КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1013
УДК 004.76 004.7

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

# КОНТЕКСТНО ОРІЄНТОВАНИЙ ПІДХІД ОРГАНІЗАЦІЇ МЕРЕЖЕВИХ ПОЛІТИК БЕЗПЕКИ В АРХІТЕКТУРІ НУЛЬОВОЇ ДОВІРИ

**Анотація.** Актуальність залучення нових підходів та практик організації та контролю доступу в мережевих інфраструктурах обґрунтовується зростанням прірви між вимогами сучасних безпекових стандартів та можливостями засобів організації мережевої безпеки які працюють на 3-4 рівнях OSI моделі. У роботі аналізуються рекомендовані сучасними безпековими вимогами та галузевими практиками принципи побудови моделей безпеки в інформаційних інфраструктурах та досліджуються їхні шляхи реалізації з використанням доступних на ринку засобів та заходів контролю мережевого доступу. Методологічну основу запропонованого підходу становить поєднання принципів нульової довіри описаних в спеціальній публікації NIST 800-207, інструментів доступних в портфоліо виробників сучасних міжмережевих екранів нового покоління та авторських методологій і практик поєднання безпекових систем різного призначення для формування та насичення контекстом мережевого доступу політик безпеки файрволів. Запропонований підхід дозволяє забезпечити відповідність принципам нульової довіри та підтримувати операційну якість і високу продуктивність роботи мережевої інфраструктури не виходячи за межі допустимої собівартості обслуговування та володіння інфраструктурних ресурсів. Визначені ключові елементи та підходи організації безпекової інфраструктури, необхідні для досягнення поставлених цілей. Наукова новизна запропонованого підходу полягає в зміні парадигми контролю мережевого доступу від моделі контролю адреси вузла корпоративної мережі до моделі контролю доступу користувача та перевірки відповідності безпекового стану пристрою з якого здійснюється запит. Запропоновані контекстні атрибути для політик безпеки та оптимальні методи організації рівнів доступу вузла в конфігурації міжмережевих екранів. Практика збору та насичення мережевим контекстом точок забезпечення дотримання політик безпеки надає гнучкість та технічну можливість які необхідні для дотримання принципів нульової довіри при побудові безпекової моделі корпоративної інфраструктури. Недоліками методу є складність операційної підтримки, підвищена вартість, а також залежність від інших систем що може впливати на продуктивність мережевої інфраструктуру та розширювати ландшафт компрометації самого безпекового комплексу.

**Ключові слова**: контекст мережевого доступу, брандмауер нового покоління, нульова довіра, зіставлення ідентифікатора користувача, стан мережевого вузла, динамічна адресна група.

## ВСТУП

У сучасних умовах стрімкого розвитку кіберзагроз традиційна модель периметральної безпеки втрачає свою ефективність. Використання хмарних сервісів, мобільних робочих місць та взаємопов’язаних корпоративних мереж зумовлює те, що будь-яка довіра всередині мережі стає суттєвим ризиком. Для подолання цих викликів організації впроваджують архітектуру нульової довіри (Zero Trust Architecture, ZTA) — модель безпеки, що відмовляється від концепції «довірених зон» і базується на принципі «ніколи не довіряй, завжди перевіряй».

Ключову роль у реалізації принципів ZTA відіграють засоби контролю доступу до мережі та політики файрволів. Якщо раніше файрволи ґрунтувалися переважно на аналізі IP-адрес, портів і протоколів прикладних служб, то нині вони здебільшого є критичними точками прийняття рішень щодо надання доступу в умовах мікросегментації. У моделі нульової довіри політики файрволів не можуть залишатися статичними: вони повинні динамічно адаптуватися відповідно до ідентичності користувача, стану пристрою, рівня чутливості робочих навантажень та інших контекстуальних факторів.

У цій парадигмі особливого значення набувають контекстні політики у файрволах нового покоління (Next-Generation Firewalls, NGFW). Вони виходять за межі статичних правил, інтегруючи у процес прийняття рішень такі атрибути, як роль користувача, рівень безпеки пристрою, географічне розташування, тип застосунку та навіть поведінкові показники. Завдяки використанню контексту сучасні NGFW забезпечують вищу деталізацію, гнучкість і зменшення ризиків, пов’язаних із надмірно дозволяючими чи застарілими правилами. Контекстуальні політики стають необхідною умовою збереження балансу між безпекою та зручністю в масштабних, розподілених і гібридних інфраструктурах.

Проте розширення функціоналу файрволів заради можливостей моніторингу та перевірки контекстів мережевого доступу приносить нові виклики та завдання, пов'язані з додатковими залежностями, технологічними складностями, суттєвим операційним навантаженням, а також кібербезпековими ризиками.

**Аналіз останніх досліджень і публікацій.** Дотримання принципів архітектури Zero Trust (ZTA) зумовлює потребу використання складніших методів та засобів управління мережевим трафіком. Дослідники відзначають обмеження статичних політик доступу в умовах сучасних хмарних і розподілених середовищ. Такі механізми не здатні адаптуватися до змін у поведінці користувача або стані пристрою, що створює необхідність у більш динамічному та детальному контролі доступу. [1] Контекстно-орієнтований контроль доступу дозволяє впроваджувати адаптивні політики, засновані на оцінці ризику в реальному часі, часто з використанням телеметрії з платформ ідентифікації та безпеки [2-5].

Новітні архітектурні підходи показують, як контекстні дані можуть інтегруватися у ZTA. Наприклад, Routray і Bera (2025) запропонували Zero Trust Adaptive Authorization Architecture (ZTAAC), яка застосовує шифрування на основі атрибутів (CP-ABE), дозволяючи доступ лише за наявності правильного поєднання статичних і динамічних атрибутів, таких як стан пристрою, місцезнаходження користувача та поведінкові шаблони. [6]

У схожому напрямку Ahmadi (2025) представив модель автономного сегментування загроз, яка використовує машинне навчання для аналізу шаблонів входу, типу пристрою, геолокації та часу доступу, щоб призначити динамічні рівні ризику. На основі цих даних система автоматично регулює дозволи доступу, мінімізуючи внутрішні загрози та переміщення атак всередині мережі.[7]

Практичні реалізації контекстно-орієнтованих підходів до ZTA демонструються в корпоративних середовищах. Наприклад, у хмарному середовищі .NET було реалізовано політики умовного доступу з використанням Azure AD і OAuth 2.0, які враховують ідентичність користувача, відповідність пристрою політикам безпеки та місцезнаходження. Ці політики адаптуються до загроз у реальному часі завдяки інтеграції з телеметрією безпекових платформ.[8]

В умовах федеративних систем контекст збирається з багатьох джерел даних. У моделі Zero Trust Federation (ZTF), запропонованій автором Hirai та іншими, реалізовано

механізм централізованого збору контексту (Context Aggregation Point, CAP) з таких джерел, як RADIUS і MDM. Це дозволяє приймати більш точні рішення щодо доступу на основі агрегованого контексту.[9]

Інтеграція штучного інтелекту в архітектуру Zero Trust дає змогу реалізувати більш гнучке управління доступом. Наприклад, Oluoha і Odeshina запропонували AI-фреймворк для безперервного управління доступом (Continuous Access Governance), який аналізує поведінкові шаблони, довіру до пристрою та ризики сеансу, автоматизуючи управління ролями та перевірки прав доступу згідно з вимогами GDPR і NIST.[10]

Щоб систематизувати знання у сфері контекстної безпеки, Xiao та співавтори провели комплексне дослідження, що демонструє точки перетину між контекстно-орієнтованими, ризик-орієнтованими та Zero Trust-політиками. Автори стверджують, що використання динамічних атрибутів, як-от місцезнаходження користувача, поведінка або стан пристрою, значно покращує точність контролю доступу.[11]

Водночас залишаються певні виклики. Інтеграція контекстної перевірки в застарілі системи потребує значних архітектурних змін та уніфікації джерел даних.[12] Також виникають питання конфіденційності, пов’язані зі збором поведінкових і екологічних даних, які можуть призводити до помилкових спрацьовувань або зниження користувацького досвіду.

