Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи магістра

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

світньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Технологія аналізу помилкових налаштувань NGFW»

Виконавець: студентка ІІ курсу, групи КБм-21

Анна КИРИЛЕНКО
(підпис) (прізвище, ім’я та по-батькові)

	Ім’я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Іван ПАРХОМЕНКО.	

Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувачки КБм-21 (група) Кириленко Анни Ігорівни (прізвище, ім'я та по-батькові)

Тема кваліфікаційної роботи: Технологія аналізу помилкових налаштувань NGFW

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20 жовтня 2022 року.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень: процес аналізу помилкових налаштувань міжмережевих екранів нового покоління

Предмет досліджень: помилкові налаштування міжмережевих екранів, що впливають на ефективність міжмережевого екрану, та заходи протидії помилковим налаштуванням міжмережевих екранів, що допомагають нівелювати ці аномалії

Мета досліджень: підвищення ефективності міжмережевих екранів нового покоління шляхом дослідження помилкових налаштувань та заходів протидії їм.

Вихідні дані для проведення роботи: статистика помилкових налаштувань міжмережевих екранів, заходів та інструментів протидії їм, вивчення різних аспектів очищення правил міжмережевих екранів

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна: удосконалено підхід до підвищення ефективності міжмережевих екранів за рахунок висвітлення проблематики помилкових налаштувань та такого заходу протидії їм як системи керування міжмережевими екранами; вперше розроблено комплексну покрокову технологію для попереднього аналізу помилкових налаштувань міжмережевого екрану для впровадження процесу очищення за допомогою систем керування міжмережевими екранами

Практична цінність: технологія була використана в процесі очищення правил міжмережевого екрану для компанії А від помилкових налаштувань, які виникли в результаті консолідації шести міжмережевих екранів; дана технологія може бути використана як початкова точка при впровадження процесу очищення помилкових налаштувань в міжмережевих екранах з залученням систем керування міжмережевими екранами для організацій будь-якого масштабу та галузі

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів роботи	**Строки виконання робіт (початок-кінець)**
Уточнення постановки задачі	24.10.2022 – 20.11.2022
Розробка плану для досягнення мети роботи	21.11.2022 – 04.12.2022
Аналіз літературних джерел	05.12.2022 – 03.02.2023
Дослідження міжмережевих екранів нового покоління та першопричини появи прогалин в безпеці	04.02.2023 – 19.02.2023
Аналіз помилкових налаштувань міжмережевих екранів	20.02.2023 – 25.02.2023
Вивчення заходів протидії помилковим налаштуванням міжмережевих екранів	26.02.2023 – 08.03.2023
Найменування етапів роботи	**Строки виконання робіт (початок-кінець)**
Розробка технології попереднього аналізу для очищення правил міжмережевого екрану	09.03.2023 - 09.04.2023
Обґрунтування специфіки використання технології	10.04.2023 – 14.04.2023
Оформлення пояснювальної записки	15.04.2023 – 10.05.2023
Підготовка до захисту кваліфікаційної роботи	11.05.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект: Підвищення ефективності роботи міжмережевих екранів та відповідно зменшення збитків, нанесених через численні інциденти безпеки, що були пов’язані з помилковими налаштуваннями в них

Соціальний ефект: Підвищення обізнаності адміністраторів, які будуть впроваджувати процес очищення правил міжмережевих екранів, за рахунок надання комплексної і структурованої покрокової технології початкового аналізу

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Іван ПАРХОМЕНКО
(підпис) (прізвище, ініціали)

Завдання прийняла до виконання _____ Анна КИРИЛЕНКО
(підпис) (прізвище, ініціали)

Дата видачі завдання: від 24 жовтня 2022 року.

Термін подання кваліфікаційної роботи до ЕК: 19 травня 2023 року.

УДК. 004.056

РЕФЕРАТ

Пояснювальна записка містить 80 сторінок, 17 рисунків, 1 таблицю, 1 додаток, список використаних джерел з 42 найменувань.

Об’єкт дослідження: процес аналізу помилкових налаштувань міжмережевих екранів нового покоління.

Мета кваліфікаційної роботи: підвищення ефективності міжмережевих екранів шляхом дослідження помилкових налаштувань та заходів протидії їм.

Методи дослідження: методи наукової абстракції, індукції та дедукції, аналізу, максимальної правдоподібності та синтезу, структурування, алгоритмізація та макетування.

В роботі проведено аналіз помилкових налаштувань міжмережевих екранів та заходів протидії їм. Запропоновано застосування розробленої технології для підвищення ефективності процесу очищення міжмережевих екранів.

Актуальність: Причина більшості порушень міжмережевої безпеки викликані не вразливостями, а людською недбалістю. Дослідження від Gartner свідчать про те, що 95% всіх порушень міжмережевого екрана сталося через помилкові налаштування, а не через вразливості. А у 2016 році Gartner прогнозував, що до 2020 року цей показник зросте до 99%, і ця тенденція лише підтвердилася.

Практичне значення роботи полягає у можливості використати розроблену технології при впровадженні процесу очищення помилкових налаштувань в міжмережевих екранах з залученням систем керування міжмережевими екранами для організацій будь-якого масштабу та галузі.

Наукова новизна дослідження полягає в розробленні комплексної технології для попереднього аналізу помилкових налаштувань міжмережевого екрану для впровадження процесу очищення за допомогою систем FMS.

Ключові слова: помилкові налаштування, міжмережеві екрани, системи керування міжмережевим екраном, очищення правил.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ACL – Access Control List

ALF – Application level firewall

ATP – Advanced Threat Protection

CIS – Center for Internet Security

DEC – Digital Equipment Corporation

DPI – Deep Packet Inspection

FA – Firewall Assurance

FISMA – Federal Information Security Modernization Act

FMS – Firewall Management System

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

IP – Internet Protocol

IPS – Intrusion Prevention System

ISMS – Information Security Management System

IT – Information Technology

MAC – Media Access Control

NAT – Network address translation

NGFW – Next-Generation Firewalls

NIST – National Institute of Standards and Technology

OSI – Open Systems Interconnection

PCI DSS – Payment Card Industry Data Security Standard

SIEM – Security Information and Event Management

SOX – Sarbanes-Oxley Act

SSH – Secure Socket Shell

SSL – Secure Sockets Layer

URL – Uniform Resource Locators

UTM – Unified Threat Management

VPN – Virtual Private Network

ЗМІСТ

ВСТУП

У період першої кібервійни, захист кіберпростору став критичним не лише для авторитетних організацій зі стандартизації, а й для захисту людей, бізнесу та держави. Це призвело до значного зацікавлення в засобах кіберзахисту, включаючи міжмережевий екран, який є необхідним елементом мережевої безпеки.

Більшість порушень міжмережевої безпеки викликані не тим, що методи злому стали непоборними, а справжня причина полягає в людського факторі. Дослідження від Gartner свідчать про те, що 95% всіх порушень міжмережевого екрана сталося через помилкові налаштування, а не через вразливості. А у 2016 році Gartner прогнозував, що до 2020 року цей показник зросте до 99%, а в 2019 році ця тенденція лише підтвердилася. Це свідчить про те, що проблема помилкових налаштувань міжмережевих екранів стає все більш актуальною з часом, і вимагає подальших досліджень.

Помилкові налаштування міжмережевих екранів трапляються щодня і ця тема знайшла віддзеркалення у багатьох дослідженнях. Так Бернадетт Вілсон у статті “Why Firewall Misconfigurations Are Putting Your Clients At Risk” назвав часті зміни причиною появи некоректностей. Більше того, аналітика Cyber Security Intelligence Index датована 2014 роком від IBM Security Services висвітлює, що помилкові налаштування найчастіше виникають через людську помилку. Легко зрозуміти, як це могло статися: розглянемо різницю між «neq» і «eq» — одна буква диктує протилежні значення. Тому не дивно, опитування AlgoSec State of Automation у 2016 році показало, що 20% організацій мали порушення безпеки, 48% мали відключення додатків і 42% відключення мережі через помилки під час ручного процесу, пов’язаного з безпекою.

Таким чином, актуальним науковим завданням, що має практичне значення, є розробка нових та удосконалення наявних заходів протидії помилковим налаштуванням міжмережевих екранів, спричинених людським фактором.

Метою кваліфікаційної роботи є підвищення ефективності міжмережевих екранів нового покоління шляхом дослідження помилкових налаштувань та заходів протидії їм.

Для досягнення мети кваліфікаційної роботи були поставлені такі окремі завдання:

- визначити основні причини появи порушень інформаційної безпеки міжмережевих екранів;
- категоризувати та дослідити основні аспекти типів помилкових налаштувань міжмережевих екранів;
- дослідити основні типи заходів протидії помилковим налаштуванням міжмережевих екранів;
- провести аналіз організаційних заходів протидії помилковим налаштуванням міжмережевих екранів;
- провести аналіз технічних заходів протидії помилковим налаштуванням міжмережевих екранів;
- дослідити основні аспекти систем керування та безпеки міжмережевих екранів;
- дослідити основні ситуації, коли необхідно впроваджувати процес очищення правил міжмережевого екрану;
- запропонувати покрокову технологію попереднього аналізу правил міжмережевого екрану для проведення очищення з визначенням ролі систем керування міжмережевим екраном в цьому процесі.

Об’єкт дослідження – процес аналізу помилкових налаштувань міжмережевих екранів нового покоління.

Предмет дослідження – помилкові налаштування міжмережевих екранів, що впливають на ефективність міжмережевого екрану, та заходи протидії помилковим налаштуванням міжмережевих екранів, що допомагають нівелювати ці аномалії.

При вирішенні поставлених завдань у кваліфікаційній роботі використані: методи наукової абстракції, індукції та дедукції, аналізу (при розкритті основних аспектів, причин появи помилкових налаштувань); метод максимальної

правдоподібності (для обґрунтування покрокової технології очищення правил міжмережевого екрану); метод синтезу (при дослідженні окремих технологій, засобів та заходів для побудови ефективної технології для підвищення ефективності міжмережевого екрану).

Теоретична і методична значущість отриманих результатів:

– удосконалено підхід до підвищення ефективності міжмережевих екранів за рахунок висвітлення проблематики помилкових налаштувань та такого заходу протидії їм як системи керування міжмережевими екранами;

– вперше розроблено комплексну покрокову технологію для попереднього аналізу помилкових налаштувань міжмережевого екрану для впровадження процесу очищення за допомогою систем керування міжмережевими екранами.

Практична цінність роботи полягає в наступному:

– технологія була використана в процесі очищення правил міжмережевого екрану для компанії А від помилкових налаштувань, які виникли в результаті консолідації шести міжмережевих екранів;

– дана технологія може бути використана як початкова точка при впровадження процесу очищення помилкових налаштувань в міжмережевих екранах з залученням систем керування міжмережевими екранами для організацій будь-якого масштабу та галузі.

Основні наукові положення і результати доповідалися та обговорювалися на V Міжнародно-науковій конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» (Київ, 2022), VI Міжнародно-науковій конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» (Київ, 2023).

Окремі аспекти кваліфікаційної роботи були опубліковані за результатами VIII Міжнародно-науковій конференції «Інформаційні технології та впровадження» (IT&I-2021).

РОЗДІЛ 1
РОЗВИТОК МІЖМЕРЕЖЕВИХ ЕКРАНІВ

1.1 Історія виникнення міжмережевих екранів

Міжмережеві екрани були розроблені, щоб створити надійний бар’єр між приватною внутрішньою мережею та зовнішніми мережами, такими як Інтернет. Ідея міжмережевого екрану сягає перших днів створення комп’ютерних мереж, коли стало зрозуміло, що існує потреба в механізмі контролю доступу до мережевих ресурсів.

Перший міжмережевий екран був розроблений наприкінці 1980-х років групою інженерів Digital Equipment Corporation (DEC) під керівництвом Білла Чесвіка та Стіва Белловіна. Вони працювали над проектом із покращення безпеки мережевого протоколу DECnet і зрозуміли, що їм потрібен спосіб контролювати доступ до мережі [1].

Міжмережевий екран був простим фільтром пакетів, який перевіряв кожен пакет, що проходив через мережу, і або дозволяв йому пройти, або блокував його на основі набору правил. Ця базова концепція міжмережевого екрану з фільтрацією пакетів використовується й сьогодні, хоча сучасні міжмережеві екрани стали набагато складнішими та можуть виконувати широкий спектр функцій безпеки [2].

Розробка міжмережевих екранів була зумовлена все більшим використанням Інтернету та потребою організацій захищати свої внутрішні мережі від зовнішніх загроз. Із зростанням популярності Інтернету стало зрозуміло, що існує потреба в стандартизованому підході до безпеки мережі, і це призвело до розробки перших стандартів міжмережевих екранів на початку 1990-х років [3].

Сьогодні міжмережеві екрани є важливим компонентом мережевої безпеки та використовуються організаціями будь-якого розміру для захисту своїх мереж від широкого спектру загроз, включаючи віруси, зловмисне програмне забезпечення та несанкціонований доступ.

1.2 Еволюція міжмережевих екранів відносно технології

Еволюція мережевих екранів була зумовлена змінами в технологіях і зміною ландшафту загроз [4, 5]. Нижче наведено короткий огляд:

- Міжмережеві екрани з фільтрацією пакетів (англ. “packet-filtering firewalls”, кінець 1980-х - середина 1990-х): перші мережеві міжмережеві екрани були простими фільтрами пакетів, які перевіряли кожен пакет, що проходить через мережу, і або дозволяли йому пройти, або блокували його на основі набору правил. Ці міжмережеві екрани були обмежені у своїх можливостях і могли фільтрувати трафік лише на основі базової інформації, такої як IP-адреси джерела та призначення і номери портів.
- Міжмережеві екрани з перевіркою стану (англ. “stateful inspection firewalls”, середина 1990-х - початок 2000-х): міжмережеві екрани з перевіркою стану додали можливість відстежувати стан мережевих з’єднань, що дозволило їм приймати більш складні рішення щодо фільтрації. Ці міжмережеві екрани можуть перевіряти вміст пакетів і порівнювати його з набором правил, які враховують контекст з’єднання.
- Шлюзи прикладного рівня (англ. “application-level gateways”, середина 1990-х - початок 2000-х років): шлюзи прикладного рівня (також відомі як проксі-сервери) були розроблені, щоб забезпечити додатковий рівень безпеки, за рахунок посередництва між внутрішніми клієнтами та зовнішніми серверами. Ці шлюзи можуть перевіряти трафік на прикладному рівні та фільтрувати будь-який потенційно шкідливий трафік до того, як він досягне внутрішньої мережі.
- Система уніфікованого керування загрозами (англ. “unified threat management” – абревіатура UTM, початок 2000-х років – теперішній час): UTM – це комплексні системи безпеки, які поєднують численні функції безпеки (наприклад, міжмережевий екран, антивірус, виявлення та запобігання вторгненням, а також фільтрацію вмісту) в одному пристрої. Ці пристрої розроблені для спрощення керування мережевою безпекою та забезпечення комплексного захисту від широкого спектру загроз.
- Міжмережеві екрани наступного покоління (англ. “next-generation firewalls” – абревіатура NGFW, середина 2000-х років - теперішній час): NGFW є пізнішою розробкою в еволюції міжмережевих екранів. Вони включають в себе функції

традиційних міжмережевих екранів, міжмережевих екранів з перевіркою стану та UTM, а також додають розширені можливості, такі як глибока перевірка пакетів, розпізнавання додатків і аналіз загроз. NGFW розроблено для забезпечення покращеного захисту від сучасних загроз і є ключовим компонентом стратегій мережевої безпеки багатьох організацій.

Загалом, еволюція міжмережевих екранів була зумовлена необхідністю адаптації до нових технологій і загроз, а також забезпечення все більш досконалого захисту від кібератак.

1.3 Еволюція міжмережевих екранів відносно моделі OSI

Також, еволюцію міжмережевих екранів можна простежити через рівні моделі OSI, яка є концептуальною моделлю, що описує, як має відбуватися мережевий зв’язок (рис.1.1).

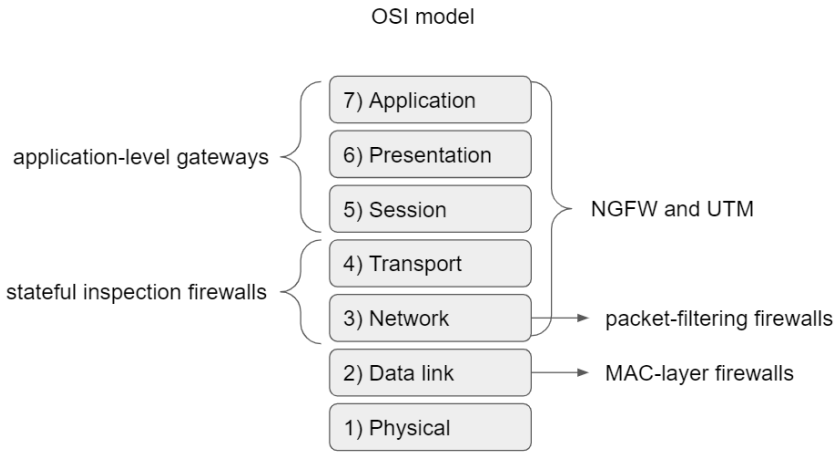

Рисунок 1.1 – Еволюція міжмережевих екранів відносно моделі OSI

Нижче наведено короткий огляд еволюції міжмережевих екранів відповідно до моделі OSI [6]:

- Рівень 1 – Фізичний рівень (англ. “physical layer”): міжмережеві екрани не працюють на фізичному рівні моделі OSI, оскільки цей рівень стосується фізичної передачі даних через мережу.

- Рівень 2 – Канальний рівень (англ. “data link layer”): міжмережеві екрани зазвичай не працюють на канальному рівні моделі OSI, оскільки цей рівень стосується фізичної адресації мережевих пристроїв. Тим не менш, міжмережеві екрани рівня MAC (англ. “MAC-layer firewalls”) деколи зараховують до категорії міжмережевих екранів на канальному рівні, хоча насправді це просто механізм.
- Рівень 3 – Мережевий рівень (англ. “network layer”): найперші міжмережеві екрани, такі як міжмережеві екрани з фільтрацією пакетів, працюють на мережевому рівні моделі OSI, відповідно звідти вони й отримали таку свою назву.
- Рівень 4 – Транспортний рівень (англ. “transport layer”): міжмережеві екрани з перевіркою стану працюють на транспортному рівні моделі OSI.
- Рівень 5 – Сеансовий рівень (англ. “session layer”): міжмережеві екрани зазвичай не працюють на сеансовому рівні моделі OSI, точніше не спеціалізуються явно і виключно на цьому рівні, оскільки цей рівень пов’язаний із встановленням і підтримкою сеансів між мережевими пристроями.
- Рівень 6 – Рівень презентації (англ. “presentation layer”): шлюзи прикладного рівня (також відомі як проксі-сервери) працюють на рівні презентації моделі OSI.
- Рівень 7 – Прикладний рівень (англ. “application layer”): міжмережеві екрани наступного покоління (NGFW) працюють на прикладному рівні моделі OSI.

Щодо згаданих вище міжмережевих екранів рівня MAC, також відомих як фільтрація MAC-адрес (англ. “MAC address filtering”) – це механізм, що використовується в безпеці мережі, який дозволяє або блокує мережевий трафік на основі адрес керування доступом до медіа (англ. “Media Access Control” – абревіатура MAC) пристроїв у мережі [7].

Однак фільтрація MAC-адрес зазвичай не вважається справжнім міжмережевим екраном, оскільки вона працює на канальному рівні моделі OSI і не здатна забезпечити рівень безпеки подібний до міжмережевого екрану мережевого рівня або прикладного рівня.

