COMPUTER SYSTEMS AND NETWORKS

Vol. 7, No. 1, 2025

DOI: https://doi.org/10.23939/csn2025.01.261

УДК 621.3

ОСОБЛИВОСТІ УПРАВЛІННЯ МЕРЕЖЕВИМ ДОСТУПОМ КОРПОРАТИВНИХ СИСТЕМ В АРХІТЕКТУРІ НУЛЬОВОЇ ДОВІРИ

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

Розглянуто основні принципи нульової довіри та проаналізовано складнощі щодо їх дотримання під час розгортання мережевої інфраструктури з використанням класичних підходів влаштування безпекової моделі. Використання традиційних підходів під час написання правил мережевого файрвола не дає змогу гнучко регулювати доступ до корпоративних систем в мережі та забезпечувати принцип найменших привілеїв, а потреба постійної перевірки та автентифікації вузлів перед надання їм мережевого доступу піднімає проблематику інтеграції аплікаційних процесів в мережеву взаємодію хоста та файрвола.

Досліджено сучасні практики написання правил файрвола та способи дотримання принципів побудови архітектури нульової довіри зі застосуванням передових технічних можливостей файрволів нового покоління. Проаналізовані шляхи мінімізації шпаринкового доступу під час написання правил контролю доступу на файрволі. Досліджено варіанти насичення політик безпеки додатковими контекстними умовами та знайдено шляхи автентифікації мережевих вузлів засобами файрволів нового покоління.

Запропоновано методологію написання правил мережевих файрволів з дотриманням принципу найменших привілеїв та досліджено можливості технології мапінгу користувач - IP-адреса для побудови постійної аутентифікації та авторизації вузлів в мережі в угоду дотримання принципу "ніколи не довіряй, завжди перевіряй". Дотримуючись описаних практичних рекомендацій, організації можуть посилити захист власної мережевої інфраструктури, покращити видимість в мережі та забезпечити стійке її функціонування в умовах, коли довіра більше не є implicit (неявною), а здобувається на кожному етапі доступу.

Ключові слова: управління мережевим доступом, корпоративні системи, архітектура нульової довіри, авторизація, контроль.

Вступ

Зі зростанням популярності хмарних технологій, віддаленої роботи та взаємопов'язаних систем, традиційна модель мережевої безпеки "замок з ровом" стрімко втрачає свою актуальність. У часи, коли кіберзагрози стають дедалі витонченішими, архітектура нульової довіри (Zero Trust Architecture, ZTA) пропонує більш надійну та орієнтовану на майбутнє систему безпеки. Принцип Zero Trust базується на тому, що жодному суб'єкту - ні всередині мережі, ні за її межами - не можна довіряти автоматично, і передбачає постійну валідацію та перевірку кожного запиту на підключення.

В основі будь-якого впровадження Zero Trust лежать ретельно продумані, чітко дотримувані політики фаєрвола. Якщо за традиційних підходів безпека покладалася на статичні периметри та широку неявну довіру в межах мережі, то принципи Zero Trust потребують мікросегментації, контекстно залежних правил і доступу за принципом найменших привілеїв на кожному рівні. Це змінює роль фаєрволів із пасивних "сторожових брам" на динамічні точки реалізації політик безпеки, які інтегрують ідентичність користувачів, стан пристроїв та дані про загрози в реальному часі для ухвалення більш чіткіших рішень.

Точок реалізації політик, згідно з вимогами мікросегментації, стає суттєво більше. Набір умов згідно з якими буде виконуватися чи не виконуватися дія конкретної політики також суттєво розширюється порівняно з традиційними політиками безпеки. Таке ускладнення в масштабах інфраструктури середньостатичної компанії породжує суттєве операційне навантаження як за первинної реалізації чи міграції до мікросегментованої мережі з відповідними точками контролю трафіку в усіх можливих місцях, так і за повсякденного управління. Пошук балансу між закручуванням гайок в угоду безпеці, недопущенням припинення надання мережевих сервісів, якими послуговуються корпоративні системи, та можливістю якісно та вчасно все це обслуговувати, не перетинаючи рівень виділених ресурсів, є актуальною, але доволі нетривіальною задачею.

Аналіз літературних джерел

У сучасних літературних джерелах питання стратегії і підходів управління політиками в архітектурі нульової довіри описується концептуально та узагальнено. Різні автори акцентують увагу на різних стратегіях та описують їх актуальність та перевагу з безпекової точки зору. У праці [1] звертають увагу на переваги децентралізації точок керування політиками файрволів: проєкти Zero Trust часто централізують рішення, що може створити вузькі місця. Децентралізовані підходи дають змогу окремим компонентам мережі приймати рішення щодо безпеки, підвищуючи масштабованість і стійкість [1]. Згідно з дослідженнями, які провели автори праці "An intelligent security architecture for distributed firewalling environments", автоматизоване створення та адаптація правил брандмауера на основі поведінки трафіку та виявлення загроз нульового дня може покращити реагування на інциденти безпеки [2]. Також однією з важливих стратегій, про яку наголошують автори у публікації [3], є використання інструментів та методологій для відстеження дотримання вимог та оцінювання ефективності робочих процесів політики, необхідних для керування складностями ZTA й підтримання детальних стандартів безпеки.

