ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод впровадження ZTNA моделі мережевої безпеки на підприємстві»

зі спеціальності *126 Інформаційні системи та технології*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційні системи та технології*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Любомир ФЕДОРОВ
(підпис)

Виконав: здобувач вищої освіти групи ІСД-42
Любомир ФЕДОРОВ
(прізвище, ім'я)

Керівник PhD, доцент каф. ІСТ Дмитро КОЗЛОВ
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційних систем та технологій
Ступінь вищої освіти бакалавр
Спеціальність 126 Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
Каміла СТОРЧАК

“____” _____2026 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Федорову Любомиру Володимировичу
(прізвище, ім’я, по батькові здобувача)

1.Тема кваліфікаційної роботи: «Метод впровадження ZTNA моделі мережевої безпеки на підприємстві»
керівник кваліфікаційної роботи: Козлов Дмитро, PhD, доцент кафедри ІСТ
(ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “ 20 ” лютого 2026 р. №

2. Строк подання кваліфікаційної роботи «1» червня 2026 р.

3. Вихідні дані кваліфікаційної роботи:
1. Дані про топологію мережі та віддалений доступ до CRM-системи ТОВ «Арма Моторс».
2. Міжнародні стандарти архітектури Zero Trust.
3. Технічна документація платформи Cloudflare та вебсервера Nginx.
4. Аналітичні звіти щодо кіберзагроз і вразливостей VPN.
5. Статистичні та фінансові дані для розрахунку економічної ефективності.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Аналіз кіберзагроз та вразливостей традиційних VPN-мереж.
2. Теоретичні основи та стандарти архітектури Zero Trust.

3. Практичне проєктування інфраструктури нульової довіри
4. Оцінка ризиків та розрахунок економічної ефективності впровадження.

5.Перелік ілюстраційного матеріалу: *презентація*
6. Дата видачі завдання «20» лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Пошук, збір та аналіз науково-технічної літератури щодо проблематики VPN та концепції Zero Trust.	24.02-03.03.25	
2.	Дослідження архітектури традиційних периметральних мереж та аналіз сучасного ландшафту кіберзагроз.	04.03-17.03.25	
3.	Теоретичне та архітектурне обґрунтування моделі Zero Trust, вивчення міжнародних стандартів	18.03-31.03.25	
4.	Проєктування інфраструктури нульової довіри на базі Cloudflare та розрахунок економічної ефективності.	01.04-24.04.25	
5.	Написання висновків, оформлення пояснювальної записки та списку джерел.	25.04-16.05.25	
6.	Перевірка роботи на наявність академічного плагіату, усунення зауважень, отримання відгуку керівника.	19.05-20.05.25	
7.	Оформлення бакалаврської роботи, підготовка презентації.	21.05-30.05.25	

Здобувач вищої освіти _____ Любомир ФЕДОРОВ
(підпис) *(ім'я, ПРІЗВИЩЕ)*
Керівник кваліфікаційної роботи _____ Дмитро КОЗЛОВ
(підпис) *(ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 67 сторінок, 25 рисунків, 4 таблиці, 24 джерела.

Мета роботи – підвищення рівня інформаційної безпеки корпоративної мережі підприємства, зокрема доступу до внутрішньої системи управління відносинами з клієнтами ТОВ «Арма Моторс», шляхом проєктування, налаштування та практичного впровадження архітектури Zero Trust Network Access.

Об'єкт дослідження – процес забезпечення інформаційної безпеки та захисту корпоративних інфраструктур підприємств в умовах використання віддаленого та гібридного режимів роботи.

Предмет дослідження – методи, моделі та технологічні засоби побудови архітектури Zero Trust Network Access на прикладі платформи Cloudflare для ізоляції та захисту внутрішніх вебсервісів.

Короткий зміст роботи: Робота присвячена міграції ТОВ «Арма Моторс» із застарілих VPN-технологій на архітектуру нульової довіри. Перший розділ обґрунтовує вразливість традиційного мережевого периметра. Другий розділ містить аналіз стандартів NIST і CISA та методів мікросегментації корпоративної інфраструктури. Третій розділ описує розгортання безпекової екосистеми Cloudflare. Технологія Cloudflare Tunnel ліквідувала вхідні порти, а політики доступу забезпечили перевірку кінцевих пристроїв. Фінансові збитки підприємства від кібератак зменшено вдесятеро. Розрахунок економічного коефіцієнта ROSI повністю підтвердив високу доцільність модернізації захисту корпоративної мережі.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ, ZERO TRUST, ZTNA, VPN, МІКРОСЕГМЕНТАЦІЯ, CLOUDFLARE, УПРАВЛІННЯ РИЗИКАМИ, ROSI.

ЗМІСТ

ВСТУП 8
1 ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ПОБУДОВИ ЗАХИЩЕНИХ МЕРЕЖ ЗА МОДЕЛЛЮ ZERO TRUST 11
1.1. Аналіз сучасного стану кіберзагроз та вразливостей традиційних VPN мереж 11
1.2. Теоретичні концепції та архітектура моделі Zero Trust Network Access 14
1.3. Порівняльний аналіз сучасних програмних рішень класу Zero Trust Network Access 16
1.4. Архітектурні засади ізоляції корпоративних ресурсів за моделлю Zero Trust 19
1.5 Проєктування політик безпеки та мікросегментація в архітектурі ZTNA 22
2 АНАЛІЗ СТАНУ МЕРЕЖЕВОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ 30
2.1. Загальна характеристика ІТ-інфраструктури та діючої системи інформаційної безпеки підприємства 30
2.2. Аналіз вразливостей, загроз та оцінка ризиків існуючої мережевої архітектури 31
2.3. Обґрунтування проблематики діючої системи безпеки та необхідності переходу до моделі ZTNA на досліджуваному підприємстві 36
3 ПРОЄКТУВАННЯ ТА ПРАКТИЧНЕ ВПРОВАДЖЕННЯ АРХІТЕКТУРИ ZERO TRUST 38
3.1. Розробка покрокового методу (алгоритму) впровадження моделі ZTNA в корпоративну мережу підприємства 38
3.2. Вибір програмно-апаратних засобів та формування архітектури рішення для досліджуваної організації 40
3.3. Технічна реалізація та експериментальна перевірка працездатності розробленого рішення 43
3.4. Оцінка ефективності запропонованого методу та розрахунок доцільності його практичного впровадження 58
ВИСНОВКИ 64
ПЕРЕЛІК ПОСИЛАНЬ 66
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 69

ВСТУП

Актуальність теми. Невпинний розвиток інформаційних технологій, ускладнення інфраструктури та глобальний перехід компаній до гібридного або повністю віддаленого формату роботи викликали зміну підходів до побудови корпоративних мереж. Традиційно склалося так, що при створенні більшості мереж, покладалися на периметральну модель безпеки, наприклад, використання віртуальних приватних мереж – VPN. Ця модель базується на помилковому припущенні, що всі користувачі та пристрої всередині корпоративної мережі є довіреними за замовчуванням.

Сучасний ландшафт кіберзагроз доводить неефективність такого підходу. Використання традиційних VPN вимагає відкриття портів на маршрутизаторах, що робить інфраструктуру вразливою до автоматизованого сканування, підбору паролів та експлуатації вразливостей шлюзів. Це критично для таких підприємств, як ТОВ «Арма Моторс», де корпоративна система управління відносинами з клієнтами містить конфіденційні дані. Злам периметра дозволяє зловмиснику отримати безперешкодний доступ до внутрішніх ресурсів та розгорнути шкідливе програмне забезпечення.

У зв'язку з цим виникає гостра необхідність переходу від застарілих моделей до сучасної архітектури нульової довіри, відомої як Zero Trust Network Access. Ця парадигма передбачає повну відмову від концепції довіреної мережі. В архітектурі нульової довіри доступ до додатків надається виключно після суворої багатофакторної ідентифікації користувача та глибокої перевірки безпекового стану його пристрою, незалежно від того, звідки відбувається підключення. Більше того, використання хмарних брокерів та захищених вихідних тунелів дозволяє повністю ізолювати корпоративні ресурси від публічного інтернету. Відповідно, дослідження та практичне впровадження архітектури Zero Trust Network Access для захисту корпоративних ресурсів підприємства є актуальним науково-практичним завданням.

Мета дослідження – підвищення рівня інформаційної безпеки корпоративної мережі підприємства, зокрема доступу до внутрішньої системи управління відносинами з клієнтами ТОВ «Арма Моторс», шляхом проєктування, налаштування та практичного впровадження архітектури Zero Trust Network Access.

Завдання дослідження:

1. Проаналізувати сучасні кіберзагрози спрямовані на віддалений доступ та виявити критичні вразливості традиційних периметральних мереж.
2. Дослідити теоретичні засади та базові принципи побудови інфраструктури за моделлю нульової довіри.
3. Спроєктувати нову безпекову топологію мережі підприємства з використанням хмарного брокера та мікросегментації доступу.
4. Практично реалізувати тестовий стенд архітектури нульової довіри на базі технологій Cloudflare шляхом розгортання захищеного тунелю, налаштування політик авторизації та перевірки міжмережевого екрана кінцевої точки.
5. Провести тестування впровадженої системи безпеки під час імітації спроб несанкціонованого доступу та економічно обґрунтувати доцільність впровадження розробленого рішення.

Об'єкт дослідження – процес забезпечення інформаційної безпеки та захисту корпоративних інфраструктур підприємств в умовах використання віддаленого та гібридного режимів роботи співробітників.

Предмет дослідження – методи, моделі та технологічні засоби побудови архітектури Zero Trust Network Access на прикладі платформи Cloudflare для ізоляції та захисту внутрішніх вебсервісів.

Методи дослідження. Під час виконання роботи використовувалися метод системного аналізу для вивчення недоліків класичних віртуальних приватних мереж, метод топологічного моделювання для проєктування нової архітектури мережі, а також методи натурного експерименту та тестування під час розгортання та перевірки працездатності практичного стенда.

Наукова новизна одержаних результатів полягає в удосконаленні архітектурного підходу до захисту віддаленого доступу до критичних корпоративних ресурсів підприємства. На відміну від традиційних рішень, у роботі запропоновано та обґрунтовано комплексну модель мікросегментації доступу для підприємства автомобільної галузі на базі концепції нульової довіри з використанням хмарного брокера. Набув подальшого розвитку метод ізоляції мережевої інфраструктури, що за рахунок використання вихідних шифрованих тунелів дозволило реалізувати парадигму невидимої мережі, тобто відмову від відкритих вхідних портів маршрутизатора, та якісно підвищити стійкість корпоративної системи до автоматизованого сканування і кібератак.

Практична значущість. Одержані результати мають безпосереднє прикладне значення. Розроблена мережева архітектура, протестований програмно-апаратний стенд та сформована матриця контролю доступу готові до повноцінного розгортання в робочій інфраструктурі ТОВ «Арма Моторс». Впровадження запропонованого рішення дозволяє компанії відмовитися від публічних вхідних портів на маршрутизаторах і гарантовано мінімізувати ризики компрометації внутрішньої системи управління відносинами з клієнтами у випадку цілеспрямованих кібератак.

Апробація результатів. Основні положення та результати дослідження пройшли апробацію на:

1. VII Науково-технічна конференція «Сучасний стан та перспективи розвитку IoT» (Київ, ДУІКТ, 20 квітня 2026р.). Тези доповіді на тему «Метод підвищення безпеки IoT-мереж на основі архітектури zero trust» опубліковані у збірнику матеріалів конференції (стор. 240).

2. III Всеукраїнська науково-технічна конференція «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» (Київ, ДУІКТ, 18 листопада 2025 р.). Тези доповіді на тему «Екологічна модернізація мережевої інфраструктури» опубліковані у збірнику матеріалів конференції (стор. 222).

1 ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ПОБУДОВИ ЗАХИЩЕНИХ МЕРЕЖ ЗА МОДЕЛЛЮ ZERO TRUST

1.1. Аналіз сучасного стану кіберзагроз та вразливостей традиційних VPN мереж

Протягом останнього десятиліття, а особливо після масового переходу компаній до гібридних форматів роботи, вимоги до корпоративних мереж зазнали суттєвих трансформацій. Раніше інформаційні ресурси підприємств знаходилися переважно у фізичних межах офісів, що дозволяло досить ефективно захищати їх за допомогою класичних міжмережевих екранів. На теперішній час необхідність забезпечення постійного віддаленого доступу для співробітників, підрядників та партнерів повністю розмила традиційний мережевий периметр.

