COMPUTER SYSTEMS AND NETWORKS

Vol. 7, No. 2, 2025

DOI: https://doi.org/10.23939/csn2025.02.193

УДК 621.3

ОПТИМІЗАЦІЯ УПРАВЛІННЯ ПОЛІТИКАМИ ФАЙРВОЛІВ В МІКРОСЕГМЕНТОВАНИХ МЕРЕЖАХ

Р. М. Сиротинський, І. Я. Тишик

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: roman.m.syrotynskyi@lpnu.ua, ivan.y.tyshyk@lpnu.ua

Проаналізовано задачі та виклики щодо управління складними корпоративними мережами, які виникають під час міграції моделі периметральної безпеки до архітектури нульової довіри. Встановлено, що нехтування ними може призвести як до зниження якості сервісів у мікросегментованій мережевій інфраструктурі, так і до підвищення ризиків, пов'язаних із надмірним ускладненням правил в брандмауерах.

Оптимізація набору правил файрволів є важливим аспектом управління безпекою мережі, особливо в середовищах, які використовують архітектуру нульової довіри (ZTA) та мікросегментацію. Розглянуто стратегії оптимізації розгортання та адміністрування політик доступу з акцентом на автоматизацію та ефективність. Проаналізовано основні сценарії доступу до інформаційних ресурсів в корпоративних мережах та обговорюється актуальність впровадження автоматизації зі застосуванням інструментів на кшталт Ansible, Rundeck чи Terraform, що спрощує початкове розгортання конфігурацій у мікросегментованих структурах. Також запропоновано шаблон для автоматичної чи напівавтоматичної генерації правил та наведені сценарії його застосування.

Розглянуто ключові безпекові виклики, які виникають під час експлуатації мереж із дотриманням принципів нульової довіри. Запропоновано підходи щодо ефективного управління масивами правил файрволів, включно з їх узагальненням та життєвим циклом, нові механізми впровадження динамічних політик доступу. Встановлено, що запропоновані рішення сприяють зменшенню надмірності конфігураційних даних мережевих екранів, зниженню загалом операційного навантаження на команду адміністраторів, скороченню поверхні потенційних атак і, як наслідок, підвищенню продуктивності корпоративної мережі.

Ключові слова: мікросегментація, політики безпеки, файрвол, оптимізація, автоматизація, структуризація мережі.

Вступ

В архітектурі нульової довіри (ZTA) правила (або політики) файрволів відіграють фундаментальну роль у забезпеченні суворого, детального контролю доступу між усіма мережевими об'єктами, заснованого на принципі "ніколи не довіряй, завжди перевіряй". На відміну від традиційної безпеки на основі периметра ZTA перевіряє всі під'єднання всередині мережі та потребує постійної верифікації атрибутів користувача, пристрою й контексту, перш ніж дозволити будь-який зв'язок. У цьому випадку правила брандмауерів гарантують, що між сегментованими зонами, застосунками чи

сервісами передаватиметься лише санкціонований трафік. Це робить їх невід'ємним елементом мікросегментації, обмежуючи горизонтальний рух, а отже, знижуючи ймовірність виникнення інцидентів.

Керування правилами файрволів в контексті архітектури нульової довіри (ZTA) створює низку операційних та технічних проблем, які значно перевищують ті, що виникають у традиційних моделях безпеки на основі периметра. Одним з основних викликів, притаманних архітектурі Zero Trust, є стрімке зростання кількості правил та їх ускладнення через високу деталізацію контролю доступу між усіма об'єктами, включаючи користувацькі підключення, пристрої та сервери. Потенційне значне збільшення кількості політик безпеки, яке часто називають "вибухом правил", може ускладнити налаштування операційних середовищ, обслуговування обладнання та їх перевірку. Зі зростанням масштабу мікросегментації зростає ймовірність виникнення перекриття політик, конфліктів та надмірностей, що потенційно може призвести до ненавмисних дозволів на доступ або перебоїв у роботі послуг.

Ще однією критичною проблемою є необхідність контекстного та динамічного застосування політик. На відміну від статичних наборів правил політики ZTA часто залежать від таких атрибутів, як ідентифікація користувача, стан пристрою, геолокація та оцінка ризиків у режимі реального часу. Щоб файрволи могли оцінювати ці фактори, потрібна інтеграція з різноманітними зовнішніми системами, зокрема платформами керування ідентифікацією та доступом (IAM), інструментами виявлення та реагування на кінцеві точки (EDR), системами контролю доступу до мережі (NAC), рішеннями для управління інформацією та подіями безпеки (SIEM). Такі інтеграції збільшують складність системи і потребують високої сумісності та координації в гетерогенних середовищах.

З операційного погляду постійна потреба в оновленні політики відповідно до змін у мережі, додатках чи організаційній структурі створює значне адміністративне навантаження. За відсутності автоматизації та централізованого керування політиками зростає ймовірність помилкових конфігурацій, що може спричинити нові вразливості. У гібридних інфраструктурних середовищах, які охоплюють локальні центри обробки даних та певну кількість хмарних провайдерів, забезпечення послідовного та уніфікованого застосування правил брандмауерів ускладнюється через відмінності моделей політик постачальників. Крім того, в середовищах Zero Trust часто відсутній ефективний моніторинг, аудит безпекових політик та ведення системного журналу, що є важливим з погляду забезпечення безпеки. Без повного контролю трафіку та моніторингу політик файрволів ускладнюється виявлення аномалій, перевірка коректності доступу й демонстрація відповідності вимогам безпеки. Ситуацію погіршує нестача фахівців, здатних проєктувати та підтримувати складні, контекстно-залежні політики доступу.

Загалом усе це підкреслює необхідність впровадження системних підходів, таких як фреймворки "політика як код", автоматизоване управління життєвим циклом правил та використання уніфікованих платформ щодо контролю політик. Подані рішення здатні забезпечити масштабоване, надійне та ефективне управління правилами міжмережевих екранів у середовищах Zero Trust.