З приходом фаєрволів нового покоління під час побудови архітектури нульової довіри для підвищення безпеки та ефективності роботи практикується розширення традиційних умов політик фаєрволів додатковими контекстними умовами. Політики можна адаптувати на основі ідентичності або ролі користувача, гарантуючи, що доступ надається лише авторизованому персоналу для виконання певних завдань. Перевірка особи має включати надійні механізми аутентифікації, такі як багатофакторна автентифікація [4]. Також до контекстних умов належить стан пристрою та рівень довіри. Автори твердять, що умови, які залежать від справності пристрою, як-от оновлене програмне забезпечення або активний антивірус, гарантують, що лише безпечні пристрої отримають доступ [5].

До інших контекстних умов можна зарахувати теги мікросегментацій, опис застосування яких згадує автор [6]. Політики можуть використовувати мережеві теги для мікросегментації, ізоляції та контролю доступу в певних сегментах мережі. Л. Брадаш та співавтори описують актуальність застосування умов на базі оцінки ризиків в реальному часі, які можуть динамічно коригувати дозволи на основі поточної ситуації [7], а в публікації "A Zero Trust Architecture for Automotive Networks" розповідається про практики інспекції зашифрованого трафіку для виявлення шкідливого вмісту в зашифрованих каналах [8]. Згідно з опублікованими дослідженнями, включення таких розширених умов дає змогу NGFW узгоджуватися з принципами нульової довіри, забезпечуючи розширену, адаптивну безпеку, адаптовану до поведінки користувача, стану пристрою та динаміч-

них мережевих контекстів, що має забезпечити стійкість до нових кіберзагроз. Згадані контекстні умови не є єдиними, які можна використовувати, також актуальними будуть рекомендації та дослідження спільного їх використання як пошук оптимальних підходів та практик для забезпечення високого рівня безпеки, достатньої продуктивності мережевої інфраструктури та оптимального рівня операційного навантаження.

Мета статті

Мета статті - розроблення і впровадження нових підходів та стратегій для покращення ефективності безпечного керування мережевим трафіком шляхом використання якісно кращих технічних можливостей файрволів нового покоління з дотриманням принципів нульової довіри, а також дослідження можливостей додаткових безпекових атрибутів з подальшим аналізом їх застосування як додаткових умов в безпекових політиках контролю мережевим доступом в контексті побудови архітектури нульової довіри.

Забезпечення принципів нульової довіри через політики файрвола

Впровадження архітектури нульової довіри - це комплексний процес згідно з методологіями, опублікованими в спеціальній публікації NIST 800-208, що має на меті перехід безпекової моделі підприємства до більш захищеної, базованої на основних принципах нульової довіри. Одними з ключових заходів, які уособлюють нульову довіру, є мікросегментація та дотримання принципів нульової довіри. До таких принципів належать:

- нікому не довіряй, усіх перевіряй;
- відмовити за замовчуванням;
- принцип найменших привілеїв;
- контекстуальний доступ;
- припущення, що втручання вже відбулося.

Роль мережевого файрвола в архітектурі нульової довіри, порівняно з традиційними моделями безпеки, залишається критично важливою, проте способи застосування розширюються, а концепції мереж, які він обслуговує дещо змінюються. Етап контролю трафіку в мережі, а саме: створення та керування політиками безпеки тісно пов’язаний з проєктуванням та впровадженням мікросегментації. Що гранулярніша мікросегментація в мережі, то більше точок контролю трафіку в ній, а отже, ландшафт горизонтального переміщення у разі компрометації одного з її елементів зменшується. Така безпекова модель дає змогу корпоративній інфраструктурі залишатися дієздатною навіть за умови компрометації одного з її мікросегментів.

Забезпечення принципів нульової довіри здебільшого виходить за межі традиційних підходів написання політик та можливостей класичного мережевого файрвола, де політики безпеки описуються IP-адресами та протоколами і діляться на 2 підгрупи - ті що з середини в інтернет та ті, які з інтернету в середину мережі.

Принцип найменшого привілею доступу (LPA) є наріжним каменем Zero Trust Architecture (ZTA), метою якого є мінімізація ризиків безпеки шляхом надання користувачам, пристроям і програмам лише дозволів, необхідних для виконання їхніх завдань.

Традиційна політика безпеки доступу в інтернет, яка часто реалізована за замовчуванням у фаерволах, дозволяє ходити всім вузлам внутрішньої мережі в інтернет на всі напрямки і по всіх протоколах. Це яскравий приклад недотримання принципу найменших привілеїв. Така політика порушує його щонайменше тричі, а саме:

- пропускає трафік не від конкретного хоста, якому потрібен такий доступ, а від усіх, хто є в межах периметра безпеки, зокрема хости, які зберігають високочутливі дані та не потребують доступу назовні;

- пропускає трафік не до конкретних вузлів за межами периметра безпеки, а до абсолютно усіх, включаючи хости потенційних зловмисників, на адреси яких може відбуватися витік даних;
- не лімітує список вихідних портів і дає змогу під'єднуватися з використанням будь-яких протоколів, включаючи протоколи передачі даних, по яких можна несанкціоновано зливати дані на сервери зловмисників.

Методологія написання політик безпеки з дотриманням принципу найменших привілеїв передбачає структурований та ітеративний підхід для забезпечення надійного, безпечного та ефективного керування мережевим трафіком. Обмеження відкритого доступу до мінімально необхідного можна поділити на 2 етапи:

- мережевий;
- контекстний.