Для організації такого доступу розповсюдженою і загальноприйнятою стала технологія віртуальних приватних мереж або VPN [21]. Кіберзагрози та атаки розвиваються дедалі швидше та вимагають скоординованої, проактивної, адаптивної та гнучкої оборонної відповіді. Традиційні підходи до захисту периметра або «замку та рову», засновані на звичайних моделях автентифікації та авторизації, неефективно допомагають протистояти поточним і майбутнім векторам кібератак. У цій моделі міжмережевий екран виступає в ролі захисного бар'єру, а шлюз віртуальної приватної мережі виконує функцію єдиних воріт. Після того як користувач вводить правильні облікові дані, він отримує допуск всередину фортеці (рис. 1.1).

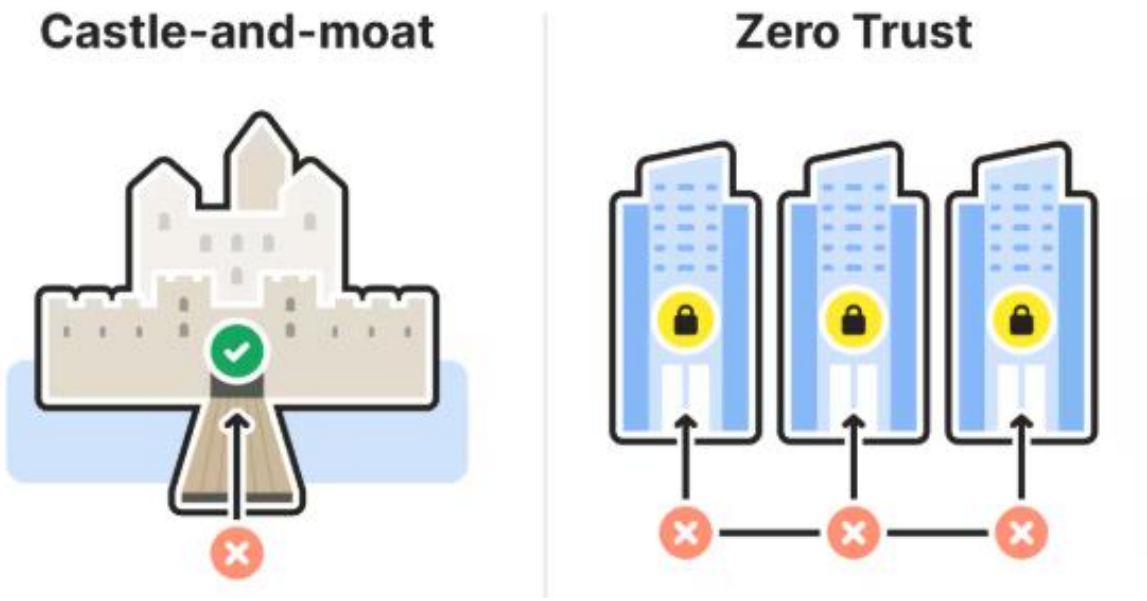


Рисунок 1.1 – Концептуальна відмінність периметральної моделі від мікросегментації Zero Trust

Аналіз сучасного ландшафту кіберзагроз доводить, що така архітектура має фундаментальні недоліки. Принцип надмірної довіри за замовчуванням є головною концептуальною вразливістю традиційних рішень. Коли користувач успішно проходить автентифікацію на шлюзі, він опиняється у внутрішній локальній мережі підприємства і найчастіше отримує широкий доступ до багатьох корпоративних ресурсів, навіть тих, які не потрібні йому для виконання безпосередніх робочих обов'язків.

У випадку компрометації облікових даних легального працівника за допомогою методів соціальної інженерії або фішингу зловмисник отримує ті ж самі широкі привілеї. Це дозволяє атакуючій стороні здійснювати горизонтальне переміщення всередині корпоративної мережі, досліджувати топологію, знаходити сервери баз даних та безперешкодно розгортати шкідливе програмне забезпечення, зокрема віруси-шифрувальники.

Окрім архітектурних прогалин, існують критичні технологічні вразливості, пов'язані з самою природою роботи віртуальних приватних мереж. Для того, щоб віддалений працівник міг підключитися до корпоративного шлюзу, на маршрутизаторі підприємства обов'язково має бути відкритий вхідний мережевий

порт, який «слухає» запити з публічного інтернету. Наявність таких відкритих портів робить компанію видимою для всього світу. Зловмисники використовують спеціалізовані автоматизовані сканери для безперервного пошуку відкритих точок входу. Виявивши такий порт, вони починають застосовувати атаки повного перебору паролів або експлуатують відомі вразливості нульового дня у програмному забезпеченні самого шлюзу [24].

Ще одним суттєвим недоліком є відсутність дієвого контролю за станом безпеки кінцевих пристроїв користувачів. Традиційні засоби віддаленого доступу фокусуються виключно на перевірці логіна та пароля, ігноруючи контекст підключення. Якщо працівник підключається до корпоративної мережі з домашнього комп'ютера, який уже заражений шкідливим кодом і не має активного антивірусного захисту, створений зашифрований тунель стає безпечним каналом для проникнення загроз безпосередньо в серцевину інфраструктури компанії.

Для сучасного бізнесу, зокрема підприємств автомобільної галузі, які оперують системами управління відносинами з клієнтами та зберігають великі масиви персональних даних, такі ризики є неприйнятними. Витік бази даних клієнтів через скомпрометований доступ або зупинка бізнес-процесів через шифрування серверів призводять до катастрофічних фінансових та репутаційних втрат.

Таким чином, результати аналізу свідчать про те, що еволюція кібератак випередила можливості класичних периметральних систем захисту [10]. Для забезпечення надійного захисту корпоративних вебсервісів та внутрішніх ресурсів підприємства демонструють необхідність нової, більш надійної системи кібербезпеки, яка сприятиме прийняттю обґрунтованих рішень на основі ризиків. Безпека на основі принципу нульової довіри усуває традиційну ідею периметрів, довірених мереж, пристроїв, персон або процесів і переходить до рівнів довіри на основі кількох атрибутів, які дозволяють застосовувати політики автентифікації та авторизації, засновані на концепції найменш привілейованого доступу. Впровадження принципу нульової довіри вимагає розробки ефективнішої

архітектури, яка покращує безпеку, взаємодію з користувачем та загальну продуктивність.

1.2. Теоретичні концепції та архітектура моделі Zero Trust Network Access

На противагу критичним недолікам традиційних периметральних мереж у сфері інформаційної безпеки виникла нова парадигма, що отримала назву нульової довіри [22]. Цю концепцію вперше запропонував Джон Кіндерваг у 2010 році, працюючи аналітиком у Forrester Research, і вона базується на простому принципі «ніколи не довіряй, завжди перевіряй». Основна ідея полягає у повній відмові від поняття довіреної внутрішньої мережі [5]. Система обробляє кожен запит на доступ так, ніби він надходить з відкритого ворожого середовища публічного інтернету і впроваджує безперервну автентифікацію та суворий контроль доступу для всіх користувачів, пристроїв й програм, незалежно від їхнього місцезнаходження чи мережі.

Архітектура Zero Trust Network Access реалізує цю парадигму на практиці, відокремлюючи площину управління доступом від площини передачі даних [14]. На відміну від класичних віртуальних приватних мереж, які надають користувачеві доступ до всієї локальної мережі після одноразової перевірки пароля, архітектура нульової довіри функціонує на рівні окремих додатків і сервісів. Це означає, що користувач отримує дозвіл на підключення лише до конкретної системи, необхідної для роботи. Наприклад, менеджер отримує доступ лише до корпоративної системи управління відносинами з клієнтами, залишаючи себе ізольованим від бухгалтерських баз даних або інших серверів підприємства. Цей підхід називається мікросегментацією мережі і базується на принципі найменших привілеїв. Побудова захищеної інфраструктури за моделлю Zero Trust спирається на кілька ключових теоретичних принципів [6, 7].

Перший принцип – динамічна та безперервна автентифікація. Система не просто перевіряє логін і пароль під час першого підключення; вона вимагає

використання багатофакторної ідентифікації і постійно аналізує контекст запиту протягом усього сеансу.

Другий принцип – оцінка безпекового стану кінцевої точки підключення. В архітектурі нульової довіри ідентифікація самого працівника недостатня для надання доступу. Система обов'язково перевіряє пристрій, з якого здійснюється спроба входу. Оцінюється наявність встановленого корпоративного клієнта безпеки, статус міжмережевого екрана операційної системи, актуальність антивірусних баз і відсутність ознак шкідливого програмного забезпечення. Якщо легальний користувач намагається увійти в корпоративну систему з неперевіреного або зараженого комп'ютера, доступ буде миттєво заблоковано в рамках політик безпеки.

Третій принцип – приховування інфраструктури від прямого публічного доступу. У моделі Zero Trust Network Access корпоративні сервери ніколи не підключаються до інтернету безпосередньо через відкриті порти маршрутизатора. Замість цього використовується концепція хмарного брокера доступу. Посередник з безпеки доступу до хмарних сервісів (CASB) захищає хмарні сервіси від загроз безпеці. Cloudflare CASB забезпечує повний огляд і контроль над внутрішніми інформаційними ресурсами, щоб запобігти витоку даних та порушенням вимог до відповідності. Він допомагає виявляти внутрішні загрози, тіньові IT-системи, ризикований обмін даними та зловмисників. Цей брокер виступає посередником між зовнішнім користувачем і внутрішнім ресурсом компанії. Всі запити на підключення спочатку надходять до хмарної інфраструктури брокера, де проходять ретельну перевірку встановлених правил. Лише після успішної авторизації брокер з'єднує користувача з необхідним ресурсом через спеціально створений безпечний канал.

Впровадження такої архітектури кардинально змінює рівень захищеності підприємства. Навіть у випадку успішної фішингової атаки і викрадення пароля співробітника, зловмисник не зможе отримати доступ до корпоративної мережі, оскільки його комп'ютер не пройде перевірку безпеки. Більше того, повна відсутність відкритих портів робить компанію невидимою для автоматизованих

хакерських сканерів, що зменшує ефективність більшості сучасних мережевих атак. Узагальнюючи ці теоретичні концепції складено порівняння основних відмінностей між загальноприйнятим підходом та моделлю ZTNA (таблиця 1.1) .

Таблиця 1.1

Порівняльна характеристика традиційної VPN-моделі та архітектури Zero Trust

Критерій порівняння	Традиційна модель безпеки (VPN)	Архітектура нульової довіри (ZTNA)
Периметр довіри	Надається за замовчуванням після перетину зовнішнього периметра	Повна відсутність довіри, постійна перевірка кожного запиту
Принцип доступу	Широкий доступ до всієї локальної мережі (VLAN)	Мікросегментація, доступ лише до конкретного дозволеного додатка
Видимість в інтернеті	Сервери мають відкриті вхідні порти, вразливі до сканування	Сервери приховані за хмарним брокером через вихідні тунелі
Контроль пристроїв	Зазвичай відсутній або мінімальний (перевіряється лише пароль)	Сувора перевірка стану кінцевої точки (антивірус, ОС, локальний брандмауер)
Наслідки компрометації пароля	Зловмисник отримує свободу горизонтального переміщення мережею	Блокування доступу через невідповідність пристрою політикам безпеки

1.3. Порівняльний аналіз сучасних програмних рішень класу Zero Trust Network Access

Швидке зростання ринку рішень для реалізації архітектури нульової довіри зумовило появу великої кількості платформ від провідних світових вендорів. Для обґрунтування вибору технології Cloudflare Zero Trust для впровадження в IT-інфраструктуру ТОВ «Арма Моторс» необхідно провести критичний огляд та порівняльний аналіз найбільш розповсюджених систем цього класу, зокрема Zscaler Private Access (ZPA), Cisco Duo та Perimeter 81.

Першим вагомим конкурентом у сегменті ZTNA є платформа **Zscaler Private Access [20]**. Це хмарне рішення корпоративного рівня, яке повністю замінює традиційні VPN. Основними перевагами Zscaler є використання глобальної мережі точок присутності та глибока перевірка трафіку без створення затримок. Однак, незважаючи на потужний функціонал, ZPA орієнтований на великі корпорації із багатотисячним штатом працівників. Процес впровадження цієї системи є надзвичайно складним та вимагає високої кваліфікації персоналу для підтримки, а гнучкість цінової політики для малих та середніх підприємств (SME), до яких відноситься досліджуване підприємство, є обмеженою.