Фільтрування MAC-адрес може бути корисною як додаткова міра безпеки, але вона не є заміною для більш комплексних заходів безпеки, таких як міжмережевий екран перевірки стану або міжмережевий екран нового покоління. До того ж,

зловмисник, знаючи MAC-адреси авторизованих пристроїв у мережі, також може легко обійти фільтрацію MAC-адрес, що робить її відносно слабким контролем безпеки.

Таким чином, хоча фільтрація MAC-адрес може бути корисним механізмом безпеки в певних ситуаціях, зазвичай вона не вважається справжнім міжмережевий екраном і не здатна забезпечити такий самий рівень безпеки, як більш комплексні рішення міжмережевих екранів.

Загалом, еволюція міжмережевих екранів була зумовлена необхідністю забезпечити все більш досконалий захист від кіберзагроз, і це призвело до розробки міжмережевих екранів, які працюють на кількох рівнях моделі OSI, такі як UTM та NGFW.

1.4 Особливості NGFW

Розуміння індивідуальних рис особистості та того, як вони впливають на поведінку, може Як було зазначено раніше, NGFW – це міжмережевий екран наступного покоління. Даний термін був вперше введений Gartner у 2007 році. До того ж, NGFW були розроблені у відповідь на мінливий характер кіберзагроз і зростання складності мережевого середовища [8].

NGFW були спроектовані кількома постачальниками, зокрема Palo Alto Networks, Fortinet і Check Point. Ці виробники визнали, що традиційних міжмережевих екранів, які в першу чергу зосереджені на фільтрації на основі портів і протоколів, уже не достатньо для захисту мереж від складних загроз і цілеспрямованих атак. NGFW були розроблені для вирішення цих проблем, забезпечуючи більш детальний контроль над мережевим трафіком, включаючи можливість ідентифікації та блокування програм і протоколів, які, як відомо, становлять загрозу безпеці [9].

Так як даний тип систем є по суті вдосконаленою та доповненою версією традиційних міжмережевих екранів, розглянемо що саме розуміється під цією категорією. Традиційний міжмережевий екран – це пристрій безпеки мережі, який

відстежує та контролює вхідний і вихідний мережевий трафік на основі набору попередньо визначених правил безпеки. Це базовий засіб безпеки, призначений для запобігання несанкціонованому доступу до мережі чи системи.

Традиційні міжмережеві екрани працюють на мережевому рівні (рівень 3) або/і транспортному рівні (рівень 4) моделі OSI. Зазвичай вони використовують списки контролю доступу (ACL), щоб визначити, який трафік дозволено чи заборонено на основі таких факторів, як IP-адреси джерела та призначення, номери портів і протоколи.

Традиційні міжмережеві екрани ефективні для блокування відомих загроз і запобігання несанкціонованому доступу до мережі, але вони мають обмеження. Вони не здатні перевіряти трафік на прикладному рівні моделі OSI (рівень 7), що означає, що вони не можуть виявляти або блокувати атаки, які використовують вразливості на рівні додатків. Крім того, традиційні міжмережеві екрани не забезпечують розширених функцій безпеки, таких як запобігання вторгненням, аналіз загроз або розширений захист від загроз [10].

NGFW розроблено для забезпечення розширених функцій безпеки, які можуть виявляти та блокувати широкий спектр кіберзагроз, що досягається за рахунок кількох ключових компонентів:

- Глибока перевірка пакетів (англ. “Deep Packet Inspection” – абревіатура DPI): DPI – це технологія, яка дозволяє NGFW досліджувати вміст мережевих пакетів і ідентифікувати використовуваний протокол прикладного рівня. Це дозволяє міжмережевому екрану застосовувати політики безпеки, які є специфічними для використовуваного додатка.
- Система запобігання вторгненням (англ. “Intrusion Prevention System” – абревіатура IPS): IPS – це система, яка може виявляти та запобігати вторгненням у мережу шляхом аналізу мережевого трафіку та пошуку відомих моделей атак.
- Розширений захист від загроз (англ. “Advanced Threat Protection” – абревіатура ATP): ATP – це набір технологій безпеки, призначених для виявлення та блокування просунутих загроз, таких як експлойти нульового дня (англ. “zero-day exploits”),

просунуті постійні загрози (англ. “advanced persistent threats” – абревіатура APT) та інші цілеспрямовані атаки.

- Обізнаність щодо додатків (англ. “Application Awareness”): NGFW мають обізнаність на прикладному рівні, що у свою чергу означає, що вони можуть виявляти та блокувати шкідливий трафік на основі сигнатур певних додатків.
- Ідентифікація користувача (англ. “User Identification”): NGFW можуть ідентифікувати користувачів у мережі на основі їхніх облікових даних, IP-адрес або іншої ідентифікаційної інформації, що у свою чергу дозволяє NGFW застосовувати засоби контролю доступу на основі ролей користувачів і обмежувати доступ до конфіденційних даних.
- Централізоване керування (англ. “Centralized Management”): NGFW зазвичай постачається з централізованою консоллю керування, яка дозволяє мережевим адміністраторам контролювати та керувати політиками безпеки по всій мережі.

Міжмережеві екрани наступного покоління (NGFW) наразі є найпоширенішим типом міжмережевого екрану в сучасній мережевій безпеці. NGFW пропонують кілька переваг перед традиційними міжмережевими екранами, зокрема:

- Розширені функції безпеки: NGFW включають розширені функції безпеки, такі як глибока перевірка пакетів, запобігання вторгненню та аналіз загроз. Ці функції дозволяють NGFW виявляти та блокувати ширший спектр загроз, ніж традиційні міжмережеві екрани.
- Обізнаність програми: NGFW здатні перевіряти трафік на прикладному рівні моделі OSI, що дозволяє їм блокувати зловмисний трафік на основі сигнатур конкретних додатків.
- Ідентифікація користувача: NGFW можуть ідентифікувати користувачів у мережі на основі їхніх облікових даних, IP-адрес або іншої ідентифікаційної інформації. Це дозволяє NGFW застосовувати засоби контролю доступу на основі ролей користувачів і обмежувати доступ до конфіденційних даних.
- Масштабованість: NGFW розроблені для обробки великих обсягів мережевого трафіку та можуть масштабуватися для підтримки великих корпоративних мереж.

•Інтеграція з іншими інструментами безпеки: NGFW можна інтегрувати з іншими інструментами безпеки, такими як системи SIEM і канали розвідки про загрози (англ. “threat intelligence feeds”), що дозволяє їм забезпечувати більш повну безпеку.

NGFW стають все більш популярними в останні роки, оскільки організації прагнуть покращити свою безпеку та захистити від широкого спектру кіберзагроз. Розширені функції безпеки, надані NGFW, а також їх здатність інтегруватися з іншими рішеннями безпеки роблять їх цінним інструментом для організацій будь-якого розміру.

1.5 Ринок виробників NGFW

Ринок NGFW в Україні спостерігав значне зростання в останні роки, що було зумовлено рядом факторів. Одним із ключових факторів є дедалі більше впровадження хмарних сервісів і потреба організацій у захисті своєї хмарної інфраструктури. Крім того, зростаюча складність кіберзагроз змусила багато організацій шукати більш просунуті та ефективні рішення безпеки, такі як NGFW.

Виходячи з мого дослідження, українських постачальників NGFW нема або вони малопомітні, що зумовлено низкою факторів, включаючи високий рівень конкуренції на ринку NGFW і проблеми, пов’язані з розробкою та маркетингом нових рішень безпеки [11]. Тож ринок постачальників NGFW в Україні висококонкурентний і представлений у вигляді міжнародних гравців, серед яких такі світові гіганти (рис.1.2).

Рисунок 1.2 – Представники світових виробників NGFW

- Cisco: Cisco є відомим постачальником мережевих рішень і рішень безпеки, зокрема NGFW. Їх NGFW відомі своєю високою продуктивністю та масштабованістю, а також розширеними функціями безпеки, такими як розшифровка SSL і аналіз загроз [12].
- Fortinet: Fortigate є ще одним великим гравцем на ринку NGFW, який пропонує ряд рішень для різних типів організацій. Їх NGFW відомі своєю високою продуктивністю та масштабованістю, а також розширеними функціями безпеки, такими як антивірус, веб-фільтрація та контроль програм [13].
- Palo Alto Networks: Palo Alto Networks є лідером на ринку NGFW, пропонуючи ряд рішень для малих, середніх і великих підприємств. Їх NGFW відомі розширеними функціями безпеки, включаючи запобігання загрозам, запобігання вторгненням і фільтрацію URL-адрес та можливостями централізованого керування [14].
- Barracuda Networks: Barracuda Networks є постачальником NGFW та інших рішень безпеки. Їх NGFW відомі своїми розширеними функціями безпеки, такими як запобігання вторгненням, веб-фільтрація та контроль програм [15].
- Sophos: Sophos є постачальником NGFW та інших рішень безпеки. Їх NGFW відомі розширеними функціями безпеки, такими як антивірус, веб-фільтрація та контроль програм. Вони також пропонують централізоване керування та можливості звітування [16].
- Check Point Software Technologies: Check Point є постачальником NGFW та інших рішень безпеки мережі. Їх NGFW відомі розширеними функціями безпеки, включаючи запобігання загрозам SandBlast, запобігання вторгненням і контроль програм [17].

Загалом ринок NGFW в Україні відносно невеликий порівняно з іншими країнами. Проте компанії в Україні все ще можуть вибирати з ряду рішень NGFW, які пропонують міжнародні постачальники. При виборі постачальника NGFW компанії в Україні повинні враховувати такі фактори, як репутація постачальника, підтримка та місцева присутність, а також характеристики, продуктивність, масштабованість і вартість рішення NGFW.

Висновки за розділом 1

Міжмережеві екрани були наріжним каменем безпеки мережі протягом десятиліть, забезпечуючи першу лінію захисту від несанкціонованого доступу, зловмисного програмного забезпечення та інших загроз. Протягом багатьох років міжмережеві екрани значно розвинулися з точки зору можливостей і складності, починаючи від простих фільтрів пакетів і закінчуючи розширеними міжмережевого екранами наступного покоління (NGFW), які поєднують численні функції безпеки та обізнаність про додатки.

NGFW, зокрема, стає все більш популярним серед організацій, які прагнуть захистити свої мережі від широкого спектру загроз, включаючи ті, які використовують веб-додатки та хмарні служби. Ці міжмережеві екрани включають запобігання вторгненням, глибоку перевірку пакетів та інші передові технології безпеки, які дозволяють їм виявляти та блокувати більш складні атаки.

Однак, незважаючи на їх розширені функції та можливості, міжмережеві екрани не є бездоганними. Помилкові налаштування є поширеною проблемою, яка може зробити організації вразливими до атак, навіть якщо встановлено найсучасніші міжмережеві екрани, що саме і підводить до проблематики дослідження. Помилкові налаштування міжмережевих екранів можуть виникнути з різних причин, зокрема людська помилка, відсутність досвіду, недостатній зв’язок тощо.

РОЗДІЛ 2
АНАЛІЗ ПОМИЛКОВИХ НАЛАШТУВАНЬ МІЖМЕРЕЖЕВИХ ЕКРАНІВ НА ПРЕДМЕТ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ВИКОРИСТАННЯ

2.1 Помилкові налаштування міжмережевих екранів як результат людського фактору

Помилкові налаштування правил контролю доступу міжмережевих екранів є поширеною проблемою, яка може виникнути в будь-якій організації, що використовує міжмережеві екрани для керування безпекою мережі. Однією з головних причин цих помилкових налаштувань є людський фактор, який включає помилки, зроблені адміністраторами під час налаштування міжмережевого екрану та проведення змін [18].

Людський фактор у помилкових налаштуваннях правил контролю доступу викликає серйозне занепокоєння, оскільки це може призвести до вразливостей і порушень безпеки. Неправильно налаштовані міжмережеві екрани можуть дозволити несанкціонований доступ до мережі або заблокувати законний трафік, що призведе до простою та потенційно значних фінансових втрат.

Щоб звести до мінімуму людський фактор у помилкових налаштуваннях правил контролю доступу, експерти з безпеки рекомендують запровадити політики та процедури безпеки, які вимагають ретельного планування та документування змін міжмережевого екрану. Важливо також переконатися, що мережеві адміністратори пройшли належне підготовче навчання щодо налаштування міжмережевого екрану та мають повне розуміння політики та процедур безпеки організації.

Автоматизовані інструменти, такі як інструменти безпеки міжмережевого екрану, також можна використовувати, щоб мінімізувати людський фактор у помилкових налаштуваннях правил контролю доступу. Ці інструменти можуть допомогти адміністраторам швидко й точно виявляти та виправляти неправильні

налаштування, зменшуючи ризик порушення безпеки. Згадані заходи протидії помилковим налаштуванням будуть розглянуті детальніше далі в розділі.

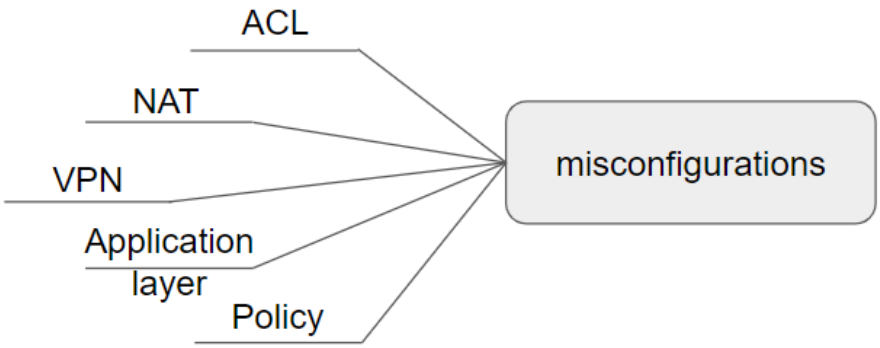

Рисунок 2.1 – Типи помилкових налаштувань міжмережевих екранів

Якщо говорити про помилкові налаштування, то вони бувають різні. У загальному значенні, помилкові налаштування – це помилки, допущені у налаштуваннях міжмережевого екрану, які можуть поставити під загрозу його ефективність і зробити організацію вразливою до кіберзагроз [19]. Існує кілька типів помилкових налаштувань міжмережевого екрану, зокрема (рис. 2.1):

•Помилкові налаштування списку контролю доступу (ACL): цей тип помилкових налаштувань передбачає помилки в правилах, які використовуються для фільтрації трафіку на основі IP-адрес джерела та призначення, портів і протоколів. Приклади включають дозвіл трафіку, який слід заблокувати, блокування трафіку, який слід дозволити, або неможливість оновлення правил, коли в мережі вносяться зміни.

•Помилкові налаштування трансляції мережевих адрес (NAT): NAT використовується для трансляції IP-адрес між приватною та публічною мережами. Помилкові налаштування в правилах NAT можуть призвести до проблем із підключенням, вразливості системи безпеки або неправильної трансляції IP-адрес.

•Помилкові налаштування віртуальних приватних мереж (VPN): VPN використовуються для створення безпечних з’єднань між віддаленими

користувачами або сайтами. Помилкові налаштування VPN можуть призвести до несанкціонованого доступу, витоку даних або розриву з'єднання.

- Помилкові налаштування рівня додатків: міжмережеві екрани рівня додатків (ALF) фільтрують трафік на основі вмісту даних додатка. Помилкові налаштування в правилах ALF можуть призвести до хибних спрацьовувань або хибних неспрацювань, дозволяючи зловмисному трафіку обходити міжмережевий екран або блокуючи законний трафік.

- Помилкові налаштування політики: політики міжмережевого екрану використовуються для визначення загального рівня безпеки організації. Помилкові налаштування параметрів політики можуть призвести до надміру дозвільних чи обмежувальних політик або політик, які конфліктують одна з одною.

Часто, коли є помилка у файлі налаштувань або пристрій підключено неправильно, це легко помітити, і часто пристрій видає попередження і не працюватиме, поки помилка не буде виправлена. Однак помилки всередині списків правил цих пристроїв – це інша історія.

Як приклад розглянемо адміністратора мережі, який має веб-сервер у своїй мережі, до якого він хоче отримати доступ з Інтернету. Він хоче заблокувати ssh, але дозволити веб-порти, тому адміністратор блокує порт 22 і створює правило, щоб дозволити порт 443. Помилково правило на дозвіл порта 443 дозволяє діапазон від 0 до 443. Відносно міжмережевого екрану, це цілком дійсне правило, і воно успішно додано. Незважаючи на те, що правило має дійсний синтаксис, цей міжмережевий екран неправильно налаштований, оскільки правила, які воно застосовує, не є тими, які передбачав користувач.

На цьому підґрунті було розглянуто тему помилкових налаштувань та виявлення таких правил (тут і надалі під помилковими налаштуваннями матимуться на увазі саме помилкові налаштування списків контрою доступу). Те, що набір правил може бути перевірений пристроєм, не означає, що вони працюють правильно.

Під час дослідження впливу людського фактору на помилкові налаштування міжмережевих екранів, було виділено, що дана проблема може бути також пов'язана з регулярною проблемою розподілу обов'язків і відповідальності між командами IT і

безпеки IT, а також з непорозумінням між цими двома групами експертів. Керування міжмережевим екраном вимагає тісної співпраці між IT-групами та командами безпеки IT, оскільки обидві мають власні ролі та обов'язки щодо забезпечення належного та безпечного налаштування міжмережевого екрану.

IT-команда зазвичай відповідає за технічні аспекти налаштування міжмережевого екрану та керування ним, як-от впровадження політик контролю доступу, керування підключенням до мережі та забезпечення належного функціонування міжмережевого екрану. Команда безпеки IT несе відповідальність за те, щоб міжмережевий екран було налаштовано відповідно до політики та стандартів безпеки організації, а також за моніторинг журналів міжмережевого екрану на предмет подій безпеки.

Непорозуміння між цими двома групами може призвести до помилкових налаштувань, оскільки IT-команда може не повністю розуміти наслідки для безпеки своїх налаштувальних рішень, а команда безпеки IT може не мати достатньо технічних знань, щоб надати конкретні вказівки щодо налаштування міжмережевого екрану або взагалі не бути частиною цього процесу. Крім того, якщо немає чіткості щодо ролей і обов'язків, певні аспекти керування міжмережевим екраном можуть бути пропущені або проігноровані.

Щоб вирішити ці проблеми, організаціям важливо встановити чіткі лінії зв'язку між своїми IT-командами та відділами безпеки, а також чіткі політики та процедури керування міжмережевим екраном. Це може включати регулярні зустрічі між двома командами для перегляду налаштувань міжмережевих екранів та виявлення потенційних проблем безпеки, а також встановлення чітких процесів для запиту на зміни налаштувань міжмережевих екранів та проведення регулярних оцінок безпеки для виявлення та усунення будь-яких вразливостей.

Загалом, адміністратори міжмережевого екрану, які стають джерелом помилкових налаштувань, можуть бути згруповані в кілька категорій на основі причин, чому вони роблять помилки (рис. 2.2):

- Брак досвіду: адміністратори, які вперше керують міжмережевим екраном, можуть припуститися помилки через брак досвіду та знайомства з системою. Вони

можуть не знати про всі функції та функції міжмережевого екрану, що призводить до помилкових налаштувань.

•Відсутність навчання: навіть досвідчені адміністратори можуть робити помилки, якщо вони не пройшли відповідного навчання системі міжмережевого екрану, якою вони керують. Без належної підготовки вони можуть не знати про найкращі методи налаштування та керування міжмережевим екраном.