Мета статті полягає у розробленні алгоритмів та підходів для підвищення ефективності контролю мережевого доступу засобами файрволів шляхом оптимізації, автоматизації, впровадження контекстних і динамічних перевірок та регламентації життєвого циклу правил, що сприятиме реалізації принципів нульової довіри.

Огляд літературних джерел

Як вже було сказано, впровадження архітектури нульової довіри (Zero Trust Architecture, ZTA) потребує переходу від парадигми периметральної безпеки до моделі постійної перевірки, де керівним принципом є "ніколи не довіряй, завжди перевіряй" [1]. У цій моделі процес керування політиками міжмережевих екранів значно ускладнюється, оскільки вони мають забезпечувати детальний, контекстно-орієнтований контроль доступу в умовах мікросегментованого середовища. Дослідження показують, що інтеграція файрволів нового покоління (Next-Generation Firewalls, NGFW) із принци-

пами ZTA здатні формувати ефективні, стійкі до сучасних кіберзагроз та постійно оновлюванні механізми захисту, де ключову роль відіграють сегментація мережі та реалізація принципу найменших привілеїв [2].

Стратегії оптимізації правил дедалі більше зосереджені на автоматизації та абстрагуванні політик. Наприклад, автори у [3] пропонують універсальну мову політик файрвола для вираження високорівневих правил безпеки, які автоматично перетворюються на синтаксис, специфічний для конкретного постачальника, що дає змогу забезпечити узгоджене виконання у розподілених системах. У дослідженні [4] автори пропонують застосовувати механізми детальнішого моніторингу відповідності для ефективного керування великою кількістю політик безпеки в середовищах ZTA.

Ще одним із перспективних напрямів оптимізації безпекових механізмів ZTA є децентралізована реалізація політик, яка переносить частину процесів прийняття рішень із центральних контролерів на локальні точки виконання, що зменшує затримки та підвищує стійкість системи до різноманітних кіберзагроз [5]. Крім того, інтелектуальні адаптивні архітектури файрволів здатні підвищити ефективність керування політиками, забезпечуючи динамічне формування правил у відповідь на аномалії чи зміни трафіку. Автори у [6] зазначають, що такі адаптивні рішення покращують масштабованість у розподілених і гетерогенних середовищах.

Постановка задачі

Перехід на архітектуру нульової довіри передбачає впровадження контролю доступу практично на усі комунікації та під'єднання в мережевій інфраструктурі організації. Мікросегментація мережі та забезпечення безпеки її об'єктів з дотриманням принципів нульової довіри потребує опису всіх мережевих з'єднань та забезпечення їх контролю правилами файрволів. Перехід на архітектуру нульової довіри суттєво збільшує навантаження на технічний персонал, який обслуговує мережеву інфраструктуру організації. Якщо операційні можливості команди не зростають пропорційно вимогам, виникає ймовірність компромісів у сфері безпеки з метою балансування між наявними ресурсами та потребами, що може суперечити базовим принципам нульової довіри.

Зважаючи на сказане, основною задачею дослідження є розроблення підходів оптимізації управління мережевим доступом для пониження операційного навантаження на технічний персонал, скорочення ландшафту кіберзагроз, пов'язаних із надлишковими або неактуальними мережевими доступами, а також підвищення ефективності управління політиками безпеки у мікросегментованих мережах з дотриманням принципів нульової довіри.

Основні розділи дослідження

Перебування в середині довіреного сегмента мережі більше не є ознакою довіри та не надає індульгенції на перевірку легітимності запиту під час мережевого під'єднання до будь-якого іншого вузла. Впровадження мікросегментації суттєво збільшує кількість точок забезпечення дотримання політик. Якісна мікросегментація потрібна для поділу мережевих доменів на дрібні сегменти. Отримана топологія мережі значно утруднює горизонтальні переміщення по усій інформаційній інфраструктурі.

Локалізація скомпрометованого сегмента узгоджується з концепцією нульової довіри, згідно з якою побудова мережевої інфраструктури вже передбачає наявність несанкціонованого вторгнення. Отож засоби протидії та механізми контролю застосовуються постійно й безперервно. Такий підхід дає змогу толерувати можливі точкові компрометації та обмежувати їхнє поширення.

Недоліком впровадження мікросегментації у корпоративній мережі з тотальним інспектуванням мережевого трафіку є потреба у мережевих з'єднаннях на межі кожного мікросегмента та створення необхідних безпекових політик для їх контролю, що потребує значних ресурсних затрат та операційних навантажень, пов'язаних з обслуговуванням мережевих доступів та файрволів. Дослідження показують, що постійна перевірка усіх з'єднань в архітектурі ZTA та забезпечення політик контролю доступу для кожного з них, може призвести до значних часових затримок та збільшити апаратурні витрати. Причому навіть застосування оптимізованих рішень призводять до

помітного споживання ресурсів, хоча часові затримки збільшуються незначно [7]. Значні обсяги набору правил та постійні оновлення політик збільшують навантаження і на адміністраторів в архітектурі ZTA з мінімальними засобами автоматизації. Також впровадження та підтримка безперервного моніторингу, постійного ідентифікаційно-орієнтованого контролю доступу, розроблення стратегій мікросегментації потребують значних організаційних зусиль [8].

На практиці це призведе до значних витрат на аналіз потоків даних та налаштування політик безпеки для кожного легітимного підключення в мережі на етапі міграції до архітектури нульової довіри. Додатково зберігається високе операційне навантаження, зумовлене необхідністю постійного управління великою кількістю правил файрволів. Це та ситуація, де з трьох можливих якостей виконання поставлених задач можливі лише дві:

Якісно і швидко – не дешево

Якісно і дешево – не швидко

Швидко і дешево – не якісно

У першому випадку виконання задач інфраструктурою супроводжуватиметься додатковими витратами, у другому випадку буде знижуватися якість наданих інфраструктурою мережевих послуг. Третій випадок характеризуватиметься можливими безпековими прогалинами, внаслідок чого не вдасться досягнути того рівня захисту, який очікується від архітектури нульової довіри.