Другим значущим гравцем є Cisco Duo [4]. Рішення фокусується переважно на автентифікації за багатьма критеріями та перевірці стану кінцевих точок. Головною перевагою Cisco Duo є легкість інтеграції з наявними апаратними брандмауерами Cisco, які часто використовуються в корпоративних мережах. Проте Duo виступає скоріше як додатковий рівень безпеки поверх існуючої інфраструктури, ніж як цілісний метод ізоляції мережевого периметра. На відміну від технології тунелювання, Cisco Duo часто потребує наявності публічних точок входу, що суперечить концепції «невидимої мережі», яка є пріоритетною для захисту CRM-системи.

Рішення Perimeter 81 позиціонується як сучасна альтернатива VPN для малого та середнього бізнесу [13]. Воно пропонує зручний веб-інтерфейс та швидке розгортання програмних шлюзів. Проте Perimeter 81 базується на моделі хмарного VPN що все ще передбачає створення віртуальних мережевих вузлів, які можуть бути ідентифіковані зловмисниками. Крім того, вартість користування цією

системою зростає в залежності від кількості підключених ресурсів та користувачів, що робить її менш привабливою з точки зору економічної ефективності.

Для систематизації результатів аналізу було сформовано порівняльну таблицю (таблиця 1.2), де оцінено ключові параметри рішень за п'ятибальною шкалою.

Таблиця 1.2

Порівняльна характеристика провідних ZTNA-рішень

Критерій порівняння	Cloudflare Zero Trust	Zscaler Private Access	Cisco Duo	Perimeter 81
Скриття мережевого периметра (Stealth)	5	5	3	4
Легкість впровадження (SME сегмент)	5	2	4	5
Перевірка стану пристрою (Posture)	5	5	5	4
Глобальна мережа передачі даних	5	5	3	3
Економічна доступність	5	1	3	4
Можливість мікросегментації	5	5	4	4

Як свідчать дані таблиці 1.2, Cloudflare Zero Trust є найбільш збалансованим рішенням для ТОВ «Арма Моторс». Його ключовою перевагою є технологія вихідних тунелів (Cloudflare Tunnel), яка дозволяє повністю закрити вхідні порти маршрутизатора, роблячи внутрішні сервери невидимими для інтернету. На відміну від конкурентів, Cloudflare надає повноцінний функціонал корпоративного

захисту безкоштовно для команд до 50 осіб, що є великою перевагою і ідеально відповідає потребам адміністративного апарату дилерського центру.

Таким чином, вибір екосистеми Cloudflare є технічно обґрунтованим та економічно доцільним кроком. Вона дозволяє реалізувати всі принципи нульової довіри – від багатофакторної ідентифікації до динамічного контролю за безпекою кінцевих пристроїв. Без закупівлі додаткового дороговартісного обладнання чи складного перепроектування існуючої топології мережі підприємства.

1.4. Архітектурні засади ізоляції корпоративних ресурсів за моделлю Zero Trust

Практична реалізація теоретичної моделі нульової довіри вимагає використання спеціалізованих платформ, які здатні виконувати роль глобального посередника між користувачами та корпоративними ресурсами. Одним із провідних рішень на сучасному ринку кібербезпеки є архітектура Cloudflare Zero Trust. Цей хмарний брокер змінює класичний принцип маршрутизації трафіку та забезпечує повну ізоляцію внутрішніх вебсервісів підприємства, зокрема систем управління відносинами з клієнтами.

Зазвичай в архітектурі Zero Trust беруть участь дві технології. По-перше, безпечний веб-шлюз (SWG) фільтрує вихідний трафік, призначений для Інтернету, і блокує доступ користувачів до веб-сайтів високого ризику, таких як ті, що беруть участь у фішингових кампаніях. Потім, щоб забезпечити віддалений доступ користувачів до SaaS-додатків, внутрішньо розміщених додатків і мереж, використовуються служби Zero Trust Network Access для створення безпечних тунелів і забезпечення доступу віддалених користувачів до приватних додатків.
На відміну від традиційної моделі, де для доступу до внутрішнього вебсервера потрібно налаштовувати переадресацію портів на зовнішньому маршрутизаторі, ця методика використовує концепцію вихідних з'єднань. Усередині локальної мережі підприємства, поруч із цільовим сервісом, розгортається легковажна служба, відома в технічні документації як демон cloudflared. Цей компонент самостійно

ініціює кілька захищених вихідних з'єднань до найближчих глобальних центрів обробки даних хмарного брокера.

Такий архітектурний підхід дозволяє системному адміністратору налаштувати головний маршрутизатор підприємства в режим повного блокування всіх вхідних з'єднань з інтернету. Оскільки внутрішній сервер сам прокладає зашифрований шлях назовні, він більше не потребує відкритих портів для очікування вхідного трафіку. Для зовнішнього спостерігача або автоматизованого хакерського сканера корпоративна мережа стає абсолютно невидимою. Вона формує ефект чорної діри, де будь-які несанкціоновані пакети даних просто відкидаються маршрутизатором без відповіді.

Доступ легальних користувачів до ізольованого вебсервісу організовується через компонент Cloudflare Access. Коли віддалений працівник намагається відкрити корпоративний портал, його запит маршрутизується не на публічну IP-адресу компанії, а безпосередньо до хмарної інфраструктури брокера. Тут, на межі мережі, відбувається перетин трафіку користувача та трафіку внутрішнього сервера.

Перед тим як дозволити даним пройти через вихідний тунель всередину корпоративної мережі, брокер застосовує суворі політики безпеки. На початку Cloudflare Access виступає як постачальник ідентифікації, вимагаючи підтвердження особи від користувача за допомогою одноразових паролів або інтеграції з корпоративними електронними адресами. Одночасно активується механізм Device Posture. Завдяки клієнту Cloudflare WARP, встановленому на комп'ютері користувача, система в реальному часі аналізує стан безпеки пристрою. Перевіряється активація локального міжмережевого екрана, наявність актуального антивірусного програмного забезпечення та інші параметри, визначені політикою підприємства.

Лише за умови одночасного успішного проходження ідентифікації особи та перевірки безпекового стану пристрою хмарний брокер з'єднує користувача з внутрішнім вебсервісом через захищений тунель. Якщо ж запит надходить від невідомого пристрою або користувач не проходить перевірку, з'єднання

розривається ще на рівні хмари, так і не досягнувши фізичного периметра підприємства.

Cloudflare дозволяє організаціям полегшувати доступ до програм за допомогою хмари підключення, яка безпечно з'єднує користувачів, програми та дані незалежно від їхнього місцезнаходження. Основою платформи є розгалужена глобальна мережа Cloudflare , яка забезпечує підключення з низькою затримкою для користувачів у всьому світі. Запускаючи кожну службу в кожному центрі обробки даних, Cloudflare застосовує функції мережі, продуктивності та безпеки за один прохід, усуваючи необхідність маршрутизації трафіку через кілька спеціалізованих серверів безпеки, а отже, зменшуючи затримку та уникаючи вузьких місць у продуктивності (рис. 1.2).

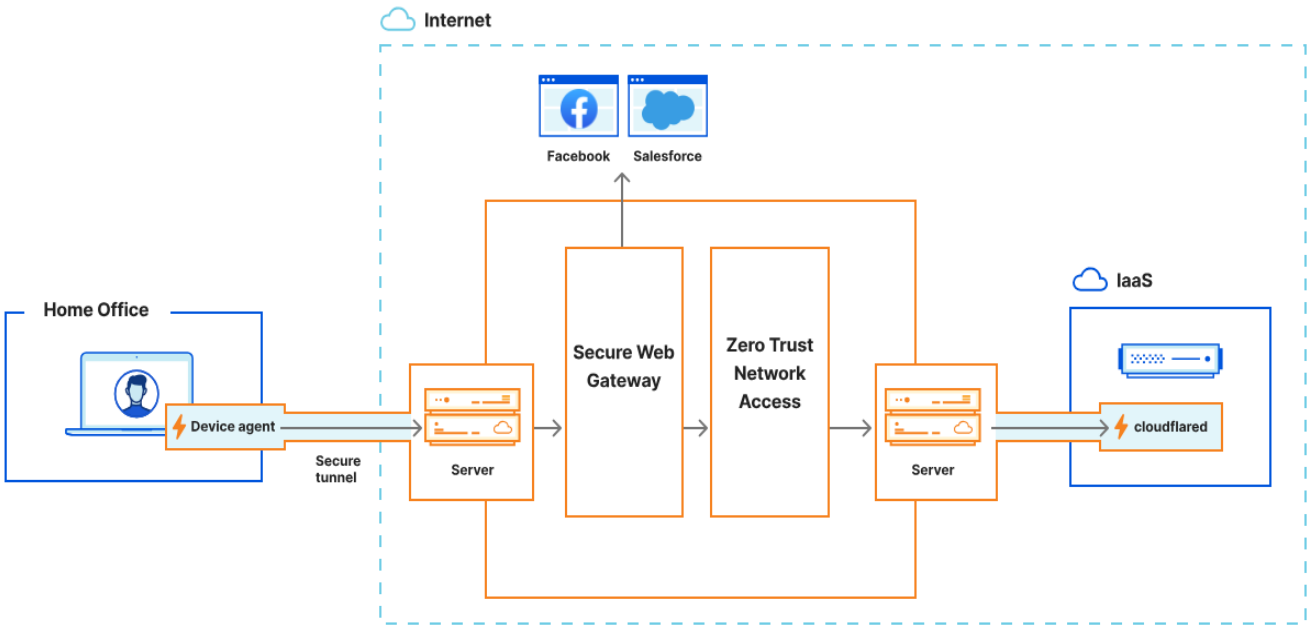


Рисунок 1.2 – Основні компоненти, що беруть участь у віддаленому доступі за допомогою сервісу ZTNA від Cloudflare.

Існує два основних способи забезпечення доступу до приватних програм та мереж: за публічним ім'ям хоста, коли запити передаються через проксі-сервер до програми, або за приватною IP-адресою, коли користувач знаходиться на пристрої

або в мережі, що підключає його до приватної корпоративної мережі через Cloudflare.

Щоб Cloudflare контролював доступ, він повинен бути перед застосунком і мати безпечний і надійний мережевий маршрут для успішно автентифікованих користувачів. Запити на доступ до застосунку спочатку надходять до Cloudflare, де застосовується політика, а потім, у разі успіху, запити користувачів перенаправляються до застосунку.

Щойно ми встановимо підключення до нашої програми, настає час забезпечити доступ користувачів. Залежно від вимог налаштованої політики, користувачі можуть отримати доступ до програми безпосередньо через інтернет-з'єднання з публічним ім'ям хоста, або для більшої безпеки рекомендовано використовувати агент пристрою, Cloudflare One Client, який створює тунель безпосередньо до Cloudflare, а також надає інформацію про кінцевий пристрій для використання в політиках доступу.

1.5 Проєктування політик безпеки та мікросегментація в архітектурі ZTNA

Важливою частиною доступу до програм є автентифікація користувача. Cloudflare має вбудований метод автентифікації на основі електронної пошти. Членство в групах є одним із найпоширеніших атрибутів визначення доступу до програм і може бути визначено вручну або імпортовано за допомогою системи керування міждоменними ідентифікаціями (SCIM). Автентифікація особи користувача є ключовим компонентом будь-якої політики нульової довіри [17]. Під час спроби входу в програму користувача буде перенаправлено до налаштованого постачальника ідентифікаційних даних. Якщо користувач не пройде автентифікацію у постачальника ідентифікаційних даних, Cloudflare не прийме його запит на доступ до програми.

Важливо що Cloudflare можна інтегрувати з усіма потрібними постачальниками ідентифікації (IdP), як корпоративними, так і споживчими. Після чого на рівні програми та політики обирається, яким IdP потрібно дозволити

автентифікацію. Наприклад, може бути програма, до якої має доступ лише обмежена кількість співробітників. В такому випадку слід увімкнути лише свого корпоративного IdP. Для іншої програми можливо дозволити доступ ширшій групі користувачів, які не є співробітниками, таким як підрядники або сторонні партнери. Деяких із цих користувачів можливо автентифікувати за допомогою їхніх облікових даних GitHub або LinkedIn [8].

Коли користувач намагається отримати доступ до програми, йому буде представлено сторінку входу, де він може вибрати, за допомогою якого постачальника ідентифікаційних даних проводити автентифікацію. Для програм з лише одним постачальником ідентифікаційних даних ви можете автоматично перенаправляти користувача до цього постачальника. Також можна налаштувати програму на відображення всіх можливих налаштованих постачальників ідентифікаційних даних, що дозволить додавати нових постачальників у майбутньому без необхідності оновлення політики (рис. 1.3).

