високої кваліфікації фахівців та ретельного планування. Неправильна конфігурація або недостатнє тестування можуть призвести до вразливостей у системі захисту або конфліктів між різними компонентами.

2) Витрати на інтеграцію: Вартість інтеграції може бути значною, особливо якщо потрібно адаптувати або замінювати існуючі системи для

забезпечення сумісності з MME NG. Це включає витрати на програмне забезпечення, обладнання, навчання персоналу та підтримку.

3) Забезпечення безперебійної роботи: Під час інтеграції важливо забезпечити безперебійну роботу всіх компонентів системи безпеки. Це включає планування резервних копій, тестування на витривалість та відновлення після аварій, щоб мінімізувати ризики простоїв та збоїв.

Висновок

Інтеграція MME рішень покоління NG до складу комплексних систем захисту [5,13,15] є критично важливим елементом сучасної кібербезпеки. Інтеграція NGFW дозволяє підвищити ефективність захисту, покращити видимість мережевої активності, швидко реагувати на загрози та формувати інформативний аудиторський слід *(стосовно мережевмх подій та передумов їх виникнення).* Проте, процес розміщення та налаштувань NGFW у відповідності до специфіки функціонування та топології кожній окремої ІКС [5,7,16], потребує ретельного попереднього планування, високої кваліфікації фахівців і всебічного врахування потенційних загроз. Виконання цих умов, забезпечує швидку адаптацію системи MME під фактичні умови роботи кожній конкретної ІКС та підтримує прозорість й сумістність всіх елементів в межах единої комплексної системи захисту [13].

ВИСНОВКИ

У рішень рівня NGFW є хороший потенціал: - вони пропонують більш широкий спектр функцій безпеки, ніж попередні релізи MME, крім того, вони можуть бути розгорнуті в хмарі та виявляти і блокувати шкідливий трафік, фішинг-атаки [19], атаки відмови в обслуговуванні й інші загрози ІБ [5,12-13,16].

NGFW використовують технології *AI* та *LM* для виявлення як нових, так й мутуючих загроз [12,11], що значно полегшує завдання їх парирування в разі коли вони не можуть бути виявлені традиційними методами (*наприклад, сигнатурним скануванням*) [20].

До основних тенденцій, які будуть безпосередньо впливати на подальший розвиток та впровадження *NGFW* слід віднести наступне:

- зростання впливу технологій *AI* та *LM*. Тобто, *NGFW* будуть все більш покладатись на можливості *AI* і *LM* для виявлення нових та еволюціонуючи типів загроз безпеки [12,15];
- зростання темпів впровадження хмарних технологій та технології інтернету речей. В наслідок цих технологічних трендів, *NGFW* будуть все частіше тяготити до розгортання в хмарі, що може зробити їх більш доступними та зручнішими (*юзабіліті*) в обслуговуванні й користуванні;
- зростання масштабів застосування та інтегральності сучасних загроз ІБ. Вочевидь, що в цьому сенсі, *NGFW* мають більший потенціал проти мережевих бот-систем [8,15,20], котрі генерують складні поліморфні та/чи таргетовані під конкретні вразливості [12,19], різновиди зловмисного програмного коду.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Брандмауер (FireWall). Режим доступу: http://surl.li/tuggo
2. What Is a Firewall? Режим доступу: http://surl.li/fdtbp
3. Next-Generation Firewalls. Режим доступу: https://www.paloaltonetworks.com/network-security/next-generation-firewall
4. Who Invented the Firewall? History, Types, and Generations of Firewall. 28th September 2023 by Manish Sahay. Режим доступу: https://www.thepcinsider.com/whoinvented-firewall-history-evolution-types-generations/
5. John Mallery, & Jason Zann. Hardening Network Security. 2005 Pp. 608.
6. Information Technology Gartner Glossary. Режим доступу: https://www.gartner.com/en/information-technology/glossary/next-generationfirewalls-ngfws
7. Січкар, М., & Малахов, С. Огляд стану питань стосовно технологій міжмережевого екранування рівня Next-Generation. Proceedings of the VII International Scientific and Practical Conference. Copenhagen, Denmark. 2023. Pp. 301-307. Available at: DOI – 10.46299/ISG.2023.2.7
8. Азаров, С., Нємцев, М., & Малахов, С. Огляд аналогій та обгрунтування принципів створення демон юнітів відстеження мережевої активності користувачів. Proceedings of the XX International Scientific and Practical Conference. Graz, Austria. 2023. Pp. 447-453. Режим доступу: https://isgkonf.com/technologies-innovative-and-modern-theories-of-scientists/
9. 8 Types of Firewalls: Know Which One Is Best for Your Network By John Villanueva / May 19, 2022. Режим доступу: https://techgenix.com/types-of-firewalls
10. What are the Types of Firewalls? Режим доступу: https://www.zenarmor.com/docs/network-security-tutorials/what-is-firewall
11. Яремчук, К., Воскобойников, Д., & Мелкозьорова, О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. Комп’ютерні науки та

кібербезпека, (2), 28-34. Режим доступу: https://periodicals.karazin.ua/cscs/article/view/21038/19744

12. Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. Комп'ютерні науки та кібербезпека, (2), 35-40. Режим доступу: https://periodicals.karazin.ua/cscs/article/view/21039/19745

13. Погоріла К.В., Богданова Є.С., Колованова Є.П. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 07.10.2022 р. / МЦНД. − Вінниця: Європейська наукова платформа, 2022. - 142 с. DOI 10.36074/mcnd-07.10.2022

14. What is a Next-Generation Firewall (NGFW)? Режим доступу: https://www.zenarmor.com/docs/network-security-tutorials/next-generationfirewall

15. 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. Режим доступу: https://isg-konf.com/scientistsand-methods-of-using-modern-technologies

16. 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. Режим доступу: https://periodicals.karazin.ua/cscs/article/view/15614/14707

17. Top Next-Generation Firewall (NGFW) Software By Jenna Phipps July 19, 2022. Режим доступу: https://www.cioinsight.com/security/ngfw-software/#What-isa-next-generation-firewal

18. How to Test a Firewall? Режим доступу: https://www.zenarmor.com/docs/network-security-tutorials/how-to-test-a-firewall#1-firewall-location

19. Лєсная, Ю., Малахов, С. Узагальнення основних передумов реалізації фішингових атак. Proceedings of the XVII International Scientific and Practical

Conference. Ankara, Turkey. 2023. Pp.453-457. Режим доступу: https://isgkonf.com/system-analysis-and-intelligent-systems-for-management/

20. Січкар, М., & Малахов, С. (2024). Узагальнення особливостей відомих засобів міжмережевого екранування. Proceedings of the XXI International Scientific and Practical Conference. Sofia, Bulgaria. 2024. Pp. 370-376 . Режим доступу: https://isg-konf.com/innovative-solutions-in-public-communications-and-international-relations/