**Проблематика дослідження.** Традиційні системи контролю доступу до мережі історично ґрунтувалися на статичних правилах файрволів, які визначаються з урахуванням IP-адрес, а також TCP/UDP-портів протоколів відповідних служб. Такий підхід дозволяє реалізувати базову сегментацію трафіку, однак у сучасних масштабних і динамічних корпоративних мережах це є вже недостатньо. У контексті архітектури нульової довіри (ZTA) статичні правила створюють низку обмежень: вони є надто загальними, не забезпечують достатньої гнучкості й часто призводять до надмірних повноважень на доступ. Це формує ризик неконтрольованого поширення надмірного доступу до критично важливих ресурсів, а також ускладнює підтримку безпеки у середовищі, де користувачі, пристрої й сервіси динамічно змінюють параметри взаємодії.

**Мета роботи:** Метою цієї статті є дослідження ролі контекстних політик файрволів та особливостей їхнього застосування у межах архітектури нульової довіри. Зокрема, для посилення контролю доступу будуть розглянуті типи додаткових атрибутів політик безпеки, технології, які дозволяють збирати та інтегрувати ці дані у роботу NGFW, а також стратегії і підходи щодо управління контекстними правилами та їх оптимізації у масштабованих мережевих середовищах.

## ОСНОВНА ЧАСТИНА

Традиційно мережевий доступ описується такими полями як айпі адреси, протокол, порт та дія: дозволити чи заборонити. Такий спосіб регуляції мережевого доступу працює здебільшого на 3 та 4 рівнях OSI моделі та в дійсності дозволяє певний доступ не конкретному хосту чи системі, а власне тим, хто надсилає пакети з відповідними значеннями в полях “source ip”, “destination ip” та “protocol+port”. На цих принципах грунтувалася робота первинних файрволів, що здебільшого було прийнятним. Проте організація контрол мережевих підключень у відповідності до принципів нульової довіри з використанням лише базових умов (полів айпі і порт) не є достатньо ефективним

щодо забезпечення безпеки мережевої архітектури з огляду на погану гнучкість, надмірну статичність, відсутність автентифікації відправника та обмежену видимість.

Розуміння контексту підключення значно розширює можливості управління доступом. З використанням додаткових контекстних атрибутів більш прецезійно можна описати політиками безпеки дозвіл чи заборону на конкретний доступ. Насичення політик файрвола додатковими атрибутами, які описують контекст мережевого підключення, відкриває нові можливості управління мережевим доступом. Перш за все це можливість реалізації більш гнучкого підключення. Додаткові перевірки дозволять точково обмежувати надання доступу, що знизить ризик виникнення айпі спуфінгу та інших атак, які базуються на підлаштуванні під дозволений доступ.

Інтеграція перевірки ідентичності в політику файрвола дозволяє більше не привязуватися до мережевої адреси вузла, доступ якому надається або забороняється. Це принципово змінює концепцію контролю доступу мережевого трафіку. При застосування атрибуту “identity” політика файрволу контролює доступ користувача чи сервісу а не мережі в якій вони знаходяться. Така зміна підходу надає наступні переваги:

- є можливість відрізнити пдключення конкретного користувача чи системи від інших членів мережі;
- постійна перевірка ідентичності забезпечує відповідність принципам нульової довіри
- спрощується процес керування доступом в динамічних середовищах де користувач чи сервіс можуть з'являтися в різних сегментах мережі;
- суть динамічного контролю доступу змінюється: від додавання хоста в дозволену мережу до додавання користувача в дозволену identity provider групу. (чи їх вилучення).

Перевірка аплікацій в правилі файрвола на додаток або заміну до традиційних порт\протокол дозволяє більш прецезійно контролювати доступ, який використовує одинаковий порт, але різні за типом аплікації. Таким чином в підключеннях по tcp 443 можна розрізняти тип аплікацій і контролювати їх окремо.

Контекстні атрибути які використовуються в правилах файрволів можна згрупувати в наступні категорії:

**Контекст користувача та ідентичності.** До цієї категорії належать атрибути, що характеризують суб’єкта доступу: роль користувача, приналежність до підрозділу, метод аутентифікації тощо. Інтеграція таких атрибутів зазвичай здійснюється через служби каталогів (Active Directory, LDAP) або системи єдиного входу (SSO) з використанням протоколів SAML чи OAuth. Це дозволяє встановлювати політики на основі функціональної ролі користувачів та забезпечувати контроль доступу з урахуванням їхнього робочого контексту.

**Контекст пристрою та кінцевої точки.** Цей контекст охоплює характеристики технічних засобів, з яких здійснюється доступ: тип пристрою, версію операційної системи, рівень відповідності політикам безпеки (наприклад, актуальність оновлень чи наявність антивірусного захисту). Для інтеграції використовуються системи управління мобільними пристроями (MDM) та засоби захисту кінцевих точок (EDR). Врахування таких параметрів дозволяє блокувати доступ із вразливих або некоректно налаштованих пристроїв.

**Контекст мережі та сесії.** Цей тип контексту стосується параметрів мережевого з’єднання: зони джерела і призначення, підмережа, стан VPN-з’єднання, геолокація клієнта тощо. Використання таких атрибутів дозволяє, наприклад, обмежувати доступ лише для підмереж, що вважаються довіреними, або для користувачів, які автентифікувалися через корпоративний VPN.

**Контекст застосунків та даних.** До даного класу належать атрибути, що описують тип застосунку, сервіс чи рівень чутливості даних. Це дозволяє впроваджувати політики доступу на основі категоризації інформаційних ресурсів, наприклад, дозволяючи роботу з конфіденційними документами виключно через санкціоновані корпоративні сервіси (наприклад, SharePoint). Такий підхід поєднує мережеву безпеку з елементами захисту даних (Data Security).

**Контекст навколишнього середовища.** Цей контекст враховує динамічні зовнішні фактори, зокрема час доби, день тижня, фізичне розташування користувача, а також виявлені аномалії у поведінці пристрою. Застосування таких атрибутів дозволяє обмежувати критичні операції, наприклад, забороняти адміністративний доступ до хмарних ресурсів поза робочим часом або з нетипових геолокацій.

**Технології NGFW для підтримки контекстуальних політик**

Технології збору та перевірки контекстної інформації виходять за межі та можливості передачі даних з використанням стандартних полів айпі пакета. Без додаткових засобів файрвол не може дізнатися про контекст мережевого підключення. Технологічні засоби, необхідні для реалізації перевірки контекстної інформації, залежать від типу контексту та є різними.

Побудова політик безпеки на базі перевірки ідентичності вимагає вирішення не простих задач, а саме розпізнавання користувача від якого відбувається підключення та перевірки членства облікового користувача в групах служб каталогів ідентичності. Так як файрвол працює на мережевому рівні - необхідний механізм ідентифікації користувача для перевірки в мережевому підключенні. Сучасні міжмережеві екрани пропонують технології інтеграції з надавачами послуг ідентичності та з іншими системами, які дозволяють визначити співвідношення айпі адреси до облікового запису користувача. Таким чином файрвол, який має в політиці безпеки вказаний конкретний обліковий запис, знає з якої айпі адреси він прийде і динамічно відкриває доступ саме для цієї айпі адреси. Основна задача полягає в формуванні таблички user-id mapping та передачі її в файрвол для використання політиками безпеки. Також необхідні механізми вичитування груп з каталогів директорій та перевірки членства облікових записів користувачів в цих групах. Політики на основі ідентифікатора користувача функціонують, пов'язуючи ідентифікатор користувача з його поточною IP-адресою або контекстом сеансу. Ідентифікатори користувача часто отримуються із централізованих систем автентифікації або каталогів, таких як Active Directory, LDAP, єдиний вхід на основі SAML або постачальників хмарних ідентифікаційних даних, таких як Azure AD або Okta, див. рисунок 1. Це зіставлення дозволяє брандмауеру застосовувати правила доступу на рівні окремих осіб або груп, а не сегментів мережі.