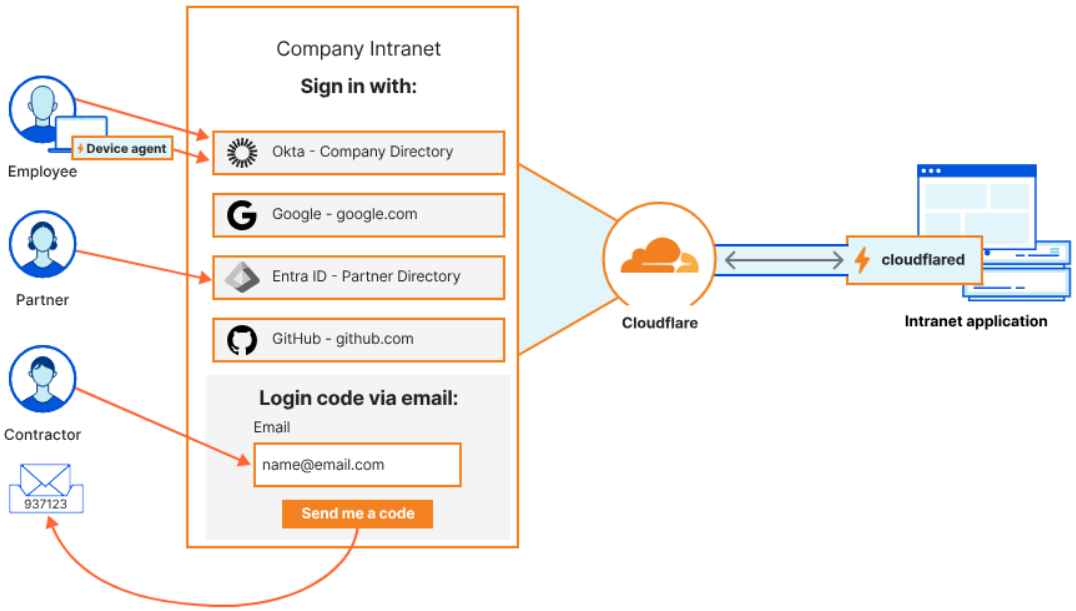


Рисунок 1.3 – Співробітники з різних частин організації автентифікуються в одній і тій самій програмі

Переходячи до опису ключового функціонала системи, необхідно зупинитися на розробці політик управління доступом до корпоративних додатків.

Ці політики виступають інтелектуальним ядром архітектури ZTNA, оскільки саме на цьому рівні відбувається динамічне прийняття рішень щодо надання або блокування запитів (рис. 1.4).

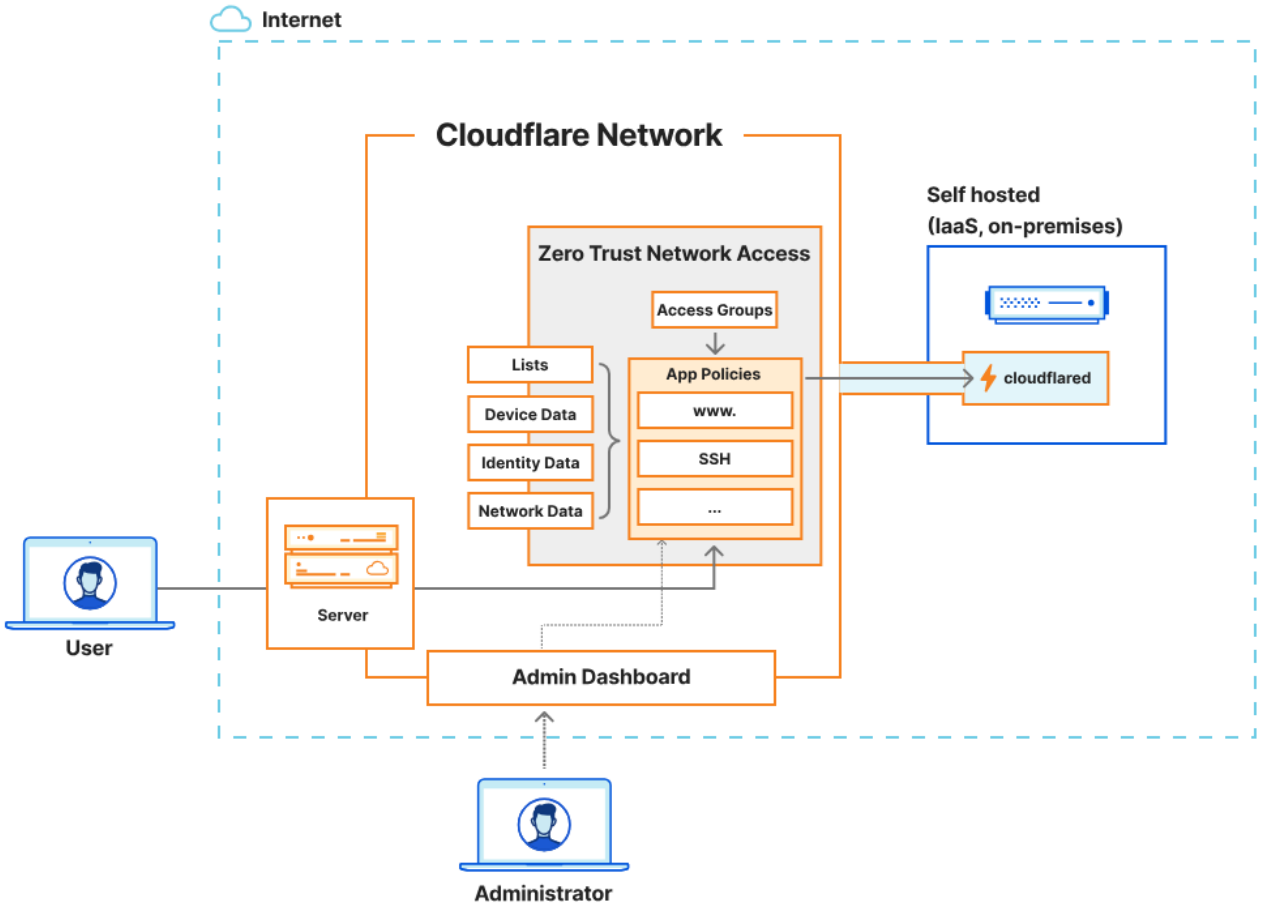


Рисунок 1.4 – Спектр атрибутів у політиці доступу

В екосистемі Cloudflare Zero Trust кожна цільова програма може захищатися набором політик доступу, які обробляються системою у визначеному порядку пріоритетності. Враховуючи можливу складність багаторівневих конфігурацій, для перевірки коректності останніх, розробниками передбачено інструмент моделювання (Policy Tester), що дозволяє оцінити права доступу конкретного користувача до застосування правил у робочому середовищі.

Структурно кожна політика управління доступом складається з наступних базових елементів:

1. Назва політики (Name). Хоча цей параметр є базовим ідентифікатором, розробникам систем кібербезпеки критично важливо дотримуватися єдиної стратегії іменування (наприклад, «Дозволити доступ штатному персоналу» або «Блокувати ризикові підключення»). Уніфікована номенклатура значно спрощує подальший аудит прав доступу та адміністрування IT-інфраструктури підприємства.

2. Дія (Action). Цей параметр визначає реакцію системи у випадку, коли суб'єкт запиту відповідає встановленим критеріям. Згідно з концепцією нульової довіри, Cloudflare Access функціонує за принципом заборони за замовчуванням (Default Deny), отже, якщо запит не відповідає жодній політиці, він автоматично відхиляється. Передбачено чотири основні типи дій:

- Дозволити (Allow) – надає доступ до цільового ресурсу після успішної ідентифікації на сторінці авторизації.
- Блокувати (Block) – примусово забороняє доступ. Застосовується для явного обмеження за певних умов або для скорочення ланцюжка обчислень: якщо політика блокування має вищий пріоритет, оцінка інших політик негайно припиняється.
- Обхід (Bypass) – дозволяє користувачам або службам підключатися без застосування стандартних заходів перевірки (наприклад, для публічно доступних кінцевих точок API).
- Автентифікація служби (Service Auth) – використовується для міжсервісної взаємодії (Machine-to-Machine) на основі сертифікатів mTLS або сервісних токенів. Це дозволяє здійснювати запити між додатками без залучення графічного інтерфейсу користувача.

3. Тривалість сеансу (Session Duration). Визначає період валідності стану автентифікації користувача після успішного входу. Відповідно до базового принципу ZTNA «ніколи не довіряй, завжди перевіряй», для критично важливих корпоративних додатків цей параметр може вимагати безперервної переоцінки. Навіть за умови первинної відповідності стану пристрою, постійний моніторинг

гарантує підтвердження прав доступу при кожному новому запиті, що мінімізує часове вікно для реалізації потенційної загрози.

4. Правила оцінки (Rules). Ключовий інтелектуальний компонент політики, який визначає логіку прийняття рішень. Правила будуються на основі пар «селектор-значення» та працюють за принципом багаторівневого фільтра. Вони поділяються на три логічні категорії:

- Правила включення (Include). Визначають початковий пул суб'єктів, які є кандидатами на отримання доступу. Усі правила цієї категорії обробляються за логічною операцією «АБО» (OR) – для проходження достатньо відповідності хоча б одному критерію (наприклад, належність до корпоративної групи або наявність затвердженої електронної адреси).
- Правила обов'язкової відповідності (Require). Встановлюють жорсткі додаткові умови для суб'єктів, які пройшли етап включення. Вони функціонують за логікою «ТА» (AND) – кожна визначена вимога має бути обов'язково виконана (наприклад, використання апаратного ключа MFA).
- Правила виключення (Exclude). Виконують роль абсолютних обмежень. Якщо атрибути запиту підпадають під правило виключення, доступ миттєво блокується, незалежно від виконання умов «Include» та «Require» (наприклад, ізоляція користувачів із групи високого безпекового ризику).

Корисний спосіб уявити, як застосовуються ці різні типи правил – це уявити воронку продажів. Селектори «Включити» визначають, які атрибути користувача, трафіку чи пристрою включені до політики, що будуть Дозволені, Заблоковані тощо. Потім селектори «Вимагати» додатково фільтрують зі списку, які атрибути мають бути пов’язані з користувачем, а тип «Виключити» фільтрує користувачів, які відповідають як «Включити», так і «Вимагати» (рис. 1.5).

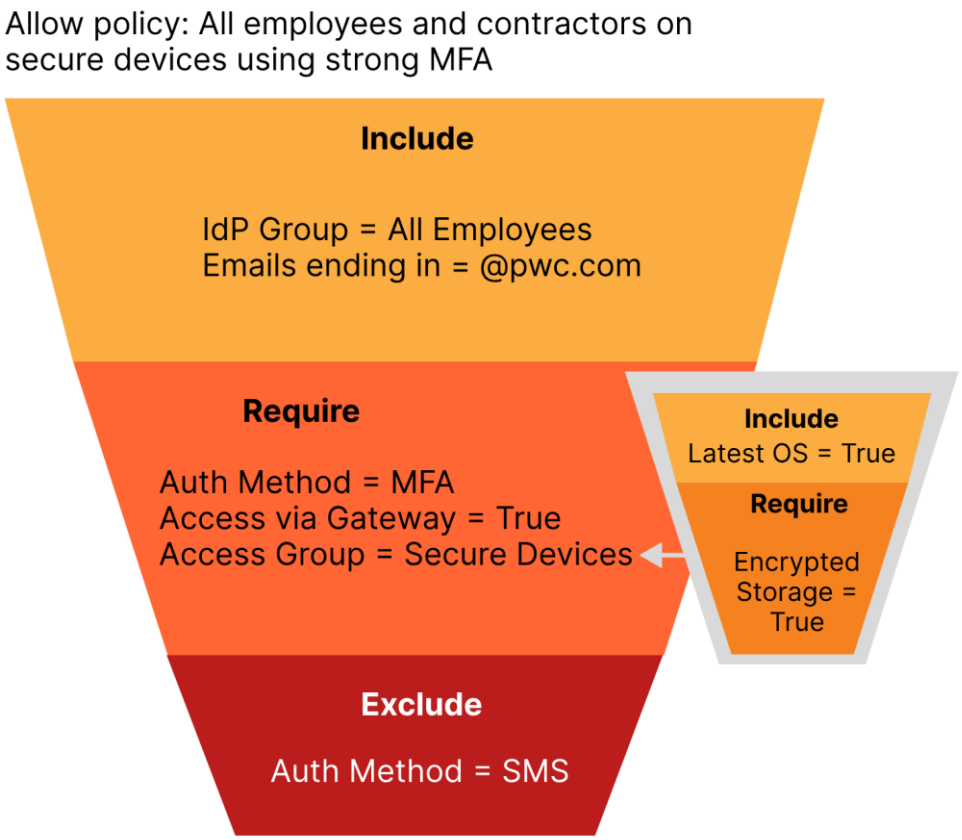


Рисунок 1.5 – Логічна структура оцінювання правил доступу за принципом воронки

Наведена вище діаграма візуалізує приклад політики «Усі співробітники та підрядники на захищених пристроях використовують надійну багатофакторну автентифікацію». Будь-хто в групі «Усі співробітники» або підрядники, які пройшли автентифікацію за допомогою імені користувача в домені своєї компанії, відповідатиме цій політиці. Вони повинні використовувати пристрій з найновішою ОС та зашифрованим сховищем. Вони повинні пройти автентифікацію за допомогою фактора багатофакторної автентифікації, але не за допомогою SMS. Крім того, вони повинні отримувати доступ до програми через захищений веб-шлюз Cloudflare.