•Відсутність зв'язку: непорозуміння між командами безпеки IT та IT-командами також може призвести до помилкових налаштувань. Наприклад, якщо команда безпеки IT надає список правил, які слід застосувати на міжмережевому екрані, але IT-команда не розуміє причини, що стоять за ними, вони можуть зробити помилки під час впровадження правил або взагалі проігнорувати поставлене завдання.

Поспішні або неповні зміни: адміністратори можуть припуститися помилки, поспішаючи впроваджувати зміни або вносячи зміни, не розуміючи повного впливу, який вони матимуть на систему. Це може бути особливо проблематично в ситуаціях високого тиску, наприклад під час інциденту безпеки.Людська помилка: навіть уважні та досвідчені адміністратори можуть припуститися помилки через звичайний людський фактор, наприклад помилку під час введення або пропуск важливих деталей [20].

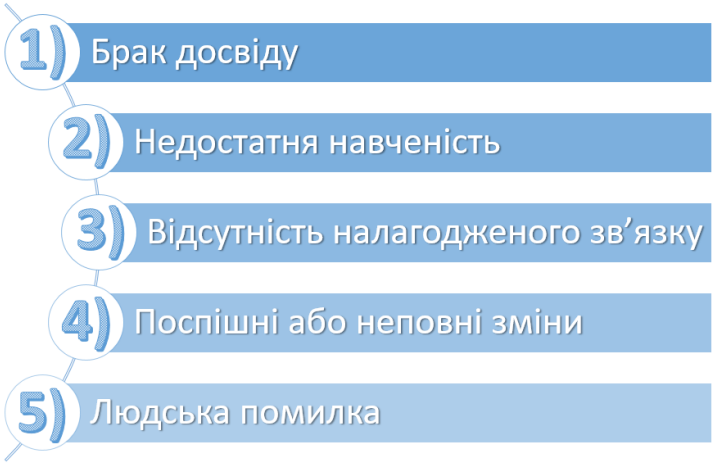

Рисунок 2.2 – Причини створення помилкового налаштування адміністраторами міжмережевих екранів

Загалом для організацій важливо мати належне навчання, комунікацію та процеси, щоб мінімізувати ризик помилкових налаштувань правил контролю доступу міжмережевих екранів через людський фактор.

2.2 Типи помилкових налаштувань міжмережевих екранів

Засоби керування безпекою можна згрупувати за призначенням. Групуючи засоби контролю відповідно до їхньої мети дій, організації можуть краще зрозуміти, як їхні засоби контролю працюють разом для захисту їхніх активів і ресурсів, і можуть визначити області, де можуть знадобитися додаткові засоби контролю [**Ошибка! Источник ссылки не найден.**].

Усі зібрані висвітлюють щонайменше одну з трьох найпоширеніших помилок, а саме затінення, кореляцію та надмірність правил (рис. 2.3). Існують інші типи помилкових налаштувань, але вони залежать від конкретної платформи або можуть виникати лише тоді, коли в одній мережі є кілька рішень контролю доступу до мережі [21].

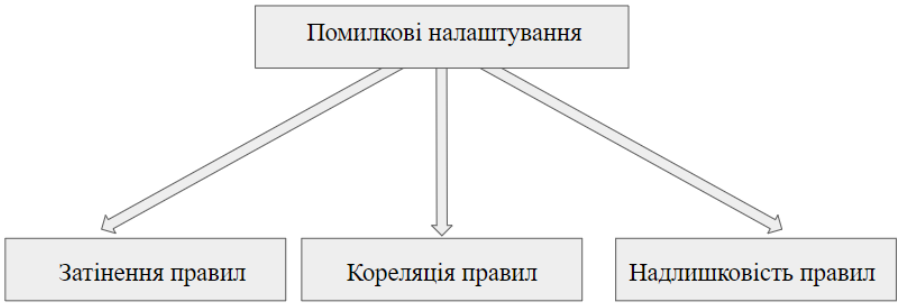

Рисунок 2.3 – Типи помилкових налаштувань міжмережевих екранів

Прикладами цього є аномалії декількох міжмережевих екранів або неправильне налаштування потоку всередині IDS/IPS. Більшість перерахованих помилкових налаштувань є результатом множинних правил, які перетинаються за обсягом. Списки правил міжмережевого екрану зазвичай мають деякі навмисно перекриваючі правила. Більшість автоматизованих інструментів сповіщають користувача про потенційну проблему.

2.2.1 Затінення правил контролю доступу

Затінене правило (від англ. “shadowed rule”) – це таке правило, коли попереднє правило відповідає всім пакетам, які відповідають цьому правилу так, що затінене правило ніколи не буде активовано [22]. Більш загальне правило з широкою сферою дії запобігає активації другого правила з більш вузькою сферою дії (рис. 2.4).

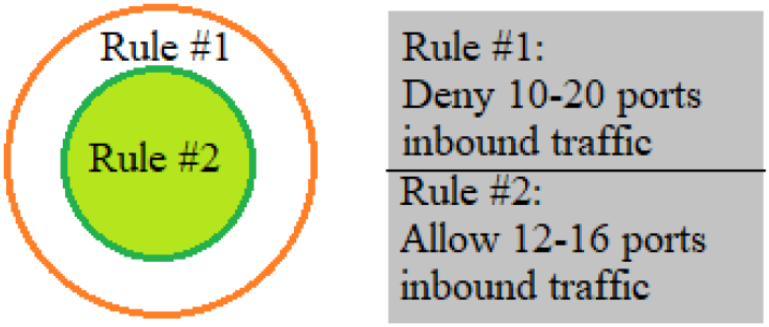

Рисунок 2.4 – Діаграма Вена “Затінені правила”

І є ще одна умова, що два правила повинні мати різні дії, якщо затінене правило є дозволеним, правило затінення має бути запереченням і навпаки. Ця відмінність важлива, оскільки саме вона відрізняє затінювання від інших помилкових налаштувань.

Традиційно в міжмережевих екранах правила застосовуються в тому порядку, в якому вони зустрічаються в списку правил. Затінення відбувається, коли правило, що знаходиться вище в списку, повністю перекриває правило нижче в списку. Якщо у вас є правило з областю дії, яка повністю міститься в іншому правилі, затінення може відбуватися залежно від того, в якому порядку вони відбуваються. Наявність правильних правил не має значення, якщо вони розташовані в неправильному порядку.

Затінення відбувається не лише тоді, коли одне правило повністю охоплює інше. Є ще тотальне затінення правил (від англ. “totally shadowed rule”) – це коли комбінована область дії кількох правил охоплює всю область дії іншого правила. Як

приклад, припустимо, що є просте правило блокування портів, яке блокує вхідний трафік між портами з 1 по 100. Затінена сукупність може бути одним правилом дозволу від 1 до 50 і другим від 51 до 100. Це призводить до того, що початкове правило блокування буде затьмарюватися двома іншими правилами разом (рис. 2.5).

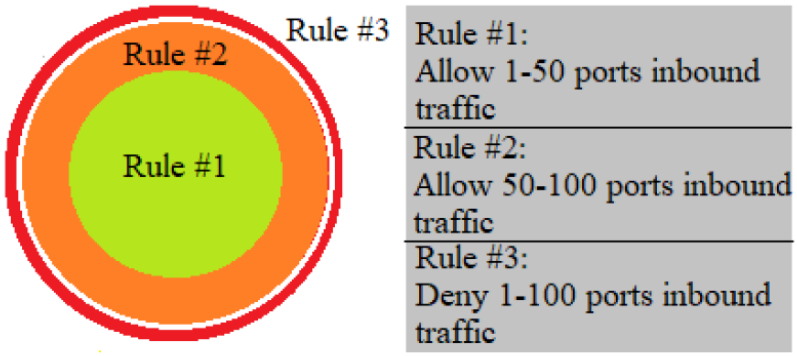

Рисунок 2.5 – Діаграма Вена “Тотально затінені правила”

Затінення є серйозною помилкою, оскільки його існування в наборі правил повністю зводить нанівець інші правила. Хоча це може статися навмисно, наприклад, залишення старих правил, ненавмисне перекриття може призвести до багатьох проблем. Це може спричинити відмову в законному трафіку, що може зашкодити продуктивності організації та спричинити проблеми для користувачів.

Що ще гірше, це може призвести до проходження шкідливого трафіку, оскільки правило, яке блокує його, затінено. Оскільки затінене правило не може бути активоване, його видалення не впливає на список правил міжмережевого екрану. Проблема в тому, що просте видалення затіненого правила може бути не найкращим способом дій, якщо воно повинно перехоплювати певний трафік. Крім того, може бути більш бажаним видалити правило, обмеживши сферу дії затінюючого правила [23].

Коли тіньове правило виявляється в списку правил, важливо, щоб проблема була виявлена якомога швидше, оскільки випадкове включення затінення може бути руйнівним. Незалежно від того, чи забороняють правила хороший трафік, чи дозволяють поганий трафік, ця аномалія в кращому випадку дратує користувачів, а в гіршому — загроза для всієї мережі. Висока серйозність затінення пов’язана з тим,

що воно спричиняє помилкові дії, навіть якщо немає проблем із будь-яким окремим правилом, яке може викликати помилку міжмережевого екрану або IDS/IPS. З цієї причини затінення та повне затінення може бути важко діагностувати без використання автоматизованих інструментів, тому важливо оцінити вплив взаємодії старих правил з новими.

2.2.2 Кореляція правил контролю доступу

Аномалія кореляції схожа на затінення. Кореляція (від англ. “correlation”) — це коли одне правило відповідає деяким пакетам, які може захопити інше правило, а інше правило відповідає деяким пакетам, які фіксує початкове правило, правила можуть бути кореляційними. Однак дії двох правил мають бути різними [24].

Коротше кажучи, кореляцію можна розглядати як часткове затінення. Два правила частково збігаються в області дії, через що правило вищого пріоритету перехоплює трафік, який відповідає критеріям цього збігу. Лише в частині, що перекривається, у відповідних сферах дії двох правил виникне проблема. Це те, що відрізняє кореляцію від затінення, тобто той факт, що правило ненавмисно змінюється деякий час, а не весь час. Те, як виникає ця аномалія, також дуже схоже на те, що відбувається при затіненні. Попереднє правило у списку правил застосовується першим перед корелюючим правилом пізніше у списку.

Незалежно від того, яке правило перекриває інше, основна причина кореляції полягає в тому, що два правила мають частково перекриваючі області дії. Найпростіший спосіб уявити це як діаграму Венна, частина, де два кола перекриваються, є місцем, де виникає проблема (рис. 2.6). Якщо припустити, що це перекриття не є навмисним, це означає, що в цій спільній області вживаються помилкові дії. Незалежно від того, чи спричиняють відповідні правила заборону або дозвіл трафіку, коли ця дія не має бути такою, ці правила слід ретельно оцінити, щоб внести правильні зміни для досягнення бажаного результату.

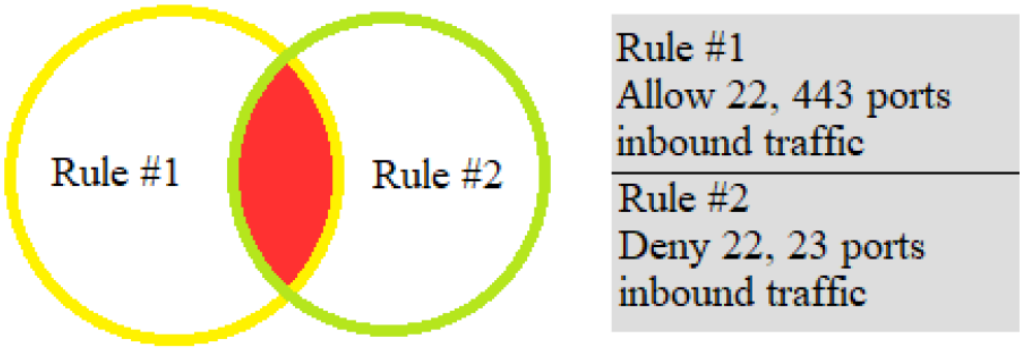

Рисунок 2.6 – Діаграма Вена “Корелятивні правила”

Кореляція є серйозним неправильним налаштуванням з тих же причин, що й затінення: вона викликає неправильну дію на трафік. Однак без інструментів кореляцію може бути важко діагностувати. У випадку затінення дуже ясно, що щось дозволяється або відмовляється щоразу, коли цього не повинно бути. Кореляція створює ситуацію, коли політика іноді спрацьовує [25].

Цей непостійний вигляд може бути проблематичним через те, що правило може працювати належним чином для одних людей або машин, а для інших ні. Це може призвести до припущення, що проблема полягає в налаштуванні певного комп’ютера або в діях деяких користувачів. Після того, як буде виявлено, що проблема полягає в правилах міжмережевих екранів, потрібно буде внести зміни, щоб перекриття або було усунено, або було зроблено більш конкретне правило, щоб не блокувати передбачуваний трафік, або змінити порядок правил для правильного порядку дій.

2.2.3 Надлишковість правил контролю доступу

Надлишковість (від англ. “redundancy”) є найменш серйозною помилкою. Надлишковість настільки ж проста, як це звучить: це коли два різних правила охоплюють одні й ті ж потенційні пакети і виконують однакову дію. Як і затінення, це може мати бути як два однакових правила так і загальне правило, за яким слідує більш конкретне [26]. Скажімо, наприклад, міжмережевий екран має два правила, які блокують порти 20–30; ці правила є зайвими, оскільки обидва правила виконують однакові дії з тими самими пакетами. Це також випадок надлишковості, якщо правило

блокує той самий діапазон від 20 до 30, але друге правило блокує лише порт 22. Оскільки порт 22 знаходиться в діапазоні від 20 до 30, немає необхідності мати інший порт для блокування правила 22. оскільки воно вже заблоковано першим правилом (рис. 2.7).

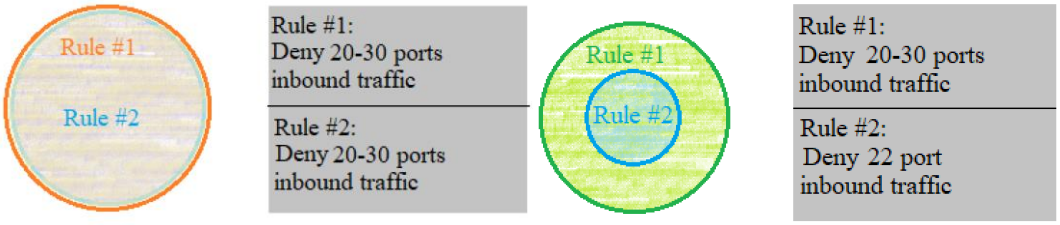

Рисунок 2.7 – Діаграма Вена “Надлишкові правила”

Надлишковість – одна з небагатьох помилок, яка не впливає на загальну безпеку мережі. Наявність кількох копій одного правила навіть на кількох пристроях не впливає на виконання політики. Єдиний вплив надмірності на мережу - це продуктивність. Проблема із зайвими правилами полягає в тому, що вони сповільнюють їх виконання. Міжмережевий екран намагатиметься зіставити пакет із одним із наявних правил, і якщо він не відповідає жодному, він виконує дію за замовчуванням [27]. Проблема із надлишковістю полягає в тому, що щоразу, коли надходить пакет, він перевіряється більшою кількістю правил, ніж це повинно бути. Кожен раз, коли пакет перевіряється на відповідність надлишковому правилу, час і продуктивність пристрою витрачаються даремно. Зайві правила можна безпечно видалити з міжмережевого екрана, оскільки їх видалення не вплине на безпеку і приведе до кращої продуктивності міжмережевого екрану.

2.3 Заходи протидії помилковим налаштуванням

Як було наведено раніше, помилкові налаштування міжмережевого екрану – це помилки, допущені у налаштуванні міжмережевого екрану, які можуть поставити під загрозу його ефективність і зробити організацію вразливою до кіберзагроз.

Міжмережевий екран – це критично важливий засіб безпеки, який допомагає захистити мережі від несанкціонованого доступу та зловмисного трафіку. Однак міжмережеві екрани ефективні, лише якщо вони правильно налаштовані та обслуговуються. Помилкові налаштування можуть виникати з різних причин, у тому числі людська помилка, неправильне спілкування, відсутність документації та зміни мережевого середовища. Незалежно від причини, помилкові налаштування міжмережевого екрану можуть мати серйозні наслідки, включаючи витік даних, простої мережі та втрату репутації.

ACL є одним із ключових компонентів політики безпеки міжмережевого екрану. ACL використовуються для визначення правил фільтрації трафіку, які контролюють, якому трафіку дозволено проходити через міжмережевий екран, а який блокувати. ACL можна застосовувати як до вхідного, так і до вихідного трафіку та використовувати для фільтрації трафіку на основі різноманітних критеріїв, таких як IP-адреса джерела, IP-адреса призначення, номер порту та протокол [28].

Помилкові налаштування ACL можуть виникнути, якщо правила, які визначають ACL, розроблені, задокументовані або перевірені неналежним чином. Щоб мінімізувати ризик помилкових налаштувань ACL, важливо застосувати найкращі методи керування ACL. Це включає документування правил і змін ACL, ретельне тестування ACL перед їх застосуванням і регулярний перегляд ACL, щоб переконатися, що вони ефективні та актуальні. Крім того, мережеві адміністратори повинні розглянути можливість використання автоматизованих інструментів, щоб допомогти керувати списками доступу та забезпечити узгодженість між багатьма міжмережевими екранами або мережевими пристроями.

Зведення до мінімуму помилкових налаштувань ACL міжмережевого екрану можна здійснити за допомогою поєднання організаційних і технічних засобів. Якщо структурувати підходи до зменшенню ризику, який можуть нести потенційні неправильні налаштування, то список матиме такий вигляд:

Організаційні засоби можуть включати:

- Встановлення та впровадження політик і стандартів безпеки, які стосуються керування ACL міжмережевого екрану, включаючи регулярні перевірки, аудити та документування правил.
- Проведення навчання та навчання мережевих адміністраторів і персоналу безпеки, щоб переконатися, що вони розуміють важливість належного керування ACL міжмережевого екрану та як це робити ефективно.
- Впровадження процесів керування змінами, які вимагають перегляду та затвердження перед внесенням будь-яких змін до правил міжмережевого екрану, а також відстеження та звітування про всі зміни.

До технічних засобів можна віднести:

- Впровадження автоматизованих інструментів для керування ACL міжмережевого екрану, включаючи створення, перегляд і перевірку правил.
- Використання інструментів моніторингу та оповіщення, які можуть виявляти та сповіщати адміністраторів про будь-які неправильні налаштування або несанкціоновані зміни правил міжмережевого екрану.
- Впровадження сегментації мережі та керування доступом для обмеження доступу до конфіденційних даних і систем, зменшення потенційного впливу будь-яких помилкових налаштувань.
- Реалізація багатофакторної автентифікації, щоб забезпечити доступ до правил міжмережевого екраун та керування ними лише авторизованому персоналу.

Поєднуючи організаційні та технічні засоби, організації можуть мінімізувати ризик помилкових налаштувань ACL міжмережевого екрану та краще захистити свої мережі та дані. З наведеного переліку заходів, організаційний захід, що стосується “політик і стандартів безпеки” у поєднанні з технічним – “автоматизованими інструментами для керування ACL” є найбільш перспективним та буде детально розглядатися в роботі.

2.3.1 Стандарти безпеки як організаційний захід протидії

Використання стандартів безпеки для налаштування міжмережевих екранів, зокрема списків контролю доступу (ACL), має вирішальне значення для мінімізації ризику помилкових налаштувань. Ці стандарти містять набір вказівок, правил і найкращих практик, які забезпечують узгоджену та ефективну конфігурацію міжмережевих екранів. Дотримуючись цих стандартів, адміністратори можуть переконатися, що налаштування міжмережевих екранів безпечні, надійні та оптимізовані для конкретних потреб організації.