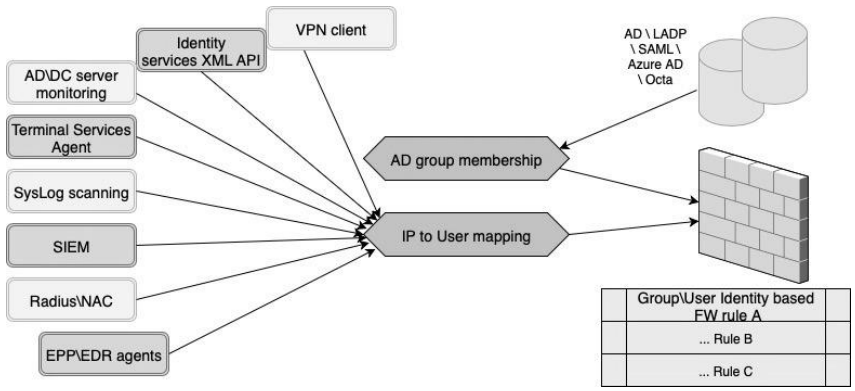


*Рис. 1. Базований на ідентичності контроль доступу мережевого трафіку*

Основною технологією, що лежить в основі цієї реалізації, є механізм зіставлення ідентифікатора користувача, який можна встановити кількома способами:

- Моніторинг журналів на основі агентів: спеціальний агент ідентифікатора користувача відстежує журнали автентифікації (наприклад, події Kerberos або NTLM) на контролерах домену, щоб пов'язати IP-адреси з логінами користувачів.

- Збір ідентифікаційних даних на основі системного журналу/API: брандмауери отримують дані системного журналу від VPN-концентраторів, серверів RADIUS або систем NAC, які містять події автентифікації.

- Звітування про ідентифікацію на основі кінцевих точок: агенти брандмауера або платформи захисту кінцевих точок (EPP/EDR) безпосередньо повідомляють інформацію про ідентифікацію та стан користувача брандмауеру.

- Портали автентифікації та твердження SAML: у контексті гостьових систем або некерованих пристроїв брандмауери можуть перенаправляти користувачів на портали автентифікації або використовувати твердження SAML для розпізнавання ідентифікаційних даних.

Перевірка стану та безпекового статусу кінцевої точки є важливим фактором при прийнятті рішень надання чи ненадання мережевого доступу. Важливими є не лише статично описані правила та умови, а й динамічна реакція файрвола на зміну такого статусу кінцевих точок. Для реалізації використання контексту пристроїв в політиках брандмауерів можуть застосовуватися наступні технології:

1. Виявлення та реагування на кінцевих точках (EDR) / Розширене виявлення та реагування (XDR). В таких засобах агенти EDR/XDR постійно контролюють поведінку кінцевих точок, цілісність файлів, активність процесів та потенційні компрометації. Провідні постачальники, такі як CrowdStrike, Microsoft Defender for Endpoint та Palo Alto Cortex XDR, надають API або генерують сповіщення, які можуть використовуватися брандмауерами або платформами SOAR.

2. Засоби керування мобільними пристроями (MDM) / Керування кінцевими точками (UEM). Рішення MDM, такі як Jamf, Intune або VMware Workspace ONE, підтримують дані про відповідність та конфігурацію, які можна використовувати для визначення контролю доступу. Інтеграція з брандмауером часто відбувається через теги (наприклад, «сумісний», «некорпоративний»), Ідентифікатори пристроїв, статус на основі запитів API. Це дозволяє застосовувати політики, наприклад такі як: «Блокувати пристрої, не зареєстровані в MDM, від доступу до конфіденційних програм».

3. Деякі постачальники NGFW збирають дані кінцевих точок безпосередньо через агентів, наприклад GlobalProtect HIP (Palo Alto) збирає дані про ОС, антивірус, шифрування диска тощо. Чи FortiClient від Fortinet передає інформацію про відповідність пристроїв та стан до FortiGate. Або Cisco AnyConnect + ISE забезпечують файрвол інформацією про стан через ISE та pxGrid.

4. SOAR / Агрегатори контексту. Інструменти оркестрації безпеки (наприклад, Cortex XSOAR, Splunk SOAR, Tines) можуть нормалізувати дані з кількох джерел та надсилати контекстні теги до брандмауерів через API або системний журнал. Ці теги (наприклад, "high_risk_device") потім можуть споживатися динамічними адресними групами (PaloAlto) або тегами ZTA (Fortinet).

Сценарій: пристрій із застарілим антивірусним програмним забезпеченням позначено CrowdStrike. Послідовність дій:

- CrowdStrike EDR надсилає сповіщення до XSOAR.
- XSOAR зіставляє IP-адресу з тегом AV_outdated.
- Тег передається до Palo Alto NGFW через API.

- Політика NGFW: ЗАБОРОНИТИ доступ до внутрішніх програм, ЯКЩО вихідна
- IP-адреса в DAG:AV_outdated

Доступ до пристрою блокується, доки антивірус не буде оновлено, а тег не буде видалено.

Фільтрація з урахуванням додатків є основною особливістю брандмауерів наступного покоління (NGFW), що дозволяє застосовувати політики безпеки на основі даних про аплікацію на прикладному рівні (рівень 7), а не виключно на основі IP-адреси, порту чи протоколу. Ця технологія базується на глибокій перевірці пакетів (DPI), яка аналізує корисне навантаження пакетів для точної ідентифікації додатків незалежно від порту чи шифрування. Крім того, для розпізнавання поведінки додатків та виявлення методів ухилення, таких як тунелювання або перемикання портів, використовуються декодери протоколів та евристичний аналіз трафіку. Деякі брандмауери використовують дешифрування SSL/TLS для перевірки зашифрованого трафіку, забезпечуючи видимість додатків, що працюють через HTTPS. Підписи додатків, які регулярно оновлюються постачальниками, зіставляються з потоками трафіку для класифікації тисяч відомих додатків. Такі постачальники, як Palo Alto Networks (App-ID), Fortinet (App Control) та Cisco (NGFW Snort/NGIPS), впроваджують власні механізми для підтримки цієї функціональності. Фільтрація з урахуванням додатків також дозволяє застосовувати політики на основі ідентифікації та ролей, обмежуючи певні дії в додатку (наприклад, чат у Facebook, але не завантаження файлів). Інтеграція з базами даних хмарних додатків та аналіз загроз у режимі реального часу підвищують точність виявлення веб-трафіку та трафіку SaaS. Зрештою, фільтрація з урахуванням додатків покращує точність політик та зменшує поверхню атаки, дозволяючи організаціям визначати доступ на основі використання аплікацій, а не лише підключення [13].