Остання передумова для створення справді ефективних політик доступу – це налаштування стану пристрою . Під час використання агента пристрою Cloudflare має доступ до різноманітної інформації про пристрій, яку потім можна використовувати в політиці доступу. Під час використання безагентного методу

доступу до програм доступна лише інформація про ідентифікацію користувача. Також підтримується використання інформації про стан пристрою від інших постачальників , таких як Microsoft, Crowdstrike та Sentinel One (рис. 1.6).

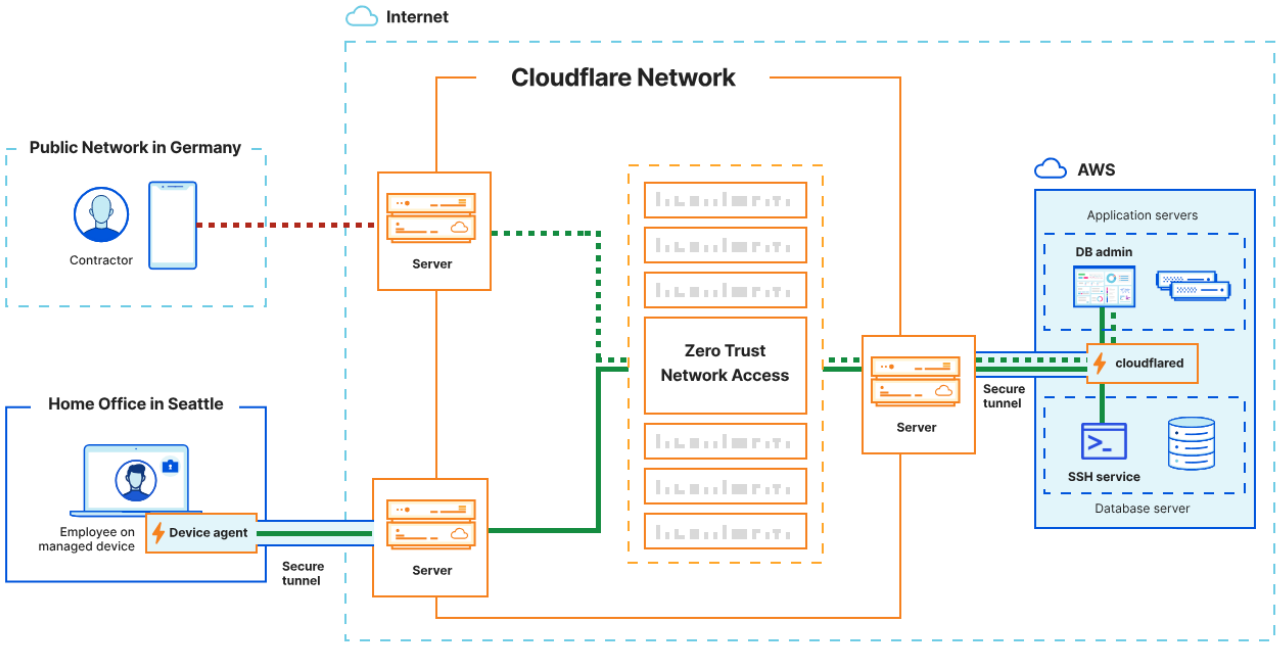


Рисунок 1.6 – Механізм застосування політик Cloudflare Access залежно від наявності клієнтського агента

Одним із найважливіших аспектів визначення політик ZTNA є використання елементів багаторазового використання, які називаються групами доступу . Кожна група доступу використовує ті самі правила, які були описані раніше, для визначення користувачів, трафіку або пристроїв. Ці групи потім можна використовувати в багатьох політиках, щоб дозволити, заборонити, обійти або ізолювати доступ до програми.

Наприклад, ви можете один раз визначити «Співробітників» як групу доступу, а потім використовувати це в кожній політиці програми, де потрібно посилатися на співробітників. Оновлення цієї групи доступу потім відображатимуться в кожній політиці. Це також гарний спосіб включити вкладену логіку (наприклад, користувачі з пристроєм Linux та ввімкненим антивірусним програмним забезпеченням).

Нижче наведено діаграму групи доступу під назвою «Адміністратори безпеки», яка використовує низку атрибутів для визначення характеристик адміністраторів безпеки. На діаграмі показано додавання двох інших груп доступу в межах «Адміністратори безпеки». Ці групи включають пристрої, що працюють під керуванням останньої версії Windows або macOS, а також вимогу, щоб пристрій мав доступ до файлів (рис 1.7).

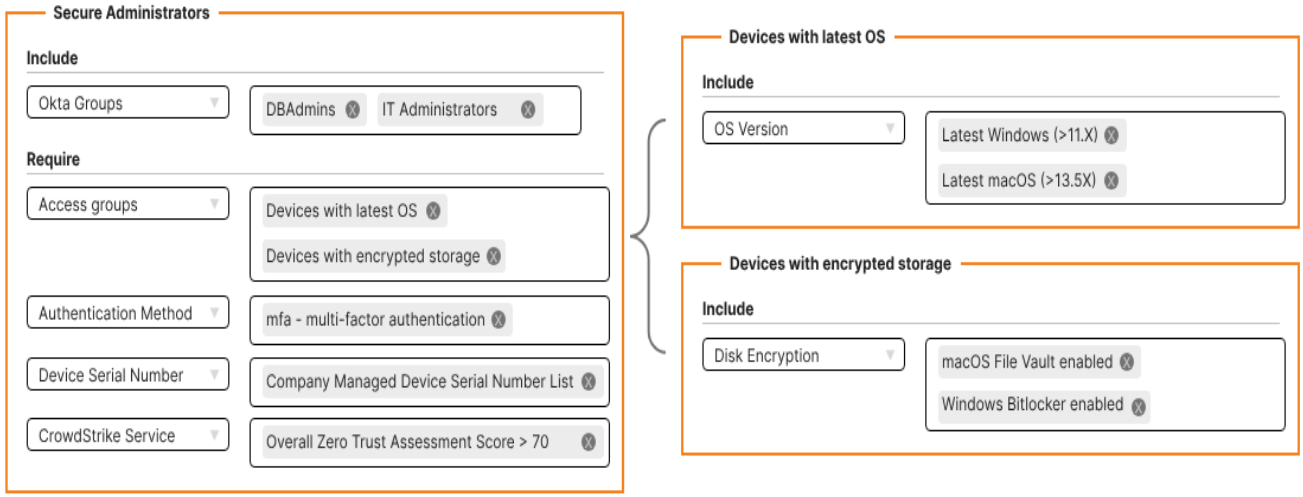


Рисунок 1.7 – Група доступу, яка відповідає IT-адміністраторам у захищених системах.

Таким чином, методика ізоляції вебсервісів за допомогою інструментів Cloudflare створює гранульоване, мікросегментоване середовище. Вона чудово підходить для захисту критично важливих баз даних клієнтів в організаціях автомобільного сектору. Ця методика повністю унеможливлює прямі мережеві атаки, приховує інфраструктуру від сканування та гарантує дотримання принципу найменших привілеїв під час віддаленої роботи співробітників. Успішне впровадження ZTNA – це більше, ніж просто технічна конфігурація, воно вимагає ретельного врахування конкретних потреб організації, робочих процесів користувачів та вимог безпеки. Гнучкість Cloudflare дозволяє почати з базових політик безпечного доступу, а потім розвивати їх у міру зміни потреб організації та розвитку вимог безпеки.

2 АНАЛІЗ СТАНУ МЕРЕЖЕВОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

2.1. Загальна характеристика IT-інфраструктури та діючої системи інформаційної безпеки підприємства

Товариство з обмеженою відповідальністю «Арма Моторс» є потужним автомобільним дилерським центром. Воно продає транспортні засоби, надає гарантійне та післягарантійне технічне обслуговування, а також продає оригінальні запасні частини. Постійна робота цих бізнес-процесів повністю залежить від стабільного функціонування корпоративної IT-інфраструктури.

Фізична топологія мережі побудована за ієрархічним принципом і об'єднує кілька функціональних сегментів. До них входять адміністративний блок для керівництва і бухгалтерії, демонстраційна зона шоу-руму з терміналами для менеджерів із продажу, сервісна зона з мобільними діагностичними станціями та складський комплекс. Ядром мережі є серверна кімната, де на базі гіпервізорів розгорнуто пул віртуальних серверів. Серед критично важливих вузлів інфраструктури є контролер домену служби каталогів Active Directory для управління обліковими записами, сервери баз даних, файлові сховища корпоративної документації та спеціалізовані шлюзи для захищеного обміну даними з серверами виробника автомобілів.

Найбільшу комерційну цінність у цій екосистемі має корпоративна система управління відносинами з клієнтами, відома як CRM-система. Вона функціонує як внутрішній вебсервіс і накопичує велику кількість конфіденційної інформації. База даних містить персональні дані власників автомобілів, історію їхніх звернень, деталі фінансових транзакцій, умови кредитних угод та корпоративні плани продажу.

На поточному етапі система інформаційної безпеки реалізована за класичною периметральною моделлю. На межі корпоративної мережі та публічного інтернету встановлено апаратний маршрутизатор з функціями міжмережевого екрана. Цей пристрій виконує основну фільтрацію вхідного та вихідного трафіку, трансляцію

мережевих адрес і маршрутизацію пакетів. Внутрішня безпека забезпечується встановленням антивірусного програмного забезпечення на робочих станціях і застосуванням групових політик безпеки на рівні домену, які обмежують доступ користувачів до системних налаштувань.

Для віддаленого доступу співробітників керівництва, бухгалтерів та маркетологів використовується віртуальна приватна мережа. На головному маршрутизаторі налаштовано сервер віддаленого доступу, який приймає підключення з інтернету. Співробітники встановлюють на своїх домашніх або мобільних пристроях відповідне програмне забезпечення, вводять логін та пароль, після чого між їхнім пристроєм і маршрутизатором створюється зашифрований тунель. Отримавши внутрішню IP-адресу, віддалений працівник може працювати з корпоративною CRM-системою та іншими серверами так, ніби він фізично знаходиться в будівлі дилерського центру.

2.2. Аналіз вразливостей, загроз та оцінка ризиків існуючої мережевої архітектури

Детальний аналіз поточної архітектури виявляє кілька критичних вразливостей. Вони пов'язані з природою класичної моделі периметрального захисту та роботою віртуальних приватних мереж.

Першою очевидною технічною вразливістю є наявність відкритих вхідних портів на зовнішньому інтерфейсі маршрутизатора компанії. Щоб сервер віртуальної приватної мережі міг приймати підключення від легальних працівників, маршрутизатор постійно прослуховує відповідний мережевий порт. У сучасному глобальному інтернеті це означає, що IP адреса компанії видима для різних пошукових систем темної частини мережі та автоматизованих сканерів зловмисників(рис. 2.1). Хакери постійно сканують адресний простір у пошуках відкритих точок входу. Знайшовши такий порт, вони можуть застосовувати атаки на основі повного перебору паролів або намагатися використати відомі вразливості в операційній системі самого маршрутизатора.