Використання високорівневих описів політик безпеки та автоматичної генерації правил файрвола знижує складність управління і підвищує відповідність корпоративним вимогам безпеки. Такий підхід допомагає уникати людських помилок і забезпечує узгоджене застосування правил на кількох брандмауерах [9]. Оптимізація управління мережевими доступами без зниження рівня захищеності в мікросегментованій мережі дає змогу підвищити ефективність адміністрування, скоротити витрати на обслуговування та зменшити поверхню атаки, оскільки усуваються надлишкові й застарілі правила, які можуть залишити небажані відкриті доступи. Такі підходи також пришвидшують первинне налаштування корпоративних файрволів і підвищують ефективність подальшого операційного супроводу мережевої інфраструктури.

Мережі в інформаційних інфраструктурах здебільшого гетерогенні. Ступінь гетерогенності залежить від виду діяльності компанії, її розмірів та інших індивідуальних факторів. Така різнорідність ускладнює процес автоматизації. Проте є низка сервісів, вузлів та елементів комп'ютерних мереж, які трапляються практично в кожній мережі. Саме на них буде робитися акцент під час пошуку алгоритмів напівавтоматичного розгортання політик безпеки міжмережевих екранів.

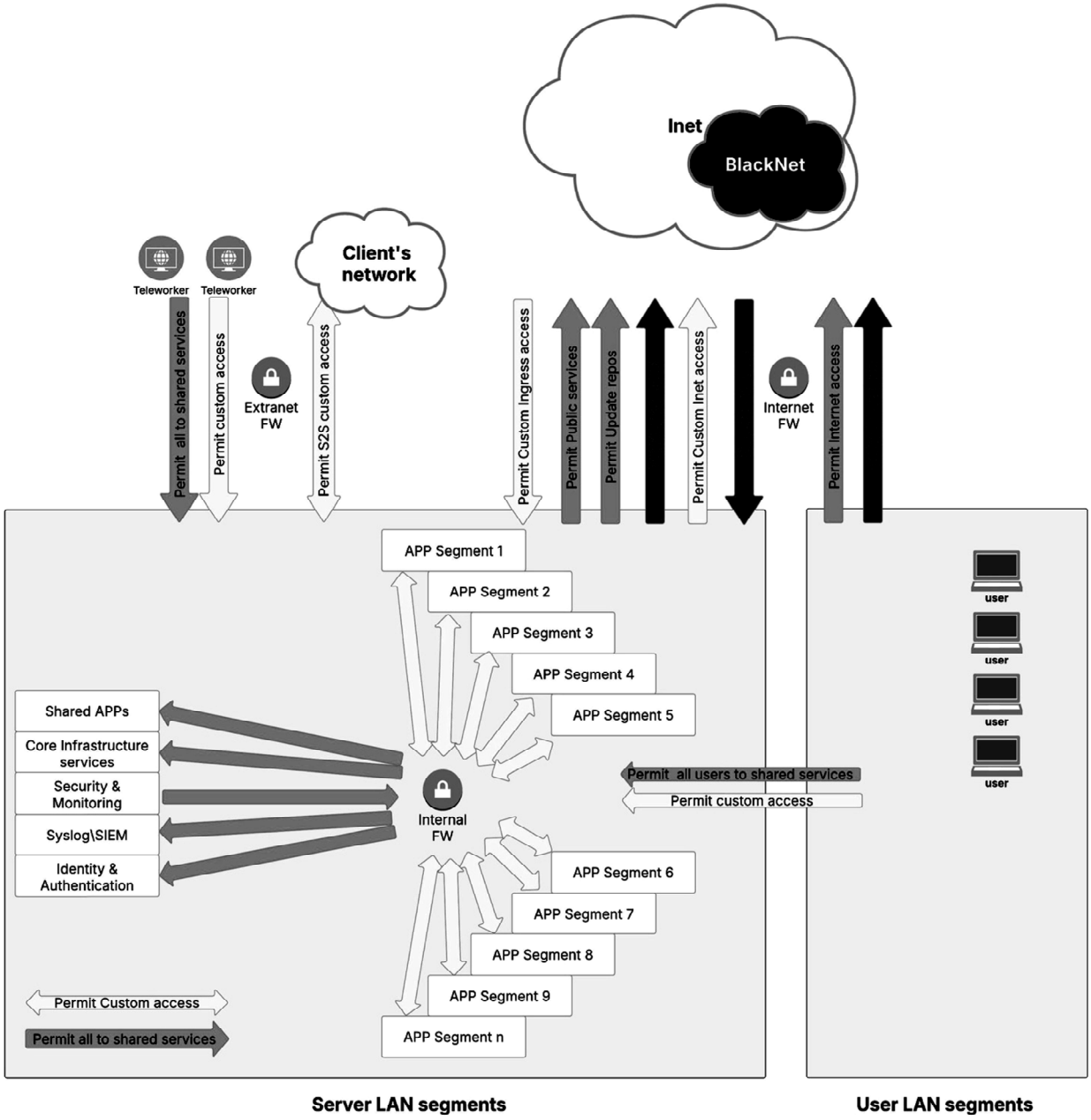
З погляду формування політик безпеки, мережу можна поділити на сегменти, які контролюватимуть файрволи різного призначення. Зазвичай розглядають три основні ролі, характерні для більшості мереж. У невеликих інфраструктурах ці ролі можуть співіснувати на одному пристрої, тоді як у великих – поділятися за виконуваними функціями та масштабуватися відповідно до потреб. Наприклад, можуть бути такі рольові поділи:

- Інтернет-файрвол;
- Екстранет-файрвол;
- Внутрішній файрвол.

Інтернет-брандмауер фільтрує трафік з внутрішніх мереж в інтернет і навпаки, а також обслуговує демілітаризовані зони. Екстранет брандмауер зазвичай розгортається для захисту та контролю трафіку між корпоративною мережею та зовнішніми, довіреними мережами третіх сторін.

Внутрішній міжмережевий екран виконує задачі фільтрації трафіку між мікросегметами корпоративної мережі, які можна назвати внутрішніми мережами.

