КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1194
УДК 004.72; 004.7

Сиротинський Роман Михайлович
Аспірант, асистент
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0009-0002-6280-3290
roman.m.syrotynskyi@lpnu.ua

Тишик Іван Ярославович
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

ЖИТТЄВИЙ ЦИКЛ ДОСТУПУ ДО МЕРЕЖІ: СТРУКТУРОВАНИЙ ПІДХІД ДО УПРАВЛІННЯ ПРАВИЛАМИ БРАНДМАУЕРА В СЕРЕДОВИЩІ НУЛЬОВОЇ ДОВІРИ

Анотація. У роботі розмірковується над наслідками безконтрольної конфігурації правил мережевого доступу в корпоративних мережах та розглядаються ризики до яких призводить їх хаотичне нагромадження. Для контролю та управління політиками безпеки та доступовими списками пропонується запровадження життєвого циклу мережевих доступів як єдиної методології створення, операційного супроводу та їх деактивації в корпоративній інфраструктурі. Передбачаються обов'язкові структурні етапи, послідовність та досліджується їхня методологія проведення. Зазначаються необхідні складові та атрибути кожного з етапів життя мережевого доступу Методологічну основу запропонованого підходу становить поєднання настанов щодо файрволів та їх політик, описаних в публікації NIST 800-41 rev. 1, принципів нульової довіри описаних в спеціальній публікації та NIST 800-207, та авторських методологій і практик організації процесу життя мережевого доступу та розроблення процедури його ресертифікації. Керований супровід народження, життя та завершення правил доступу в корпоративних мережевих середовищах це чіткий процес що дозволяє відстежувати та регулювати відкриті доступи в міжмережевих екранах, місця застосування списків доступу, безпекові групи та правила доступу в мережевих сутностях хмарних оточень на предмет їхньої актуальності в конкретний період часу та відповідності поставленими завданнями на етапі ініціації та принципам нульової довіри. В статті пропонується методологія проведення періодичного перегляду та валідації безпекових політик як основоположного етапу життєвого циклу мережевих доступів. Підхід включає алгоритм визначення періоду ресертифікації, структуру критеріїв оцінки правил а також визначає перелік потенційних рішень що приймаються щодо об'єктів перегляду. Описуються важливість застосування автоматизації при роботі з правилами доступу та визначаються переваги які вона приносить. Пропонується впровадження та застосування тегів як ефективного механізму структурування правил в великих середовищах. Наголошується на важливості дотримання конвенції імен при створенні політик безпеки в розподілених та гібридних інфраструктурах.

Ключові слова: політики безпеки, життєвий цикл, ресертифікація правил, мережевий файрвол, нульова довіра, контроль змін, визначення актуальності.

ВСТУП

Сучасний ландшафт кіберзагроз суттєво підвищує вимоги до влаштування безпекової моделі та архітектури побудови корпоративної інфраструктури. Дотримання рекомендацій поточних безпекових стандартів, галузевих практик та спеціальних публікацій призводить до побудови складних систем контролю доступу та громіздких конфігурацій міжмережевих екранів та інших сутностей, які забезпечують захищеність

інформаційних ресурсів та даних від несанкціонованого доступу. Потреба контролю та видимості кожного мережевого підключення в корпоративній інфраструктурі породжує значну кількість конфігурації списків доступу та політик файрволів, які описують та визначають цей доступ. При численних розподілених мережах, багаторічних конфігураціях і відсутності життєвого циклу доступів раніше ефективний контроль може перетворитися на непрозорий, дрейфуючий та ризикований "спагетті" код.

Постановка проблеми. Безконтрольна конфігурація правил, з роками призводить до негативних наслідків. Симптоми що щось "ламається" є наступні:

Розростання правил і дрейф політик. З роками правила накопичуються. Причиною є не лише логічний наслідок розбудови корпоративної інфраструктури, а й нагромадження дублікатів, конфліктних політик та тимчасових винятків, які створюються і ніколи не видаляються. Правила стають неконсистентними. Політики які мають бути однакові, наприклад в виробництві, в тест середовищі, в місцях підключення віддаленого доступу чи в хмарах стають різними через хаотичність їх модифікації. Зростає кількість "осиротілих" правил, а саме таких в яких немає власника чи відповідального, відсутні обґрунтування, строк дії. Ніхто не розуміє можливих ризиків при їх видаленні. Правила залишаються в системі з мотивами "щоб нічого не поламати".