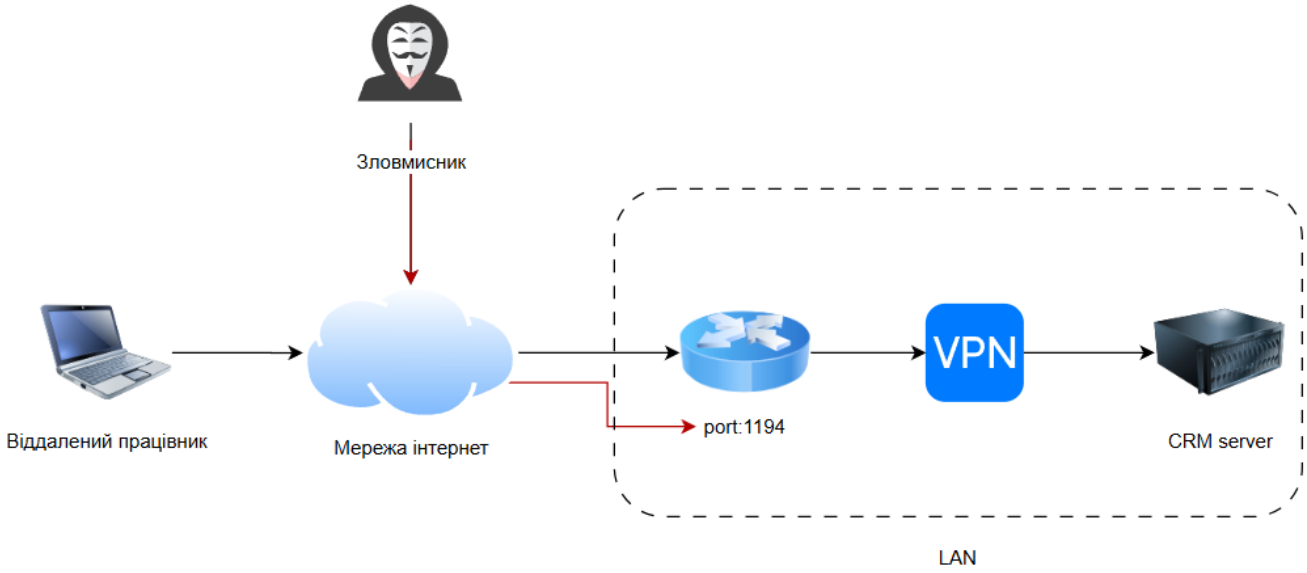


Рисунок 2.1 – Традиційна архітектура віддаленого доступу з відкритими вхідними портами

Друга критична вразливість пов'язана з надмірною довірою до користувача після успішної автентифікації. Діюча система безпеки лише перевіряє правильність введених облікових даних. Якщо зловмисник, використовуючи соціальну інженерію або фішинг, отримує логін та пароль легального співробітника, він здобуває безперешкодний доступ до корпоративної мережі. Потрапивши за периметральний міжмережевий екран, атакуюча сторона може вільно переміщуватися в інфраструктурі компанії. Зловмисник може безперешкодно сканувати внутрішні підмережі, виявляти сервери баз даних та отримувати доступ до ресурсів, які не потрібні скомпрометованому обліковому запису для виконання звичайних робочих завдань.

Третьою небезпечною проблемою є повна відсутність контролю за безпекою кінцевих пристроїв віддалених працівників. Класична віртуальна приватна мережа забезпечує лише шифрування каналу зв'язку, але не перевіряє пристрій, з якого відбувається підключення. Якщо співробітник працює з домашнього комп'ютера, який не має оновленого антивірусного захисту і вже заражений шкідливим програмним забезпеченням, створений тунель стає ідеальним шляхом для

проникнення загроз у корпоративну мережу. Захищений канал шифрує трафік, і корпоративний міжмережевий екран не може проаналізувати його вміст, пропускаючи шкідливий код до серверного сегмента.

Для більш глибокого розуміння критичності виявлених вразливостей периметральної архітектури доцільно провести моделювання типового сценарію цілеспрямованої кібератаки (Advanced Persistent Threat) на IT-інфраструктуру дилерського центру з використанням відкритого порту віртуальної приватної мережі. Цей сценарій демонструє поетапний розвиток інциденту інформаційної безпеки від моменту первинної розвідки до повної компрометації цільового ресурсу – CRM-системи підприємства. Моделювання базується на класичному ланцюжку реалізації кіберзагроз (Cyber Kill Chain) (рис. 2.2).

Рисунок 2.2 – Моделювання етапів цілеспрямованої кібератаки на традиційну периметральну мережу

Етап 1. Зовнішня розвідка та ідентифікація точок входу (Reconnaissance). Атака розпочинається зі збору інформації про IT-інфраструктуру ТОВ «Арма Моторс» із відкритих джерел (OSINT). Використовуючи публічні реєстри та бази

даних тіньового сегмента інтернету, зловмисники встановлюють пул зовнішніх IP-адрес, що належать компанії. Далі застосовуються спеціалізовані інструменти масового мережевого сканування, такі як Nmap або масиви даних пошукової системи Shodan. Оскільки для роботи класичного VPN-шлюзу маршрутизатор підприємства змушений тримати відкритими порти (наприклад, UDP 1194 для OpenVPN або TCP 443 для SSL VPN), сканери зловмисників миттєво ідентифікують цю точку входу. За допомогою аналізу відповідей сервера (граббінг банерів) хакери встановлюють точну версію програмного забезпечення, що використовується на шлюзі підприємства.

Етап 2. Початкове проникнення та компрометація периметра (Initial Access). Виявивши відкритий порт мережевого екрана, атакуюча сторона переходить до спроб проникнення всередину. У межах традиційної архітектури зловмисники мають два основні вектори дій. Перший вектор полягає в експлуатації відомих вразливостей (CVE) або вразливостей нульового дня (Zero-day) у мікропрограмному забезпеченні самого маршрутизатора. Якщо пристрій вчасно не отримав оновлення безпеки, хакери відправляють спеціально сформований пакет даних, який викликає переповнення буфера і дозволяє виконати віддалений код, минаючи етап авторизації.

Другий, найбільш розповсюджений вектор – це атаки на облікові дані легальних користувачів. Зловмисники використовують методи перебору по словнику (Brute-force) або підстановки раніше викрадених паролів (Credential Stuffing). Крім того, застосовується цілеспрямований фішинг проти віддалених співробітників компанії. Оскільки традиційний VPN не здійснює перевірку стану кінцевого пристрою (Device Posture), зловмиснику достатньо заволодіти лише логіном та паролем менеджера, щоб його неавторизований комп'ютер легітимно підключився до корпоративного шлюзу.

Етап 3. Закріплення та горизонтальне переміщення (Lateral Movement). Після успішної авторизації пристрій хакера отримує внутрішню IP-адресу та опиняється за межами захисного периметра, тобто всередині довіреної локальної мережі підприємства. Діюча архітектура надає такому підключенню надмірні привілеї.

Користуючись цією довірою, зловмисник розпочинає внутрішню розвідку (Internal Reconnaissance). За допомогою протоколів ARP та сканування внутрішніх підмереж він створює топологічну карту інфраструктури, виявляючи контролери домену, сервери резервного копіювання та головну ціль – сервер управління відносинами з клієнтами (CRM).

На цьому етапі хакер здійснює горизонтальне переміщення. Якщо скомпрометований обліковий запис звичайного менеджера не має прав адміністратора на CRM-сервері, зловмисник використовує інструменти для підвищення привілеїв (Privilege Escalation), експлуатуючи локальні вразливості застарілих операційних систем всередині мережі або перехоплюючи хеші паролів системних адміністраторів.

Етап 4. Ексфільтрація даних та реалізація деструктивного впливу (Action on Objectives). Отримавши адміністративний доступ до сервера бази даних, атакуюча сторона переходить до фінальної стадії. Спочатку відбувається прихована ексфільтрація (вивантаження) масивів конфіденційної інформації. Персональні дані клієнтів, їхні контактні номери, історія обслуговування автомобілів та фінансові транзакції копіюються на зовнішні тіньові сервери хакерів. Ця інформація в подальшому використовується для шантажу підприємства (метод подвійного вимагання) або продається на чорному ринку конкурентам та шахраям [11].

Завершальним кроком кібератаки є розгортання вірусу-шифрувальника (Ransomware). Шкідливе програмне забезпечення одночасно запускається на CRM-сервері та серверах резервного копіювання, незворотно криптуючи всі файли баз даних. З цього моменту IT-інфраструктура ТОВ «Арма Моторс» вважається повністю паралізованою, а підприємство зазнає колосальних фінансових і репутаційних збитків [12].

Проведене моделювання сценарію атаки наочно доводить, що наявність відкритого порту та відсутність динамічного контролю за станом пристрою після проходження периметра роблять традиційну мережеву архітектуру критично вразливою до сучасних загроз. Захист від подібних багатовекторних атак вимагає

повної відмови від публічних точок входу та запровадження суворої мікросегментації на рівні кожного окремого сервісу.

Оцінка ризиків для ТОВ «Арма Моторс» показує, що найвищий рівень загрози стосується саме CRM-системи підприємства. Ймовірність компрометації облікових даних віддалених працівників або використання вразливостей відкритого порту вважається високою. Вплив такої події може бути катастрофічним. Проникнення вірусу-шифрувальника всередину мережі призведе до повного блокування баз даних. Це зупинить роботу відділів продажу та сервісу, унеможливить виконання зобов'язань перед клієнтами та імпортером, спричинить фінансові втрати через простій, а також потенційні юридичні наслідки за витік конфіденційних даних.

2.3. Обґрунтування проблематики діючої системи безпеки та необхідності переходу до моделі ZTNA на досліджуваному підприємстві

Дослідження показує, що сучасна парадигма периметрального захисту підприємства вичерпала свій потенціал. Посилення архітектури шляхом ускладнення політик паролів або оновлення мікропрограмного забезпечення маршрутизаторів є лише тимчасовими заходами, які не усувають основних архітектурних недоліків системи.

Основна проблема функціонування поточної системи безпеки полягає у протиріччі між бізнес-потребами та технологічними обмеженнями. Дилерському центру необхідний надійний і швидкий механізм віддаленої роботи для оперативного прийняття управлінських рішень. Проте використання традиційних методів такого доступу вимагає залишати мережеві порти відкритими, що створює постійну загрозу для найцінніших активів компанії з боку зовнішнього середовища.

Єдиним логічним і технічно обґрунтованим рішенням цієї проблеми є повна відмова від використання відкритих вхідних портів і перехід корпоративної мережі ТОВ «Арма Моторс» до архітектури нульової довіри [19]. Впровадження цієї

моделі дозволить усунути всі виявлені під час аудиту вразливості завдяки впровадженню кількох ключових змін.

По-перше, використання хмарних брокерів і концепції вихідних тунелів дозволяє налаштувати головний маршрутизатор підприємства на повне блокування вхідного трафіку. У результаті корпоративна мережа не реагуватиме на зовнішні запити, що робить її невидимою для автоматизованих сканерів та унеможливлює атаки на мережевий периметр.

По-друге, впровадження мікросегментації забезпечить доступ не до всієї локальної мережі, а лише до конкретного ресурсу. Віддалений співробітник взаємодіятиме виключно з веб-інтерфейсом CRM-системи, і навіть у разі компрометації облікових даних зловмисник не зможе отримати доступ до інших серверів дилерського центру.

По-третє, впровадження обов'язкової багатокритеріальної перевірки дозволить оцінювати не лише ідентичність користувача за допомогою двофакторної автентифікації, а й стан безпеки його кінцевого пристрою. Доступ до корпоративних баз даних буде автоматично заблоковано, якщо пристрій не відповідатиме встановленим корпоративним стандартам безпеки.

Аналіз стану ІТ-інфраструктури ТОВ «Арма Моторс» свідчить, що впровадження архітектури Zero Trust Network Access є не лише технологічним трендом, а й критичною бізнес-необхідністю. Такий підхід мінімізує ризики цілеспрямованих кібератак, захищає конфіденційні дані клієнтів та забезпечує безпечну масштабованість ІТ-екосистеми дилерського центру у майбутньому.

3 ПРОЄКТУВАННЯ ТА ПРАКТИЧНЕ ВПРОВАДЖЕННЯ АРХІТЕКТУРИ ZERO TRUST

3.1. Розробка покрокового методу впровадження моделі ZTNA в корпоративну мережу підприємства

Перехід від традиційної периметральної моделі захисту до архітектури нульової довіри є комплексним процесом, який вимагає чіткої послідовності дій для уникнення збоїв у бізнес-процесах підприємства. Для успішної реалізації цього завдання на базі ТОВ «Арма Моторс» було розроблено поетапний метод впровадження концепції Zero Trust Network Access. Запропонований алгоритм складається з п'яти логічно пов'язаних етапів і є універсальним керівництвом для модернізації мережевої інфраструктури.