Стандарти безпеки забезпечують основу для дотримання адміністраторами міжмережевих екранів та гарантують, що вони впроваджують найкращі галузеві практики. Вони містять вказівки щодо захисту доступу до міжмережевого екрану, налаштування безпечних правил, керування налаштуваннями міжмережевого екрану та моніторингу його продуктивності. Відповідність цим стандартам може допомогти зменшити ризик помилок або помилкових налаштувань, які можуть призвести до порушень безпеки, збоїв у роботі служби або недотримання відповідності регуляторним стандартам.

Крім того, використання стандартів безпеки забезпечує спільну мову для спілкування між різними командами, відповідальними за керування міжмережевим екраном, такими як мережеві адміністратори, аналітики безпеки та спеціалісти з відповідності стандартам та нормам. Це гарантує, що всі працюють за одним і тим самим посібником, зменшуючи ймовірність непорозумінь і помилок.

Дотримуючись стандартів безпеки, організації можуть бути впевнені, що їхні налаштування міжмережевих екранів оптимізовані для забезпечення безпеки та продуктивності, що знижує ризик інцидентів безпеки та покращує загальну безпеку мережі.

Деякі стандарти безпеки, які стосуються керування списків контролю доступу міжмережевого екрану, включають:

- ISO/IEC 27001:2013 – це міжнародний стандарт для систем керування інформаційною безпекою (ISMS), який містить вимоги щодо встановлення,

впровадження, підтримки та постійного вдосконалення керування інформаційною безпекою в організації. Розділ A.12.1.1 стандарту стосується керування мережевою безпекою та політикою міжмережевого екрану [29].

- NIST SP 800-53 ред. 5 – це система контролю безпеки та конфіденційності, розроблена Національним інститутом стандартів і технологій (NIST). Сімейство керування AC-17 (контроль доступу) стосується встановлення, впровадження та підтримки правил міжмережевого екрану [30].
- CIS Controls Version 8.0 – це набір найкращих методів захисту організацій від поширених кібератак, розроблених Центром безпеки в Інтернеті (CIS). Контроль 13 (Захист кордону) стосується використання міжмережевий екранів та керування ними [31].
- PCI DSS 3.2.1 – це набір стандартів безпеки, розроблених великими компаніями, що надають кредитні картки, щоб гарантувати, що організації, які обробляють операції з кредитними картками, підтримують безпечне середовище. Вимога 1.3.1 стандарту стосується використання міжмережевих екранів та керування їх конфігурацією [32].

Стандарти надають набір передових методів і вказівок щодо налаштування міжмережевих екранів, допомагаючи переконатися, що вони налаштовані правильно та мінімізувати ризик помилкових налаштувань. Дотримання таких стандартів, як NIST SP 800-53, може допомогти інженерам реалізувати ефективні налаштування міжмережевого екрану з більш практичними рекомендаціями. Це може сприяти покращенню безпеки та захисту від кіберзагроз.

2.3.2 Специфіка стандарту безпеки NIST SP 800-53

NIST SP 800-53 вважається одним із найповніших і найавторитетніших стандартів безпеки для налаштування міжмережевих екранів, включаючи керування ACL, щоб мінімізувати ризик помилкових налаштувань. На відміну від інших стандартів безпеки, таких як ISO/IEC 27001:2013, CIS Controls 8.0 і PCI DSS 3.2.1, які

забезпечують більш глобальний погляд і стандарти організаційного рівня, NIST SP 800-53 розроблено як технічний посібник для інженерів, які будуть впроваджувати кращі практики. Цей стандарт містить детальні вказівки щодо впровадження засобів контролю безпеки, включаючи керування правилами контролю доступу міжмережевих екранів, які можна налаштувати відповідно до конкретних потреб організації.

NIST SP 800-53 також містить більше практичних рекомендацій і прикладів, що полегшує командам безпеки розуміння, як налаштувати міжмережеві екрани, щоб мінімізувати ризик помилкових налаштувань. Це широко визнаний стандарт, який часто використовується урядовими установами та приватними організаціями як основа для їхніх політик безпеки.

Дотримуючись стандарту NIST SP 800-53, організації можуть переконатися, що їх міжмережеві екрани налаштовані правильно та відповідають найкращим галузевим практикам. Це може допомогти зменшити ризик помилкових налаштувань, які можуть призвести до порушень безпеки, простоїв та інших проблем. Загалом, використання добре встановленого та технічно орієнтованого стандарту, такого як NIST SP 800-53, може надати командам безпеки вказівки, необхідні для ефективного налаштування міжмережевих екранів і забезпечення безпеки своїх організацій.

NIST SP 800-53 надає комплексний набір заходів безпеки для федеральних інформаційних систем і організацій у Сполучених Штатах. Нижче наведено приклади деяких елементів керування, пов’язаних із керуванням міжмережевим екраном [33]:

- AC-4: Контроль доступу до мереж: цей контроль вимагає, щоб мережеві пристрої були захищені та керовані за допомогою механізмів контролю доступу, таких як міжмережеві екрани. Цей контроль також вимагає наявності політик і процедур для керування пристроями контролю доступу до мережі.
- AC-17: Віддалений доступ: цей контроль вимагає, щоб віддалений доступ до інформаційних систем і мереж контролювався за допомогою механізмів контролю доступу, таких як міжмережеві екрани. Цей контроль також вимагає моніторингу та реєстрації віддаленого доступу.

- SC-7: Захист меж: цей контроль вимагає, щоб інформаційні системи були захищені за допомогою механізмів межового захисту, таких як міжмережеві екрани. Цей контроль також вимагає наявності політики та процедур для керування пристроями захисту меж.

Що стосується керування правилами контролю доступу, деякі елементи керування, пов’язані з ним, є:

- AC-6: Найменші привілеї: цей контроль вимагає, щоб доступ до інформаційних систем і ресурсів був обмежений лише тим особам або процесам, які потребують доступу для виконання своїх обов’язків. Цей контроль можна реалізувати за допомогою ACL, які обмежують доступ за принципом найменших привілеїв.
- AC-17 (1): Віддалений доступ: цей контроль вимагає, щоб віддалений доступ до інформаційних систем і мереж контролювався за допомогою механізмів контролю доступу, таких як міжмережеві екрани. Цей контроль можна реалізувати за допомогою списків керування доступом, які обмежують доступ на основі ідентичності віддаленого користувача, місцезнаходження чи інших факторів.
- CM-7: Найменша функціональність: Цей елемент керування вимагає, щоб інформаційні системи були налаштовані для надання лише необхідних функцій, необхідних для виконання авторизованих завдань. Цей контроль можна реалізувати за допомогою ACL, які обмежують доступ до непотрібних служб або портів.

NIST SP 800-41 – це рекомендації щодо керування інцидентами безпеки інформаційних технологій, які містять рекомендації щодо підготовки, виявлення, аналізу, локалізації, усунення та відновлення після інцидентів безпеки. Він охоплює життєвий цикл керування інцидентами, від розробки політик і процедур реагування на інциденти до проведення заходів після інцидентів.

NIST SP 800-53 – це структура безпеки, яка надає каталог заходів безпеки та конфіденційності для федеральних інформаційних систем і організацій. Він містить набір інструкцій щодо вибору та впровадження заходів безпеки для інформаційних систем та організацій і використовується для забезпечення конфіденційності, цілісності та доступності інформації та інформаційних систем.

Що стосується того, як правильно керувати міжмережевим екраном, NIST SP 800-41 також містить певні рекомендації, а саме [34]:

- Розробка, впровадження та підтримка політик і процедур міжмережевого екрану, які стосуються мети, обсягу, ролей, обов'язків, зобов'язань керівництва, координації між організаційними підрозділами та відповідності.
- Обмеження вхідного і вихідного мережевого трафіку за допомогою політики заборони за замовчуванням, яку має переглянути та схвалити уповноважений персонал.
- Використання безпечних зашифрованих протоколів для віддаленого адміністрування міжмережевого екрану та обмеження кількості персоналу, який має права віддаленого доступу.
- Регулярний перегляд та оновлення наборів правил міжмережевого екрану, щоб переконатися, що вони точно відображають поточну політику безпеки організації та необхідні для підтримки дозволених бізнес-діяльності.
- Впровадження процедур контролю змін, щоб переконатися, що зміни в наборах правил міжмережевого екрану авторизовані, задокументовані та перевірені перед впровадженням.
- Періодичний перегляд наборів правил міжмережевого екрану, щоб переконатися, що вони все ще необхідні та ефективні для досягнення цілей безпеки організації.
- Використання підходу до керування налаштуваннями міжмережевого екрану, заснованого на оцінці ризиків, враховуючи критичність систем і даних, захищених міжмережевим екраном, ймовірність і вплив потенційних загроз, а також толерантність організації до ризику.

А ще NIST SP 800-41 містить певні рекомендації стосовно найкращих методів керування правилами ACL, зокрема:

- Має бути розроблено вичерпний список правил ACL для кожного міжмережевого екрану та задокументовано призначення та функцію кожного правила.

- Регулярний перегляд правил ACL з метою підтвердження їх актуальності для досягнення цілей безпеки організації.
- Обмеження кількості правил ACL до мінімуму, необхідного для підтримки потрібних бізнес-функцій.
- Групування правил ACL за функцією або додатком для полегшення керування та перегляду.
- Використання змістовних назв для правил ACL для полегшення їх розуміння та керування ними.
- Має бути розглянуто можливість використання автоматизованого інструменту для керування правилами ACL, який може допомогти визначити та видалити невикористані або зайві правила, а також може надавати сповіщення про зміну наборів правил.

Загалом, NIST SP 800-53 містить набір заходів безпеки, пов’язаних із безпекою мережі, включаючи керування міжмережевим екраном і контроль доступу. Елементи керування, пов’язані з керуванням міжмережевого екрану і керуванням ACL, включають вимоги до керування політиками міжмережевого екрану, керування доступом до мережі та керування доступом до мережевих пристроїв. Стандарт містить докладні вказівки щодо ефективного впровадження цих засобів керування та посилається на інші публікації NIST, включаючи SP 800-41, для більш детальних вказівок щодо реагування на інциденти. Впроваджуючи засоби контролю безпеки, викладені в NIST SP 800-53, організації можуть покращити керування своїми міжмережевими екранами та засобами контролю доступу та зменшити ризик помилкових налаштувань та інших інцидентів безпеки.

2.3.3 Автоматизовані інструменти як технічний захід протидії

Поява засобів автоматизації для керування міжмережевими екранами стала вирішенням проблематичності і складності, пов’язаних із керуванням правилами та налаштування міжмережевих екранів вручну. Зі збільшенням кількості міжмережевих екранів і мережевих пристроїв керування правилами контролю

доступу міжмережевих екранів та підтримка їх в актуальному стані стало складним завданням для IT-команд і груп безпеки. Крім того, ручне керування схильне до людських помилок, що призводить до помилкових налаштувань та порушень безпеки.

Інструменти автоматизації забезпечують більш ефективний і надійний підхід до керування міжмережевим екраном. Вони дозволяють адміністраторам автоматизувати рутинні завдання, такі як резервне копіювання та відновлення, зміни налаштувань та оновлення правил. Крім того, вони можуть допомогти адміністраторам візуалізувати налаштування та залежності міжмережевого екрану, визначити зайві та суперечливі правила та надати пропозиції щодо оптимізації наборів правил.

Крім того, інструменти автоматизації можуть допомогти подбати про стан набору правил контролю доступу міжмережевого екрану, гарантуючи, що міжмережевий екран постійно перебуває в сумісному стані. Це важливо для дотримання нормативних вимог і підтримки безпеки. Автоматизуючи моніторинг і оцінку наборів правил міжмережевого екрану, адміністратори можуть гарантувати, що будь-які відхилення або зміни будуть негайно виявлені та вирішені.

Загалом інструменти автоматизації стали невід’ємною частиною керування міжмережевим екраном і покращення стану безпеки організацій. Вони забезпечують спрощений та ефективний спосіб керування правилами міжмережевого екрану та гарантують, що вони відповідають стандартам безпеки та нормативним вимогам.

2.3.4 Системи керування міжмережевим екраном

Автоматизовані інструменти для керування ACL для міжмережевого екрану зазвичай відомі як рішення для керування міжмережевим екраном (англ. “Firewall Management System” – абревіатура FMS). Розвиток FMS був зумовлений зростанням складності корпоративних мереж і зростаючою важливістю безпеки мережі. Оскільки корпоративні мережі зростали в розмірах і складності, кількість міжмережевих екранів та інших пристроїв безпеки, розгорнутих для захисту цих мереж, також

зросла. Через це мережевим адміністраторам було важко керувати та підтримувати політики безпеки, які керували цими пристроями [35].

Щоб вирішити цю проблему, постачальники почали розробку рішень FMS, які могли б автоматизувати багато завдань, пов'язаних із керуванням міжмережевим екраном, включаючи керування ACL, керування змінами, аналіз ризиків і звітування про відповідність (рис. 2.8). Автоматизуючи ці завдання, рішення FMS можуть допомогти організаціям зменшити ризик помилкових налаштувань та інших проблем безпеки, які можуть виникнути під час керування великою кількістю міжмережевих екранів.

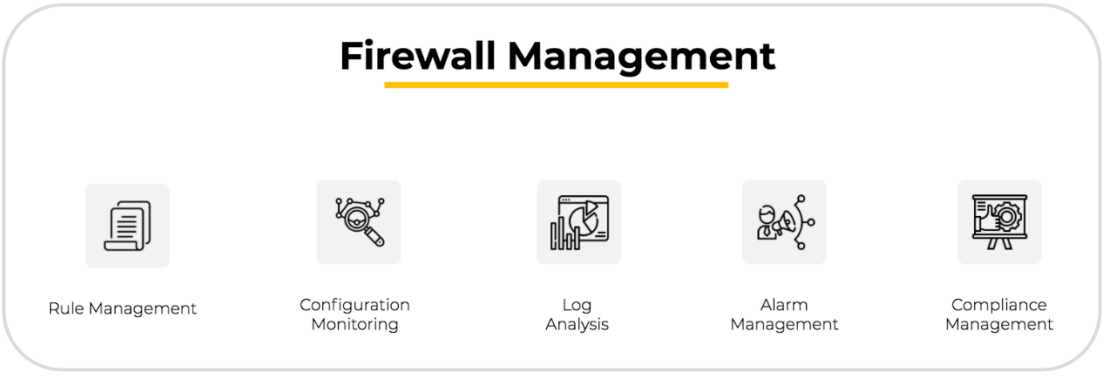

Рисунок 2.8 – Можливості FMS рішень

Сьогодні рішення FMS стали важливим інструментом для багатьох організацій, яким потрібно керувати та підтримувати велику кількість міжмережевих екранів та інших пристроїв безпеки. Рішення FMS доступні від багатьох постачальників, включаючи традиційних постачальників мережевої безпеки, а також нових гравців, які зосереджуються виключно на керуванні міжмережевим екраном, серед яких можна виокремити таких представників ринку (рис. 2.9) [36]:

- Tufin SecureTrack: рішення для керування міжмережевим екраном, яке включає автоматизоване керування ACL, аналіз ризиків, керування змінами та звітування про відповідність.
- AlgoSec Security Management Suite: інструмент, який забезпечує автоматизацію та оркестровку для керування політикою міжмережевого екрану,

включаючи керування ACL, керування змінами, аналіз ризиків та звітування про відповідність.

- FireMon Security Manager: рішення для керування міжмережевим екраном, яке забезпечує автоматичне керування ACL, відстеження змін, аналіз ризиків і звітування про відповідність.
- Skybox Security Suite: інструмент, який забезпечує автоматизацію керування міжмережевим екраном, включаючи керування ACL, керування змінами, аналіз ризиків і звітування про відповідність.
- ManageEngine Firewall Analyzer: інструмент, який забезпечує автоматичний аналіз журналу міжмережевого екрану, звітування та керування ACL.
- SolarWinds Network Configuration Manager: інструмент керування змінами та налаштуваннями мережі, який допомагає організаціям керувати своїми мережевими пристроями та забезпечувати відповідність різним стандартам безпеки. Він забезпечує автоматичне резервне копіювання та відновлення, моніторинг змін у реальному часі та аудит налаштувань.

Рисунок 2.9 – Постачальники FMS рішень

Загалом, системи керування міжмережевим екраном (FMS) — це автоматизовані інструменти, які допомагають організаціям керувати своїми міжмережевими екранами та гарантувати правильне виконання їхніх політик безпеки. Автоматизуючи такі завдання, як аналіз правил, оптимізація та керування змінами,

FMS може зменшити ризик помилкових налаштувань та покращити загальну безпеку мережі організації.

2.3.5 Системи безпеки міжмережевого екрану

Інструменти безпеки міжмережевого екрану (англ. “Firewall Assurance” – абревіатура FA) були розроблені для вирішення проблем керування та захисту сучасних корпоративних мереж, які покладаються на складну інфраструктуру міжмережевого екрану. Міжмережевий екрани є критично важливими компонентами безпеки мережі, але вони також складні, і ними важко керувати, особливо коли мережі стають все більшими та складнішими [37].

Традиційно керування міжмережевим екраном виконувалося вручну, що займало багато часу, викликало помилки та часто призводило до помилкових налаштувань і прогалин у безпеці. Оскільки безпека мережі ставала все більш критичною, а вимоги до відповідності – більш суворими, організації почали усвідомлювати важливість автоматизації завдань керування міжмережевим екраном для покращення безпеки, зменшення помилок і забезпечення відповідності.

Розвиток інструментів безпеки міжмережевого екрану можна простежити на початку 2000-х років, коли були представлені перші рішення для керування міжмережевим екраном. Ці перші рішення часто були обмежені за обсягом і функціональністю та вимагали значного налаштування для задоволення конкретних потреб кожної організації.

З часом ринок інструментів безпеки міжмережевого екрану виріс і став більш зрілим, а постачальники почали пропонувати широкий спектр рішень, які стосуються різних аспектів керування та безпеки міжмережевого екрану. Серед прикладів популярних інструментів безпеки міжмережевого екрану можна назвати наступні:

- Tufin SecureTrack – забезпечує аналіз політики міжмережевого екрану, автоматизацію змін і звітування про відповідність.
- FireMon Security Manager – забезпечує аналіз політики міжмережевого екрану, оцінку ризиків і звітність про відповідність.

- AlgoSec FireFlow – забезпечує аналіз політики міжмережевого екрану, автоматизацію змін і звітність про відповідність.
- Skybox Security Suite – забезпечує аналіз політики міжмережевого екрану, керування вразливістю та звітування про відповідність.
- ManageEngine Firewall Analyzer – забезпечує аналіз журналу міжмережевого екрану, аналіз трафіку та звітування про відповідність.

Сьогодні інструменти безпеки міжмережевого екрану є важливими для керування безпекою та відповідністю вимогам великих, складних інфраструктур міжмережевих екранів, і вони відіграють вирішальну роль у захисті корпоративних мереж від кіберзагроз. Так як FA є по суті підсистемою або зазвичай одним з модулів FMS, то цей функціонал є лише частиною цілісного продукту. Саме з цієї причини, назви продуктів у переліку не відрізняються від попереднього, адже це складові більш збірних систем.

2.3.6 Відмінності системи керування і безпеки міжмережевого екрану

Системи безпеки міжмережевого екрану пов’язані з рішеннями для керування міжмережевим екраном (FMS), але вони не зовсім однакові. Інструменти безпеки міжмережевого екрану призначені для перевірки ефективності та правильності налаштувань, політик і правил міжмережевого екрану. Ці інструменти використовуються для проведення оцінки безпеки налаштувань міжмережевого екрану та виявлення вразливостей безпеки або помилкових налаштувань, які можуть наражати мережу на кіберзагрози. Інструменти безпеки міжмережевого екрану можуть включати сканери вразливостей, інструменти тестування на проникнення та інструменти аналізу налаштувань.