Хоча в мікросегментованих мережах різниця між типами сегментами, як і між ролями файрволів, часто розмивається, для кращого сприйняття можна умовно виокремити принаймні три категорії доступу. Кожна з них має характерні типові сценарії, які є у більшості мережевих інфраструктур. Автоматизація налаштування правил для кожної категорії такого доступу є доцільною та дасть змогу суттєво підвищити ефективність управління корпоративною мережею.



Структура мережевих доступів в корпоративній мережі

Доступи, які контролює інтернет-файрвол, можна поділити на такі категорії:

– Індивідуальний вхідний доступ. Може надаватися сервісам, розміщеним в демілітаризованій зоні, для надання публічних послуг зовнішнім користувачам.

– Індивідуальний вихідний доступ в інтернет для корпоративних сервісів та аплікацій. Згідно з ідеологією нульової довіри, вихідний доступ важливо контролювати для зменшення ймовірності витоку даних та протидії складним загрозам.

– Доступ до інтернету для користувачів може надаватися за замовчуванням, за умови, що вони розміщені у відділених від аплікацій сегментах мережі та мають обмежений горизонтальних трафік.

– Заборона на вхідний та вихідний доступи для адрес з поганою репутацією. Гарною практикою є інтеграція брандмауерів з постачальниками інформації про загрози та щоденні поновлення списків недовірених IP-адрес та доменів.

– Доступ до загальновживаних зовнішніх аплікацій та сервісів.
– Доступ до репозиторіїв обновлення операційних систем та додатків.

Серед перелічених категорій доступів перші дві є індивідуальними для корпоративних інфраструктур різних компаній і зазвичай не повторюються. Їх доцільно налаштовувати вручну та супроводжувати в межах життєвого циклу правил файрволів. Автоматизація у цьому випадку не знижує операційне навантаження на технічну команду, оскільки витрати на її розробку та впровадження будуть співмірними зі створенням правил в ручному режимі.

Натомість контроль доступу користувачів до інтернету, блокування небажаних ресурсів, а також відкриття доступу до поширених зовнішніх застосунків і репозиторіїв є завданням, яке виконується майже у кожній корпоративній мережі. Такі правила можна згрупувати, а також створити пакетом. У великих інфраструктурах таке подання дасть змогу суттєво зменшити зусилля на їх первинне налаштування.

Окрему роль відіграє внутрішній міжмережевий екран, який контролює процеси між сегментами мережі. Він забезпечує контроль доступу користувачів до внутрішніх застосунків і найважливіше – регулює взаємодію між самими застосунками. Такий контроль знижує ризик нелегітимного горизонтального переміщення у випадку компрометації окремої ділянки системи. Специфіка цих доступів переважно унікальна та залежить від діяльності компанії. Водночас, як і у випадку з інтернет-файрволом, існують спільні сервіси, якими користуються всі або більшість вузлів мережі. Автоматизація створення політик брандмауерів для доступу до таких сервісів дає змогу скоротити витрати на їх первинну генерацію. До них можна зарахувати такі категорії доступу:

– Спільні аплікації.
– Сервіси основної інфраструктури.
– Безпека та моніторинг.
– Системний журнал та SIEM.
– Ідентифікація та автентифікація.

На рисунку зображена організація корпоративних файрволів та категорії доступу, які реалізуються ними в мережевій інфраструктурі. Доступи, що позначені зеленим та червоним кольорами, відображають спільні правила, які надаються для усіх сегментів мережі. Такі правила можна створювати масово з використанням підходів автоматичного або напівавтоматичного створення.

Кожен сегмент мікросегментованої мережі являє собою індивідуальний VLAN другого рівня моделі OSI, також subnet мережі третього рівня та індивідуальні інтерефейс та інтерфейсна зона. Вхідний та вихідний доступ регулюється набором політик безпеки між зоною файрвола, яка належить цьому сегменту мережі, та іншими зонами.

Типовий набір правил для кожного сегмента мережі є набором політик, які надають мінімальний доступ на конкретні напрямки чи вузли мережі. Використання умов типу “any” має строго регулюватися або не використовуватися (за змоги) взагалі. Однакові та періодично повторювальні політики варто шаблонізувати.

Генерація політик за шаблонами дає змогу автоматизувати процес їх поширення за допомогою інструментів на кшталт Ansible. Натомість індивідуальні політики доцільно створювати вручну після ретельного їх аналізу, з поетапним погодженням і тестуванням, щоб гарантувати високу точність і відповідність корпоративним стандартам безпеки.

Глобально структура шаблона для генерації політик міжмережевого екрана складатиметься з трьох частин:

1. Метадані (тип шаблона, сценарій, інше).
2. Опис змінних вхідних даних.
3. Текст конфігурації політик.