Через надмірність конфігурації та утруднену навігацію зростає ймовірність появи "тіньових" правил. Можуть появлятися ненавмисні дозволи, де широке правило перекриває більш специфічну заборону знизу, чи навпаки.

Зростає ризик модифікації політик: кожна зміна в правилах є страшною: щоб "не зламати прод", приймаються та додаються усе ширші дозволи. Можуть з'являтися прогалини в спостереженні, спричинені неконтрольованими винятками. Наприклад: на "лише цьому" правилі немає журналювання чи інспекції; винятки в обхід TLS-розшифрування чи IPS стають постійними.

З'являються проблеми продуктивності та керованості: величезні набори правил сповільнюють коміти, збільшують затримку пошуку й досягають лімітів конфігураційних об'єктів в файрволі. Описані випадки призводять до низки ризиків, описаних в таблиці 1.

Таблиця 1

Ризики безконтрольного ведення безпекових політик

Безпекові ризики	- горизонтальне переміщення і зростання радіуса ураження - використання старих тимчасових доступів хакерами для організації атак - ризики витоку даних - обхід контролів через виключення та винятки - широкі повноваження на партнерських\екстранет підключеннях
Операційні ризики	- конфліктні allow/deny на різних хопах та асиметрія трафіку - деградація мережевих сервісів через запізнілі зміни та помилки в конфігурації - слабка реакція на інциденти
Регуляторні ризики	- провали аудитів - регуляторні санкції та атестаційні ризики - прогалини в криміналістиці
Ризики вартості та продуктивності	- неефективні платформи: великі набори політик збільшують навантажують CPU\RAM, час комітів і дистрибуцію правил - зростання витрат на операційне обслуговування - ризики затримки проєктів

Аналіз останніх досліджень і публікацій. Zero Trust Architecture (ZTA) базується на принципі “ніколи не довіряй, завжди перевіряй” і вимагає безперервної аутентифікації користувачів, пристроїв та процесів незалежно від їхнього місця в мережі. Це означає відмову від традиційних периметрових моделей безпеки на користь мікросегментації та детального контролю доступу [1]. Подібно, дослідження в IEEE Proceedings вказує, що Zero Trust перетворює концепцію довіри з географічної чи топологічної на динамічну, контекстну модель на основі ризиків [2].

Традиційні підходи до створення правил міжмережевих екранів часто не відповідають принципу найменших привілеїв, що ускладнює управління доступом і створює “бекдори” у корпоративних системах. Нові методики передбачають динамічне оновлення політик на основі контексту користувача та пристрою [3]. Інше дослідження розробляє узагальнену мову політик для опису правил міжмережевого екрану в Zero Trust мережах, з подальшим автоматичним відображенням цих правил у синтаксис конкретного файрвола [4].

Останні тенденції вказують на застосування машинного навчання для автоматизованого створення та оптимізації правил доступу. Наприклад, фреймворк ZT-SDN автоматично генерує правила доступу на основі аналізу мережевого трафіку, виявляючи дозволені транзакції між сутностями та адаптуючи політики до динамічних умов мережі [5]. Подібні підходи реалізовано у ZT-XPN, який дозволяє описувати мережеві політики у вигляді графів і автоматично компілює їх у програми для програмованих мережевих пристроїв [5].

Дослідження також підкреслюють, що фаза видалення або деактивації правил має бути автоматизована для запобігання накопиченню застарілих або конфліктних записів, як це описано у моделі Enhanced Zero Trust Implementation, яка пропонує відстеження відповідності політик протягом усього їхнього життєвого циклу. [6] Нарешті, для створення правил у Zero Trust середовищі важливо застосовувати мікросегментацію, де будь-який невідомий трафік автоматично блокується, а політики формуються за принципом позитивної безпеки – “дозволено лише те, що явно визначено” [7].

Сучасні підходи до життєвого циклу мережевих доступів у Zero Trust середовищах поєднують автоматизацію, машинне навчання, мікросегментацію та адаптивне управління ризиками. Ефективне управління правилами міжмережевих екранів передбачає постійний моніторинг, контекстну перевірку і гнучке оновлення політик, що забезпечує реалізацію принципів “найменших привілеїв” і “постійної перевірки” у кожній фазі життєвого циклу доступу.