З іншого боку, рішення для керування міжмережевим екраном (FMS) призначені для автоматизації та керування завданнями, пов’язаними з керуванням міжмережевим екраном, такими як налаштування, керування політикою та правилами, керування змінами та звітування про відповідність. Рішення FMS

зазвичай не використовуються для оцінки безпеки налаштувань міжмережевого екрану або виявлення вразливостей безпеки.

Незважаючи на те, що між функціональними можливостями інструментів безпеки міжмережевого екрану та рішень FMS може бути певне збігання, вони зазвичай вважаються різними видами інструментів з різними цілями. Ба більше, FA зазвичай є просто підсистемою для більш всеохоплюючого FMS рішення або доповнення до нього, так як аналіз наборів правил контролю доступу це лише одна з функцій систем керування міжмережевим екраном, і зазвичай ці рішення продаються по модульно, тож за потреби компанія може придбати тільки модуль, що відповідає за FA.

2.3.7 Особливості Tufin SecureTrack

Tufin SecureTrack – це рішення для керування міжмережевим екраном, призначене для автоматизації та оптимізації керування політиками безпеки та налаштуваннями міжмережевого екрану. Він є частиною Tufin Orchestration Suite, який надає наскрізну автоматизацію політик безпеки та можливості оркестровки для корпоративних мереж (рис. 2.10). Tufin SecureTrack розроблено компанією з кібербезпеки Tufin, заснованою в 2005 році. Штаб-квартира компанії розташована в Ізраїлі та має офіси в США, Європі та Азіатсько-Тихоокеанському регіоні [38].

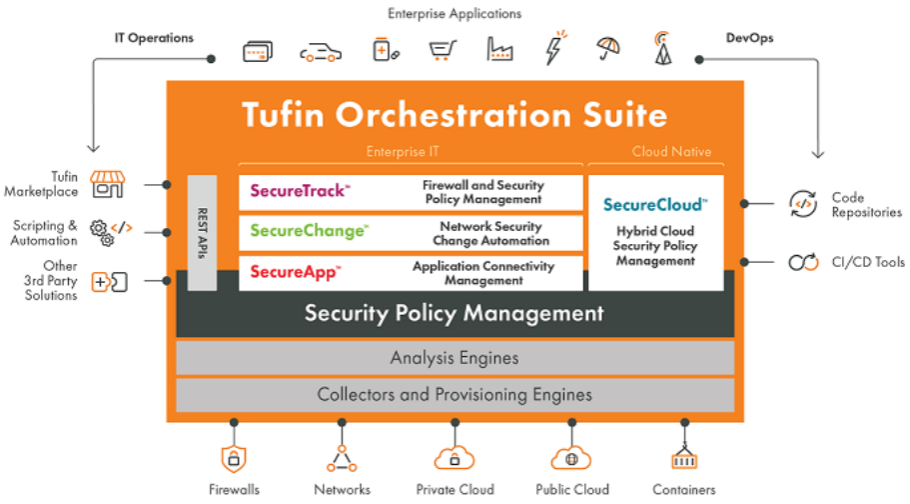

Рисунок 2.10 – Компоненти Tufin Orchestration Suite

Деякі з ключових можливостей Tufin SecureTrack включають:

•Візуалізація політики: дозволяє мережевим адміністраторам переглядати та аналізувати політики безпеки та налаштування своїх міжмережевих екранів, маршрутизаторів і комутаторів у режимі реального часу. Це допомагає їм виявляти та усувати порушення політики, зменшувати ризик збоїв у мережі та підвищувати загальну безпеку мережі.

•Аналіз та оптимізація політики: пропонує інструменти для аналізу та оптимізації політик і налаштувань міжмережевого екрану. Це допомагає визначити невикористані або зайві правила, запропонувати зміни чи видалення правил, а також оптимізувати політики для покращення продуктивності та безпеки мережі (рис. 2.11).

•Керування відповідністю: дає змогу адміністраторам мережі визначати та запроваджувати політики відповідності нормативним вимогам для своїх мережевих пристроїв. Він автоматизує відстеження порушень відповідності, надає журнали аудиту та створює звіти для перевірок відповідності.

•Керування змінами: забезпечує наскрізну видимість і контроль над змінами правил міжмережевого екрану. Він автоматизує весь процес керування змінами, від планування до впровадження та перевірки, і гарантує, що зміни належним чином перевірені та затверджені перед впровадженням.

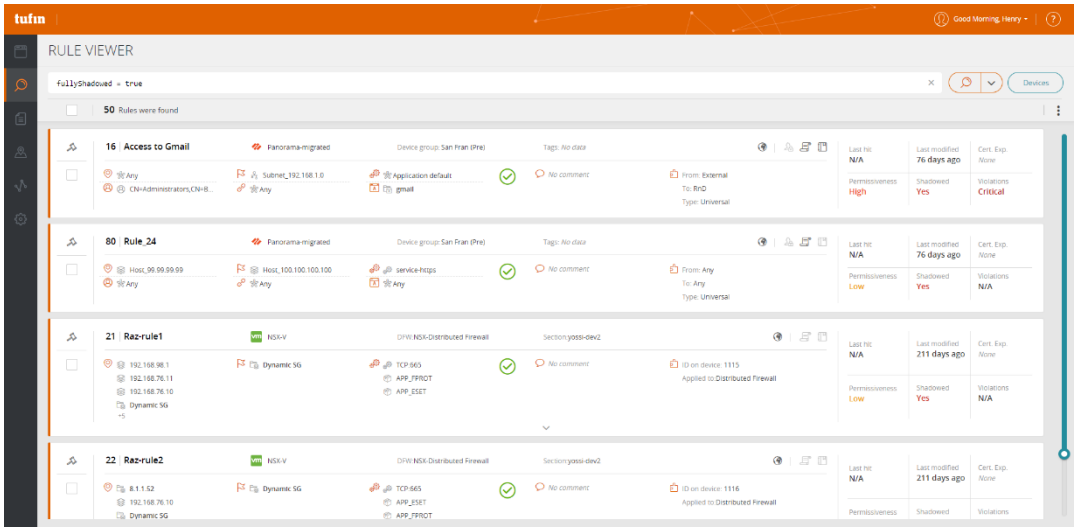

Рисунок 2.11 – Вікно аналізу правил контролю доступу

Tufin SecureTrack широко використовується на великих підприємствах, державних установах і постачальниках послуг для керування складними політиками безпеки мережі та налаштуваннями. Він набув популярності завдяки простоті використання, масштабованості та розширеним можливостям аналізу політики та оптимізації.

Tufin має потужну присутність на світовому ринку кібербезпеки та співпрацює з різними дистриб'юторами та торговими посередниками по всьому світу, щоб надати свої рішення клієнтам. В Україні Tufin SecureTrack доступний через мережу авторизованих торгових посередників та системних інтеграторів, які надають послуги впровадження, навчання та підтримки, такими як IIT Distribution, Infopulse та Netico Solutions.

Також Tufin SecureTrack забезпечує автоматичне звітування про відповідність і постійний моніторинг відповідності світовим стандартам аудиту міжмережевого екрану, зокрема:

- Стандарт безпеки даних платіжних карток (PCI DSS) – для відповідності стандартам безпеки даних кредитних карток.
- Закон Сарбейнса-Окслі (SOX) – для фінансової звітності та аудиту публічних компаній.
- Закон про перенесення та підзвітність медичного страхування (HIPAA) – для захисту конфіденційності та безпеки інформації про здоров'я пацієнтів.
- Федеральний закон про керування інформаційною безпекою (FISMA) – для забезпечення інформаційної безпеки у федеральних агентств.
- ISO/IEC 27001 – для систем керування інформаційною безпекою.
- Концепція кібербезпеки Національного інституту стандартів і технологій (NIST) – для керування та зниження ризиків кібербезпеки.
- Центр безпеки в Інтернеті (CIS) – для покращення стану кібербезпеки та зниження ризику.

Загалом Tufin SecureTrack – це потужне рішення для керування міжмережевим екраном, яке забезпечує наскрізну видимість і контроль над політиками та налаштуваннями безпеки мережі. Він вперше з'явився на українському IT-ринку

кілька років тому, і його популярність неухильно зростає, оскільки все більше організацій визнають важливість ефективного керування міжмережевим екраном та безпеки мережі. Тож ця система широко використовується на великих підприємствах і державних установах.

2.3.8 Особливості Skybox Security Suite

Skybox Security Suite — це всеосяжний інструмент захисту міжмережевого екрану, який надає організаціям можливість у режимі реального часу бачити стан безпеки мережі [37]. Набір включає ряд інструментів і можливостей, які дозволяють організаціям швидко й ефективно виявляти та виправляти проблеми безпеки (рис. 2.12).

Рисунок 2.12 – Вікно аналізу правил контролю доступу

Skybox Security Suite розроблено Skybox Security, компанією з кібербезпеки, що базується в Сан-Дієго, Каліфорнія. Компанія була заснована в 2002 році і з тих пір стала провідним постачальником рішень для кібербезпеки.

FA є одним з модулів Skybox платформи, а загало стек можливостей включає (рис. 2.13):

- Автоматичне моделювання мережі: Skybox Security Suite надає детальну карту мережі, яка допомагає організаціям зрозуміти топологію мережі та визначити потенційні ризики для безпеки.

•Сканування вразливостей: Інструмент містить вбудований сканер вразливостей, який визначає вразливості в мережі та рекомендує відповідні дії з усунення.

•Керування міжмережевим екраном: Skybox Security Suite надає можливості керування міжмережевим екраном, які дозволяють адміністраторам керувати політикою міжмережевого екрану та забезпечувати відповідність галузевим стандартам і нормам.

•Аналіз ризиків: пакет містить інструмент аналізу ризиків, який забезпечує оцінку ризиків у реальному часі на основі даних із багатьох джерел, включаючи сканування вразливостей, аудит налаштувань та канали аналізу загроз.

•Звітування про відповідність: Skybox Security Suite містить механізм звітності, який створює звіти про відповідність різноманітним галузевим стандартам і нормам, зокрема PCI DSS, HIPAA та GDPR.

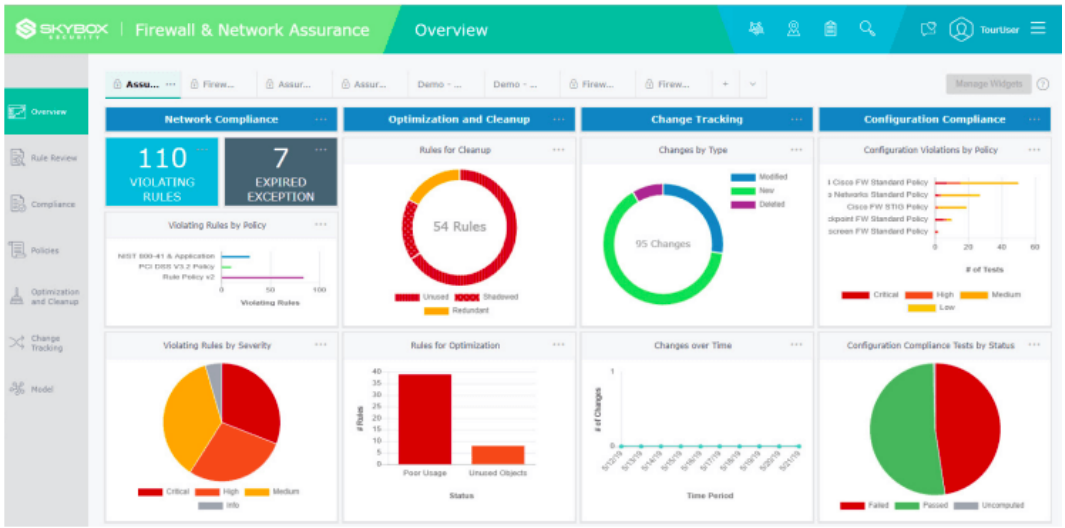

Рисунок 2.13 – Вікно FA модулю

Skybox Security Suite широко визнаний як один із провідних інструментів безпеки міжмережевого екрану на ринку. Інструмент отримав численні нагороди та похвали від галузевих аналітиків і експертів з кібербезпеки. Skybox Security також було названо «провидцем» у Magic Quadrant для міжмережевих екранів Gartner.

Skybox Security має глобальну мережу партнерів і дистриб’юторів, у тому числі в Європі та регіоні СНД. В Україні офіційним дистриб’ютором є ВАКОТЕСН, з яким можна безпосередньо зв'язатися для отримання додаткової інформації про системних інтеграторів.

Skybox Security Suite використовується організаціями в багатьох галузях, включаючи фінансові послуги, охорону здоров’я та уряд. Інструмент особливо корисний для великих організацій зі складним мережевим середовищем, яке вимагає постійного моніторингу та керування. Skybox Security Suite відповідає декільком стандартам аудиту міжмережевого екрану, зокрема:

- PCI DSS (Стандарт безпеки даних індустрії платіжних карток) – цей стандарт застосовується до компаній, які обробляють інформацію про кредитні картки, і вимагає суворого контролю безпеки мережі.
- NIST SP 800-53 – це стандарт, розроблений Національним інститутом стандартів і технологій (NIST), який містить вказівки щодо захисту федеральних інформаційних систем і даних.
- ISO 27001 – це міжнародний стандарт, який описує найкращі практики для систем керування інформаційною безпекою.
- GDPR (Загальний регламент захисту даних) – це регламент Європейського Союзу, який встановлює суворі правила збору, обробки та зберігання персональних даних [39].
- HIPAA (Закон про перенесення та підзвітність медичного страхування) – це закон США, який встановлює стандарти безпеки та конфіденційності особистої медичної інформації [40].

Дотримуючись цих стандартів, Skybox Security Suite гарантує, що його інструменти аудиту та керування міжмережевим екраном відповідають суворим вимогам безпеки та можуть довіряти організаціям для захисту своїх мереж і даних.

Загалом Skybox Security Suite надає організаціям потужний набір інструментів і можливостей для керування безпекою мережі. Завдяки можливостям автоматизованого моделювання мережі, сканування вразливостей і аналізу ризиків

цей інструмент дозволяє організаціям швидко й ефективно виявляти й усувати проблеми безпеки.

2.3.9 Порівняння Tufin SecureTrack та Skybox Security Suite

Tufin SecureTrack і Skybox Security Suite є інструментами безпеки міжмережевого екрану, які надають можливості для керування міжмережевим екраном, аналізу політики та оцінки ризиків. Однак між цими двома інструментами є деякі відмінності.

Таблиця 2.1 – Порівняння систем безпеки міжмережевого екрану

Назва	Tufin SecureTrack	Skybox Security Suite
Можливості	• Керування змінами міжмережевого екрану, • звітування про аудит і відповідність, • аналіз ризиків, • візуалізація топології мережі, • автоматичне створення політики.	Пропонує подібні можливості, але також включає: • керування вразливістю, • розвідку про загрози, • моделювання мережі.
Інтерфейс користувача	Має зручний інтерфейс із більш простим робочим процесом для внесення змін до політики міжмережевого екрану, надає автоматичні пропозиції щодо оптимізації політики та зменшення ризиків, що полегшує	Має більш складний інтерфейс, але пропонує більш детальний контроль над керуванням політиками та оцінкою ризиків, надає детальну візуалізацію топології мережі та шляхів атак, дозволяючи

Назва	Tufin SecureTrack	Skybox Security Suite
	мережевим адміністраторам впровадження найкращих практик.	адміністраторам визначати вразливі місця та зменшувати ризики.
Інтеграція	Інтегрується з широким спектром сторонніх систем безпеки, таких як рішення SIEM, захист кінцевих точок і сканери вразливостей.	Інтегрується зі сторонніми системами безпеки, такими як захист кінцевих точок, SIEM і системи керування виправленнями.

Обидва інструменти широко використовуються в промисловості, причому Tufin SecureTrack більш популярний в деяких регіонах і галузях, тоді як Skybox Security Suite більш популярний в інших. Зрештою, вибір між Tufin SecureTrack і Skybox Security Suite залежатиме від конкретних потреб організації, таких як розмір і складність її мережі, рівень стійкості до ризику та бюджет, доступний для інструментів безпеки.

2.4 Поєднання стандартів та автоматизованих інструментів

Стандарти безпеки для керування міжмережевим екраном містять вказівки та найкращі методи налаштування та керування міжмережевим екраном, щоб забезпечити їх ефективність у захисті мереж від загроз. Системи безпеки міжмережевого екрану, такі як Tufin SecureTrack і Skybox Security Suite, містять можливості, визначені цими стандартами, щоб допомогти організаціям покращити захист міжмережевого екрану.

Дотримуючись стандартів безпеки, системи безпеки міжмережевого екрану можуть допомогти організаціям переконатися, що їх міжмережеві екрани правильно налаштовані, політики правильно визначені та засоби контролю доступу ефективно

реалізовані. Наприклад, стандарти безпеки, такі як PCI-DSS, ISO 27001 і NIST SP 800-53, містять конкретні вимоги до керування міжмережевим екраном, включаючи правила контролю доступу, журналювання та моніторингу. Системи безпеки міжмережевого екрану можуть використовувати ці вимоги як основу для оцінки стану безпеки міжмережевого екрану та визначення областей для покращення.

Крім того, стандарти безпеки забезпечують спільну мову та структуру для оцінки безпеки міжмережевих екранів. Системи безпеки міжмережевого екрану можуть використовувати ці стандарти як еталон для оцінки ефективності засобів контролю безпеки та надання рекомендацій щодо покращення безпеки міжмережевого екрану.

Загалом, включення можливостей, визначених у стандартах безпеки для керування міжмережевими екранами, допомагає системам безпеки міжмережевого екрану надавати більш ефективні рішення безпеки, які відповідають найкращим галузевим практикам і вимогам відповідності.

Висновки за розділом 2

Міжмережеві екрани є важливим компонентом безпеки сучасної мережі, забезпечуючи критичний рівень захисту від несанкціонованого доступу та витоку даних. Однак навіть найдосконаліші міжмережеві екрани можуть стати неефективними через помилкові налаштування, що може зробити мережі підданими широкому спектру загроз безпеці.

Помилкові налаштування можуть виникнути з різних причин, зокрема людська помилка, відсутність досвіду та неналежний зв’язок між командами IT та безпеки. Зокрема, помилкові налаштування правил доступу можуть бути значною проблемою, що призводить до помилок, які можуть дозволити несанкціонований доступ або скомпрометувати конфіденційні дані.

Щоб вирішити цю проблему, організації повинні застосувати комплексний підхід до керування міжмережевими екранами, реалізуючи найкращі практики та використовуючи автоматизовані інструменти для мінімізації ризику помилкових

налаштувань. Стандарти безпеки, такі як NIST SP 800-53, забезпечують основу для ефективного керування міжмережевим екраном, включаючи правильне налаштування правил контролю доступу.

Останніми роками інструменти забезпечення міжмережевого екрану, такі як Tufin SecureTrack і Skybox Security Suite, стали потужними рішеннями для керування міжмережевим екраном, пропонуючи розширені можливості для автоматизації керування правилами ACL і забезпечення відповідності стандартам безпеки.

Незважаючи на ці досягнення, людський фактор залишається критичною проблемою, оскільки неправильне спілкування та відсутність чітко визначених обов’язків можуть сприяти помилковим налаштуванням. Вирішуючи ці проблеми та впроваджуючи комплексний підхід до керування міжмережевим екраном, організації можуть ефективно мінімізувати ризик помилкових налаштувань та посилити загальну безпеку мережі.