Шаблон може бути написаний на YAML, оскільки його легко використовувати в Terraform, Ansible або власному API-скрипті, але та сама структура чисто конвертується в JSON або CSV, якщо утиліта імпорту вибраного файрвола надає перевагу саме цим форматам. Для прикладу створимо фрагмент шаблона для генерації політик, необхідних під час додавання нового мережевого сегмента.

```
# new-segment-zta.yml
# Template for bulk creation of NGFW rules for new network segment
# ──────────────────────────────────────────
meta:
  policy_set: new-segment-zta
  description: >  create new network   version: "1.2"
  last_review: "2025-06-15"

# ── 1. Global variables ──────────────
vars:
  # Core infrastructure
  dns_servers:    [10.10.0.10, 10.10.0.11]
  ntp_servers:    [10.10.0.20]
  ad_dc:          [10.20.0.10, 10.20.0.11]
  pki_ocsp_crl:   ["ocsp.pki.company.com", "crl.pki.company.com"]

  # Security / monitoring
  siem_collector: [10.30.0.50]
  flow_collector: [10.30.0.60]

  # Patch / config
  wsus_servers:   [10.40.0.5]
  linux_repos:    ["mirror.company.com"]
  config_master:  [10.50.0.10]

# ── 2. Re-usable service objects ─────
services:
  dns:  { proto: tcp_udp, ports: 53 }
  ntp:  { proto: udp,     ports: 123 }
  ldap: { proto: tcp_udp, ports: [88,389,636,3268,3269] }
  radius: { proto: udp, ports: [1812,1813] }
  syslog: { proto: tcp_udp, ports: [514,6514] }
  ssh: { proto: tcp, ports: 22 }
  https: { proto: tcp, ports: 443 }
  snmp: { proto: udp, ports: [161,162] }
  # ...

# ── 3. Rule blocks  (order matters!) ──────────────
# <SRC_ZONE>, <DST_ZONE>,
# <SRC_ADDR>, <DST_ADDR> are
# placeholders that pipeline substitutes
# with the real zones/subnets for each
# micro-segment.
# rules:
  # 3.1 Core infrastructure
  - name: allow-dns
    src_zone: "<SRC_ZONE>"
    dst_zone: "<DST_ZONE>"
    src_addr: "${segment_address}"
    dst_addr: "${dns_servers}"
    service:  dns
    action:   allow
    log:      session-end
    tags:     [baseline, dns]

  - name: allow-ntp
    src_zone: "<SRC_ZONE>"
    dst_zone: "<DST_ZONE>"
    src_addr: "${segment_address}"
    dst_addr: "${ntp_servers}"
    service:  ntp
    action:   allow
    log:      session-end
    tags:     [baseline, ntp]

  # 3.2 Security & monitoring
  - name: send-syslog
    src_zone: "<SRC_ZONE>"
    dst_zone: "<DST_ZONE>"
    src_addr: "${segment_address}"
    dst_addr: "${siem_collector}"
    service:  syslog
    action:   allow
    log:      session-start     # high-volume: log only start
    tags:     [baseline, logging]

  - name: send-netflow
    src_zone: "<SRC_ZONE>"
    dst_zone: "<DST_ZONE>"
    src_addr: "${segment_address}"
    dst_addr: "${flow_collector}"
    service:  { proto: udp, ports: [2055,4739,9995] }
    action:   allow
    log:      disable
    tags:     [baseline, flow]

  # 3.3 Patch & config management
  - name: wsus-updates
    src_zone: "<SRC_ZONE>"
```

```
  dst_zone: "<DST_ZONE>"
  src_addr: "${segment_address}"
  dst_addr: "${wsus_servers}"
  service:  https
  action:   allow
  tags:     [baseline, patch]

- name: linux-repos
  src_zone: "<SRC_ZONE>"
  dst_zone: "<DST_ZONE>"
  src_addr: "${segment_address}"
  dst_addr: "${linux_repos}"
  service:  https
  action:   allow
  tags:     [baseline, patch]


# 3.4 Egress control (proxy break-out pattern)
- name: web-proxy-egress
  src_zone: "<SRC_ZONE>"
  dst_zone: "<DST_ZONE>"
  src_addr: "${segment_address}"
  dst_addr: "${proxy_ip1}"
  service:  https
  action:   allow
  tags:     [baseline, egress]

# 3.5 Operations / management plane
- name: netops-ssh
  src_addr: "${netops_jump}"
  dst_addr: "${segment_address}"
  src_zone: "<SRC_ZONE>"
  dst_zone: "<SEG_ZONE>"
  service:  ssh
  action:   allow
  tags:     [baseline, ops]

- name: snmp-polling
  src_addr: "${nms}"
  dst_addr: "${segment_address}"
  src_zone: "<SRC_ZONE>"
  dst_zone: "<SEG_ZONE>"
  service:  snmp
  action:   allow
  tags:     [baseline, ops]

# 3.6 Catch-all deny (implicit)
- name: deny-all
  src_zone: "<SEG_ZONE>"
  dst_zone: any
  service: any
  action: deny
  log: session-end
  tags: [implicit-deny]

# ── 4. Defaults for new micro-segments
──────────

defaults:
  log_setting: "traffic-log"
  inspection_profile: "full-threat-prevention"
  schedule: "24x7"
```

Продемонстрований підхід дає змогу швидко розгорнути набір стандартних правил для контролю доступу одного сегмента мережі. Інша частина доступів буде індивідуальною та створюватися вручну. Застосувавши цикли та ускладнивши логіку, можна генерувати конфігурацію для багатьох сегментів одночасно.

Описаний шаблон орієнтований на генерацію доступів до різних корпоративних сервісів для одного або декількох новостворених сегментів мережі. Залежно від типу мережевого сегмента може бути різний набір необхідних політик. Застосування тегів забезпечує координацію необхідного набору політик для мікросегментів різного призначення (залежно від аплікації чи хоста, який послуговується цим сегментом).

З іншого боку, генерацію правил можна організувати не лише для мережевого сегмента, а й для загальнодоступного сервісу. У такому випадку логіка формування правил доступу ґрунтується на описі однієї політики для певного сервісу та визначенні переліку сегментів, до яких ця політика застосовуватиметься. Отож для кожного корпоративного сервісу можна сформувати окремий шаблон. Поданий підхід дає змогу збалансувати індивідуальний доступ і автоматичну генерацію наборів стандартних правил та є особливо зручним під час налаштування доступу до нового сервісу у вже побудованій інфраструктурі. Шаблон може використовуватися для створення коду політик з подальшим ручним завантаженням їх на групу файрволів. Також можна автоматично вносити згенеровані політики безпосередньо в конфігурацію брандмауерів через налаштоване підключення.

Для застосування шаблонів конфігурації політик безпеки доцільно використати зв'язку Ansible + Rundeck. Ansible реалізує концепцію політики як коду "policy as code"; а Rundeck – безпечної оркестрації з самообслуговуванням. Разом вони перетворюють ручні зміни в конфігурації політик безпеки з клік-операцій на повторювані, схвалені та аудитовані завдання, які будь-хто в NOC/SOC може виконувати без прямого SSH-підключення. Рішення може також мати графічний інтерфейс для введення параметрів і запуску сценаріїв, що підвищує зручність використання.