На так званому мережевому етапі написання політики необхідно максимально точно вказати зону та адресу джерела, зону та адресу призначення, а також протокол і порт. Навіть якщо адреса призначення є за межами периметра безпеки, тобто в інтернеті, вказування конкретної адреси, куди потрібен доступ, є важливим та необхідним. Конкретизація адреси призначення та протоколу і порту виключить можливість зливати дані з джерела у випадку його компрометації. Цей підхід надання доступу є доволі ефективним з точки зору мережевої безпеки, але складним з точки зору створення повного набору політик необхідних для певного роботи цього хоста та його операційної підтримки. А в певних випадках з огляду на динамічну природу сервісів, доступ до яких необхідно надати, і взагалі є неможливим. Ще одним з важливих недоліків є можливість сценарію підміни IP-адреси зловмисного хоста (спуфінг) для імітації оригінального хоста та використання доступів, які йому надані.

Використання файрволів нової генерації дає можливість розширювати мережеві умови в політиках безпеки додатковими умовами. Такі умови дають можливість описувати необхідний контекст виконання політики у разі їх дотримання та ще більше конкретизовувати необхідний доступ, так зменшуючи розмір безпекової дірки, якою може скористатися зловмисник для здійснення неправомірного проходження через файрвол.

Дотримання принципу мінімально потрібних привілеїв в налаштуваннях файрволів під час побудови архітектури нульової довіри не позбавлене суттєвих недоліків. До таких належать:

- потреба детального розуміння всіх необхідних доступів кожного з вузлів корпоративної мережі;
- кількість та складність політик корпоративних файрволів суттєво збільшується, що потребує більш складного та вартісного обладнання, а також більше ресурсів на їх написання;
- операційна підтримка такого набору політик може бути суттєво утруднена, що позначається на вартості їх підтримання і на якості мережевих послуг, якими послуговуються корпоративні системи.

Ще однією з цікавих та корисних функцій файрволів нової генерації є можливість розрізняти трафік на аплікаційному рівні. Не секрет, що різні сервіси, доступ до яких може регулюватися файрволом, можуть використовувати нестандартні порти. Для прикладу ніщо не заважає зловмиснику підлаштовувати різні аплікації під вже відкриті порти і обходити, до прикладу, заборону на використання певних додатків. Отож керування доступом з використанням протоколу ТСП чи УДП та номером порту є малоефективним, оскільки під хоча б один відкритий порт можна підставити будь-яку аплікацію зміною її стандартного порту. Фаєрволи нового покоління наділені можливостями розрізняти трафік на аплікаційному рівні та застосовувати аплікацію як атрибут політики фаєрвола на додачу до номера порту. Отже, можна дозволити конкретно певну аплікацію і виключити можливість кастомізації стандартного порту та обходу обмежень на доступ організованих з використанням порту і протокола.

Фільтрація URL. В архітектурі нульової довіри фільтрація URL-адрес у NGFW є потужним інструментом для забезпечення детального контролю доступу, мінімізації ризиків і забезпечення відповідності. Він доповнює принципи ZTA шляхом динамічного моніторингу та контролю доступу до вебресурсів, так захищаючи мережу як від зовнішніх, так і від внутрішніх загроз. URL-фільтрація може застосовуватися в політиках безпеки як альтернатива умові "адреса призначення" або може доповнювати її. Цей функціонал дає змогу організаціям обмежувати доступ до певних вебсайтів або категорій на основі бізнес-потреб і ролей користувачів. Блокуючи доступ до зловмисних або несанкціонованих вебсайтів, фільтрація URL-адрес знижує ризик зараження зловмисним програмним забезпеченням, фішингових атак і викрадення даних. Іншим, не менш корисним, варіантом застосування URL-фільтрації є спосіб створення політик безпеки файрвола із застосуванням УРЛів як елемента адреси призначення, куди необхідно надати доступ. Такого формату політики безпеки дають можливість надавати доступ до динамічних вебресурсів, які важко описуються IP-адресами та відповідають принципу найменших привілеїв.

Дотримання принципу мінімальних привілеїв потребує більш ретельних підходів описування умов проходження трафіку в політиках безпеки. Одним з шляхів ущільнення доступу, який необхідно відкрити, може бути фактор часу. Тобто якщо певний доступ необхідний не 24х7, а строго за графіком - можна скористатися планувальником в політиці безпеки і створити часовий проміжок, коли це правило буде актуальним. Це може бути як одноразова подія, так і регулярна на щоденній, щотижневій чи щомісячній основі. Отже, доступ, потребу в якому можна спрогнозувати, буде надаватися лише в строго запрограмований період, що зменшить часовий проміжок, коли файрвол може пропустити підключення, а отже, можливість горизонтального руху у випадку компрометації джерела підключення знижується. Ця практика має і свої недоліки, оскільки помилки з плануванням можуть призвести до зупинки сервісів, які послуговуються корпоративними мережами у випадку розсинхронізації між подіями передачі даних та етапами запрограмованими в планувальнику.

Ніколи не довіряй, завжди перевіряй. У традиційній безпековій моделі "фортеця і рів" вважається, що якщо хост знаходиться в середині периметра безпеки, то він є довіреним і контролювати його доступ в межах периметра не потрібно. Це приклад неявної або прихованої довіри. Приховану довіру можна порівняти з політикою "відкритих дверей". У межах такої моделі кожен, хто перебуває в певній системі, за замовчуванням вважається надійним, а його права доступу й дії визнаються чинними. По суті, якщо у вас є відповідні облікові дані, ви можете під'єднатися до системи з будь-якого пристрою або місця та виконувати дії, дозволені вашими повноваженнями, без додаткової перевірки. Хоча такий підхід може бути зручним для користувачів, адже дає змогу вільно пересуватися системою з мінімальними перешкодами, він також створює суттєві ризики безпеки. Зловмисники, які здобувають доступ, можуть скористатися вбудованою довірою в системі та заподіяти їй значної шкоди.