РОЗДІЛ 3
ТЕХНОЛОГІЯ ОЧИЩЕННЯ ПРАВИЛ МІЖМЕРЕЖЕВОГО ЕКРАНУ ЗА ДОПОМОГОЮ FMS

3.1 Упорядкований підхід до технологія очищення правил міжмережевого екрану за допомогою FMS

Міжмережеві екрани є критично важливими компонентами інфраструктури мережевої безпеки, відповідальними за виконання політик контролю доступу шляхом дозволу або заборони трафіку на основі попередньо визначеного набору правил. Однак керування політиками міжмережевого екрану може бути складним і трудомістким завданням, особливо у великих і складних мережевих середовищах. Системи керування міжмережевим екраном (FMS) були розроблені, щоб допомогти організаціям ефективніше керувати політикою міжмережевого екрану шляхом автоматизації аналізу політики, керування правилами та аудиту відповідності.

Хоча FMS може бути корисним для виявлення та вилучення помилкових налаштувань у правилах контролю доступу міжмережевого екрану, критичною проблемою залишається те, як підійти до впровадження змін на основі неточностей і рекомендацій, виділених FMS. Однією з ключових проблем є те, що постачальники не надають інструкцій щодо визначення пріоритетів і вирішення проблем у належному порядку, що може призвести до заплутаного вороху проблем, які не вирішуються належним чином.

Таким чином, мета цього дослідження полягає в дослідженні технології використання FMS для ефективного усунення неправильних налаштувань у правилах контролю доступу міжмережевого екрану. Запропонована технологія забезпечить покроковий підхід до виявлення та визначення пріоритетів проблем, виявлених FMS, з кінцевою метою підвищення ефективності та безпеки міжмережевого екрану.

Щоб досягти цієї мети, у дослідженні спочатку буде розглянуто відповідну літературу про використання FMS для керування політикою міжмережевого екрану

та виявлено типові помилкові налаштування в правилах контролю доступу міжмережевого екрану, такі як затемнення, кореляція та надмірність. Дослідження також вивчатиме обмеження існуючих підходів і запропонує покращену та упорядковану технологію для вирішення цих проблем.

Запропонована технологія складатиметься з наступних кроків:

1. Попередній аналіз: задокументуйте всю інформацію про правила міжмережевого екрану та топологію мережі.

2. Дедуплікація: визначте та видаліть повторювані правила, щоб зменшити розмір набору правил.

3. Виявлення затінених правил: визначте та видаліть правила, які повністю затінені іншими правилами.

4. Групування правил за службами: групуйте правила на основі служб, які вони призначені підтримувати.

5. Виявлення частково затінених правил: визначте та видаліть правила, які частково затінені іншими правилами на основі контексту груп послуг.

6. Деталізація широких правил: визначте широкі правила та розбийте їх на більш конкретні правила.

7. Перегрупування правил: перегрупуйте правила на основі їхніх служб і налаштуйте порядок правил.

8. Уточнення назв і цілей правил: оновіть назви та описи правил, щоб уточнити їх мету та спростити керування правилами в майбутньому.

9. Виявлення надлишкових і корельованих правил: визначте та видаліть надлишкові та корельовані правила.

10. Пост-аналіз: задокументуйте очищений набір правил і топологію мережі.

Запропонована технологія буде перевірена шляхом застосування її до реального сценарію, в якому виявлено проблемний міжмережевий екран і реалізовано систему FMS для виявлення помилкових налаштувань. Результати дослідження продемонструють ефективність запропонованої технології для усунення неправильних налаштувань у правилах контролю доступу міжмережевого екрану та покращення загального стану безпеки мережі.

На завершення, це дослідження має на меті забезпечити практичну та ефективну технологію використання FMS для усунення помилкових налаштувань у правилах контролю доступу міжмережевого екрану. Запропонована технологія допоможе організаціям ефективніше керувати політикою міжмережевого екрану та гарантувати, що їх мережа захищена від кіберзагроз.

3.2 Ідентифікація ситуацій, що вимагають очищення правил міжмережевого екрану

Міжмережеві екрани є критично важливими компонентами інфраструктури безпеки організації, відповідальними за фільтрацію вхідного та вихідного мережевого трафіку для запобігання несанкціонованому доступу та витоку даних. Однак з часом правила контролю доступу в межах міжмережевого екрану можуть стати складними та громіздкими, що призведе до неправильної конфігурації та вразливості безпеки. У цій главі ми обговоримо ситуації, у яких слід запровадити процес очищення правил міжмережевого екрану. Буде також приклад, щоб проілюструвати необхідність процесу очищення правил міжмережевого екрану.

Причини для впровадження процесу очищення правил міжмережевого екрану [41]:

- Зміни в мережі. Однією з найпоширеніших причин очищення правил міжмережевого екрану є зміни в мережевій інфраструктурі. Це може включати додавання або видалення сегментів мережі, впровадження нових програм або послуг або зміни загальної топології мережі. У результаті цих змін набір правил міжмережевого екрану може стати застарілим і неефективним, що призведе до значного збільшення ризику порушень безпеки та проблем із продуктивністю. Щоб переконатися, що міжмережевий екран залишається ефективним, важливо проводити регулярне очищення набору правил.
- Вимоги до відповідності. Іншою причиною впровадження процесу очищення правил міжмережевого екрану є дотримання галузевих або нормативних стандартів. Організації, які обробляють конфіденційні дані, як-от постачальники медичних

послуг або фінансові установи, повинні відповідати нормам HIPAA або PCI DSS відповідно. Ці правила передбачають суворий контроль безпеки, включаючи підтримку актуального та точного списку мережевих пристроїв і правил контролю доступу. Процес очищення правил міжмережевого екрану може допомогти організаціям забезпечити відповідність цим нормам шляхом виявлення та видалення застарілих або непотрібних правил, які можуть призвести до порушень безпеки.

- Проблеми з продуктивністю: з часом, коли кількість правил контролю доступу в міжмережевому екрані збільшується, міжмережевий екран може стати повільнішим і менш чуйним, що призведе до затримки мережі та зниження продуктивності. Це може призвести до проблем з продуктивністю, оскільки міжмережевий екран повинен обробляти кожне правило в наборі правил, навіть якщо воно не стосується трафіку, що перевіряється. Реалізація процесу очищення правил міжмережевого екрану може допомогти зменшити розмір набору правил і підвищити продуктивність.

- Злиття та поглинання: коли компанії зливаються або купують інші компанії, їм часто потрібно інтегрувати IT-інфраструктуру обох організацій. Це може вимагати об’єднання наборів правил міжмережевого екрану двох компаній в єдиний уніфікований набір правил. Невиконання цього може призвести до вразливості системи безпеки, а також до проблем із продуктивністю. Очищення правил міжмережевого екрану може допомогти усунути надлишкові або суперечливі правила та забезпечити безпечність та ефективність нової мережевої архітектури.

- Інциденти безпеки: нарешті, після інциденту безпеки може знадобитися процес очищення правил міжмережевого екрану. Якщо організація стикається з порушенням даних або іншим інцидентом безпеки, важливо провести ретельний перегляд правил контролю доступу в межах міжмережевого екрану, щоб виявити будь-які неправильні конфігурації або вразливі місця, які могли сприяти інциденту. Процес очищення правил міжмережевого екрану може допомогти організаціям виявити та усунути ці вразливості, зменшивши ризик майбутніх інцидентів безпеки.

Оскільки зміни в мережі переважно є основною рушійною силою для впровадження процесу очищення правил міжмережевого екрану, цей сценарій буде детально розглянуто з точки зору конкретних причин:

- Зміни архітектури: коли компанії вносять значні зміни у свою IT-архітектуру, наприклад переходять до хмарного середовища або віртуалізують свою мережу, їм може знадобитися відповідним чином оновити набір правил міжмережевого екрану. У таких випадках очищення правил міжмережевого екрану може допомогти компанії визначити застарілі або зайві правила та переконатися, що новий набір правил узгоджується з оновленою архітектурою.

- Оновлення апаратного та програмного забезпечення: Оновлення апаратного та програмного забезпечення може призвести до змін у наборі правил міжмережевого екрану. У деяких випадках для нових функцій або можливостей може знадобитися додавання нових правил, тоді як старі правила можуть більше не знадобитися. Очищення правил міжмережевого екрану може допомогти переконатися, що набір правил оптимізовано для нового апаратного та програмного забезпечення.

- Перехід на новий міжмережевий екран: під час переміщення даних з одного міжмережевого екрану на інший через зміну обладнання чи архітектури мережі може знадобитися переглянути та змінити набір правил. Очищення правил міжмережевого екрану може допомогти консолідувати, упорядкувати й оптимізувати набір правил для нового міжмережевого екрану, забезпечуючи плавний перехід.

- Об’єднання міжмережевих екранів: якщо компанія об’єднує кілька міжмережевих екранів в один, необхідний процес очищення правил міжмережевого екрану. У цьому сценарії набори правил із кількох міжмережевих екранів мають бути консолідовані, а дублікати та застарілі правила мають бути видалені, щоб створити ефективний і ефективний набір правил.

Приклад: процес очищення правил міжмережевого екрану для компанії з об’єднаними міжмережевими екранами

Щоб продемонструвати важливість очищення правил міжмережевого екрану, буде представлено справжнє практичне дослідження. Згідно з угодами про нерозголошення, ані назва компанії, ані галузь, до якої вона належить, не можуть бути розкриті, а також жодні конкретні деталі, такі як тип пристрою, конфігурація, список набору правил або супровідні звіти та знімки екрана. Тим не менш, описана ситуація є похідною від реального сценарію та була анонімна для забезпечення

конфіденційності компанії. Для цілей цієї роботи компанія буде називатися Компанією А.

Компанія А нещодавно переглянула свою мережеву архітектуру для підвищення простоти та резервування. Щоб досягти цього, вони вирішили об’єднати шість міжмережевих екранів в одне централізоване місце. Це рішення було прийнято, щоб спростити керування доступом і зменшити сегментацію логічної мережі, яка раніше була розподілена між різними місцями.

Однак після консолідації шести наборів правил в один міжмережевий екран отриманий набір правил перетворився на повний безлад. Політика складалася з понад 3500 правил, з багатьма дублікатами та складними правилами, якими було важко керувати. Це створювало проблеми з продуктивністю, оскільки набір правил був великим, і новим адміністраторам було важко знайти сенс у правилах і керувати повсякденною роботою. Крім того, ця складність створила можливість для інцидентів безпеки через погане керування міжмережевим екраном.

Компанія А визнала необхідність процесу очищення правил міжмережевого екрану для вирішення цих проблем. Вони вирішили запровадити комплексний процес очищення, який включав кроки, описані в попередньому розділі. Більш детально сама технологія та необхідні кроки будуть описані в наступних розділах.

Підсумовуючи, процес очищення правил міжмережевого екрану є критично важливим кроком у підтримці ефективного та дієвого міжмережевого екрану. У цьому розділі ми обговорили різні ситуації, які вимагають процесу очищення правил міжмережевого екрану, і представили практичне дослідження, щоб проілюструвати необхідність такого процесу. Запровадивши комплексний процес очищення правил міжмережевого екрану, компанії можуть переконатися, що їхні міжмережеві екрани працюють оптимально та забезпечують максимальний захист їхніх мереж.

3.3 Виклики та найкращі практики впровадження FMS у очищення правил міжмережевого екрану

Керування міжмережевим екраном може бути складним завданням, і очищення правил міжмережевого екрану не є винятком. В останні роки системи керування міжмережевим екраном (FMS) з'явилися як рішення, яке допомагає організаціям автоматизувати процес очищення правил міжмережевого екрану. Хоча FMS може принести значні переваги, організації також можуть зіткнутися з проблемами під час їх впровадження. У цій главі буде висвітлено деякі проблеми, з якими можуть зіткнутися організації, і перераховано найкращі практики, які допоможуть їм подолати ці проблеми та отримати максимальну віддачу від інвестицій у FMS.

Щоб забезпечити успішне впровадження FMS, організації повинні знати про виклики, з якими вони можуть зіткнутися. Ось деякі з найпоширеніших проблем [42]:

- Складність і масштаб.

Однією з найбільших проблем впровадження FMS у очищення правил міжмережевого екрану є складність і масштаб процесу. Очищення правил міжмережевого екрану передбачає аналіз великої кількості правил, політик і налаштувань, щоб визначити, які правила необхідні, а які можна безпечно видалити. Цей процес може зайняти багато часу та ресурсів, особливо у великих організаціях із кількома міжмережевими екранами.

- Стійкість до змін.

Стійкість до змін — поширена проблема, з якою стикаються організації під час впровадження систем керування міжмережевим екраном (FMS) для очищення правил міжмережевого екрану. Співробітники можуть чинити опір запровадженню FMS, побоюючись зміни своїх посадових обов'язків або скорочення. Опір може виникнути через необхідність перегляду існуючих процесів змін, занепокоєння щодо безпеки роботи, перевантаження від вивчення нових інструментів і брак розуміння переваг FMS.

- Сумісність із існуючими системами міжмережевого екрану.

Іншою проблемою, з якою можуть зіткнутися організації під час впровадження систем керування міжмережевим екраном (FMS), є сумісність із існуючими міжмережевими екранами. Для організацій вкрай важливо забезпечити бездоганну інтеграцію FMS із поточною інфраструктурою міжмережевих екранів, щоб уникнути додаткових витрат і операційних перешкод.

- Інтеграція з існуючими системами.

Крім того, інтеграція FMS з існуючими системами створює ще одну проблему, оскільки організації часто мають різноманітні рішення безпеки. Забезпечення плавної інтеграції та координації між цими системами може бути складним і складним завданням, яке потенційно може призвести до неефективності під час процесу очищення правил.

- Відсутність навчання, досвіду та ресурсів.

Недостатня підготовка персоналу, так як і нестача досвіду і ресурсів створюють значні проблеми при впровадженні систем управління міжмережевим екраном (FMS). Організаціям часто важко забезпечити всебічне навчання співробітників, що призводить до неоптимального використання системи. Відсутність досвіду налаштування та ефективного використання FMS може призвести до помилок, які ставлять під загрозу безпеку інфраструктури міжмережевого екрану. Крім того, недостатність ресурсів, включаючи персонал, обладнання та програмне забезпечення, можуть спричинити затримки та перешкодити загальній ефективності впровадження FMS. Подолання цих викликів вимагає від організацій пріоритетного навчання персоналу, інвестування в придбання необхідного досвіду та виділення достатніх ресурсів для забезпечення успішного впровадження FMS.

- Обмежена видимість.

Іншою проблемою, з якою можуть зіткнутися організації під час впровадження FMS у очищення правил міжмережевого екрану, є обмежена видимість інфраструктури міжмережевого екрану. Без повної видимості інфраструктури міжмережевого екрану виявити зайві, застарілі або невикористані правила може бути складно. Ця відсутність видимості також може призвести до вразливостей безпеки,

оскільки може бути важко виявити неавторизовані зміни налаштувань міжмережевого екрану.

Незважаючи на ці проблеми, існують найкращі практики, яких організації можуть дотримуватися, щоб подолати їх і отримати максимальну віддачу від своїх інвестицій у FMS. Ось деякі практичні поради:

- Починайте з малого та будуйте поступово.

Щоб зменшити складність і масштаб впровадження FMS у очищення правил міжмережевого екрану, організаціям слід починати з малого та поступово створювати. Почати роботу з одного міжмережевого екрану або невеликої підмножини правил міжмережевого екрану може допомогти організаціям отримати досвід роботи з інструментом FMS і зміцнити впевненість у його ефективності. З цього моменту організації можуть поступово розширювати використання FMS до додаткових міжмережевих екранів і правил міжмережевого екрану.

- Залучення зацікавлених сторін і ефективна комунікація.

Щоб подолати опір змінам, організації повинні залучати зацікавлені сторони до процесу впровадження FMS і ефективно спілкуватися з ними. Зацікавлені сторони мають включати працівників, які використовуватимуть інструмент FMS, а також менеджерів і керівників, які підзвітні за інфраструктуру міжмережевих екранів. Ефективна комунікація може допомогти зацікавленим сторонам зрозуміти переваги FMS і вирішити будь-які проблеми, зокрема і опір змінам.

- План інтеграції.

Щоб забезпечити успішне впровадження FMS, організації повинні визначити пріоритетність планування інтеграції з існуючими системами. Ретельно оцініть сумісність FMS з поточною інфраструктурою міжмережевого екрану, вирішуючи потенційні проблеми на ранніх стадіях. Інтеграція FMS має бути зкоординована з іншими рішеннями безпеки, враховуючи взаємодію та уникаючи неефективності. Має бути розроблений структурований план інтеграції, що включатиме оцінку сумісності, координацію зацікавлених сторін і стратегії подолання викликів.

- Проведення початкової всебічної оцінки.

Перш ніж запроваджувати FMS, важливо повністю зрозуміти поточну конфігурацію правил міжмережевого екрану організації. Проведення ретельного аналізу існуючих правил міжмережевого екрану допоможе виявити зайві та застарілі правила, що дозволить організаціям видалити їх і оптимізувати свої набори правил. Цей процес не тільки допоможе зменшити складність правил і ризик помилок, але й оптимізує продуктивність міжмережевого екрану.

- Визначення чіткої політики очищення правил міжмережевого екрану.

Чітка і вичерпна політика очищення правил міжмережевого екрану необхідна для того, щоб правила міжмережевого екрану залишалися точними і актуальними. Ця політика має визначати, хто має повноваження створювати, змінювати та видаляти правила міжмережевого екрану, а також як часто набори правил слід переглядати й актуалізовувати.

- Використання підходу, що ґрунтується на оцінці ризику.

Застосування підходу, що ґрунтується на оцінці ризику, для очищення правил міжмережевого екрану передбачає виявлення додатків і потоків даних із найвищим ризиком у мережі та зосереджені на них у першу чергу. Цей підхід допомагає визначити пріоритети для очищення правил і гарантує наявність критично важливих засобів контролю безпеки.

- Автоматизація процесу очищення правил.

Впровадження інструментів FMS дозволяє організаціям автоматизувати процес очищення правил міжмережевого екрану, заощаджуючи час і знижуючи ризик людської помилки. Автоматизація процесу також може допомогти організаціям дотримуватися галузевих норм і уникнути потенційних порушень безпеки.

- Інвестування в навчання і експертизу, та виділення ресурсів.

Щоб забезпечити успішне впровадження FMS, організації повинні інвестувати в навчання та експертизу. Ці інвестиції мають включати навчання співробітників щодо ефективного використання інструменту FMS, а також наймання експертів із керування міжмережевим екраном для налаштування та контролю за FMS. Крім того, організації повинні виділити необхідні ресурси, включаючи персонал, обладнання та

програмне забезпечення, для ефективного впровадження та управління FMS. Це включає планування поточного обслуговування та оновлень.

- Регулярний моніторинг та тестування.

Нарешті, організації повинні регулярно моніторити та тестувати свої набори правил міжмережевого екрану, щоб переконатися, що вони функціонують належним чином. Цей процес може включати періодичне тестування на проникнення, сканування вразливостей і аналіз журналу міжмережевого екрану. Регулярний моніторинг і тестування допоможуть виявити будь-які проблеми або помилкові налаштування та оперативно їх усунути.

Очищення правил міжмережевого екрану є критично важливим завданням для підтримки стану безпеки організації. FMS може допомогти автоматизувати цей процес, але організації повинні знати про проблеми, з якими вони можуть зіткнутися під час впровадження FMS. Дотримуючись цих найкращих практик, організації можуть подолати проблеми, пов’язані з впровадженням FMS у процес очищення правил міжмережевого екрану, і оптимізувати продуктивність і безпеку свого міжмережевого екрану.