Контекст часу та місцезнаходження. Політики можуть обмежувати доступ за часом доби, геолокацією або мережевою зоною. Наприклад: блокування доступу адміністратора поза робочим часом, заборона входу VPN з непідтверджених країн. Контекстні політики часу/місцезнаходження допомагають запровадити динамічні правила ZTA поза статичними визначеннями. [14]

Окрім традиційних поколінь брандмауерів та загальновідомих контекстних вхідних даних, таких як ідентифікація користувача, стан пристрою та обізнаність про програми, з'явилися новіші технології для підтримки розширеного контекстного забезпечення політик. Одним із таких розробок є використання модельно-орієнтованих фреймворків контролю доступу, таких як GemRBAC+CTX, які дозволяють детально визначати просторово-часові атрибути (наприклад, час, місцезнаходження, стан навколишнього середовища) безпосередньо в політиках контролю доступу. Ці системи формалізують контекстні обмеження за допомогою моделей та логічних мов, таких як OCL, що дозволяє механізмам забезпечення дотримання вимог міркувати над складними сценаріями, не покладаючись виключно на статичні параметри[15]. Іншим новим підходом є інтеграція контролю доступу, покращеного блокчейном, де динамічні атрибути, такі як час або місцезнаходження, криптографічно застосовуються за допомогою смарт-контрактів для розподіленої довіри та захисту від несанкціонованого доступу, що робить забезпечення дотримання політик більш прозорим та стійким у хмарних середовищах [16]. Ці новітні технології підкреслюють тенденцію до контекстуальної децентралізації, дозволяючи політикам розвиватися в режимі реального часу та на основі багатших, багатовимірних вхідних даних, ніж це було можливо раніше.

**Проблеми та недоліки застосування контекстних політик.**

Безперечно застосування контекстних політик збільшує гнучкість керування мережевим доступом та підвищує захищеність інформаційної інфраструктури. Перехід до ідеології - доступ для користувача а не для мережі в якій він знаходиться змінює парадигму файрволінгу в корпоративних мережах.

Потреба синхронізації правил доступу в залежності від точок входу в мережу та задача диференціації підключення від підключень інших користувачів на рівні правил брандмауера, особливо в мережах з динамічною адресацією, стають більше не актуальними. Натомість визначається один набір мережевих правил для одного облікового запису чи групи облікових записів.

Проте унікальний функціонал є складним та вартісним в організації. Лише лідери ринку підтримують з коробки всеможливі контекстні політики та мають запропоновані засоби інтеграції та збору контекстної інформацію в своєму портфоліо. Попри ці недоліки робота мережевих сервісів ще стає залежною від сторонніх систем, що розширює можливий ландшафт відмов та компрометацій в інформаційних інфраструктурах.

Зростає і складність налаштування, підтримки та аналізу спрацювання політик безпеки брандмауерів. Насичення їх додатковими контекстними атрибутами породжує проблему надмірно складних правил. Такі правила можуть містити велику кількість умов, атрибутів або винятків, що ускладнює їх розуміння та підтримку. Хоча складність може бути необхідною для точного контролю, надмірно складні правила можуть збільшити ризик неправильної конфігурації, прогалин у безпеці та проблем з продуктивністю.

До прикладу, є правило на корпоративному файрволі, призначене для дозволу доступу до конфіденційного внутрішнього веб-сервера (SecretServer) лише для співробітників, які використовують керовані пристрої, розташовані в певних офісах, у робочий час, з певними ролями (наприклад, RND або IT) та з певних діапазонів IP-адрес.

Ось приклад надмірно складного правила:

*Allow access to SecretServer:*

*- If the user is authenticated with Active Directory and belongs to the "RND" or "IT" group*

*- If the user is accessing from one of the following offices (Kyiv, Lviv, Zatemne)*

*- If the device has a valid endpoint security posture (Antivirus installed, OS version X or higher)*

*- If the access request is between 9 AM to 6 PM local time of the office location*

*- If the source IP is one of the following (10.0.10.5, 10.0.20.5, 10.0.30.5, etc.)*

*- If the device is connected via the corporate VPN, and the VPN profile matches one of the predefined configurations*

*- If the user hasn't failed more than 3 authentication attempts in the past 24 hours*

Впровадження надмірно складних контекстних політик безпеки призводить до переліку проблем та труднощів. Серед них:

Занадто багато умов. Перевіряється кілька атрибутів (роль користувача, безпека пристрою, час, вихідна IP-адреса, конфігурація VPN, невдалі спроби входу). Ця складність збільшує ризик неправильних конфігурацій, і важко відстежити, чи всі умови налаштовані належним чином.

Зріст витрат на обслуговування. Зі зростанням списку IP-адрес, офісів або ролей, керувати ними стає складно, особливо якщо відбуваються часті зміни в мережі або ролях користувачів.

Складність у вирішенні проблем. Якщо доступ для авторизованого користувача заблоковано і трафік не попадає в політику безпеки яка є громіздкою, знайти першопричину може бути складно. Чи це стан пристрою, вихідна IP-адреса, невдалі спроби входу чи розташування офісу?

Іншим прикладом проблемної ситуації є конфігурація що містить кілька вкладених правил для конкретних випадків використання: уявимо правило, де адміністратор намагаєтеся вказати різні рівні доступу для одного й того ж хоста чи користувача на основі комбінації ролей, типу пристрою та часу доби:

*Rule 1: Allow "RND" users to access SecretServer if:*
*- Device is a laptop or desktop*
*- Access is from Lviv or Kyiv offices*
*- Between 9 AM to 6 PM local time*
*- If they are part of "RND" Active Directory group*

*Rule 2: Allow "Admin" users to access SecretServer if:*
*- Device is a laptop or desktop*
*- Access is from any office in LvivRegion (except Lviv)*
*- Between 7 AM to 9 AM or 6 PM to 9 PM*
*- If they are part of "Admin" Active Directory group*
*- If they have MFA enabled*

*Rule 3: Allow "Manager" users to access SecretServer if:*
*- Device is a mobile phone*
*- Access is from Kyiv office*
*- During any time of day*
*- If they are part of "Manager" Active Directory group*

Такий підхід конфігурації правил породжує труднощі подібні до наслідків нагромадження надлишкової конфігурації, а саме:

Кілька вкладених правил: кожне правило вводить багато умов і певних часових рамок доступу, створюючи складний набір правил, які перетинаються. Брандмауеру може знадобитися оцінити кілька умов, перш ніж дозволити доступ, що може вплинути на продуктивність.

Підвищений ризик перекриття: ці вкладені правила можуть призвести до надмірності та потенційного перекриття, коли різні ролі підпадають під суперечливі умови.

Плутанина у застосуванні правил: у разі конфліктів між правилами (наприклад, різні часові обмеження або типи пристроїв) може бути важко зрозуміти, яке правило має пріоритет і як вони взаємодіють. Практика написання правил для організації винятків для окремих користувачів з загальноприйнятих правил суттєво масштабує складність конфігурації, створює навантаження на файрвол що може відображатися в зниженні продуктивності, погано масштабується та важко аналізується під час пошуку та усунення неполадок.

**Проєктування ефективних контекстних політик.** Щоб отримати цінність від впровадження передових мережевих та безпекових технологій важливо шукати баланс поміж розлогими конфігураціями і складними кіберсистемами з одного боку, та лаконічними наборами правил і нечисленними залежностями від інших систем з іншого. Ефективною безпековою системою може бути рішення яке не гальмує загальну продуктивність мережевої інфраструктури та може підтримуватися наявним технічним персоналом в межах допустимих термінів.

В випадку з контекстними політиками важливим є пошук найбільш ефективних комбінацій контекстних атрибутів та правил на їх основі. Гарне збалансоване правило — це правило, яке забезпечує дотримання принципів нульової довіри, залишаючись при цьому керованим, чітким та ефективним. Воно має бути достатньо точним, щоб забезпечувати дотримання політик безпеки, не будучи надмірно складним, і має враховувати критичний контекст, такий як ідентифікація користувача, безпека пристрою та доступ за часом, без зайвих винятків.