Мета статті. Метою даної роботи є розгляд ризиків безконтрольної генерації правил міжмережевих екранів і списків контролю доступу та побудова процесу управління життєвим циклом мережевих доступів в корпоративних інфраструктурах. Зокрема: створення структури підходу, визначення кроків і послідовності, дослідження критеріїв ресертифікації правил та опис її можливих результатів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Життєвий цикл мережевого доступу – це керований, комплексний процес, що регулює всі життєві етапи мережевого доступу, а саме: як саме підключення запитується, проєктується, авторизується, впроваджується, моніториться, періодично повторно сертифікується й у підсумку виводиться з експлуатації відповідно до принципів найменших привілеїв і Zero Trust. Він забезпечує, щоб кожен потік – від

користувача до застосунку, між застосунками та між сервісами – мав задокументоване бізнес-обґрунтування, вимірювану ризик-позицію та безперервну верифікацію через журнали й атестації, запобігаючи накопиченню правил за принципом «додав і забув». На практиці цей життєвий цикл зменшує «сповзання» правил, прискорює відповідні вимогам зміни й забезпечує аудито-готові докази того, що доступ залишається необхідним, пропорційним і безпечним у часі. Якщо дотримуватися методології і робити все правильно – то це консистентний процес, а не підхід «додав правило й забув». На рисунку 1 зображені основні етапи циклу.

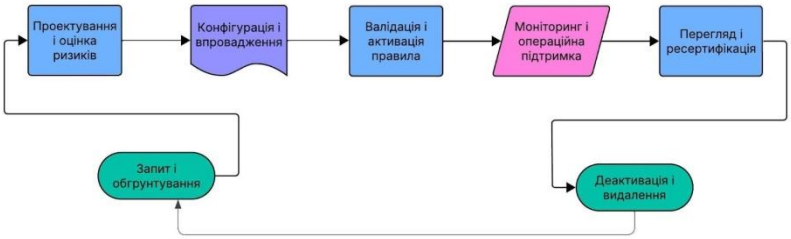

Рисунок 1. Структура життєвого циклу мережевого доступу

Початковим елементом життєвого циклу є народження доступу, а саме запит і обґрунтування. Зацікавлена сторона робить формальний запит на доступ в мережі. До запиту додаються опис необхідного доступу та документація рішення елементом якого запитаний доступ є. Правило з'являється лише у відповідь на документовану бізнес-потребу: хто/що має спілкуватися з чим, на яких портах/протоколах, для якої програми, хто є власником. Обов'язкові поля: бізнес-власник, технічний власник, мета, чутливість даних, середовище, очікуваний профіль трафіку, дата закінчення або дата перегляду. Часто реалізується як робочий процес в ITSM (ServiceNow тощо).

На наступному етапі проводяться проєктування та оцінка ризиків. Запит трансформується в політику. Застосовуються принципи найменших привілеїв, Zero Trust ("лише те, що потрібно, лише звідти, де довірено, лише коли виправдано"), мікросегментації та відповідності вимогам. Використовуються такі рішення як матриця "зона-до-зони", застосування груп/тегів, ідентичність користувача проти підмережі, App-ID проти портів, рівень журналювання, профіль інспекції тощо. Спроєктований доступ слід перевірити на конфлікти з глобальною політикою, наявними правилами та відомими загрозами.

По завершенню попереднього етапу слідує планування впровадження політик доступу на пристроях чи платформах. Конфігурація формується як стандартизовані об'єкти/шаблони, а не "сніжинки" на кожному пристрої. Для узгоджених правил у багатьох файрволах і хмарних середовищах ефективним заходом є використання автоматизації/оркестрації політик (Panorama, NSX-T, хмарні SG/NSG, Tufin/AlgoSec тощо). Важливими є дотримання конвенцій імен, в різних середовищах. Це дозволяє структурувати правила за певними ознаками що полегшує навігацію та фільтрування при різнорідних середовищах та великій кількості правил. До прикладу правила що описують доступ до конкретного сервісу можуть мати спільний префікс в назвах правил, однаково на усіх платформах. До запуску політики попередньо валідуються: симуляція зміни (де підтримується), пошук тіньових/дубльованих/надто широких правил, підтвердження, що зміна не ламає більш пріоритетні контролі. Процес розгортання відбувається через контрольовані процеси: управління змінами, квиток на впровадження чи протокол технічного обслуговування (МОР).