Перший етап алгоритму передбачає проведення глибокого аудиту існуючої IT-інфраструктури та інвентаризацію цифрових активів [18]. На цьому кроці фахівці з інформаційної безпеки визначають повний перелік корпоративних ресурсів, до яких надається віддалений доступ. Критично важливим завданням є картографування потоків даних та ідентифікація найцінніших систем. Для досліджуваного підприємства таким пріоритетним об'єктом визначено корпоративну систему управління відносинами з клієнтами. Після виділення цільового ресурсу проводиться аналіз наявних точок входу, зокрема фіксуються всі відкриті порти на зовнішньому маршрутизаторі, які підлягають подальшому блокуванню.

Другий етап фокусується на проєктуванні політик ідентифікації та розмежуванні доступу на основі ролей. На відміну від класичних рішень, архітектура нульової довіри вимагає точного визначення груп користувачів та їхніх повноважень. Адміністратор системи розробляє профіль кожної посади: від системного адміністратора до лінійного персоналу сервісної зони. Паралельно визначаються критерії безпекового стану кінцевих пристроїв, які будуть вважатися

еталонними для надання дозволу на з'єднання. Результатом цього етапу є створення формалізованої матриці управління доступом.

Третій етап охоплює практичне розгортання інфраструктури хмарного брокера та конекторів. Замість налаштування вхідних правил на міжмережевому екрані, всередині локальної мережі підприємства розгортається спеціалізована служба маршрутизації. Цей програмний компонент встановлюється безпосередньо в серверному сегменті поруч із цільовим вебсервісом. Його головним завданням є ініціація та підтримка постійних зашифрованих вихідних з'єднань з глобальними центрами обробки даних обраного провайдера рішень безпеки. Таким чином формується захищений транспортний канал, який не потребує публічної видимості підприємства в інтернеті.

Четвертий етап полягає в налаштуванні механізмів авторизації кінцевих точок та інтеграції з постачальниками ідентифікації. На цьому кроці хмарний брокер об'єднується з корпоративною службою каталогів або системою електронної пошти для забезпечення багатофакторної перевірки користувачів. Одночасно на робочі пристрої співробітників встановлюється спеціальне програмне забезпечення, яке в режимі реального часу збирає телеметрію про стан операційної системи, активність антивірусних рішень та статус локального міжмережевого екрана. Ці дані безперервно передаються до хмарного брокера для прийняття динамічних рішень щодо надання або розірвання доступу.

П'ятий, завершальний етап алгоритму передбачає тестування впровадженої моделі та остаточну ізоляцію інфраструктури. Процес переходу відбувається в режимі паралельного функціонування: спочатку нова архітектура працює в тестовому режимі лише для обмеженої групи адміністраторів. Після підтвердження стабільності доступу до системи управління клієнтами через хмарного брокера відбувається переключення всього трафіку. Фінальною дією адміністратора є повне видалення правил трансляції адрес та закриття всіх вхідних портів на головному маршрутизаторі ТОВ «Арма Моторс». З цього моменту підприємство остаточно переходить у режим так званої невидимої мережі.

Послідовне виконання розробленого алгоритму гарантує безшовну інтеграцію моделі нульової довіри. Запропонований метод мінімізує ризики простою критичних сервісів під час міграції та дозволяє підприємству поступово адаптувати свої бізнес-процеси до нових, значно вищих стандартів кібербезпеки [23].

3.2. Вибір програмно-апаратних засобів та формування архітектури рішення для досліджуваної організації

Реалізація розробленого алгоритму вимагає підбору оптимального технологічного стека, здатного забезпечити мікросегментацію та приховування мережевого периметра. Як базову платформу для впровадження архітектури нульової довіри в ТОВ «Арма Моторс» обрано екосистему Cloudflare Zero Trust. Цей вибір обґрунтовано відсутністю потреби в масштабній заміні існуючого апаратного маршрутизатора підприємства, оскільки рішення функціонує як накладена мережа поверх існуючої інфраструктури.

Основним компонентом запропонованої архітектури виступає технологія Cloudflare Tunnel. Для її роботи на внутрішньому сервері підприємства, розташованому в одному мережевому сегменті із системою управління відносинами з клієнтами, встановлюється легковагова програмна служба cloudflared. Цей програмний модуль ініціює постійне вихідне зашифроване з'єднання з найближчим центром обробки даних хмарного брокера, формуючи захищений транспортний канал.

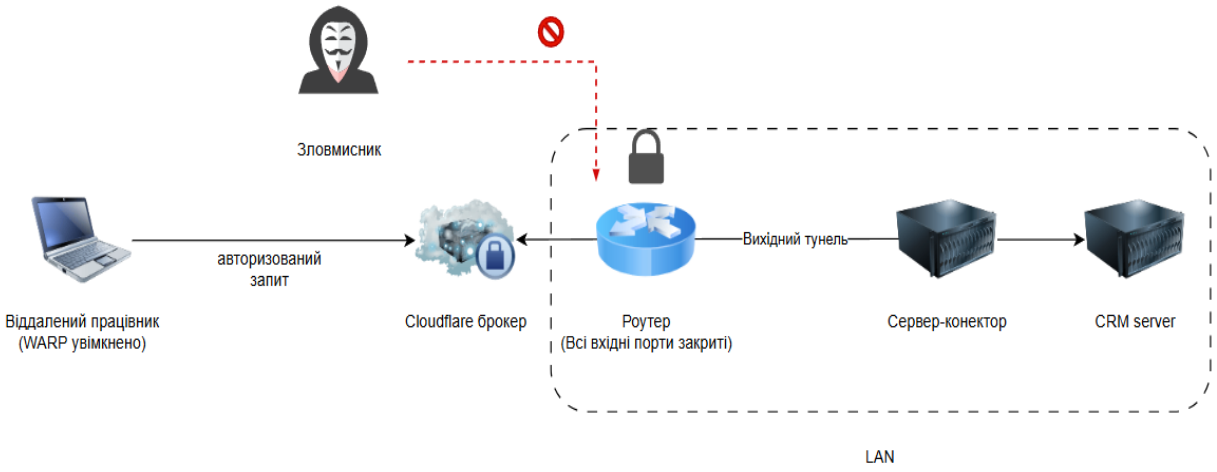


Рисунок 3.1 – Архітектура віддаленого доступу за моделлю Zero Trust

Як показано на рисунку 3.1, запропонована архітектура докорінно змінює вектор маршрутизації трафіку. Головний маршрутизатор підприємства переводиться в режим повного блокування вхідних з'єднань. Авторизований віддалений працівник взаємодіє виключно з хмарним брокером, де його трафік зустрічається з відповіддю корпоративного сервера в ізольованому середовищі. Будь-які неавторизовані запити або спроби автоматизованого сканування відхиляються на зовнішньому інтерфейсі маршрутизатора, що забезпечує ефект невидимої мережі.

Другим ключовим компонентом рішення є сервіс Cloudflare Access, який виконує роль центрального контролера політик безпеки. Він інтегрується з корпоративним поштовим доменом для забезпечення багатофакторної автентифікації користувачів. Третім обов'язковим елементом виступає клієнтське програмне забезпечення Cloudflare WARP, що встановлюється на кінцеві пристрої співробітників. Цей клієнт безперервно аналізує стан безпеки пристрою, передаючи хмарному брокеру актуальну телеметрію про статус локального міжмережевого екрана та антивірусного захисту.

Для формалізації політик безпеки було розроблено матрицю управління доступом. Вона визначає суворі критерії, за умови виконання яких система приймає динамічне рішення про надання доступу до ресурсу (табл. 3.1).

Таблиця 3.1

Матриця управління доступом за моделлю Zero Trust на прикладі цільового ресурсу CRM

Цільовий ресурс	Група користувачів	Правила ідентифікації	Вимоги до стану пристрою	Дія системи
Система управління клієнтами	Системні адміністратори	Багатофакторна автентифікація	Клієнт шифрування активний, міжмережевий екран та антивірус увімкнено	Дозволити
Система управління клієнтами	Менеджери з продажу	Багатофакторна автентифікація, запит у робочий час	Клієнт шифрування активний, міжмережевий екран увімкнено	Дозволити
Система управління клієнтами	Лінійний персонал сервісу	Успішна автентифікація	Повна відповідність політикам безпеки	Заблокувати
Система управління клієнтами	Будь-який авторизований працівник	Успішна автентифікація	Клієнт шифрування активний, міжмережевий екран вимкнено	Заблокувати
Корпоративна мережа загалом	Невідомі пристрої та сканери	Відсутній доступ до порталу авторизації	Відсутній корпоративний клієнт шифрування	Ігнорувати запит

Застосування розробленої матриці гарантує суворе дотримання принципу найменших привілеїв та розмежування на основі ролей. Архітектура нульової довіри оцінює запити комплексно. Якщо лінійний персонал сервісної зони використовує повністю захищений корпоративний пристрій та успішно проходить багатофакторну автентифікацію, доступ до системи управління клієнтами буде миттєво заблоковано. Посадові обов'язки цієї групи користувачів передбачають роботу виключно у спеціалізованих діагностичних програмах, виключаючи авторизовану потребу взаємодії з фінансовими базами даних.

Паралельно з цим для співробітників, які працюють із клієнтською базою, система висуває жорсткі вимоги до стану їхнього обладнання. Спроба підключення з комп'ютера з вимкненим локальним міжмережевим екраном розцінюється системою як критична загроза і відхиляється до моменту усунення вразливості на кінцевій точці. Запити від неавторизованих зовнішніх пристроїв відкидаються ще на рівні хмарного брокера без генерування будь-якої відповіді.

3.3. Технічна реалізація та експериментальна перевірка працездатності розробленого рішення

Практичне впровадження моделі Zero Trust для ТОВ «Арма Моторс» було реалізовано шляхом створення комплексного технічного стенда, який повністю відтворює запропоновану мережеву архітектуру. Процес розгортання охоплював підготовку локального серверного середовища, реєстрацію доменного імені, конфігурацію хмарного брокера, встановлення конекторів та тестування розроблених політик безпеки на кінцевих пристроях.

Етап 1. Підготовка базової інфраструктури та цільового вебсервера. Основою для локальної частини архітектури стала віртуальна машина, розгорнута в середовищі гіпервізора. На першому етапі було здійснено інсталяцію операційної системи Ubuntu Server. Вибір цієї серверної платформи зумовлений її високою надійністю та повною сумісністю з інструментарієм Cloudflare (рис. 3.2).