Основні засади побудови контекстних політик базуються на чіткості, гнучкості та структурованості. Правило повинно добре масштабуватися: у міру зростання організації воно повинно легко застосовуватися до інших груп або ресурсів, змінюючи групу користувачів або ресурс (наприклад, замінивши «Відділ кадрів» на «Фінанси» або «Адміністратор»). Політики не повинні знижувати продуктивність файрвола та погіршувати якісні характеристи мережі. Опрацювання трафіку з перевіркою контекстних атрибутів може збільшувати затримку при опрацюванні, оскільки задіяні додаткові засоби. Таким чином кількість правил для унікального користувача варто робити мінімальним, дотримуючись при цьому принципу мінімальних привілеїв.

Зручність у підтримці: У міру змін в організації існуючий набір контекстних правил повинен дозволяти змінювати умови (наприклад, коригувати часові рамки або додавати нові вимоги до пристроїв), не перевантажуючи структуру самих правил.Не варто створювати складні ієрархічні рівні контекстних політик в міжмережевих екранах. Також не рекомендується практика опису вийнятків до загальноприйнятих політик. Такі нестандартизовані правила складно супроводжувати чи масштабувати.

Принцип найменших привілеїв повинен бути не тільки каталізатором опису додаткових контекстних атрибутів в політиці але й індикатором коли політика вже достатньо прецизійна і не потрібно її обкладати ще уточнюючими перевірками. Надмірно насичена перевірками політика породжує проблему важкого траблшутинга. Це яскраво проявляється в ситуації коли в неї не попадає трафік і треба знайти причину котра конкретно з умов не виконується.

Для кожного з контекстних атрибутів, який перевіряється в політиці, повинен існувати механізм його валідації. Це необхідно для проведення діагностики на випадок якщо політика не спрацьовує, оскільки логування трафіку зазвичай відбувається за умови проходження трафіку нею, а якщо умови доступу описані атрибутами не співпали, спрацювання не відбулося, то і логування не буде.

Використовуючи контекстні політики файрволів можна побудувати структуру рівнів доступу користувача чи системи в мережі в залежності від повноти відповідності умовам, поданим в правилах. Це дозволяє знижувати рівень доступу якщо знижується відповідність контекстним критеріям. Виникає структура правил яку називають вкладеними - коли правила накладаються і повторюються між собою з невеликою різницею в умовах та в результаті. Створення багаторівневих вкладених правил (nested rules) не є рекомендованою практикою, оскільки вона суттєво ускладнює їхню подальшу операційну підтримку та може впливати на продуктивність мережі.

Достатньо ефективною системою рівнів доступу може бути 3 рівнева модель.

Дана модель передбачає 3 рівні доступу з опційною нотифікацією користувача.

В залежності від виконання умов політики допускається 3 рівні доступу користувача чи системи до цільових ресурсів, а саме:

- Повний доступ
- Обмежений доступ
- Відсутній доступ

Використання шаблонів і стандартизованих структур правил із змінними для ролей, пристроїв, застосунків і мережевих сегментів дозволяє значно скоротити дублювання, полегшити аудит і спростити обслуговування. Крім того, політики мають бути адаптивними та здатними реагувати в реальному часі на зміни контексту, такі як несумісність пристроїв, аномальна поведінка користувачів або підвищений рівень загроз, визначений інтегрованими системами загроз або аналітики поведінки.

Баланс між безпекою та зручністю користування є ключовим; надмірно суворі політики можуть ускладнювати легітимні операції та призводити до обхідних шляхів, тоді як недостатньо детальні правила можуть дозволити несанкціонований доступ. Модульні та лаконічні структури політик допомагають мінімізувати складність, зменшити ймовірність неправильного налаштування та підвищити продуктивність файрвола. Інтеграція з зовнішніми джерелами контексту—IAM, MDM/EDR, джерела загроз та SIEM/UEBA—забезпечує динамічне та обґрунтоване застосування політик.

*Таблиця 1.*

**Приклад збалансованої контекстної політики**

| **Атрибут** | **Умова** | **Дія** |
|---|---|---|
| Роль користувача | Фінанси | Дозвіл |
| Стан пристрою | Відповідний, оновлений | |
| Дані джерела | VPN / довірена підмережа | |
| Час | 08:00–18:00 | |
| Дані призначення | CMDB | |
| Аплікація | ssl | |
| | Всі перечислені умови | |
| | Будь-який інший випадок | Заборона |

Ця таблиця демонструє чітку, керовану та контрольовану політику, яка включає багатовимірний контекст та може динамічно адаптуватися у разі зміни стану пристрою або доступу поза робочим часом, відображаючи принципи Zero Trust. Застосування контролю доступу на базі ролей з використанням групи користувацької групи та перевірка стану пристрою забезпечують відповідність принципам нульової довіри.

**Технологічні рішення з використанням контекстних політик.**

Застосування технологій контекстних та динамічних політик дозволяє охоплювати клас технічних та бізнес завдань які виходять за межі та можливостей класичних файрволів та традиційних підходів управління мережевим доступом статичними айпі політиками.В даному абзаці наведемо декілька технічних задач які виникають в корпоративних інформаційних інфраструктурах в умовах сучасних безпекових викликів.

Автоматичне управління мережевим доступом працівників. Надання або позбавлення доступу до корпоративних ресурсів є невід'ємною частиною процесу найму або звільнення нових працівників. В великих компаніях це доволі динамічний та постійний процес. Технології перевірки облікового запису користувача в файрволах нового покоління дозволяють керувати доступом використовуючи об'єкти Active Directory в політиках безпеки замість айпі адрес. Перевагою є можливість надавати доступ з гранулярністю до 1 користувача або групи. Застосування груп Active Directory в політиці безпеки дозволяє винести точку надання та позбавлення доступу за межі файрвола.

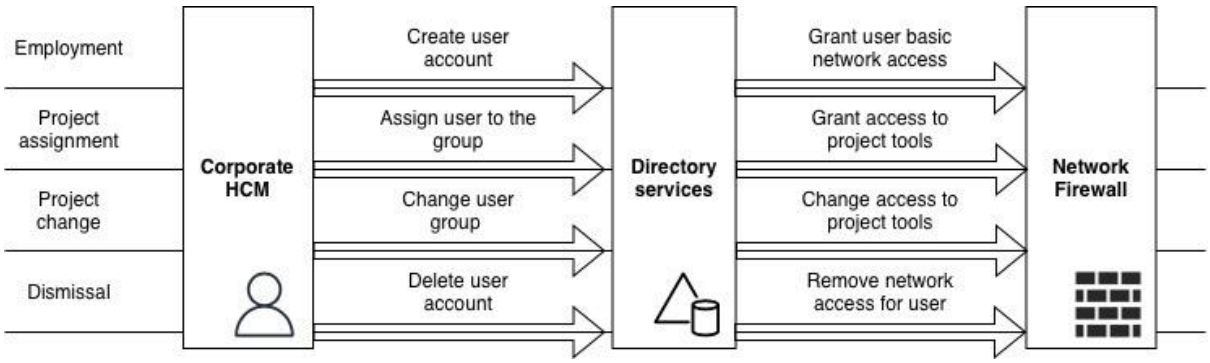


*Рис 2. організація управління мережевим доступом в життєвому циклі користувача*

Таким чином, при створенні об'єкта в Active Directory та поміщенні його в певну групу, яка вже є замаплена в файрволі та використовується в правилі, доступ буде наданий для нового користувача автоматично без жодної зміни в конфігурації правила. Даний підхід переносить точку прийняття рішення про надання або заборону мережевого доступу користувача за межі мережевого файрвола. Таким чином відповідні команди, відповідальні за певні бізнес процеси можуть уникнути затримок та керувати доступом людей без залежності на технічні команди обслуговування інфраструктури. Приклад організації автоматичного управління мережевим доступом з використанням інтеграцій між системою управління людським капіталом (Human capital management, HCM), корпоративним сервісом каталогів та файрвола зображений на рисунку 2.