Ідеологія нульової довіри, яка декларується принципом "ніколи не довіряй, завжди перевіряй", полягає у пропагуванні явної довіри. Ця модель потребує від кожного користувача та пристрою підтвердити свою особу та потребу в доступі до певної інформації, перш ніж надавати дозвіл на доступ і дії. Явна довіра потребує безперервної авторизації для кожної дії та запиту на доступ, включаючи перевірку пристрою, місцезнаходження та схвалення певних дій [9].

Можливості сучасних фаєрволів нового покоління дають змогу здійснювати автентифікацію ідентичності, яка ініціюватиме підключення до іншого ресурсу, а також проводити перевірку різних контекстних елементів цього підключення. Метод здійснення згаданих активностей полягає у використанні розширених умов перевірки трафіку політиками безпеки.

Кому надається доступ визначає поле "джерело" в політиці безпеки. Проте джерело не вказує конкретно, хто підключається, а лише дає можливість описати мережу, з якої відбуватиметься підключення, хай навіть якщо там вказана 1 IP-адреса. Щоб перевірити, хто саме підключається, як того вимагає ідеологія нульової довіри, необхідно автентифіковувати ініціатора підключення та

використати його ідентичність в політиці безпеки як додатковий контекстний елемент. Відображення ідентифікаторів користувачів у брандмауері наступного покоління (NGFW) є важливою функцією для реалізації архітектури нульової довіри (ZTA). Це дає змогу ґрунтувати політики доступу не лише на традиційних параметрах, таких як IP-адреси та порти, а й на ідентифікаційних даних користувача, які динамічно прив'язуються до автентифікації та контекстних даних. Застосування атрибуту user-id у політиках безпеки файрвола пов'язує ідентифікатори користувачів (наприклад, облікові записи Active Directory, атрибути SAML) із мережевими діями, забезпечуючи видимість того, "хто" ініціює запит, а не просто "що" (наприклад, IP-адреса).

Як це працює: NGFW інтегрується з постачальниками ідентифікаційної інформації (IdP), такими як LDAP, Okta або Azure AD, для отримання та відображення інформації користувача. Кожен мережевий запит позначається відповідним ідентифікатором користувача, що дає змогу детально застосовувати політику. Зіставлення користувача з IP-адресою динамічно оновлюється, коли користувачі входять або змінюють місце розташування, забезпечуючи точність правил. Така практика також надає можливість уніфікувати рівень доступів з гранулярністю до 1 користувача, незалежно від того, з якої сторони він під'єднаний до мережі. Локально чи віддалено, через вайфай чи дротовим підключенням, з однієї корпоративної локації чи з іншої.

Використання ідентичності в політиках мережевого фаєрвола також знижує можливість підміни хоста під дозволений айпі IP-адрес (спуфінг) та дає можливість більш прецезійно керувати доступом. Відстеження активності користувачів, пов'язаної з ідентифікаційними даними, є основоположним елементом Zero Trust, що забезпечує кращий моніторинг і виявлення аномалій [10].

Один з варіантів написання політик, які дотримуються принципу "ніколи не довіряй, завжди перевіряй", - технологія надання доступу з використанням безперервної оцінки довіри. Кожен запит на доступ оцінюється в режимі реального часу за набором динамічних критеріїв, таких як ідентифікація користувача, положення пристрою, геолокація, поведінка та розвідка про загрози. Оцінка довіри розраховується для кожного запиту доступу на основі контекстних факторів.

Доступ надається, відмовляється або обмежується на основі цього бала. Такий підхід дає змогу динамічно керувати умовами доступу, завдяки чому можна компенсовувати якісь конкретні невідповідності політиці безпеки іншими компенсуючими мірами. Щоб отримати доступ, потрібно набрати певну кількість балів і дотягнутися до прохідного рівня. Такий підхід в керуванні доступом потребує спеціалізованого обладнання з підтримкою постійної оцінки довіри та безпекових політик на базі безпекового рейтингу.

Переваги використання технології User ID Mapping в політиках фаєрволів:

- покращена безпека - забезпечує доступ до конфіденційних ресурсів лише аутентифікованим користувачам із відповідними ролями [11];
- детальна видимість - надає чітке розуміння того, "хто що зробив" у мережі [10];
- динамічні та адаптивні політики - політики розвиваються на основі поведінки користувачів і контексту в реальному часі [12].

Відображення ідентифікаторів користувачів у NGFW є невід'ємною частиною реалізації політик нульової довіри завдяки ввімкненню контролю доступу на основі ідентифікаційних даних. Він виходить за межі традиційних правил на основі IP-адреси, включаючи атрибути користувача та динамічний контекст для підвищення безпеки та узгодження з принципами нульової довіри. Це гарантує, що лише автентифіковані та авторизовані користувачі можуть отримати доступ до ресурсів, зменшуючи внутрішні та зовнішні загрози.

Одним з базових підходів, який забезпечує постійну перевірку, є саме збільшення точок перевірки підключень в інфраструктурі, а саме: поділ мережі на дрібні сегменти - впровадження мікросегментації. Цей підхід дає змогу зменшувати безконтрольні підключення між різними вузлами інфраструктури та збільшувати кількість точок контролю доступу між ними і так перевіряти їх. Така практика суттєво знижує горизонтальні переміщення в мережі у випадку

компрометації якоїсь її частини. У парі з резервуванням критичних елементів на рівні мікросегментації, навіть за компрометації і подальшої ізоляції будь-якого з сегментів, така інфраструктура може зберігати до 100 % своєї роботоздатності, ізолювавши виведений з ладу сегмент.