3.4 Комплексна попередня оцінка та технологія очищення правил міжмережевого екрану

Впровадження FMS для очищення правил міжмережевого екрану може бути складним і клопітким завданням через величезний масштаб заходу. Під час роботи з великими мережами з кількома міжмережевого екранами та складними наборами правил завдання ретельного аналізу існуючих правил міжмережевого екрану може зайняти багато часу та ресурсів. Важливо підійти до цього завдання з добре продуманою стратегією та комплексним планом.

Попереднє завдання проведення ретельного аналізу існуючих правил міжмережевого екрану є важливим кроком у процесі впровадження FMS. Однак це завдання може бути складним, особливо для організацій із великими та складними

мережами. Важливо підходити до цього завдання систематично, щоб забезпечити всебічний і впорядкований перегляд правил міжмережевого екрану.

Першим кроком у проведенні комплексного аналізу існуючих правил міжмережевого екрану є визначення всіх міжмережевих екранів у мережі організації. Це передбачає інвентаризацію всіх мережевих пристроїв і документування їх налаштувань. Другим кроком є визначення всіх діючих правил міжмережевого екрану, включаючи ті, які більше не потрібні або можуть бути зайвими. Це вимагає ретельного вивчення кожного правила міжмережевого екрану, щоб визначити його призначення та відповідність поточним потребам організації.

Після визначення всіх правил міжмережевого екрану наступним кроком є їх класифікація на основі їх функції та відповідності поточним потребам організації. Це вимагає глибокого розуміння бізнес-процесів організації та вимог до мережі. Це також може включати консультації з ключовими зацікавленими сторонами та бізнес-підрозділами для визначення важливості кожного правила міжмережевого екрану.

Після класифікації правил міжмережевого екрану наступним кроком є їх пріоритетність на основі їх критичності для безпеки мережі організації. Це передбачає визначення найбільш важливих правил міжмережевого екрану, які необхідно підтримувати, і гарантування того, що їм надається пріоритет у процесі очищення правил. Цей крок має вирішальне значення для забезпечення захисту найбільш важливих активів організації та одночасного зниження ризику порушення безпеки.

У випадку компанії А потреба в процесі очищення правил міжмережевого екрану стала очевидною після консолідації шести окремих міжмережевих екранів в одному централізованому місці. Хоча метою консолідації було спростити керування доступом і сегментацію мережі, результатом цього стало політика, що складалася з понад 3500 правил, з багатьма дублікатами та складними правилами, якими було важко керувати. Ця складність не лише створила проблеми з продуктивністю, але й створила можливість для інцидентів безпеки через неякісне керування міжмережевим екраном.

Розмір і складність набору правил міжмережевого екрану в цьому випадку демонструють проблеми, з якими можуть зіткнутися організації під час впровадження

FMS у процес очищення правил міжмережевого екрану. Коли ви маєте справу з такою великою кількістю правил, проведення ретельного аналізу існуючих правил міжмережевого екрану може зайняти багато часу та ресурсів. Це вимагає системного підходу, щоб гарантувати, що аналіз є всебічним і впорядкованим.

Використання інструменту FMS може допомогти спростити процес очищення правил міжмережевого екрану, але важливо спочатку провести ретельний аналіз існуючих правил, щоб переконатися, що інструмент FMS налаштовано правильно. Цей аналіз має включати комплексний перегляд усіх правил міжмережевого екрану, включаючи дублікати, складні правила та правила, які більше не використовуються. Роблячи це, організації можуть визначити, які правила можна безпечно видалити або консолідувати, а які правила потрібно змінити або оновити.

Незважаючи на труднощі, пов’язані з проведенням ретельного аналізу правил міжмережевого екрану, це критичний крок у забезпеченні ефективності процесу очищення правил міжмережевого екрану. Організації повинні інвестувати необхідний час і ресурси для проведення цього аналізу під час впровадження інструменту FMS. Роблячи це, вони можуть гарантувати, що їхні інвестиції в FMS використовуються максимально повно, а їх міжмережеві екрани працюють оптимально та забезпечують максимальний захист мережі.

Як згадувалося раніше, проведення ретельного аналізу існуючих правил може бути складним і трудомістким завданням, особливо для організацій із великими та складними наборами правил міжмережевого екрану, як-от компанія A. Через відсутність системних підходів до такої діяльності було вирішено консолідувати результати реального кейсу в технологію. Ця технологія містить короткий огляд кроків, які слід виконати, як їх робити, у якому порядку та з скількох кроків вона складається, щоб виконати завдання аналізу найкращим і найефективнішим способом.

Відсутність консолідованого документа для чіткого вирішення цієї проблеми є загальною проблемою, з якою стикаються багато організацій. Хоча є доступна документація від постачальників FMS і стандартів, таких як NIST, які містять міжмережеві екрани, немає жодного консолідованого документа, який би містив

вичерпний посібник для проведення ретельного аналізу існуючих правил міжмережевого екрану. Це є причиною для дослідження цієї теми та пошуку можливих рішень.

У наступній главі ми обговоримо технологію, розроблену для проведення комплексного аналізу правил міжмережевого екрану за допомогою FMS. Ця технологія забезпечує структурований підхід до очищення правил міжмережевого екрану та допомагає організаціям подолати труднощі керування великими та складними наборами правил міжмережевого екрану. Дотримуючись цієї технології, організації можуть гарантувати, що їхні правила міжмережевого екрану оптимізовані для продуктивності, керованості та безпеки.

3.5 Концепція технології попереднього оцінювання очищення правил міжмережевого екрану

Ефективне керування правилами міжмережевого екрану має вирішальне значення для підтримки безпеки мережі та оптимізації продуктивності. Однак робота з великими та складними наборами правил може бути нелегким і трудомістким завданням. Щоб вирішити цю проблему, була розроблена комплексна технологія для проведення попередньої оцінки правил міжмережевого екрану в процесі очищення правил. У цій главі детально розглядається ця технологія, окреслюються ключові кроки та міркування.

Тепер, коли встановлено важливість систематичного підходу та переваги, які він приносить, настав час зануритися в детальні кроки технології попередньої оцінки в очищенні правил міжмережевого екрану. Дотримуючись цих кроків, організації можуть ефективно аналізувати та оптимізувати свої правила міжмережевого екрану, створюючи більш безпечну та ефективнішу мережеву інфраструктуру. Давайте детально дослідимо кожен крок, щоб отримати повне розуміння процесу та його реалізації.

1. Попередній аналіз: перший крок передбачає проведення ретельного попереднього аналізу, де документується вся відповідна інформація про правила

міжмережевого екрану та топологію мережі. Ця початкова оцінка служить важливою основою для подальших кроків, забезпечуючи повне розуміння існуючого набору правил та мережевої інфраструктури.

2. Усунення дублікатів: на цьому етапі основна увага зосереджена на виявленні та видаленні повторюваних правил, щоб оптимізувати розмір набору правил. Усунувши надлишкові правила, організації можуть спростити конфігурацію міжмережевого екрану та підвищити загальну ефективність.

3. Виявлення затінених правил: третій крок присвячений ідентифікації та видаленню правил, які повністю затінені іншими правилами. Ці тіньові правила не мають функціонального призначення та можуть створити плутанину та потенційну вразливість безпеки. Їх видалення забезпечує більш чистий і ефективний набір правил.

4. Групування правил за службами: цей крок включає класифікацію правил на основі конкретних служб, які вони призначені підтримувати. Групування правил за службами допомагає адміністраторам легко визначати та керувати правилами, пов’язаними з певними функціями мережі, сприяючи ефективному керуванню правилами.

5. Виявлення частково затінених правил: ґрунтуючись на попередньому кроці, цей крок зосереджується на визначенні правил, які частково затінені в певних групах послуг. Вилучивши ці частково затінені правила, організації можуть додатково оптимізувати керування правилами та забезпечити послідовне виконання правил.

6. Деталізація загальних правил: шостий крок підкреслює важливість поділу загальних правил на більш конкретні. Цей детальний підхід покращує керування правилами, дозволяючи точно контролювати мережевий трафік і гарантуючи, що правила тісно відповідають вимогам бізнесу.

7. Перегрупування правил: на цьому кроці правила перегруповуються на основі їх служб, а порядок правил уточнюється. Організовуючи правила логічно, адміністратори можуть оптимізувати набір правил, підвищити чіткість правил і оптимізувати роботу міжмережевого екрану.

8. Уточнення назв правил і цілей: Оновлення назв і описів правил є основним напрямком цього кроку, який спрямований на чітке формулювання мети кожного правила. Переконавшись, що назви та описи правил є лаконічними та описовими, організації можуть спростити майбутнє керування правилами та покращити загальне розуміння.

9. Виявлення надлишкових і корельованих правил: цей крок включає ідентифікацію та видалення надлишкових і корельованих правил. Усунувши непотрібну складність, організації можуть оптимізувати свої набори правил, що призведе до більш ефективної та керованої конфігурації міжмережевого екрану.

10. Пост-аналіз: Останнім кроком є документування очищеного набору правил і топології мережі. Це служить оновленим записом конфігурації міжмережевого екрану та надає цінну інформацію для майбутнього обслуговування, перевірок і довідкових цілей.

Дуже важливо створити резервну копію існуючого набору правил перед внесенням будь-яких змін, щоб забезпечити можливість повернутися до попереднього робочого стану, якщо виникнуть несподівані проблеми. Крім того, слід провести ретельне тестування після впровадження змін, щоб переконатися, що міжмережевий екран працює належним чином без будь-яких негативних наслідків для мережі. Також рекомендується відстежувати версії набору правил для легкого відстеження та повернення змін, коли це необхідно, забезпечуючи додатковий рівень безпеки та забезпечуючи швидке виправлення будь-яких помилок без істотного впливу на бізнес. А також проводити зміни пропонується ітераційно невеличкими групами правил, щоб можна було відстежити як зміни вплинули на роботу міжмережевого екрану і спростити процедуру відкату у випадку невдачі.

Наведена вище технологія пропонує комплексний і структурований підхід до проведення ретельного аналізу правил міжмережевого екрану. Дотримуючись цих кроків, організації можуть переконатися, що їхні міжмережеві екрани налаштовані для максимального підвищення безпеки, продуктивності та відповідності. У той час як успіх у проекті аналізу правил міжмережевого екрану залежить від різних факторів, ця технологія забезпечує добре організовану, цілеспрямовану та ефективну

структуру, яка дає відповідні рекомендації щодо ефективного керування правилами міжмережевого екрану.

3.6 Роль FMS на кожному кроці технології очищення правил міжмережевого екрану

Безсумнівно, вимоги є відправною точкою для кожного процесу. Як хтось сказав: «Не має значення, скільки у вас ресурсів, якщо ви не вмієте ними користуватися, цього ніколи не буде достатньо» [**Ошибка! Источник ссылки не айден.**].

Системи керування міжмережевого екрану (FMS) відіграють вирішальну роль в успішному впровадженні технології очищення правил міжмережевого екрану. Інструменти FMS, такі як Tufin SecureTrack або Skybox Security Suite, пропонують повний набір модулей і функцій, спеціально розроблених для підтримки організацій в ефективному управлінні конфігураціями міжмережевого екрану. Ці інструменти надають адміністраторам централізовану платформу для нагляду та контролю наборів правил міжмережевого екрану, забезпечуючи оптимальну безпеку, продуктивність і відповідність. Розглянемо детально як саме системи FMS допомагають проводити очищення помилкових налаштувань і наборах правил контролю доступа міжмережевого екрану за наданою раніше технологією попереднього аналізу (рис. 3.1).

Технології попереднього оцінювання очищення правил міжмережевого екрану

1. Попередній аналіз
2. Дедуплікація
3. Виявлення затінених правил
4. Групування правил за службами
5. Виявлення частково затінених правил
6. Деталізація широких правил
7. Перегрупування правил
8. Уточнення назв і цілей правил
9. Виявлення надлишкових і корельованих правил:
10. Пост-аналіз

Рисунок 3.1 – Фрагмент файлу аналізу набору правил за допомогою FMS для компанії A

Попередній аналіз: інструменти FMS пропонують автоматизовані можливості для збору та документування вичерпної інформації про правила міжмережевого екрану та топологію мережі. Ці інструменти можуть сканувати й аналізувати існуючий набір правил і мережеву інфраструктуру, надаючи адміністраторам детальне розуміння поточного стану конфігурацій міжмережевого екрану.

Дедуплікація: інструменти FMS можуть виконувати аналіз і порівняння правил, автоматично виявляючи повторювані правила в наборі правил. Використовуючи свої можливості керування правилами, інструменти FMS можуть допомогти адміністраторам легко визначати та усувати зайві правила, оптимізуючи розмір набору правил і підвищуючи ефективність.

Виявлення затінених правил: інструменти FMS можуть проводити поглиблений аналіз набору правил, щоб ідентифікувати правила, які повністю затінені іншими. Завдяки візуалізації правил і вдосконаленим алгоритмам ці інструменти можуть виявляти та позначати тіньові правила, дозволяючи адміністраторам видаляти їх і підтримувати чистіший набір правил.

Групування правил за послугами. Інструменти FMS надають функції для класифікації та групування правил на основі конкретних послуг, які вони підтримують. Використовуючи функції керування правилами, адміністратори можуть ефективно організовувати правила відповідно до вимог служби, спрощуючи керування правилами та забезпечуючи кращу видимість залежностей правил.

Виявлення частково затінених правил: інструменти FMS можуть допомогти у визначенні частково затінених правил у певних групах послуг. Аналізуючи взаємодію правил і залежності, ці інструменти допомагають адміністраторам виявляти та видаляти частково затінені правила, забезпечуючи послідовне виконання правил і подальшу оптимізацію набору правил.

Деталізація широких правил: інструменти FMS пропонують можливість аналізувати та розбивати широкі правила на більш конкретні. Візуалізуючи взаємозв’язки та залежності правил, ці інструменти допомагають адміністраторам

уточнювати та налаштовувати визначення правил, що забезпечує більш детальний контроль над мережевим трафіком і покращує керування правилами.

Перегрупування правил: інструменти FMS надають функціональні можливості для перегрупування правил на основі їхніх послуг і точного налаштування порядку правил. Пропонуючи можливості візуалізації та оптимізації правил, ці інструменти допомагають адміністраторам логічно організовувати правила, підвищуючи чіткість правил і оптимізуючи роботу міжмережевого екрану.

Уточнення імен правил і цілей: інструменти FMS полегшують процес оновлення назв і описів правил. Забезпечуючи зручні інтерфейси та можливості централізованого керування правилами, ці інструменти дозволяють адміністраторам легко змінювати та уточнювати назви та описи правил, спрощуючи майбутнє керування правилами та покращуючи загальне розуміння.

Виявлення надлишкових і корельованих правил: інструменти FMS включають розширені алгоритми та функції аналізу правил для виявлення надлишкових і корельованих правил. Завдяки автоматизації процесу ідентифікації ці інструменти допомагають адміністраторам визначити непотрібну складність у наборі правил, дозволяючи видаляти зайві та корельовані правила та покращувати загальну ефективність правил.

Пост-аналіз: інструменти FMS можуть створювати докладні звіти та документацію щодо очищеного набору правил і топології мережі. Ці звіти служать оновленими записами конфігурації міжмережевого екрану, надаючи цінну інформацію для майбутнього обслуговування, аудитів і довідкових цілей. Інструменти FMS забезпечують спрощений і точний процес документування, дозволяючи адміністраторам підтримувати актуальний огляд конфігурацій міжмережевого екрану.

Таким чином, системи керування міжмережевого екрану, такі як Tufin SecureTrack або Skybox Security Suite, відіграють важливу роль у виконанні кожного кроку технології. Використовуючи можливості автоматизації, аналізу та візуалізації цих інструментів, організації можуть оптимізувати процес очищення правил міжмережевого екрану, оптимізувати свої набори правил і забезпечити відповідність

конфігурацій міжмережевого екрану найкращим практикам безпеки, вимогам відповідності та бізнес-цілям.

Приклад: процес очищення правил міжмережевого екрану для компанії А з об’єднаними міжмережевого екранами

Впровадивши системи керування міжмережевого екрану (FMS), як-от Tufin SecureTrack або Skybox Security Suite, компанія А змогла ефективно вирішити проблеми, пов’язані з безладним набором правил, що виник у результаті консолідації їхніх міжмережевих екранів. Ці інструменти FMS відіграли вирішальну роль у допомозі Компанії А подолати складність, проблеми з продуктивністю та ризики безпеки, пов’язані з їх об’єднаним міжмережевого екрану.

Інструменти FMS надали розширені функції, які значно допомогли Компанії А у проведенні комплексного процесу очищення правил міжмережевого екрану. Ці інструменти запропонували можливості автоматизованого аналізу та візуалізації, дозволяючи Компанії А отримати глибоке розуміння свого набору правил та мережевої інфраструктури. Завдяки можливості сканування та аналізу консолідованого набору правил інструменти FMS швидко виявляли повторювані правила, складні правила та інші недоліки, якими важко керувати вручну.

У випадку компанії А для виконання процесу очищення використовувалися Tufin SecureTrack і Skybox Security Suite. Ці інструменти FMS дозволили Компанії А оптимізувати набір правил шляхом визначення та видалення повторюваних правил, спрощення конфігурації та підвищення загальної ефективності. Функції автоматизованого аналізу та звітності інструментів FMS надали Компанії А чітке розуміння набору правил, дозволяючи їй приймати обґрунтовані рішення під час процесу очищення.

Крім того, інструменти FMS допомогли Компанії А візуалізувати набір правил і його залежності, спрощуючи керування та організацію правил. Забезпечуючи повний огляд структури набору правил і зв’язків, інструменти FMS дозволили Компанії А ефективно класифікувати та групувати правила, забезпечуючи кращий контроль і легше керування.

Крім того, інструменти FMS полегшили ідентифікацію складних і заплутаних правил, які важко зрозуміти та керувати ними. Завдяки вдосконаленим алгоритмам і можливостям аналізу правил Tufin SecureTrack і Skybox Security Suite допомогли Компанії А розбити та спростити ці правила до більш керованих і зрозумілих. Цей детальний підхід до керування правилами покращив ясність і ефективність набору правил, спростивши роботу з ним для адміністраторів і зменшивши ймовірність неправильної конфігурації або інцидентів безпеки.

Крім того, інструменти FMS забезпечували комплексні можливості звітування та документування, дозволяючи компанії А створювати детальні звіти про очищений набір правил і топологію мережі. Ці звіти слугували цінними ресурсами для поточного моніторингу, аудитів і довідкових цілей, гарантуючи, що процес очищення був добре задокументований і відповідав вимогам дотримання.

Таким чином, впровадження систем керування міжмережевого екрану, таких як Tufin SecureTrack або Skybox Security Suite, допомогло компанії А подолати труднощі, з якими зіткнулися під час очищення об’єднаного міжмережевого екрану. Ці інструменти FMS надавали можливості автоматизованого аналізу, візуалізації та звітності, дозволяючи Компанії А оптимізувати свій набір правил, підвищити чіткість правил і покращити загальну продуктивність і безпеку міжмережевого екрану. Використання цих інструментів FMS у процесі очищення гарантувало, що компанія А могла ефективно керувати своїми конфігураціями міжмережевого екрану та підтримувати безпечне й оптимізоване мережеве середовище.