Після активації правило буде спостерігатися та модифікуватися за потреби. Фіксується зміна хіт каунтів, використовуються flow-журнали/NetFlow, події IDS/IPS, UEBA тощо. Перевіряється, що профіль трафіку відповідає обґрунтуванню (джерело, призначення, порти, обсяги, географія, користувачі). По результатах можливі наступні сценарії:

- звуження (якщо правило надто широке);
- реагування на інциденти (якщо зловживають);
- очищення (якщо не використовується);
- зміни не застосовуються (все працює як очікувано).

На даному етапі процес створення нового правила доступу завершується і конфігурація продовжує працювати в операційному режимі. Історично кількість правил зазвичай збільшується з часом та конфігурації мережевих пристроїв контролю доступу збільшуються в об’ємах і в складності.

Закінчення строку, виведення з експлуатації та очищення (завершення доступу). Коли застосунок виводиться або потреба зникає, правила проходять процедуру видалення. Ефективним є підхід попереднього вимкнення правил та короткого моніторингу перед видаленням конфігурації. Перевагами такого поетапного виводу з експлуатації є швидкий відкат до попереднього стану за необхідності а також додаткова видимість при аналізі чи повністю доступ був виведений з експлуатації, чи була ще якісь правила не дублюють його в іншому місці. Разом з правилами прибираються пов’язані об’єкти (групи, сервіси, адреси). Також видаляються тіньові політики, дублікати та модифікуються правила типу «any/any», щоб зменшити площу атаки й повністю вивести доступ з експлуатації.

Важливими складовими життєвого циклу правил доступу є аудит, метрики та безперервне вдосконалення. На всіх етапах повинна бути реєстрація подій та забезпечена повна відстежуваність. Хто замовив даний доступ, хто є його власником, хто ухвалював та впроваджував, що і коли змінено, з яких причин, журналювання та протокол переглядів. Цінними є метрики які відображають % правил із власником і обґрунтуванням, % із терміном дії / останнім переглядом більшим ніж якийсь визначений максимальний термін, кількість не вживаних чи надто широких правил. До операційної складової можна віднести метрику що відображає середній час реалізації змін.На основі цього відбувається постійне вдосконалення процесу і обґрунтовуються автоматизація чи рефакторинг.

Фундаментальним елементом життєвого циклу є періодичний перегляд та ресертифікація правил доступу. Метою даного етапу є забезпечення відповідності фактичних правил до актуальних бізнес задач, які можуть з часом змінюватися чи ставати неактуальними.

Протягом життя правило доступу виконує покладену на нього функцію. Набори правил міжмережевих екранів мають управлятися через формальний контроль змін і періодично переглядатись для забезпечення відповідності організаційній політиці та ризик-апетиту [8]. Щоб впевнитися що всі сконфігуровані доступи є актуальними, мають власника та все ще використовуються – застосовується механізм періодичного перегляду те ресертифікації правил мережевого доступу. Об’єктами перегляду є самі правила/політики, пов’язані об’єкти (адресні/сервісні групи, теги), залежні артефакти (NAT, маршрути, LB listeners), а також власники (business/tech owner) і терміни дії. Структура процесу перегляду та ресертифікації пропонується з кроків що відображені на рисунку 2.

Рисунок 2. Структура процесу перегляду та ресертифікації правил доступу

В залежності від особливостей кожного окремого правила доступу – оптимальним буде різна періодичність їх перегляду. Якщо всі правила переглядати занадто рідко – є шанс упустити невідповідність нормам на тривалий період часу. Короткий інтервал перегляду всіх корпоративних доступів вирішує попереднє питання але є трудоємким процесом що вимагає додаткових ресурсів на його проведення. Таким чином пропонується підхід класифікації правил для визначення оптимального періоду перегляду та ресертифікації. (див Таблиця 2). Для всіх правил застосовується автоматичне закінчення терміну дії – поле ReviewUntil/Expiry. Після завершення терміну дії застосовується автоматичне відключення доступу (з попередженням і grace-періодом).