Сучасні інформаційні інфраструктури можуть послуговуватись різними динамічними середовищами, розміщеними за межами внутрішніх мереж, наприклад десь в інтернеті. До таких сервісів можуть відноситися як надавачі хмарних послуг так і безпекові компанії які спеціалізуються на наданні списків айпі адрес чи доменних імен з низькою репутацією. Такі списки айпі адрес є високо динамічними та можуть мінятися щодня. Конфігурація доступу до них в ручному режимі є трудомісткою.

Технологія динамічних списків доступу дозволяє міжмережевим екранам отримувати перелік айпі адрес, мереж, чи ДНС імен з зовнішніх джерел та відслідковувати зміни в них автоматично, з певною періодичністю. Приклади зовнішніх

ISSN 2663 - 4023

та внутрішніх середовищ з динамічною адресацією зображено на Рисунку 3. Таким чином налаштувавши файрвол на читання зовнішніх джерел, налаштований доступ до динамічних середовищ завжди буде актуальним при всіх їхніх майбутніх змінах.

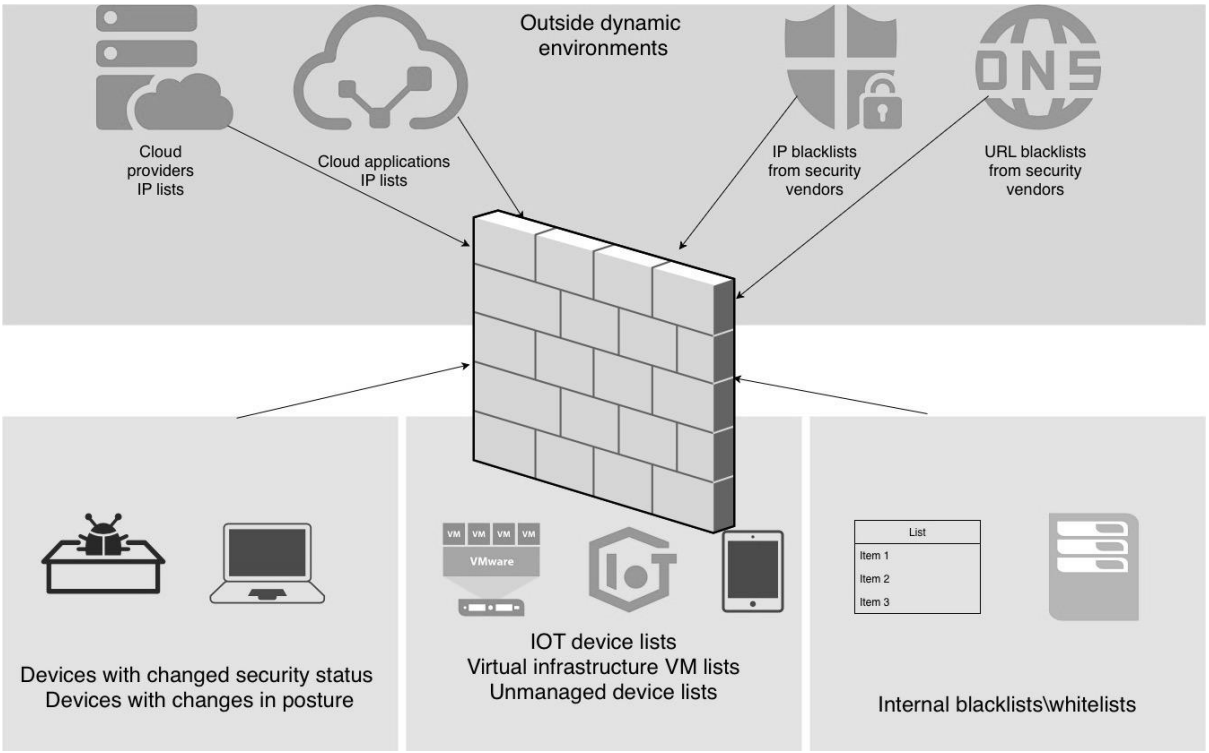


*Рис 3. Динамічні середовища в корпоративній інфраструктурі*

При застосуванні динамічних списків доступу спрацьовує керована часом логіка. Зміни в самому списку відбуваються виключно в момент вичитки списку з зовнішнього джерела, що відбувається періодично, згідно налаштованого інтервалу часу та не керується подіями, за виключенням ручної активації.

Кібербезпекова інфраструктура підприємства дозволяє відслідковувати потоки даних, уловлювати аномалії або відхилення та оперативно реагувати на них. Доступ до чутливих даних або захищених систем надається лише при виконанні чітко визначених умов. Якщо з певних причин вузли не виконують поставлених умов - потрібен механізм для негайної корекції їх доступу до чутливих даних. Дана ситуація породжує потребу в автоматичній та динамічній корекції доступу вузлів які змінили свій кібербезпековий статус. Прикладами такої змвни можуть бути: поява вразливостей на кінцевих точках, вивід пристроїв з під інструментів корпоративного управління чи банальне не проходження користувачем обов'язкових навчань. Таким чином виникає потреба застосування автоматичної корекції доступів на основі логіки що керується подіями.

Прикладами технологій що дозволяють динамічно наповнювати адресні групи файрвола айпі адресами та надавати їм певний тег є технології на кшталт “Dynamic address group” (DAG). Вони дозволяють створювати групи айпі адрес з певним унікальним тегом які можуть динамічно наповнюватися сторонніми системами з використанням технологій REST API як наслідок фіксування певних подій.

Розглянемо сценарій що є прикладом застосування DAG: антивірусна система при виявленні вірусу на кінцевій точці реєструє подію, яка додає до динамічної групи айпі адресу хоста з тегом “virus_infected”. В свою чергу на файрволі створена політика

безпеки яка включає динамічну адресну групу “virus_infected” та вводить її в дію для всіх айпі адрес які будуть в ній зареєстровані. Таким чином побудована система може автоматично коректувати доступ кінцевої точки чи користувача при зміні її кібербезпекового статусу без втручання людини.

Дана технологія дозволяє відслідковувати зміну контексту мережевого вузла та створювати сценарії негайної реакції на неї. Така логіка є керована подіями що дозволяє зменшувати до мінімум затримку між зміною безпекового контексту хоста та подальшим блокуванням його доступу.

Зниження ризику компрометації інфраструктури передбачає додаткові обмеження в наданні доступу легітимним користувачам. До таких обмежень відноситься дозвіл на підключення лише з керованих компанією кінцевих пристроїв з застосуванням машинної аутентифікації та валідації їх стану. Перевірка стану пристрою в парі з багатофакторною аутентифікацією користувача формує високо захищений стандарт доступу до корпоративної інфраструктури. Ситуації де потрібно надати доступ не корпоративним пристроям вимагають спеціальних заходів ідентифікації та розрізнення таких пристроїв. Технології контекстних політик дозволяють організовувати різні сценарії ідентифікації партнерських пристроїв. Наприклад технологія Host Information Profile, яка вбудована в ВПН клієнт, дозволяє перевіряти параметри та стан операційної системи чи наявність встановлених аплікацій. В даному випадку для організації доступу можна погодити набір обов'язкових аплікацій, які ідентифікуватимуть пристрій як партнерський, налаштувати перевірку унікального ключа в реєстрі операційної системи, чи перевірку серійного номера пристрою.