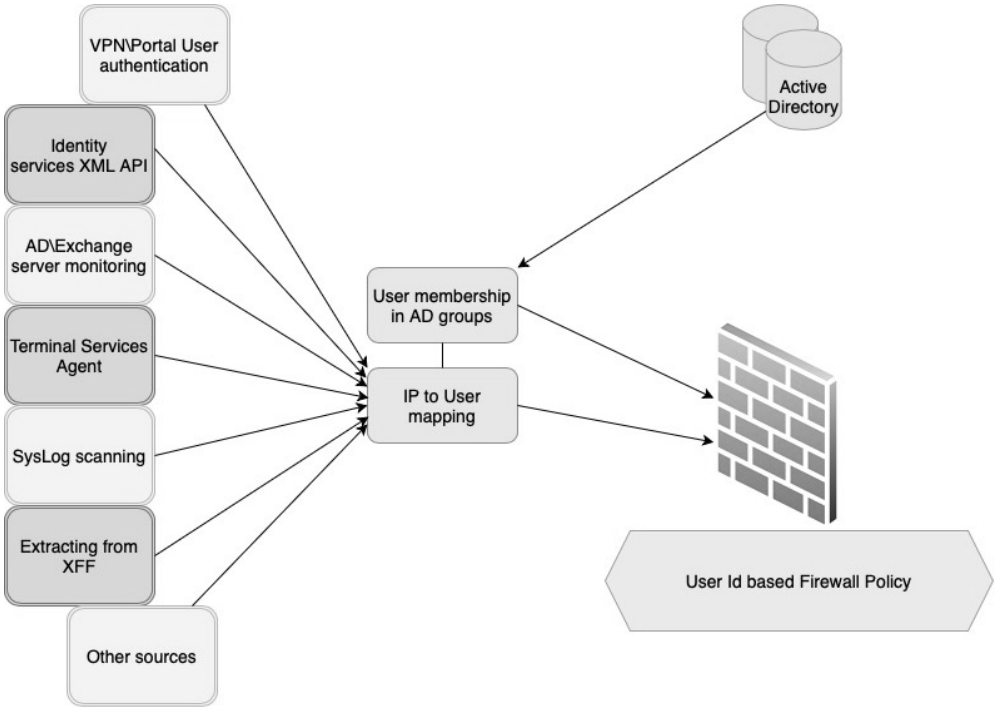

Рис. 1. Функція маппінгу айпі IP-адрес та користувачів

Застосування перевірки ідентичності користувача перед наданням доступу вирішує задачу автентифікації, проте може існувати ризик проникнення якогось шкідливого програмного забезпечення з робочої станції, котра пройшла аутентифікацію і начебто легітимно отримала доступ. Такий ризик може нівелюватися примусом до застосування робочих станцій під корпоративним управлінням, як додаток до автентифікації, де всі можливі ризики з шкідливим програмним забезпеченням чи зараженими файлами контролюються наявністю корпоративного набору безпекових аплікацій.

Відповідним елементом політики безпеки, який би це забезпечував, може бути функція оцінки стану пристрою, від якого відбувається підключення. Такий функціонал найчастіше трапляється в рішеннях ZTNA (Zero Trust Network Access), який передбачає використання спеціалізованого ВПН клієнта, з підтримкою збору інвентарної інформації хоста і передачу її фаєрвола під час підключення. Для підвищення рівня безпеки при наданні певного доступу фаєрволом важливо постійно оцінювати стан середовища робочої станції чи системи на віртуальній машині щодо наявності важливих безпекових факторів. До таких можна зарахувати:

- версія програмного забезпечення та статус оновлень;
- запущені процеси та встановлені програми;
- цілісність операційної системи;
- серійний номер.

Перевіряючи такі умови, можна впевнитися, що підключення відбувається з легітимного пристрою і наявність там шкідливого ПЗ є мінімальною, оскільки пристрій знаходиться під контролем корпоративних інструментів. Відповідність такому профілю використовується політикою безпеки файрвола як умова до її виконання, і якщо пристрій не проходить низку перевірок, то умова не виконується, і доступу ця політика не надасть.

В архітектурі нульової довіри (ZTA) запуск таких функцій безпеки, як антивірусне, антишпигунське програмне забезпечення, захист від зловмисного програмного забезпечення та фільтра-

ція даних, відіграє важливу роль у захисті ресурсів і забезпеченні надійного застосування політики. Ці функції розширюють можливості NGFW, надаючи додаткові рівні захисту від складних загроз і несанкціонованого доступу до даних.

NGFW із вбудованими можливостями захисту від вірусів і шпигунського програмного забезпечення перевіряють трафік у режимі реального часу, щоб ідентифікувати та блокувати зловмисне корисне навантаження. Системи виявлення зловмисного програмного забезпечення нульового дня використовують передові методи, як-от глибоке навчання, для виявлення невидимих загроз, забезпечуючи надійний захист від зловмисного програмного забезпечення, що розвивається [13]. Антишпигунське програмне забезпечення та поведінкова аналітика допомагають ідентифікувати та зривати APT, які часто націлені на чутливі системи, протягом тривалого часу. Нульова довіра у поєднанні з NGFW ефективно запобігає APT шляхом інтеграції мікросегментації та виявлення загроз у реальному часі [14].