Таблиця 2

Визначення періоду ресертифікації правил

Ризик	Особливості	Період перегляду
Високий	Комбінація з 2 і більше факторів: – чутливі дані – критична система – широкий доступ (any\any) – публікація в інтернет	3 місяці
Середній	Один з факторів: – чутливі дані – критична система – широкий доступ (any\any) – публікація в інтернет	6 місяців
Низький	Всі інші доступи	12 місяців

У більш динамічних IT-середовищах із частими змінами (наприклад, у хмарних або гібридних архітектурах) огляд правил рекомендується виконувати щоквартально або частіше, щоб упевнитися, що набір правил відповідає реальному трафіку та поточним загрозам [9].

На прийняття рішення при перегляді будуть впливати дані з наступних джерел:

– Логи використання: hits/bytes/5-ти перцентилі, сезонність, час останнього хіта.

– Мережеві флов-журнали: NetFlow/IPFIX, VPC Flow Logs, NSX, k8s network policy metrics.

– Ідентичність/CMDB: актуальні власники, стан застосунків (prod/dev/retired), класи даних.

– Сканери/аналітика: виявлення тіньових, дубльованих, надмірних правил; аналіз портів/протоколів.

– Відповідність: посилання на стандарти/контрольні вимоги для конкретної зони або сервісу.

Процес перегляду політик доступу починається з збору необхідних даних, а саме – правил, сформованих за критерієм «термін перегляду ≤ сьогодні» + високоризикові. Для кожного – витягуються метрики використання, власники, попередні рішення.

Для кожного правила яке проходить перегляд проводиться інформування та атестація його власника. А саме – задача, тікет чи лист наступного змісту: “Підтвердіть бізнес-необхідність, мінімальність, очікуваний профіль, термін дії, контактну особу”. Повідомлення доставляється завчасно перед кінцевою датою доступу з певним часом на опрацювання – наприклад 10 днів. Технічна валідація конфігурації правил здійснюється операційним інженером по мережах чи інформаційній безпеці. Тести та критерії валідації правил доступу можуть бути різними, один з збалансованих варіантів пропонується в таблиці 3.

Таблиця 3

Критерії оцінки правил мережевого доступу

Критерій	Варіанти визначення відповідності
Необхідність	– чи є чинне бізнес-обґрунтування? – чи є активний сервіс?
Мінімальність	– чи мінімальні джерела/призначення/порти/період ? – чи можна перейти на L7/app-ID/ID-based?
Використання	– чи проходив трафік за останні X днів ? – чи зберігається сезонний “візерунок” трафіку ?
Дублікати\тіні	– чи не перекривається іншим правилом вище? – чи не дублює об'єкти в конфігурації ?
Відповідність	– Чи потрібні і чи застосовуються: • інспекції • DLP/IPS профілі • geo-IP • TLS шифрування\розшифрування
Власність і термін	– чи призначені business+tech owner ? – чи встановлений ReviewUntil атрибут (час життя) ?
Журнали	– чи рівень логування відповідає ризику?
Док-слід	– чи вказаний номер квитка ? – чи є мапінг до сервісу/CMDB ?

Таким чином проводиться перехресна перевірка з логами, пошук альтернатив (заміна на app-ID, tag-based, service-mesh), виявлення надмірності. За результатами перегляду можуть бути прийняті рішення щодо мережевих доступів, їх особливості перелічені в таблиці 4

Таблиця 3

Варіанти рішень ресертифікації правил мережевого доступу

Рішення	Особливості
Підтверджено	– продовжити до нової дати – оновити власника/опис
Звузити	– замінити “/16, /24, /n” на список точних CIDR – зменшити діапазон портів – увімкнути app-ID/ID-based
Тимчасово продовжити	– всі винятки часово обмежені, з планом усунення – застосування додаткового моніторинг/алертів – для критичних винятків – підвищені контролі (детальні логи, IPS/SSL-inspection, geo-обмеження, rate-limits). – виняток без переатестації → автоматичне скасування.
Вимкнути/видалити	– Послідовність: – спочатку деактивація без видалення – спостереженя (напр. 7-14 днів) – видалення правила та залежних об'єктів

По прийняттю рішенння відбувається впровадження погоджених змін. Традиційно через процес “Change Management” згідно затвердженої процедури, або через автоматизований воркфлов якщо такий побудований. Для історії та аудиту важливо зберігати лінк на лог-висновки, рішення, власника та дату наступного перегляду. Також слід впевнитися що графіки та звіти що відображають статистику та метрики по обліку правил доступу коректно відобразили процес перегляду та нові дані.