Альтернативним може бути підхід з використанням сторонніх аплікацій які перевіряють стан пристрою. Наприклад антивірусний агент, чи система керування мобільними пристроями може віддавати інформацію про стан пристрою SOAR системі, котра використовуючи REST API інтерфейс реєструватиме айпі адрес в динамічній адрес групі файрвола з певним тегом, наприклад “partner_device” чи “IOT_corporate”, яка в свою чергу буде використана вже в загатовленій політиці на блокування чи на дозвіл.

Технології динамічних адрес груп дозволяють реєструвати адреси хостів в попередньо заготовлені правила на міжмережевому екрані та отримувати зміни в їхньому доступі як наслідок фіксування певних подій чи зміни їх стану в автоматичному режимі. Це дозволяє автоматизовувати процеси реакції на зміну кібербезкової ситуації в інфраструктурі, що підвищує рівень її захищеності до кіберзагроз.

Важливою та корисною функцією брандмауерів нового покоління є здатність розрізняти в мережевому трафіку відбитки аплікацій 7 рівня та контролювати доступ не тільки по комбінації сервіс\порт а ще й по додатку. Розуміння аплікацій міжмережевим екраном значно розширює гнучкість контролю доступу та підвищує ефективність в управлінні доступом. Технології розпізнавання аплікацій в айпі пакетах дозволяють більш прецезійно та ефективно контролювати доступ до різних аплікацій та сервісів навіть коли вони використовують однакові порти та протоколи для передачі даних. Для прикладу наведемо декілька сценаріїв, реалізація яких може надавати цінність як в кібербезпековій площині так і в області підвищення ефективності та гнучкості керування мережевим доступом:

- видимість аплікацій тунелювання трафіку допоможе мінімізувати потенційні сценарії безконтрольної екс-фільтрації чутливих даних з використанням неконтрольованих ВПН тунелів;

- дозвіл розважальних аплікацій за графіком дозволить підвищити ефективність роботи персоналу в бізнес години;

- правила доступу з використанням аплікацій дозволяють надавати доступ до сервісів з динамічними портами або адресами без потреби їхнього перелічення, що дозволяє не порушувати принцип найменших привілеїв навіть при роботі з динамічними середовищами.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведені дослідження показали що використання контекстних політик при організації мережевого контролю доступу в архітектурі нульової довіри відіграє ключову роль в забезпеченні відповідності основним принципам нульової довіри. Використання технології розпізнавання облікових записів користувача при запиті на підключення дозволяє здійснювати контроль мережевого доступу за допомогою ідентичності та виходити за рамки можливостей контролю доступу на основі айпі адрес.

Використання обєктів типу користувач або група користувачів в політиках безпеки дозволяє скоротити кількість політик безпеки вдвічі, беручи до уваги щонайменше 2 точки входи користувача в мережу: з середини та віддалено, а також дозволяє забезпечити принцип найменших привілеїв більш ретельно ніж з використанням правил виключно на айпі адресах та портах. Найбільш значущими контекстними атрибутами є перевірка ідентичності, перевірка стану пристрою а також розпізнавання міжмережевим екраном аплікацій 7 рівня та їх файрволінг, що зображено на рисунку 4.

Дослідження показало оптимальну глибину організації рівнів доступу для одного мережевого вузла з застосуванням контекстних перевірок - не більше ніж три рівні, з огляду на складність налаштування та процесу пошуку несправностей, а також засвідчило неефективність практики опису вийнятків мережевого доступу до загально описаних правил.

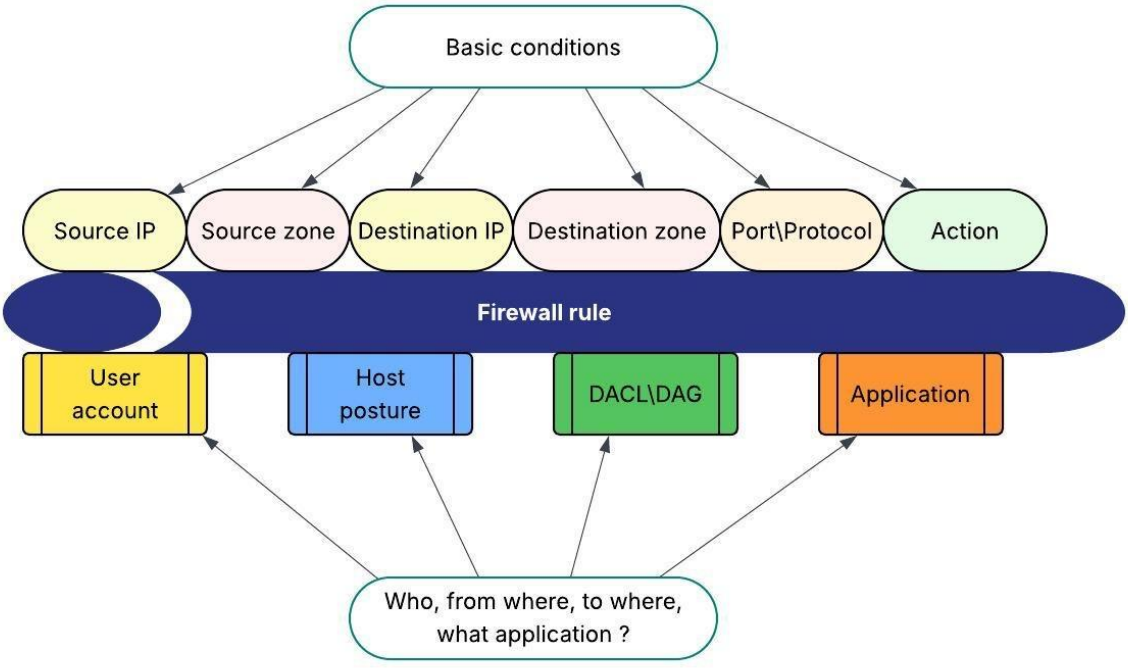


*Рис 4. Стандартні та контекстні атрибути політик доступу*

Використання контекстних перевірок в парі з застосуванням технологій динамічних списків доступу та динамічних адресних груп показали потенціал побудови сценаріїв автоматичної зміни рівня доступу хоста при зміні його безпекового стану.

Згідно з результатами дослідження інтеграції засобів збору та контролю контекстних атрибутів, попри безпекову цінність застосування в політиках безпеки файрволів, породжують певні недоілк. До таких належать: підвищення вартості володіння та обслуговування інформаційної інфраструктури, зниження продуктивність мережі через залежності від інших систем та створення ризиків пов'язаних з винесенням точок зміни рівня доступу до мережі за межі корпоративного фаервола.

## ВИСНОВОК

Значення контексту мережевого підключення в управлінні політиками доступу проявляється не лише у безпековому, а й в операційному вимірі. Нехтування контекстом зазвичай призводить до труднощів регулювання доступу в динамічних середовищах, що призводить до нагромадження правил, які важко підтримувати та які створюють потенційні вразливості. Натомість впровадження додаткових перевірок дає змогу більш прецезійно описувати необхідний доступ та знижувати кількість надлишкових правил. Важливою вимогою також є постійна перевірка атрибутів ідентичності, пристрою та мережевого середовища, що уможливлює прийняття рішень про доступ у режимі реального часу. Завдяки цьому контекстні політики виходять за межі традиційних методів і створюють більш деталізовану, гнучку та адаптивну систему контролю.

У результаті підвищується як рівень захисту критичних інформаційних ресурсів, так і ефективність роботи адміністраторів, що робить контекстні політики одним із ключових інструментів реалізації Zero Trust Architecture.

До недоліків в запропонованих методах розширеного контролю доступу відноситься потреба ускладнення інфраструктури. Залежності від сторонніх систем можуть впливати на продуктивність файрволів а недостатній захист засобів збору та надання контексту збільшує ландшафт несанкціонованого впливу та компрометацій на мережеву та безпекову інраструктури. Методики написання правил для організації багаторівневого доступу вузла в мережі або практики налаштування винятків з використання контекстних перевірок до основних правил можуть ускладнювати операційну підтримку корпоративної мережі та збільшувати трудоємкість заходів з пошуку неполадок доступу.