Завдяки цьому зменшується операційне навантаження, пов'язане зі створенням і налаштуванням нових правил у мікросегментованих мережах. Водночас варто зазначити, що формування нових політик є лише однією з переліку задач щодо управління мережевим доступом, яка потребує оптимізації, особливо у великих, розгалужених інфраструктурах.

Сучасні корпоративні мережі характеризуються безперервним зростанням кількості файрволів і правил. Стандарти кібербезпеки вимагають контролювати та логувати кожне підключення, уникаючи надмірно загальних правил на кшталт "any-to-any allow". Повний гранулярний контроль знижує ризики, але водночас створює значне навантаження на операційні команди, що може призводити до затримок у впровадженні доступів або стимулювати відкриття надмірних дозволів задля спрощення роботи.

Одним із базових методів оптимізації є групування однотипних правил і заміна їх загальними. Водночас узагальнення не має розширювати доступ порівняно з початковим набором. Допускається об'єднання правил, які відрізняються лише одним атрибутом (наприклад, джерелом, адресою призначення, сервісом чи застосунком). Якщо у правилах різняться два чи більше атрибути, результатом може стати небажаний надлишковий доступ. Описана ситуація продемонстрована у табл. 1.

Таблиця 1

Rule name	**source**	**destination**	**service**	**application**	**action**
Dns for host A	192.168.1.1	10.10.10.10	Tcp53, udp53	dns	allow
DNS for host B	192.168.10.5	10.10.10.10	Tcp53, udp53	dns	allow
DNS for host C	192.168.13.4	10.10.10.10	Tcp53, udp53	dns	allow
==========	==========	==========	==========	========	=====
DNS for hosts A,B,C	192.168.1.1, 192.168.10.5, 192.168.13.4	10.10.10.10	Tcp53, udp53	dns	allow

Отож три хости A, B і C отримують лише необхідний доступ, аналогічний наданому в індивідуальних правилах. Ситуація 2, де групування застосовано до правил, в яких є відмінності в двох атрибутах. Опис правил у табл. 2.

Таблиця 2

Rule name	**source**	**destination**	**service**	**application**	**action**
SSH to host A	172.16.20.0/24	192.168.1.1	tcp22	any	allow
SSH to host B	172.16.20.0/24	192.168.10.5	tcp22	any	allow
WEB to host C	172.16.20.0/24	192.168.13.4	tcp443	any	allow
==========	==========	==========	======	========	=====
DNS and WEB to hosts A,B,C	172.16.20.0/24	192.168.1.1 192.168.10.5 192.168.13.4	Tcp22, tcp443	any	allow

У розглянутому випадку групування правил з відмінностями у двох і більше атрибутах призводить до відкриття перехресного (надлишкового) доступу, що не відповідає принципам нульової довіри та збільшує поверхню атаки. З табл. 2 видно, що згруповане правило відкриває доступ, який був раніше відсутній, а саме: мережа 172.16.20.0/24 отримує доступ за tcp443 до хостів A та B, а також доступ за tcp22 до хоста C.

Групування політик доступу, попри перевагу в оптимізації кількості правил, має певні недоліки. Такі правила менш зручні у випадку потреби деактивації доступу, оскільки їх необхідно редагувати, а не просто видаляти. Також знижується прозорість використання: якщо трафік проходить хоча б до одного хоста або сервісу з групи, правило вважається активним, навіть якщо решта доступів не використовується. У результаті ускладнюється виявлення застарілих або непотрібних доступів.

Попри ці недоліки, групування політик доцільне там, де надмірна деталізація правил не впливає на рівень безпеки, а лише призводить до збільшення кількості правил і ускладнює їхнє адміністрування. Узагальнені правила часто створюють після аналізу поведінки трафіку у тих сегментах, де немає потреби у надмірній гранулярності.

Надлишкові правила файрволів є додатковим джерелом операційного навантаження. Зазвичай це дублікати доступів, які не використовуються, бо спрацьовує перше за пріоритетом правило. Їхня поява часто пов’язана з людським фактором: повторними заявками на доступ без перевірки вже наявних правил. Систематичний аудит політик та впровадження життєвого циклу мережевих доступів допомагають контролювати ситуацію.

У розподілених інфраструктурах брандмауери нерідко з’єднуються послідовно, що може призвести до виникнення надлишкових правил на різних рівнях. Для блокування небажаних мережевих підключень достатньо застосувати правило *deny* або *drop* на найближчому до джерела цих підключень файрволі; дублювати його далі в ланцюжку зазвичай немає сенсу.

Окремою проблемою є забезпечення контролю доступу до хостів з динамічними IP-адресами і інтернет-середовищі. Потрібно взяти до уваги, що сучасні аплікації та хмарні платформи можуть налічувати більше тисячі IP-адрес на кожен сервіс, які постійно змінюються, а провайдери безпекових послуг оновлюють чорні списки практично в реальному часі. Для роботи з такими об’ємними та динамічними списками доцільно застосовувати динамічні політики. Вони дають змогу автоматично оновлювати елементи політик за допомогою *IP feeds* або *API*. Наприклад, корпоративний SIEM може передавати у файрвол список IP-адрес із SoC, а IP-адреси зовнішніх сервісів можуть зчитуватися прямо з їхніх офіційних ресурсів. Отож динамічні політики завжди забезпечуватимуть актуальний список необхідних для контролю доступу IP-адрес з мінімальними затратами на обслуговування.

Важливо враховувати, що значна частина правил корпоративних файрволів залишається неактивною, тобто через які не проходить трафік. За результатами досліджень, від 30 % до 50 % правил у корпоративних мережах (зокрема, у середовищах Zero Trust) не використовуються протягом тривалого часового періоду: або вони ніколи не застосовувалися, або втратили актуальність через тривалу відсутність мережевого трафіку [10, 11].

Невикористані або застарілі правила брандмауера не лише ускладнюють конфігурацію, але, як підтверджують численні дослідження, створюють конкретні операційні ризики та загрози безпеці як у корпоративних мережах, так і в середовищах Zero Trust:

– Збільшена поверхня атаки. Застарілі правила можуть діяти як приховані лазівки в мережу, обходячи обмеження Zero Trust [12].