Автоматизація та корисні патерни. В життєвому циклі мережевих доступів на різних етапах роботи з правилами як правило застосовуються якісь операційні підходи та практики, що приносять певну цінність. До таких відноситься автоматизація процесів та задач. Однією з важливих активностей в циклі є аналіз правил доступу на неактивність. Це процедура яка передбачає перегляд всіх політик і повинна виконуватися регулярно, що є гарним прикладом де автоматизація допомагає зменшити трудозатрати та знизити ризик людського фактору. Якщо протягом певного визначеного часу кількість спрацювань політики є рівна нулю – це означає що з певних причин наданий доступ не використовується і в цілях безпеки правило можна деактивувати. Такі автоматично вимкнуті доступи потребують додаткової уваги та моніторингу ще певний час, щоб впевнитись що деактивація не несе якихось деструктивних змін сервісу що використовує даний доступ. Щоб пересвідчитися що деактивоване правило більше не використовується та не чекати на ймовірні скарги власника доступу – пропонується практику тимчасової зміни дії правила з permit to deny та додаткове логування/сигналізація проходження трафіку як альтернатива видаленню. Таким чином забезпечується відключення потенційно неактуальних доступів та вводиться елемент моніторингу для спостереження та валідації. Також є поширені практики автоматизованого аудиту і безперервної перевірки відповідності, що дозволяють постійно оцінювати ризики правил файрволу, мінімізуючи ручну участь адміністраторів [10]. У великих інфраструктурах, зазвичай, використовують мультивендорні платформи на кшталт AlgoSec, Tufin, FireMon, Skybox Security та RedSeal. Якщо стек більш однорідний, доречні “рідні” інструменти – Palo Alto Networks (BPA/Strata Cloud Manager), Check Point (Compliance Blade), Cisco Secure FMC та Fortinet FortiManager/Analyzer.

Використання тегів в правилах доступу дозволяє категоризувати правила, здійснювати навігацію та використовувати в автоматизованих сценаріях. Обов’язково тегувати правила з винятками та тимчасові правила. Записи з тегом temporary, migration, vendor-X отримують коротший цикл перегляду і авто-нагадування. Механізм тегів також буде в нагоді щоб прокатегоризувати доступи згідно їхньої критичності, як запропоновано в таблиці 1 та здійснювати навігацію і вибірку при роботі з правилами.

В корпоративних інфраструктурах точки застосування політики розміщуються в різних місцях і побудовані на різних платформах. Доцільним є дотримання одного шаблону правил та спільної конвенції імен для об'єктів що використовуються в політиках безпеки та розміщуються на on-prem FW, cloud SG/NSG, k8s network policies, egress-controls. Застосування уніфікації дозволяє полегшити труднощі пов'язані з інтерпретацією політик доступу та їх елементів написаних в різному форматі і як наслідок знижує затрачений час при аналізі доступів чи пошуку неполадок з доступом.

Дослідження зручності використання показали, що однією з головних проблем керування правилами брандмауера є когнітивне перевантаження через великі та складні набори правил. Організація правил у позначені групи або категорії може значно покращити керованість, особливо на етапах створення, перевірки та припинення підтримки правил [11].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведене дослідження демонструє, що впровадження керованого життєвого циклу правил мережевого доступу (FRLM) є ключовим чинником зменшення площі атаки, підвищення операційної керованості та відповідності нормативним вимогам. Емпіричний аналіз організації з великою кількістю міжмережевих екранів і гібридною інфраструктурою показав, що формалізація етапів «запит → проєктування/оцінка ризику → впровадження → моніторинг → періодичний перегляд/ресертифікація → виведення з експлуатації» забезпечує відчутне зниження «правил-спадків» (legacy), дублювань і тіньових дозволів. У типових сценаріях застосування FRLM призводить до

1) скорочення кількості неактуальних або невикористовуваних правил,

2) підвищення частки доступів, реалізованих за принципами найменших привілеїв та застосування політик з визначенням ідентичності та аплікацій (ID/App-ID),

3) покращення прозорості аудиту завдяки повній трасовності рішень, власників і строків перегляду.