Крім того, використання передових можливостей, таких як глибока перевірка пакетів (DPI), аналіз поведінки та динамічні оновлення із джерел даних про загрози, забезпечує проактивний захист від складних загроз, включно з атаками нульового дня та цілеспрямованими атаками (APT) [12]. Мікросегментація та фільтрація контенту в реальному часі додатково підсилюють безпеку шляхом ізоляції критично важливих ресурсів і забезпечення відповідності нормативним стандартам а засоби дешифрування шифрованого трафіку та фільтрування даних гарантують, що конфіденційну інформацію не викрадуть чи розкриють неавторизовані особи. Фільтрація даних у ZTA має вирішальне значення для захисту конфіденційних даних від внутрішніх і зовнішніх загроз шляхом моніторингу доступу та передачі [15].

Всі ці безпекові утиліти можна застосовувати точково до трафіку, доступ для якого описується політикою безпеки. Тобто політика безпеки, незважаючи на дію Allow, може все-таки заблокувати якусь його частину під час проходження через фаєрвол, якщо в даних, які передаються, було зафіксовані елементи заражених пакетів або ознаки якоїсь вразливості чи аномалії. Така діяльність є ще одним заходом дотримання принципу “ніколи не довіряй, завжди перевіряй” та покликана фіксувати потенційні загрози та захищати від них.

Однією з характерних особливостей фаєрволів нового покоління є використання сервісів розвідки загроз у реальному часі. Функції безпеки покладаються на дані про загрози в реальному часі, які можуть отримуватися від провайдерів таких послуг, щоб динамічно блокувати шкідливі URL-адреси, файли та IP-адреси. Оновлення в режимі реального часу дають змогу NGFW адаптуватися до нових загроз, забезпечуючи постійний захист [16]. Такі функції також можна підключати до трафіку, який описується політикою безпеки. Цей функціонал має підтримувати платформа фаєрвола, на базі якого будується архітектура нульової довіри. Такі сервіси мажуть надавати постачальники пратформи файрволу або сторонні безпекові сервер-провайдери з використанням інтеграції для динамічної доставки актуальних даних та індикаторів загроз безпосередньо до файрволів.

Результати дослідження

Особливість керування доступом політиками безпеки фаєрволів під час побудови архітектури нульової довіри полягає в насиченні політик безпеки додатковими контекстними умовами та використанні сучасних безпекових функцій фаєрволів. Такий підхід дає змогу суттєво зменшувати “щілини” у відкритому доступі, а мікросегментація і забезпечення виконання безпекових політик в кожній її точці та по всіх можливих напрямках дає змогу побудувати систему щільного контролю доступу. Порівняно з класичними політиками мережевих фаєрволів - політика безпеки в архітектурі нульової довіри обростає значною кількістю додаткових умов і атрибутів, що збільшує рівень захисту. На рис. 2 зображено структуру елементів політики фаєрвола, де зеленим кольором додано запропоновані до використанні умови, додаткові до класичних, які позначені білим. Ці атрибути має підтримувати виробник платформи мережевого файрвола та застосовувати як додаткові атрибути до основних.