– Погіршення продуктивності. Кожен пакет перевіряється послідовно за всіма правилами. Дослідження показують, що велика кількість невикористаних правил може призводити до помітної затримки, особливо в шлюзах з великим трафіком [13].

– Операційна складність та витрати. Великі й заплутані набори правил уповільнюють аудит, усунення несправностей і контроль змін. Адміністратори в одному дослідженні юзабіліті повідомляли про “когнітивне перевантаження” під час перегляду наборів правил з великою кількістю застарілих записів, що сповільнювало реагування на інциденти [14].

– Підвищений ризик помилкових налаштувань. Застарілі правила можуть конфліктувати з новими, викликаючи небажані блокування доступу або дозволяючи несанкціоновані з'єднання (проблеми затінення та надлишковості правил). У дослідженні виявлення аномалій до 40 % правил у деяких робочих файрволах були надлишковими або конфліктними, що безпосередньо сприяло порушенням політик доступу.

– Проблеми з відповідністю вимогам (compliance). Регуляторні стандарти (наприклад, PCI DSS, ISO 27001) потребують періодичного перегляду та видалення непотрібних правил доступу.

– Невикористані правила можуть стати причиною негативних результатів аудиту, що призведе до витрат на виправлення або штрафів.

Вирішенням проблеми неактивних правил є запровадження процедур регулярного аудиту. Періодичний огляд дає змогу своєчасно видаляти неактуальні або зайві записи, скорочувати їхню кількість, а також виявляти й виправляти допущені під час створення правил помилки.

Важливим аспектом є оптимізація правил та їх структурування у міжмережевих екранах або у відповідних системах централізованого керування, наприклад PaloAlto Panorama. Це дає змогу підвищити як продуктивність обладнання, так і покращити ефективність адміністрування доступу, що особливо актуально, коли кількість правил сягає декілька тисяч чи більше. Для покращення якості управління доцільно поділити правила за категоріями доступу: внутрішній чи зовнішній (інтернет), стандартний чи індивідуальний, а також за належністю до конкретного сегмента мережі чи сервісу.

Також важливо знайти баланс між структурованістю правил та частотою їх використання. Якщо ресурси файрвола дозволяють, правила доцільно впорядковувати за типом доступу, що спрощує адміністрування і знижує ризик помилок. У випадках, коли порядок розташування правил впливає на продуктивність, доцільно розміщувати найчастіше використовувані правила зверху, а навігацію по категоріях організовувати за допомогою тегів і метаданих.

Одним з фундаментальних підходів ефективного управління мережевим доступом є впровадження життєвого циклу правил брандмауерів, окремі етапи якого можуть бути автоматизовані. Автоматизація дає змогу уникнути практики "записав та забув", забезпечуючи чітке призначення кожного правила, визначаючи термін його дії та автоматично видаляючи після втрати актуальності. Це призводить до зменшення людських помилок та перевантаження політик. Основними елементами автоматизованого управління життєвим циклом правил є їх тегування метаданими, автоматичне видалення після завершення строку дії, інтеграція з іншими корпоративними системами, моніторинг числа спрацювань, виявлення неактивності та інше. Запровадження життєвого циклу правил файрвола дає змогу оптимізувати та систематизувати операційне обслуговування мережевих доступів та підвищити ефективність брандмауерів в мікросегментованих мережах.

Результати дослідження

Результатами дослідження є запропонована методологія керування мережевим доступом в мікросегментованих мережах з дотриманням принципів нульової довіри. Дослідження показало, що, попри індивідуальність мережевих інфраструктур, здебільшого можна виокремити певні категорії доступу, які є спільними та повторювальними в мікросегментах. Запропоновано підхід автоматизованого генерування політик доступу, який дасть змогу скоротити операційні затрати та пришвидшить розгортання нових сегментів мережі в архітектурі нульової довіри. Запропоновано ефективні способи управління мережевим доступом та шляхи оптимізації правил міжмережевих екранів в мікросегментованих мережах без пониження безпекового рівня та відхилення від принципів нульової довіри, а саме:

– Сумаризація гранулярних правил.
– Оптимізація правил за послідовних файрволів.
– Методи управління мережевим доступом до або від динамічних середовищ.
– Робота з надлишковими та неактивними правилами.
– Управління правилами із застосуванням життєвого циклу мережевих доступів.
– Структуризація політик безпеки в міжмережевих екранах.

Застосування прийомів ефективного управління мережевими доступами в інформаційних мережах знижує час впровадження політик доступу під час первинного налаштування або впровадження додаткових загальнодоступних сервісів, зменшує кількість політик брандмауерів, знижує витрати на операційне обслуговування мікросегментованих мереж, а також скорочує поверхню атаки на корпоративну інфраструктуру з використанням доступів у надлишкових правилах.

Вирівнювання потреб операційного обслуговування з можливостями технічного персоналу зменшує ризик відходу від принципів нульової довіри через неспроможність якісного управління громіздкими наборами політик міжмережевих екранів.

Висновки

Досліджено критичні стратегії оптимізації правил файрволів у контексті архітектури нульової довіри (ZTA) та мікросегментованих мереж. Показано, що оптимізація правил відіграє ключову роль не лише щодо підвищення рівня безпеки мережі, але й у покращенні її продуктивності, зменшенні адміністративних витрат та забезпеченні масштабованості у складних середовищах.

Особлива увага приділяється автоматизованому розгортанню правил, яке є визначальним фактором ефективного управління конфігураціями брандмауерів, зокрема під час впровадження мікросегментації. Використання інструментів на зразок Ansible, Terraform та Open Policy Agent (OPA) дає змогу автоматизувати процеси створення, розгортання та оновлення правил, що не лише пришвидшує адміністрування, а й знижує ризик людських помилок, забезпечує узгодженість конфігурацій та сприяє кращій інтеграції з динамічною природою сучасних мереж.