Кількісні ефекти, отримані під час дослідження на репрезентативному випадку, засвідчили:

(а) зниження загальної кількості правил на 20–30% без втрати функціональності сервісів завдяки консолідації, дефрагментації об’єктів і вилученню дозволів які не використовуються;

(б) зменшення середнього часу впровадження змін (Mean Time to Implement) на 20–40% через стандартизацію шаблонів і оркестрацію політик;

(в) підвищення частки правил із чинним власником, бізнес-обґрунтуванням і датою повторної атестації до 90%+, що корелює зі скороченням інцидентів, пов’язаних із надмірними правами або помилковими конфігураціями доступу. Додатково спостерігається покращення якості телеметрії (повнота логів, корисність метрик «hits/bytes/seasonality») та зростання точності ризик-оцінювання під час чергових переглядів. Практична цінність FRLM проявляється в уніфікації політик між on-prem та хмарними середовищами, у запровадженні time-bounded винятків (auto-expiry) і в можливості data-driven прийняття рішень щодо звуження доступів.

Водночас виявлені обмеження та виклики включають потребу в культурі спільної відповідальності (business owner ↔ tech owner ↔ SecOps/NetOps), необхідність інтеграції FRLM з CMDB/ITSM та журналами трафіку, а також первинні витрати на стандартизацію об’єктів і автоматизацію. Стратегічним напрямом подальших робіт є розширення Policy-as-Code, валідацій «what-if» і використання машинного навчання для рекомендацій щодо мінімізації доступів з урахуванням сезонності навантажень, а також уніфікація контролів для Kubernetes, сервіс-мешів і керованих хмарних сервісів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підсумовуючи, результати дослідження підтверджують, що FRLM є ефективним механізмом зниження ризиків і складності/громіздкості конфігурації корпоративних мережевих політик, підвищує прогнозованість змін і якість аудиту, а також створює основу для ZeroTrust – консистентного управління доступами. Запровадження FRLM у великих інфраструктурах доцільно вважати не опційною практикою, а базовою операційною дисципліною, що забезпечує довготривалу кіберстійкість і відповідність бізнес-цілям.

Перспективами подальших досліджень є дослідження ефективності застосування моделей штучного інтелекту для аналізу великих масивів правил в процесі FRLM.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ejiofor, O., Olusoga, O., & Akinsola, A. (2025). Zero trust architecture: A paradigm shift in network security. *Computer Science & IT Research Journal*. https://doi.org/10.51594/csitrj.v6i3.1871
2. Poirrier, A., Cailleux, L., & Clausen, T. (2025). Is trust misplaced? A zero-trust survey. *Proceedings of the IEEE, 113*, 5–39. https://doi.org/10.1109/JPROC.2025.3555131
3. Syrotynskyi, R., & Tyshyk, I. (2025). Features of network access management of corporate systems in zero trust architecture. *Computer Systems and Networks*. https://doi.org/10.23939/csn2025.01.261
4. Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). Access control policy enforcement for zero-trust networking. In *2018 29th Irish Signals and Systems Conference (ISSC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISSC.2018.8585365
5. Katsis, C., & Bertino, E. (2024). ZT-SDN: An ML-powered zero-trust architecture for software-defined networks. *ACM Transactions on Privacy and Security, 28*, 1–35. https://doi.org/10.1145/3712262
6. Bradatsch, L., Miroshkin, O., & Kargl, F. (2023). ZTSFC: A service function chaining-enabled zero trust architecture. *IEEE Access, 11*, 125307–125327. https://doi.org/10.1109/ACCESS.2023.3330706
7. Keeriyattil, S. (2019). Microsegmentation and zero trust: Introduction. In *Zero trust networks with VMware NSX* (pp. xx–xx). Springer. https://doi.org/10.1007/978-1-4842-5431-8_2
8. National Institute of Standards and Technology. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Rev. 1). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf
9. Palo Alto Networks. (2024). *Firewall best practices: Managing security policies effectively.* https://www.paloaltonetworks.com/cyberpedia/firewall-best-practices
10. Ruleblade. (2024). *Firewall risk and compliance automation.* https://ruleblade.io/en/firewall-risk
11. Voronkov, A., Martucci, L., & Lindskog, S. (2020). Measuring the usability of firewall rule sets. *IEEE Access, 8*, 27106–27121. https://doi.org/10.1109/ACCESS.2020.2971093