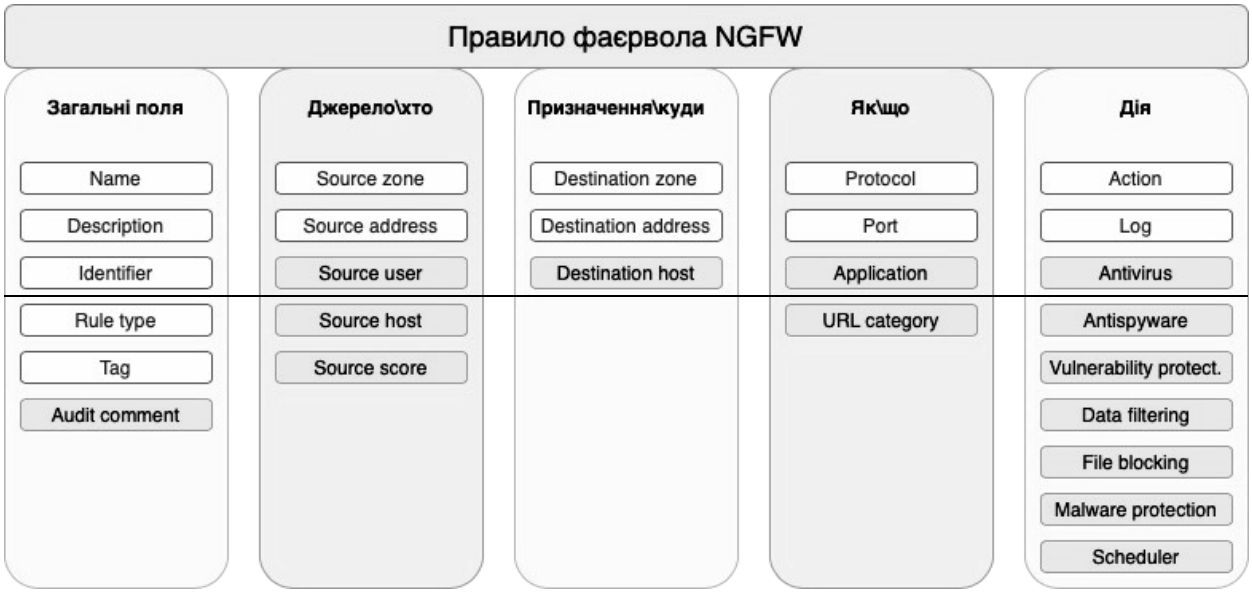

Рис. 2. Елементи політики безпеки фаєрволів нового покоління

Отже, створення політик для фаєрволів нового покоління (NGFW), що відповідають архітектурі нульової довіри (ZTA), потребує структурованого та комплексного підходу для забезпечення безпеки на кожному рівні мережевої взаємодії. Першим кроком є ідентифікація критичних ресурсів і застосування мікросегментації для їх ізоляції в менші, безпечні зони, що мінімізує ризик бічного руху загроз [17]. Політики також мають базуватися на ідентифікації користувачів, а не статичних IP-адресах, що дає змогу впроваджувати детальне управління доступом на основі ролей. Інтеграція провайдерів ідентифікації, таких як Active Directory або Okta, гарантує, що доступ до ресурсів отримують лише автентифіковані користувачі, дотримуючись принципу мінімально необхідних привілеїв [18].

Постійна автентифікація та авторизація є ключовими компонентами ZTA, які потребують перевірки користувачів та пристроїв протягом їхньої сесії. Це можна реалізувати за допомогою багатофакторної автентифікації (MFA) та моніторингу відповідності пристроїв і поведінки користувачів у реальному часі [19]. Динамічні політики, які враховують контекст, додатково підвищують рівень безпеки, адаптуючи правила на основі таких факторів, як геолокація, час доступу або стан пристрою. Наприклад, політика може обмежувати доступ до чутливих даних для користувачів, які входять у систему з ненадійних місць.

Автоматизація та штучний інтелект відіграють ключову роль у спрощенні управління політиками, даючи змогу динамічно оновлювати їх на основі даних про загрози. Автоматизовані платформи, такі як NEUTRON, оптимізують створення і тестування політик, знижуючи ризик помилок та адміністративні витрати [20]. Крім того, політики NGFW мають містити глибоку перевірку пакетів (DPI) для забезпечення захисту даних і дотримання нормативних вимог. Регулярне тестування та моніторинг цих політик є важливими для ідентифікації та усунення потенційних вразливостей перед їх впровадженням.

Керуючись принципами нульової довіри, у разі застосування тотального контролю інфраструктура підходить до стану, де будь-який її елемент у разі компрометації не буде суттєво впливати на стан і роботоздатність всіх інших систем. Тобто під час проєктування закладається таке сприйняття, що втручання вже відбулося, всі сегменти є локалізовані та компрометація будь-якого з них не має загрожувати нічим більшим, ніж той необхідний мінімальний доступ, який був наданий, і то до моменту, де стає відомо, що втручання відбулося і доступ для такого хоста блокується.

Дотримуючись цієї методології, організації можуть впроваджувати надійні політики NGFW, які відповідають принципам ZTA, забезпечуючи всебічний захист від сучасних загроз.

Висновки

Реалізація правил міжмережевого екрана (NGFW) відповідно до основних принципів архітектури нульової довіри (Zero Trust Architecture, ZTA) потребує динамічного, адаптивного та контекстно-орієнтованого підходу. Інтеграція принципів, таких як мінімально необхідний доступ, ніколи не довіряй, завжди перевіряй, постійна аутентифікація і авторизація, забезпечує надійну безпеку та зменшує поверхню атаки.

Інтеграція політик, які базуються на ідентифікації, оцінці довіри в реальному часі та передових функцій безпеки, таких як захист від шкідливих програм і фільтрація даних, дає змогу забезпечити детальний контроль за мережевим трафіком. Такий підхід не лише обмежує доступ до чутливих ресурсів, а й динамічно коригує дозволи залежно від змінних контекстних факторів, таких як стан пристрою, поведінка користувача та актуальні дані про загрози. Наприклад, динамічні політики для ефективної протидії порушенням та запобігання витоку даних, за умови нетипової активності, можуть вимагати повторну перевірку автентичності або блокувати доступ.

Отже, написання політик міжмережевого екрана для NGFW, які відповідають принципам нульової довіри, є багатогранним процесом, що вимагає постійної перевірки, динамічного виконання правил і комплексного управління загрозами. Прийняття таких стратегій дає змогу організаціям створити надійну та захищену мережеву інфраструктуру, що відповідає сучасним викликам безпеки в умовах архітектури нульової довіри.

Потрібно розуміти, що прагнення контролювати кожен необхідний доступ кожного з хостів корпоративної інфраструктури, як це трактують основні принципи на шляху до побудови архітектури нульової довіри, виливаються в значну складність, вартість та кількість ресурсів, необхідних як для побудови, так і для ефективної операційної підтримки інфраструктури зі значною кількістю точок контролю доступу. За такого ускладнення існують суттєві ризики зниження продуктивності мережевих послуг та критичного підвищення собівартості інфраструктурних та безпекових рішень, що може поставити під загрозу невиконання проєктів та задач, для яких вони будуються. Отже, напрямами майбутніх досліджень можуть бути пошуки ефективних шляхів оптимізації політик безпеки файрвола зі збереженням високого рівня захищеності корпоративної інфраструктури.