Після початкового розгортання правил брандмауерів основний акцент робиться на постійній їх оптимізації. Тут ключовою стратегією є групування подібних правил для зменшення надмірностей, що спрощує конфігурацію. Політики на основі динамічних списків доступу дають змогу правилам брандмауерів адаптовуватися до змінних мережевих середовищ без потреби постійного ручного оновлення. Крім того, чітко визначений життєвий цикл правил файрволів допомагає забезпечити своєчасне систематичне видалення або зміну застарілих, надлишкових чи невикористаних правил, запобігаючи їх накопиченню, що може призвести до погіршення продуктивності мережі та поставити під загрозу її безпеку.

Зрештою, ефективна оптимізація правил міжмережевих екранів потребує комплексного підходу, який поєднує автоматизацію, постійний перегляд правил та динамічне застосування політик. Використовуючи подані підходи, організації можуть зменшити кількість правил файрволів, підвищити операційну ефективність та мінімізувати ризик помилок, забезпечуючи високий рівень безпеки в межах принципів нульової довіри.

Список літератури

1. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero Trust Architecture. DOI: https://doi.org/10.6028/nist.sp.800-207-draft.

2. Sarkorn, T., & Chimmanee, K. (2024). Review on Zero Trust Architecture Apply In Enterprise Next Generation Firewall. 2024 8th International Conference on Information Technology (InCIT), 255–260. DOI: https://doi.org/10.1109/incit63192.2024.10810611.

3. Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). Access Control Policy Enforcement for Zero-Trust-Networking. 2018 29th Irish Signals and Systems Conference (ISSC), 1–6. DOI: https://doi.org/10.1109/ISSC.2018.8585365.

4. Gokhale, A., & Kulkarni, S. (2024). Enhanced Zero Trust Implementation - A Novel Approach for Effective Network Policy Management and Compliance Tracking. International Journal for Research in Applied Science and Engineering Technology. DOI: https://doi.org/10.22214/ijraset.2024.58201.

5. Creutz, L., & Dartmann, G. (2023). Decentralized Policy Enforcement in Zero Trust Architectures. 2023 IEEE Future Networks World Forum (FNWF), 1–6. DOI: https://doi.org/10.1109/FNWF58287.2023.10520563.

6. Santis, A., Castiglione, A., Fiore, U., & Palmieri, F. (2011). An intelligent security architecture for distributed firewalling environments. Journal of Ambient Intelligence and Humanized Computing, 4, 223–234. DOI: https://doi.org/10.1007/s12652-011-0069-8.

7. Benzaïd, C., Guerd, N., Rehouma, N., Zeraoulia, K., & Taleb, T. (2025). A Multi-Layered Zero Trust Microsegmentation Solution for Cloud-Native 5G & Beyond Networks. 2025 IEEE Wireless Communications and Networking Conference (WCNC), 1–7. DOI: https://doi.org/10.1109/WCNC61545.2025.10978671.

8. Karanam, R. (2024). Zero Trust Architecture in DevSecOps: Enhancing Security in Cloud-Native Environments. International Journal for Research in Applied Science and Engineering Technology. DOI: https://doi.org/10.22214/ijraset.2024.64045.

9. Zaborovsky, V., & Titov, A. (2009). Specialized Solutions for Improvement of Firewall Performance and Conformity to Security Policy. 603–608.

10. Zarina, D., Safawati, W., Hafiz, M., & Syafiqa, M. (2018). Firewall Redundancy Rules Filtering Using Integrity Rules Checking. Advanced Science Letters, 24, 7451–7454. DOI: https://doi.org/10.1166/ASL.2018.12957.

11. Golnabi, K., Min, R., Khan, L., & Al-Shaer, E. (2006). Analysis of Firewall Policy Rules Using Data Mining Techniques. 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006, 305–315. DOI: https://doi.org/10.1109/NOMS.2006.1687561.

12. Syrotynskyi, R., & Tyshyk, I. (2025). FEATURES OF NETWORK ACCESS MANAGEMENT OF CORPORATE SYSTEMS IN ZERO TRUST ARCHITECTURE. CSN, 2025, Computer systems and network, Volume 7, Number 1, pp. 261–271. DOI: https://doi.org/10.23939/csn2025.01.261.

13. Golnabi, K., Min, R., Khan, L., & Al-Shaer, E. (2006). Analysis of Firewall Policy Rules Using Data Mining Techniques. 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006, 305–315. DOI: https://doi.org/10.1109/NOMS.2006.1687561.

14. Voronkov, A., Martucci, L., & Lindskog, S. (2020). Measuring the Usability of Firewall Rule Sets. IEEE Access, 8, 27106–27121. DOI: https://doi.org/10.1109/ACCESS.2020.2971093.

OPTIMIZING FIREWALL POLICY MANAGEMENT IN MICROSEGMENTED NETWORKS

R. M. Syrotynskyi, I. Y. Tyshyk

Lviv Polytechnic National University,
Department of Information Protection

The article analyzes the tasks and challenges of managing complex corporate networks that arise during the migration from a perimeter-based security model to a Zero Trust Architecture (ZTA). It is established that neglecting these issues may lead both to a decline in service quality within microsegmented network infrastructures and to increased risks associated with the excessive complexity of firewall rules.

Firewall rule set optimization is identified as a crucial aspect of network security management, particularly in environments that implement Zero Trust Architecture and microsegmentation. Strategies for optimizing the deployment and administration of access policies are examined, with a focus on automation and efficiency. The paper analyzes the main scenarios of access to information resources in corporate networks and discusses the relevance of automation using tools such as Ansible, Rundeck, or Terraform, which simplify the initial deployment of configurations in microsegmented environments. A template for automatic or semi-automatic rule generation is also proposed, along with examples of its application.

The article further considers key security challenges that arise when operating networks in accordance with Zero Trust principles. Approaches are proposed for effective management of large firewall rule sets, including rule generalization and lifecycle management, as well as new mechanisms for implementing dynamic access policies. It is determined that the proposed solutions contribute to reducing firewall configuration redundancy, lowering the overall operational burden on administrator teams, minimizing the potential attack surface, and consequently improving corporate network performance.

Keywords: microsegmentation, security policies, firewall, optimization, automation, network structuring.