Перспективами подальших досліджень є аналіз ризиків неструктурованого управління мережевими доступами та розробка концепції їх життєвого циклу в корпоративній інфраструктурі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ike, C., Ige, A., Oladosu, S., Adepoju, P., Amoo, O., & Afolabi, A. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.2.1.0032.
2. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-Project Solutions for Building an Authorization System Based on the Zero Trust Concept. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242
3. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern Perspectives of Applying the Concept of Zero Trust in Building a Corporate Information Security

Policy. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

4. Tsekhmeister, R., Platonenko, A., Vorokhob , M., Cherevyk, V., & Semeniaka, S. (2025). Research of Information Security Provision Methods in a Virtual Environment. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703
5. Kostiuk, Y., Skladannyi, P., Rzaeva , S., Mazur , N., Cherevyk, V., & Anosov, A. (2025). Features of Network Attack Implementation through TCP/IP PRotocols. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
6. Routray, K., & Bera, P. (2025). ZTAAC : Zero Trust Adaptive Authorization with CP-ABE for Context-Aware Data Protection. *2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)*, 814-816. https://doi.org/10.1109/COMSNETS63942.2025.10885763.
7. Ahmadi, S. (2025). Autonomous Identity-Based Threat Segmentation in Zero Trust Architectures. *ArXiv*, abs/2501.06281. https://doi.org/10.48550/arXiv.2501.06281.
8. Yaganti, D. (2023). Securing .Net Microservices Through Conditional Access and Zero Trust Principles using Azure AD and OAUTH2. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-18000a.
9. Hirai, M., Kotani, D., & Okabe, Y. (2022). Linking Contexts from Distinct Data Sources in Zero Trust Federation. , 136-144. https://doi.org/10.48550/arXiv.2209.11108.
10. Oluoha, O., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. (2024). AI-Enabled Framework for Zero Trust Architecture and Continuous Access Governance in Security-Sensitive Organizations. *International Journal of Social Science Exceptional Research*. https://doi.org/10.54660/ijsser.2024.3.1.343-364.
11. Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and Risk Aware Access Control for Zero Trust Systems. *Security and Communication Networks*. https://doi.org/10.1155/2022/7026779.
12. 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.
13. Stojanovski, N., & Gusev, M. (2011). Architecture Of A Identity Based Firewall System. *ArXiv*, abs/1108.1344. https://doi.org/10.5121/ijnsa.
14. T. Dimitrakos *et al.*, "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, 2020, pp. 1801-1812, doi: 10.1109/TrustCom50675.2020.00247.
15. Fadhel, A., Bianculli, D., Briand, L., & Hourte, B. (2016). A Model-driven Approach to Representing and Checking RBAC Contextual Policies. *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*. https://doi.org/10.1145/2857705.2857709.
16. Panda, S., Sahoo, S., Halder, R., & Mondal, S. (2023). Contextual attribute-based access control scheme for cloud storage using blockchain technology. *Software: Practice and Experience*, 54, 2042 - 2062. https://doi.org/10.1002/spe.3250.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

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

# A CONTEXT-AWARE APPROACH TO ORGANIZING NETWORK SECURITY POLICIES IN A ZERO TRUST ARCHITECTURE

**Abstract.** The relevance of introducing new approaches and practices for organizing and controlling access in network infrastructures is justified by the widening gap between the requirements of modern security standards and the capabilities of network security tools that operate at Layers 3–4 of the OSI model. The paper analyzes security models recommended by contemporary standards and industry best practices for information infrastructures, and explores ways to implement them using available market tools and network access control measures. The methodological basis of the proposed approach combines the Zero Trust principles outlined in NIST SP 800-207, capabilities found in the portfolios of next-generation firewall vendors, and the author's methodologies and practices for integrating heterogeneous security systems to enrich firewall security policies with network-access context. The approach enables adherence to Zero Trust principles while maintaining operational quality and high performance of the network infrastructure, without exceeding acceptable total cost of operation and ownership of infrastructure resources. Key components and design patterns of the security infrastructure necessary to achieve these goals are identified. The scientific novelty of the approach lies in a paradigm shift in network access control—from a model centered on a corporate node's address to a model centered on user access control coupled with verification of the security posture of the requesting device. The paper proposes contextual attributes for security policies and optimal methods for structuring host access levels within firewall configurations. The practice of collecting and enriching policy enforcement points with network context provides the flexibility and technical means required to uphold Zero Trust principles when building a corporate security model. The drawbacks of the method include operational complexity, increased cost, and dependencies on other systems that may affect network performance and expand the compromise surface of the security stack itself.

**Keywords:** network access context, next-generation firewall, Zero Trust, user identity mapping, device/host security posture, dynamic address group.

## REFERENCES

1. Ike, C., Ige, A., Oladosu, S., Adepoju, P., Amoo, O., & Afolabi, A. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.2.1.0032.
2. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-Project Solutions for Building an Authorization System Based on the Zero Trust Concept. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242
3. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern Perspectives of Applying the Concept of Zero Trust in Building a Corporate Information Security Policy. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
4. Tsekhmeister, R., Platonenko, A., Vorokhob , M., Cherevyk, V., & Semeniaka, S. (2025). Research of Information Security Provision Methods in a Virtual Environment. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703

5. Kostiuk, Y., Skladannyi, P., Rzaeva , S., Mazur , N., Cherevyk, V., & Anosov, A. (2025). Features of Network Attack Implementation through TCP/IP PRotocols. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
6. Routray, K., & Bera, P. (2025). ZTAAC : Zero Trust Adaptive Authorization with CP-ABE for Context-Aware Data Protection. *2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)*, 814-816. https://doi.org/10.1109/COMSNETS63942.2025.10885763.
7. Ahmadi, S. (2025). Autonomous Identity-Based Threat Segmentation in Zero Trust Architectures. *ArXiv*, abs/2501.06281. https://doi.org/10.48550/arXiv.2501.06281.
8. Yaganti, D. (2023). Securing .Net Microservices Through Conditional Access and Zero Trust Principles using Azure AD and OAUTH2. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-18000a.
9. Hirai, M., Kotani, D., & Okabe, Y. (2022). Linking Contexts from Distinct Data Sources in Zero Trust Federation. , 136-144. https://doi.org/10.48550/arXiv.2209.11108.
10. Oluoha, O., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. (2024). AI-Enabled Framework for Zero Trust Architecture and Continuous Access Governance in Security-Sensitive Organizations. *International Journal of Social Science Exceptional Research*. https://doi.org/10.54660/ijsser.2024.3.1.343-364.
11. Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and Risk Aware Access Control for Zero Trust Systems. *Security and Communication Networks*. https://doi.org/10.1155/2022/7026779.
12. 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.
13. Stojanovski, N., & Gusev, M. (2011). Architecture Of A Identity Based Firewall System. *ArXiv*, abs/1108.1344. https://doi.org/10.5121/ijnsa.
14. T. Dimitrakos *et al*., "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, 2020, pp. 1801-1812, doi: 10.1109/TrustCom50675.2020.00247.
15. Fadhel, A., Bianculli, D., Briand, L., & Hourte, B. (2016). A Model-driven Approach to Representing and Checking RBAC Contextual Policies. *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*. https://doi.org/10.1145/2857705.2857709.
16. Panda, S., Sahoo, S., Halder, R., & Mondal, S. (2023). Contextual attribute-based access control scheme for cloud storage using blockchain technology. *Software: Practice and Experience*, 54, 2042 - 2062. https://doi.org/10.1002/spe.3250.