Список літератури

1. *Creutz L., Dartmann G. Decentralized Policy Enforcement in Zero Trust Architectures. 2023 IEEE Future Networks World Forum (FNWF). 2023. 1- 6. Doi: https://doi.org/10.1109/FNWF58287.2023.10520563.*
2. *Santis A., Castiglione A., Fiore U., Palmieri F. An intelligent security architecture for distributed firewalling environments. Journal of Ambient Intelligence and Humanized Computing. 2011. 4. 223- 234. Doi: https://doi.org/10.1007/s12652-011-0069-8.*
3. *Gokhale A., Kulkarni S. 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. 2024. Doi: https://doi.org/10.22214/ijraset.2024.58201.*
4. *Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. 2019. Doi: https://doi.org/10.6028/nist.sp.800-207-draft.*
5. *Zhang C., He J., Fan B., Gong Y., Li S., Yin B., Lin Y. Tag-Based Trust Evaluation In Zero Trust Architecture. 2022 4th International Academic Exchange Conference on Science and Technology Innovation (IAECST), 2022. 772- 776. Doi: https://doi.org/10.1109/IAECST57965.2022.10062213.*
6. *Keeriyattil S. Microsegmentation and Zero Trust: Introduction. Zero Trust Networks with VMware NSX. 2019. Doi: https://doi.org/10.1007/978-1-4842-5431-8_2.*
7. *Bradatsch L., Miroshkin O., Kargl F. ZTSFC: A Service Function Chaining-Enabled Zero Trust Architecture. IEEE Access. 2023. 11. 125307- 125327. Doi: https://doi.org/10.1109/ACCESS.2023.3330706.*
8. *Shipman M., Millwater N., Owens K., Smith S. A Zero Trust Architecture for Automotive Networks. SAE Technical Paper Series. 2024. Doi: https://doi.org/10.4271/2024-01-2793.*
9. *Implicit Trust vs. Explicit Trust in Access Management. URL: https://www.strongdm.com/blog/implicit-trust-vs-explicit-trust, (Accessed: 12.01.2025).*
10. *Habash R., Khalel M. Zero trust security model for enterprise networks. Iraqi Journal of Information and Communication Technology. 2023. Doi: https://doi.org/10.31987/ijict.6.2.223.*

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

12. Jin Q., Wang L. Zero-Trust Based Distributed Collaborative Dynamic Access Control Scheme with Deep Multi-Agent Reinforcement Learning. EAI Endorsed Trans. Security Safety. 2021. 8, e2. Doi: https://doi.org/ 10.4108/eai.25-6-2021.170246.

13. Kim J., Bu S., Cho S. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. Inf. Sci. 2018. 460- 461, 83- 102. Doi: https://doi.org/10.1016/j.ins.2018.04.092.

14. Da Rocha B., De Melo L., De Sousa R. Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model. 2021 Workshop on Communication Networks and Power Systems (WCNPS), 2021. 1- 6. Doi: https://doi.org/10.1109/WCNPS53648.2021.9626270.

15. Ahmed I., Nahar T., Urmi S., Taher K. Protection of Sensitive Data in Zero Trust Model. Proceedings of the International Conference on Computing Advancements. 2020. Doi: https://doi.org/10.1145/3377049.3377114.

16. Vinayakumar R., Alazab M., Member I., Poornachandran P., Venkatraman A. Robust Intelligent Malware Detection Using Deep Learning. IEEE Access. 2019. 7. 46717- 46738. Doi: https://doi.org/10.1109/ ACCESS. 2019.2906934.

17. Liu Y., Liu G., Du H., Niyato D., Kang J., Xiong Z., Kim D., Shen X. Hierarchical Micro-Segmentations for Zero-Trust Services via Large Language Model (LLM)-enhanced Graph Diffusion. ArXiv. 2024. abs/2406.13964. Doi: https://doi.org/10.48550/arXiv.2406.13964.

18. Prydybaylo O. Zero trust architecture logical components and implementation approaches. Connectivity. 2024. Doi: https://doi.org/10.31673/2412-9070.2024.030711.

19. Xu M., Guo J., Yuan H., Yang X. Zero-Trust Security Authentication Based on SPA and Endogenous Security Architecture. Electronics. 2023. Doi: https://doi.org/10.3390/electronics12040782.

20. Katsis C., Cicala F., Thomsen D., Ringo N., Bertino E. NEUTRON: A Graph-based Pipeline for Zero-trust Network Architectures. Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy. 2022. Doi: https://doi.org/10.1145/3508398.3511499.

FEATURES OF NETWORK ACCESS MANAGEMENT OF CORPORATE SYSTEMS IN ZERO TRUST ARCHITECTURE

R. M. Syrotynskyi, I. Y. Tyshyk

Lviv Polytechnic National University,
Department of Information Protection

The fundamental principles of zero trust are examined, and the challenges of adhering to them are analyzed when deploying a network infrastructure using classical security model approaches. Relying on traditional methods for writing firewall rules does not allow for flexible regulation of access to corporate systems within the network or for maintaining the principle of least privilege. Moreover, the need for continuous verification and authentication of nodes before granting network access raises the issue of integrating application processes into the network interaction between the host and the firewall.

Modern practices for writing firewall rules and methods for adhering to zero trust architecture principles are investigated, with a focus on leveraging the advanced technical capabilities of next-generation firewalls. Strategies for minimizing "backdoor" access when writing firewall access control rules are analyzed. Various options for enriching security policies with additional contextual conditions are explored, and methods for authenticating network nodes using next-generation firewalls are identified.

A methodology for writing network firewall rules in accordance with the principle of least privilege is proposed, and the potential of user-to-IP mapping technology for implementing continuous node authentication and authorization in the network is examined, all in service of the "never trust, always verify" principle. By following these practical recommendations, organizations can strengthen the protection of their network infrastructure, enhance network visibility, and ensure stable operations in an environment where trust is no longer implicit but is established at every stage of access.

Keywords: network access management, corporate systems, zero trust architecture, authorization, control.