У порівнянні зі складним Tufin SecureTrack, Skybox Security Suite пропонує більш спрощену функціональність. Проте Skybox Security Suite вирізняється своєю здатністю генерувати файли у форматі CSV, які надають повний огляд набору правил. Ці файли позначили кожне правило такими категоріями, як «ОК», «затінене», «надлишкове» або іншими неправильними конфігураціями разом із правилом, до якого воно стосувалося. Нижче наведено фрагмент одного з фактично створених файлів (рис.3.2).

	Rule Number	Original ID	Source Resolved Addresses	Destination Resolved Addresses	Services	Action	Duplicate of	Shadowed	Shadowed By
2	2775	access_1034_1_access_in_154	0.0.0.0-255.255.255.255	10.36.1.168-10.36.1.168	Any	Allow	2771	Shadowed	2771
3	2477	COMMON_access_dmzapp_166_in_70	0.0.0.0-255.255.255.255	2.210-10.36.22.210,10.36.22.212-10.36	Any	Allow	2417	Shadowed	2417
4	1468	COMMON_access_dmzie_115_in_18	0.0.0.0-255.255.255.255	10.36.27.11-10.36.27.11	Any	Allow	1467	Shadowed	1467
10	1604	COMMON_access_dmzie_165_in_104	0.0.0.0-255.255.255.255	10.36.27.12-10.36.27.12	Any	Allow	1472	Shadowed	1472
91	3099	access_fw1037_in_138	10.0.0.0-10.255.255.255	6.4.86,10.36.4.97-10.36.4.97,10.36.4.1	Any	Allow	3093	Shadowed	3093
92	3100	access_fw1037_in_139	10.0.0.0-10.255.255.255	6.4.86,10.36.4.97-10.36.4.97,10.36.4.1	Any	Allow	3093	Shadowed	3093
93	978	COMMON_access_242_in_86	10.0.0.0-10.255.255.255	10.6.4.41-10.6.4.41	Any	Allow	941	Shadowed	941
94	953	COMMON_access_242_in_61	10.0.0.0-10.255.255.255	10.6.4.55-10.6.4.55	Any	Allow	952	Shadowed	952
95	932	COMMON_access_242_in_40	10.0.0.0-10.255.255.255	10.6.4.57-10.6.4.59	Any	Allow	922	Shadowed	922
96	606	COMMON_access_157_in_10	0.0.103-10.0.0.105,10.0.0.108-10.0.0.	10.36.18.12-10.36.18.12	Any	Allow	308	Shadowed	10

Рисунок 3.2 – Фрагмент файлу аналізу набору правил за допомогою FMS для компанії А

З іншого боку, Tufin SecureTrack також мав можливість виявляти подібні проблеми в наборі правил. Однак він підтримував лише звіти HTML, що виявилося незручним для команди. Незважаючи на цей недолік, обидві системи генерували діаграми топології мережі на основі інтегрованих міжмережевих екранів, забезпечуючи чітку візуалізацію поточного стану міжмережевих екранів і мережі. Крім того, вони створили виконавчі звіти та надали змістовні рекомендації щодо очищення об’єднаного міжмережевого екрану.

Завдяки об’єднаним зусиллям і допомозі, наданій системою керування міжмережевого екрану, команда успішно скоротила набір правил із понад 3500 правил до більш керованих 300 правил. Набір правил було оптимізовано з уточненими назвами правил і згрупованими за службами, покращивши керування правилами та загальну продуктивність міжмережевого екрану. Співпраця між командою та інструментами FMS виявилася неоціненною для створення безпечної, ефективної та добре організованої конфігурації міжмережевого екрану для компанії А.

Висновки за розділом 3

Підсумовуючи, відсутність документації про те, як підійти до попереднього аналізу процесу очищення міжмережевого екрану, може створити серйозні проблеми для організацій. Без системної технології проведення ретельної оцінки існуючих правил міжмережевого екрану та топології мережі може зайняти багато часу та бути схильним до помилок. Усвідомлюючи цю потребу, було розроблено комплексну технологію, що включає 10 важливих кроків, які направляють організації через процес очищення правил міжмережевого екрану.

1. Попередній аналіз: задокументуйте всю інформацію про правила міжмережевого екрану та топологію мережі.

2. Дедуплікація: визначте та видаліть повторювані правила, щоб зменшити розмір набору правил.

3. Виявлення затінених правил: визначте та видаліть правила, які повністю затінені іншими правилами.

4. Групування правил за службами: групуйте правила на основі служб, які вони призначені підтримувати.

5. Виявлення частково затінених правил: визначте та видаліть правила, які частково затінені іншими правилами на основі контексту груп послуг.

6. Деталізація широких правил: визначте широкі правила та розбийте їх на більш конкретні правила.

7. Перегрупування правил: перегрупуйте правила на основі їхніх служб і налаштуйте порядок правил.

8. Уточнення назв і цілей правил: оновіть назви та описи правил, щоб уточнити їх мету та спростити керування правилами в майбутньому.

9. Виявлення надлишкових і корельованих правил: визначте та видаліть надлишкові та корельовані правила.

10. Пост-аналіз: задокументуйте очищений набір правил і топологію мережі.

Ця технологія забезпечує структурований підхід до вирішення типових проблем, таких як повторювані правила, тіньові правила, складність керування правилами та погана ефективність. Дотримуючись цих кроків, організації можуть оптимізувати конфігурації свого міжмережевого екрану, підвищити безпеку, покращити продуктивність мережі та оптимізувати процеси керування правилами.

Щоб проілюструвати ефективність цієї технології, було представлено приклад компанії А, компанії, яка пройшла процес консолідації міжмережевого екрану, що призвело до складного та неорганізованого набору правил. За допомогою систем керування міжмережевим екраном (FMS), таких як Tufin SecureTrack і Skybox Security Suite, команда компанії А успішно впровадила технологію.

Інструменти FMS зіграли вирішальну роль у попередньому аналізі, виявленні затінених і надлишкових правил, категоризації правил і створенні вичерпних звітів і рекомендацій. Tufin SecureTrack із розширеною функціональністю надає детальну інформацію та виконавчі звіти, тоді як Skybox Security Suite пропонує простоту та можливість генерувати файли CSV, які класифікують правила для ефективного аналізу.

Запровадивши технологію та використовуючи інструменти FMS, команда компанії A змогла скоротити свій набір правил із понад 3500 до лише 300+ правил. Правила були впорядковані, уточнені та згруповані за послугами, що призвело до більш чіткої та керованої конфігурації. Спільні зусилля між командою та інструментами FMS привели до покращеного керування правилами, підвищення безпеки мережі та підвищення ефективності.

Таким чином, розроблена технологія пропонує організаціям структурований підхід до вирішення проблем, пов’язаних із очищенням правил міжмережевого екрану. Дотримуючись 10 кроків, описаних у цій технології, і використовуючи можливості інструментів FMS, організації можуть оптимізувати конфігурації міжмережевого екрану, оптимізувати набори правил, підвищити безпеку та забезпечити відповідність. Приклад компанії A є підтвердженням ефективності цієї технології та її здатності успішно подолати складності, пов’язані з об’єднаними міжмережевими екранами.

Впровадження цієї технології та використання відповідних інструментів FMS може дати можливість організаціям підтримувати безпечну та ефективну інфраструктуру міжмережевого екрану, дозволяючи їм адаптуватися до нових загроз, покращувати продуктивність мережі та, зрештою, захищати свої важливі активи.

ВИСНОВКИ

Міжмережеві екрани відіграють важливу роль у забезпеченні безпеки сучасних мереж, надаючи критичний рівень захисту від несанкціонованого доступу та витоку даних. Незважаючи на те, наскільки передові вони можуть бути, помилкові налаштування можуть позбавити їх ефективності, ставлячи мережі під загрозу різноманітних безпекових проблем.

Це дослідження показало, що помилкові налаштування, що виникають через людський фактор є основною причиною зниження ефективності міжмережевих екранів. Саме тому пошук та впровадження комбінації найбільш перспективних заходів протидії їм є одним з головних способів убезпечення міжмережевих екранів та мереж загалом. Таким чином поєднання таких організаційних і технічних засобів як стандарт NIST та інструмент автоматизації FMS, на додачу з новою комплексною покроковою технологією попереднього аналізу правил для впровадження процесу очищення міжмережевих екранів з використанням FMS може допомогти організаціям підвищити ефективність міжмережевих екранів.

У кваліфікаційній роботі розв’язано актуальне питання підвищення ефективності міжмережевих екранів нового покоління шляхом дослідження помилкових налаштувань та заходів протидії їм. У ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1. Було визначено основні причини появи порушень інформаційної безпеки міжмережевих екранів – у 95% випадків винні помилкові налаштування, які у свою чергу виникають через людський фактор.

2. Було категоризовано помилкові налаштування міжмережевих екранів – затінення правил (часткове і тотальне), кореляційні правила та надлишкові правила. Було досліджено основні аспекти типів помилкових налаштувань міжмережевих екранів (складність виявлення, відмінності, тощо).

3. Було досліджено основні типи заходів протидії помилковим налаштуванням міжмережевих екранів – організаційні і технічні.

4. Було проведено аналіз організаційних заходів протидії помилковим налаштуванням міжмережевих екранів, детально розглянувши стандарти – NIST SP 800-53 та NIST SP 800-41.

5. Було проведено аналіз технічних заходів протидії помилковим налаштуванням міжмережевих екранів, детально розглянувши автоматизовані системи – Firewall Management System та Firewall Assurance.

6. Було досліджено основні аспекти систем керування та безпеки міжмережевих екранів на прикладі Tufin SecureTrack та Skybox Security Suite та проведено їх порівняння (функціонал, інтегрованість, зручність, поширеність на світовому і локальному ринку, популярність тощо).

7. Було розглянути основні ситуації, що зумовлюють необхідність впровадження процесу очищення правил міжмережевого екрану з більш детальним розглядом ситуацій, спричинених саме мережевими змінами, так як саме вони є зазвичай рушійною силою.

8. Було запропоновано нову комплексну і структуровану покрокову технологію попереднього аналізу правил міжмережевого екрану для проведення очищення з визначенням ролі систем керування міжмережевим екраном в цьому процесі.

Процес виконання даної роботи охоплював детальне дослідження заходів та інструментів протидії помилковим налаштуванням правил міжмережевих екранів, вивчення різних аспектів очищення правил міжмережевих екранів та розробку покрокової технології попереднього аналізу правил міжмережевого екрану для впровадження процесу очищення з залученням FMS таких як Tufin SecureTrack та Skybox Security Suite.

Результати цього дослідження відкривають нові горизонти для підвищенню ефективності боротьби з помилковими налаштуваннями міжмережевого екрану за рахунок максимізації інвестицій в системи керування міжмережевими екранами та покрокової технології, що сприятиме цьому процесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ferguson R. The history of the next-generation firewall | Computer Weekly [Електронний ресурс] / Rik Ferguson // ComputerWeekly.com. – Режим доступу: https://www.computerweekly.com/news/2240159432/The-history-of-the-Next-Generation-Firewall

2. Freda A. What is a firewall and why do you need one? [Електронний ресурс] / Anthony Freda // What Is a Firewall and Why Do You Need One?. – Режим доступу: https://www.avast.com/c-what-is-a-firewall

3. What is a firewall? Types, how it works and advantages [Електронний ресурс] // Intellipaat Blog. – Режим доступу: https://intellipaat.com/blog/what-is-a-firewall/?US

4. Arsene L. The evolution of firewalls: past, present & future - informationweek [Електронний ресурс] / Liviu Arsene // InformationWeek. – Режим доступу: https://www.informationweek.com/partner-perspectives/the-evolution-of-firewalls-past-present-and-future/a/d-id/1318814

5. Saurabh Sharma. What is firewall ?History of firewall/classification /types /what firewalls do and why do we need it ? [Електронний ресурс] / Saurabh Sharma // Blog Nirvana. – Режим доступу: https://www.blognirvana.com/2023/02/what-is-firewall.html

6. The 8 types of firewalls explained [Електронний ресурс] // phoenixNAP Blog. – Режим доступу: https://phoenixnap.com/blog/types-of-firewalls

7. Mitchell B. What is MAC address filtering, and is it useful? [Електронний ресурс] / Bradley Mitchell // Lifewire. – Режим доступу: https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571

8. George, A. Shaji & George, A.s. (2021). A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall. IJARCCE. 10. 31-37. 10.5281/zenodo.7027397.

9. Hoan, NGUYEN & Hiep, LE & Luc, Do. (2022). Study to analyse, compare and evaluate the performance of next general firewalls: Case of Palo Alto and Fortigate Firewall. Vinh University Journal of Science. 51. 10.56824/vujs.2022nt08.

10. Firewall: traditional vs next generation - sprint networks [Електронний ресурс] // Sprint Networks. – Режим доступу: https://www.sprintnetworks.com.au/blog/traditional-versus-next-generation-firewall/

11. Network security firewall market share | industry trends - 2030 [Електронний ресурс] // Allied Market Research. – Режим доступу: https://www.alliedmarketresearch.com/network-security-firewall-market-A12492

12. What Is a Next-Generation Firewall (NGFW)? [Електронний ресурс] // Cisco. – Режим доступу: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

13. Next-Generation Firewalls | NGFW | FortiGate [Електронний ресурс] // Fortinet. – Режим доступу: https://www.fortinet.com/kr/products/next-generation-firewal-bk

14. Next-Generation firewalls [Електронний ресурс] // Palo Alto Networks. – Режим доступу: https://www.paloaltonetworks.com/network-security/next-generation-firewall

15. Next-Generation firewall [Електронний ресурс] // Barracuda Networks. – Режим доступу: https://www.barracuda.com/support/glossary/next-generation-firewall

16. Sophos firewall powerful protection and performance [Електронний ресурс] // Sophos Firewall. – Режим доступу: https://www.sophos.com/en-us/products/next-gen-firewall

17. Villegas M. O. Check point next generation firewall: product overview | techtarget [Електронний ресурс] / Mike O. Villegas // Security. – Режим доступу: https://www.techtarget.com/searchsecurity/feature/Check-Point-Next-Generation-Firewall-Product-overview

18. Alicea M. Misconfiguration in firewalls and network access controls: literature review [Електронний ресурс] / Michael Alicea, Izzat Alsmadi // Future internet. – 2021. – Т. 13, № 11. – С. 283. – Режим доступу: https://doi.org/10.3390/fi13110283

19. Tran, T. Misconfiguration Analysis of Network Access Control Policies. Master’s Thesis, University of Waterloo, Waterloo, ON, Canada, 2009.

20. Human factors, human error & the role of bad luck in incident investigations [Електронний ресурс] // safetywise. – Режим доступу:

https://www.safetywise.com/single-post/2016/08/30/human-factors-human-error-the-role-of-bad-luck-in-incident-investigations

21. Aryan, R.; Yazidi, A.; Engelstad, P.E.; Kure, Ø. A general formalism for defining and detecting openflow rule anomalies. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 9–12 October 2017; pp. 426–434.

22. Chandre, P.R.; Surve, R.R.; Badhan, S.R.; Surve, A.B.; Mane, V.T. Anomalies of Firewall Policy Detection and Resolution. Int. J. Eng. Res. Appl. 2014, I, 696–701.

23. Al-Shaer, E.S.; Hamed, H.H. Modeling and management of firewall policies. IEEE Trans. Netw. Serv. Manag. 2004, 1, 2–10.

24. Geeringh, C. Generic Firewall Rule Compiler And Modeller. Master's Thesis, Napier University, Edinburgh, UK, 2007.

25. Aryan, R.; Yazidi, A.; Engelstad, P.E. An incremental approach for swift openflow anomaly detection. In Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN), Chicago, IL, USA, 1–4 October 2018; pp. 502–510.

26. Chao, C.S.; Yang, S.J. A Novel Mechanism for Anomaly Removal of Firewall Filtering Rules. J. Internet Technol. 2020, 21, 949–957

27. Hu, H. Assurance Management Framework for Access Control Systems. Ph.D Thesis, Arizona State University, Tempe, AZ, USA, July 2012.

28. Cox J. Access control list (ACL) - what are they and how to configure them! • ITT systems [Електронний ресурс] / James Cox // ITTSystems. – Режим доступу: https://www.ittsystems.com/access-control-list-acl/

29. ISO, "International Standard ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements," Iec, vol. 27001, no. 27001, 2013

30. National Institute of Standards and Technology Special Publication 800-53, Revision 5 Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5, 492 pages (September 2020)

31. CIS controls version 8 [Електронний ресурс] // CIS. – Режим доступу: https://www.cisecurity.org/controls/v8

32. DSS and PCI, Payment Card Industry (PCI) Data SecurityStandard Requirements and Security Assessment ProceduresVersion 3.2., PCI Security Standards Council, LLC, 2016

33. Rose, Rachel. (2019). New NIST revisions - What do they mean for regulatory compliance?. EDPACS. 59. 1-9. 10.1080/07366981.2019.1642559.

34. National Institute of Standards and Technology Special Publication 800-41 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev1, 48 pages (Sep. 2009)

35. Firewall management: Tools, rules, and how it works | AlgoSec [Електронний ресурс] // algosec. – Режим доступу: https://www.algosec.com/solutions/firewall-management/

36. Andrea H. 13 best firewall management software tools for rules and policies (2023) [Електронний ресурс] / Harris Andrea // Networks Training. – Режим доступу: https://www.networkstraining.com/best-firewall-management-software-tools/

37. Firewall assurance [Електронний ресурс] // Skybox Security. – Режим доступу: https://www.skyboxsecurity.com/products/firewall-assurance/

38. Tufin SecureTrack [Електронний ресурс] // Tufin. – Режим доступу: https://www.tufin.com/

39. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

40. Health Insurance Portability and Accountability Act [HIPAA] of 1996, Pub. L. No. 104-191

41. Firewall policy cleanup & optimization | managefirewalls.com [Електронний ресурс] // AlgoSec Products and Solutions | ManageFirewalls.com. – Режим доступу: https://www.managefirewalls.com/FPCO.asp

42. Firewall rule base cleanup: policy examples & best practices | tufin [Електронний ресурс] // Tufin. – Режим доступу: https://www.tufin.com/blog/how-to-clean-up-a-firewall-rulebase-tufin-firewall-expert-tip-6

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

- Kyrylenko Anna THE ELIMINATION OF HUMAN FACTOR AND ITS EFFECTS IN CORRUPTING SECURITY / Natalia Lukova-Chuiko, Volodymyr Nakonechnyi, Anastasiia Petrenko, Anna Kyrylenko // VIII International conference “Information Technology and Implementation”, December 1-3, 2021
- Kyrylenko Anna MISCONFIGURATIONS IN FIREWALLS AS A RESULT OF HUMAN FACTOR / Natalia Lukova-Chuiko, Ivan Parkhomenko, Anna Kyrylenko, Anastasiia Petrenko // “Problems of Cybersecurity of Information and Telecommunication Systems” (PCSITS): Collection of reports and abstracts; Kyiv city, 27-28 October 2022 year; Taras Shevchenko National University of Kyiv / Editorial board.: V.V. Il′chenko, Dr. Phys.-Math. Sc., Prof., (Head); and others. – К.: PPC "Kyiv University", 2022. – 159 pages (30-32 pages)
- Kyrylenko Anna STRATEGIES TO REDUCE THE IMPACT OF HUMAN FACTOR ON CYBER RESILIENCE / Ivan Parkhomenko, Anna Kyrylenko, Anastasiia Petrenko // “Problems of Cybersecurity of Information and Telecommunication Systems” (PCSITS): Collection of reports and abstracts; Kyiv city, 27 April 2023 year; Taras Shevchenko National University of Kyiv / Editorial board.: V.V. Il′chenko, Dr. Phys.-Math. Sc., Prof., (Head); and others. – К.: PPC "Kyiv University", 2023. – 166 pages (78-80 pages)