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Roman Syrotynskyi
Postgraduate student, assistant at the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0002-6280-3290
roman.m.syrotynskyi@lpnu.ua

Ivan Tyshyk
PhD, Associate Professor at the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

NETWORK ACCESS LIFECYCLE: A STRUCTURED APPROACH TO FIREWALL RULE GOVERNANCE IN ZERO TRUST ENVIRONMENTS

Abstract. This paper reflects on the consequences of uncontrolled network access rule configurations within corporate networks and examines the risks resulting from their chaotic accumulation. To monitor and manage security policies and access control lists (ACLs), the introduction of a network access lifecycle is proposed as a unified methodology for the creation, operational support, and deactivation of access rights within corporate infrastructure. The study outlines mandatory structural stages and their sequence, investigating the methodology for their implementation while specifying the necessary components and attributes for each stage of the network access lifecycle. The methodological foundation of the proposed approach consists of a combination of firewall and policy guidelines described in NIST SP 800-41 rev. 1, Zero Trust principles outlined in NIST SP 800-207, and original authorial methodologies for organizing the access lifecycle and developing recertification procedures. Managed support for the "birth," life, and termination of access rules in corporate network environments is a distinct process. It allows for the tracking and regulation of open ports in firewalls, ACL application points, security groups, and access rules in cloud network entities to ensure their relevance at any given time, compliance with initial requirements, and adherence to Zero Trust principles. The article proposes a methodology for conducting periodic reviews and recertification of security policies as a fundamental stage of the network access lifecycle. The approach includes an algorithm for determining recertification periods, a structural framework for evaluation criteria and rule validation, and a defined list of potential decisions regarding the objects under review. The importance of automation in managing access rules is described, alongside the specific benefits it provides. The implementation of tagging is proposed as an effective mechanism for structuring rules in large-scale environments. Furthermore, the paper emphasizes the necessity of following a naming convention when creating security policies in distributed and hybrid infrastructures.

Keywords: security policies, lifecycle, rule recertification, network firewall, Zero Trust, change control, relevance assessment.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ejiofor, O., Olusoga, O., & Akinsola, A. (2025). Zero trust architecture: A paradigm shift in network security. *Computer Science & IT Research Journal*. https://doi.org/10.51594/csitrj.v6i3.1871
2. Poirrier, A., Cailleux, L., & Clausen, T. (2025). Is trust misplaced? A zero-trust survey. *Proceedings of the IEEE, 113*, 5–39. https://doi.org/10.1109/JPROC.2025.3555131
3. Syrotynskyi, R., & Tyshyk, I. (2025). Features of network access management of corporate systems in zero trust architecture. *Computer Systems and Networks*. https://doi.org/10.23939/csn2025.01.261
4. Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). Access control policy enforcement for zero-trust networking. In *2018 29th Irish Signals and Systems Conference (ISSC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISSC.2018.8585365
5. Katsis, C., & Bertino, E. (2024). ZT-SDN: An ML-powered zero-trust architecture for software-defined networks. *ACM Transactions on Privacy and Security, 28*, 1–35. https://doi.org/10.1145/3712262
6. Bradatsch, L., Miroshkin, O., & Kargl, F. (2023). ZTSFC: A service function chaining-enabled zero trust architecture. *IEEE Access, 11*, 125307–125327. https://doi.org/10.1109/ACCESS.2023.3330706

7. Keeriyattil, S. (2019). Microsegmentation and zero trust: Introduction. In *Zero trust networks with VMware NSX* (pp. xx–xx). Springer. https://doi.org/10.1007/978-1-4842-5431-8_2
8. National Institute of Standards and Technology. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Rev. 1). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf
9. Palo Alto Networks. (2024). *Firewall best practices: Managing security policies effectively.* https://www.paloaltonetworks.com/cyberpedia/firewall-best-practices
10. Ruleblade. (2024). *Firewall risk and compliance automation.* https://ruleblade.io/en/firewall-risk
11. Voronkov, A., Martucci, L., & Lindskog, S. (2020). Measuring the usability of firewall rule sets. *IEEE Access, 8*, 27106–27121. https://doi.org/10.1109/ACCESS.2020.2971093

Отримано редакцією журналу / Received: 14.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 26.03.26