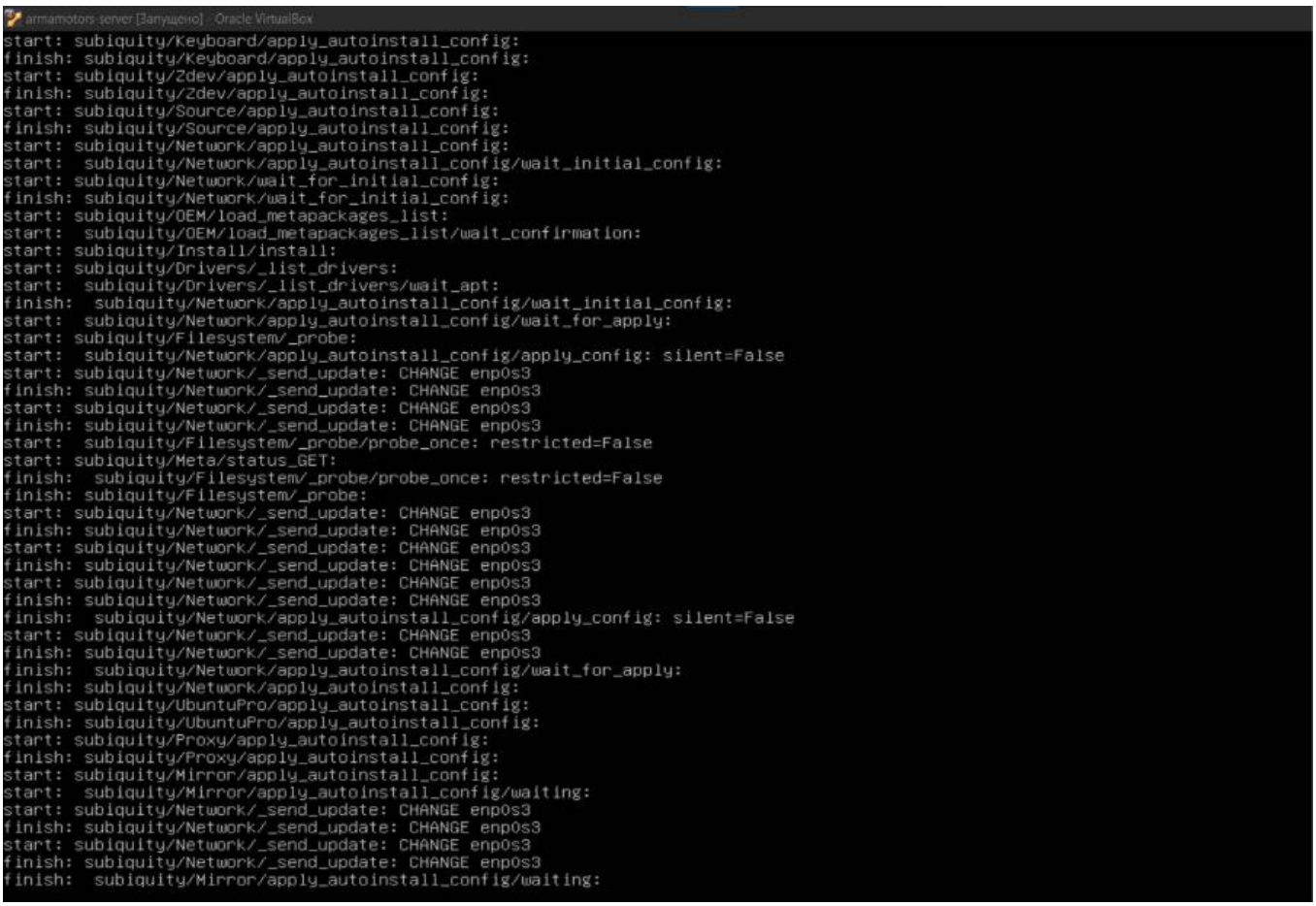


Рисунок 3.2 – Логи процесу інсталяції операційної системи Ubuntu Server

Для імітації корпоративної системи управління клієнтами (CRM), яка потребує захисту від зовнішнього доступу, було розгорнуто локальний вебсервер. За допомогою вбудованого менеджера пакетів `apt` було встановлено службу Nginx. Для наочності тестування стандартну сторінку вебсервера було замінено на кастомну корпоративну сторінку з текстом про конфіденційність доступу.

Після базової інсталяції Nginx було проведено налаштування віртуального хосту для імітації корпоративної CRM-системи. Важливим аспектом конфігурації є те, що вебсервер налаштовується на роботу виключно з локальним інтерфейсом або стандартними портами, оскільки роль зовнішнього шлюзу та інспектора трафіку повністю перебирає на себе хмарний брокер.

Фрагмент конфігураційного файлу /etc/nginx/sites-available/default, який визначає параметри обробки запитів, наведено у лістингу 3.1 [15].

Лістинг 3.1 – Конфігураційний файл віртуального хосту Nginx

```
server {
 listen 80; # Вебсервер очікує запити на стандартному порту
 server_name crm.amotors.pp.ua; # Визначення доменного імені ресурсу

 root /var/www/html;
 index index.html;

 location / {
  # Забезпечення відображення статичного контенту CRM
  try_files $uri $uri/ =404;

  # Додаткові заголовки для ідентифікації трафіку від брокера
  add_header X-Frame-Options «SAMEORIGIN»;
  add_header X-Content-Type-Options «nosniff»;
 }

 # Логування запитів для подальшого аналізу безпеки
 access_log /var/log/nginx/crm_access.log;
 error_log /var/log/nginx/crm_error.log;
}
```

Логіка взаємодії компонентів системи побудована за принципом локального проксіювання. Коли хмарний брокер отримує авторизований запит від користувача, він передає його через шифрований вихідний тунель до демона cloudflared, запущеного на сервері. Останній, у свою чергу, переспрямовує трафік на http://localhost:80, де його приймає вебсервер Nginx. Така схема дозволяє тримати порти 80 та 443 закритими для зовнішнього світу на рівні апаратного маршрутизатора підприємства, забезпечуючи доступ до вебсервера лише через ідентифікований канал зв'язку.

Для практичної реалізації цього етапу було виконано підключення до локального сервера та розгорнуто пакет вебсервера Nginx з офіційних репозиторіїв операційної системи (рис. 3.3). Вибір саме Nginx як імітаційної платформи для корпоративної CRM-системи обґрунтований його високою продуктивністю, гнучкістю налаштувань та здатністю максимально ефективно працювати в ролі зворотного проксі-сервера (reverse proxy) у зв'язці з тунелями Cloudflare.

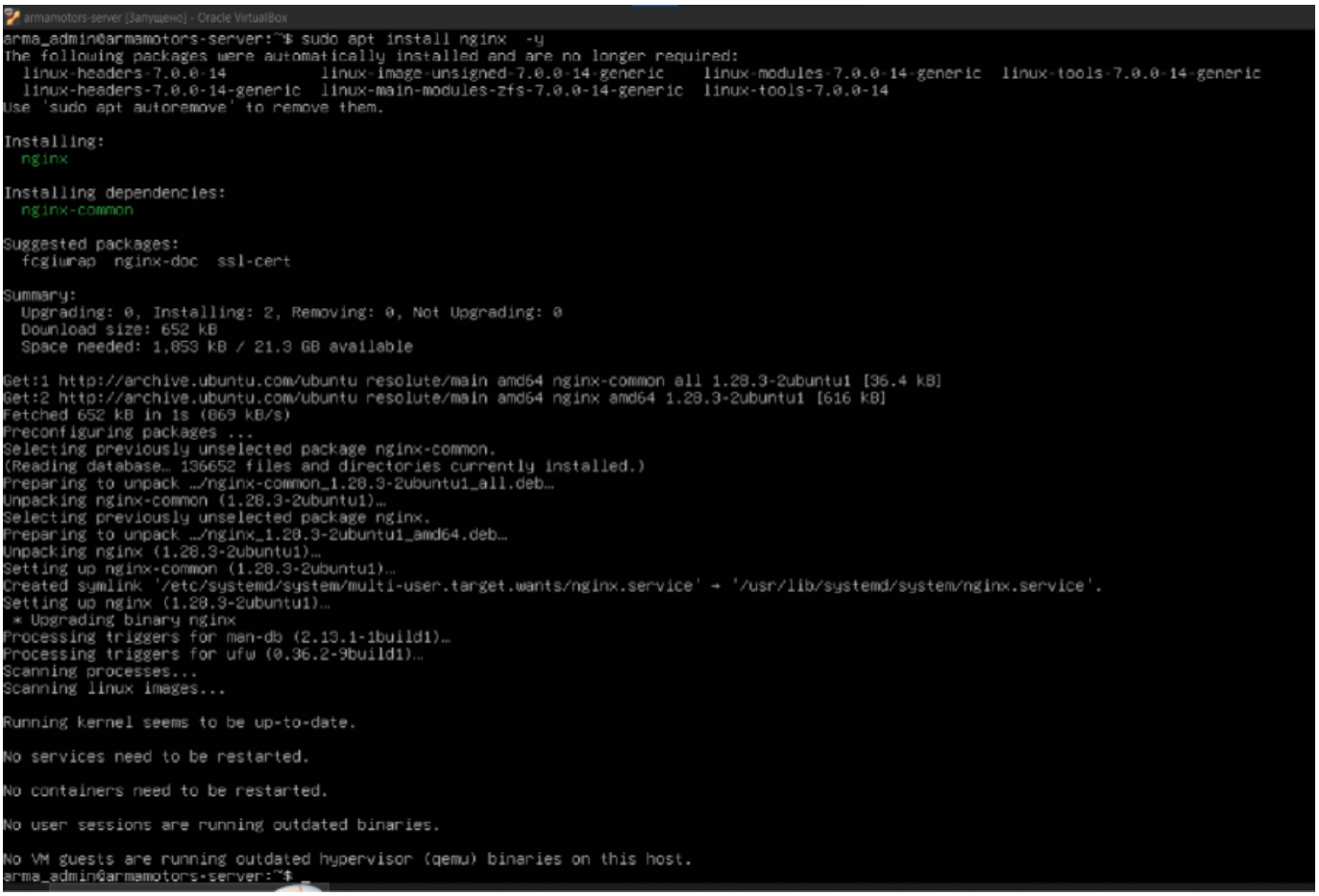


Рисунок 3.3 – Інсталяція вебсервера Nginx для імітації цільової корпоративної системи

Окрім базового встановлення, концепція безпеки Zero Trust вимагає жорсткого контролю над станом усіх локальних служб. Тому після завершення інсталяційних процесів необхідно було впевнитися, що процес Nginx не генерує помилок, коректно прив'язаний до локального інтерфейсу (localhost) і не намагається слухати зовнішні інтерфейси.

Для цього було проведено перевірку статусу служби за допомогою системної утиліти, а саме через виконання команди systemctl status nginx (рис. 3.4). Результат перевірки та детальний вивід консолі підтвердили активний стан процесу (позначка «active (running)»), відсутність критичних попереджень у логах запуску та повну готовність вебсервера приймати вхідні з'єднання всередині ізольованої локальної мережі.

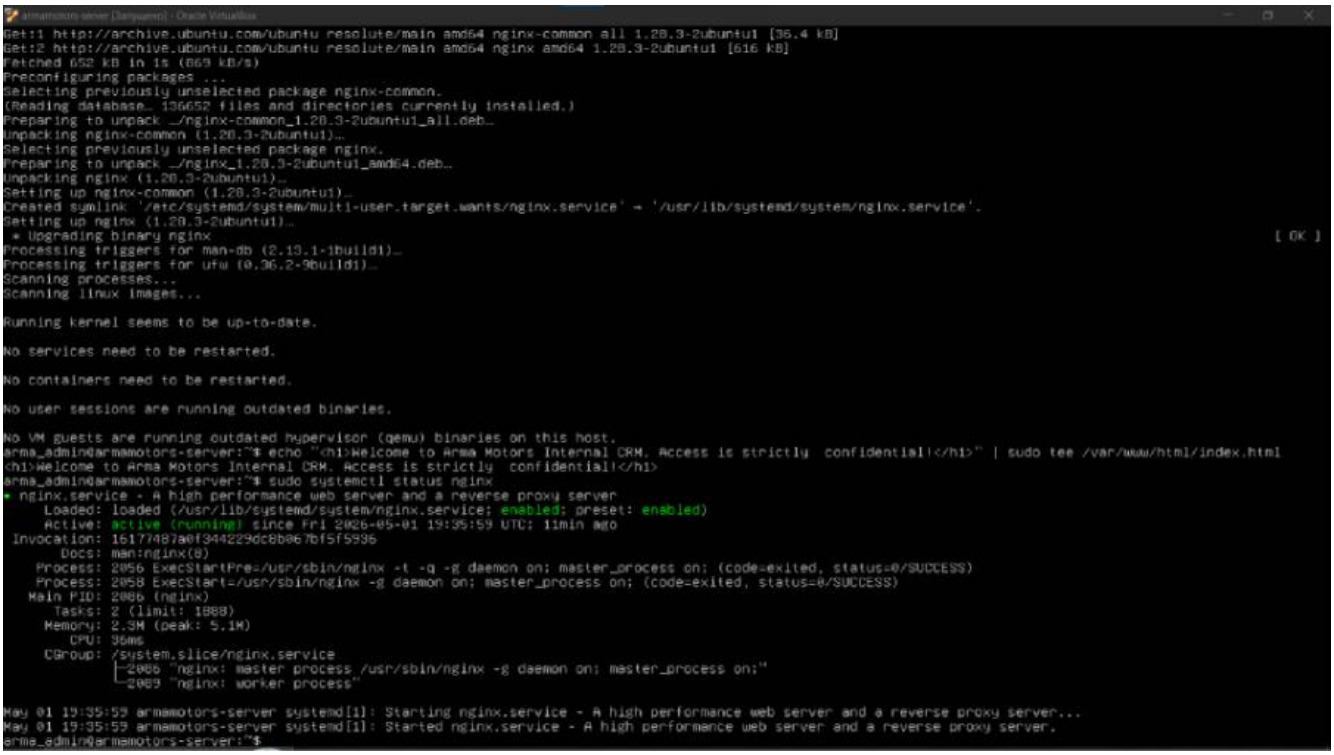


Рисунок 3.4 – Перевірка статусу функціонування цільового вебсервера Nginx

Етап 2. Для забезпечення зручної та безпечної маршрутизації трафіку віддалених працівників до внутрішніх ресурсів підприємства виникла потреба у використанні публічного доменного імені. Наявність унікального доменного імені є обов'язковою архітектурною умовою для побудови вихідних тунелів у системі Cloudflare Zero Trust, оскільки хмарний брокер доступу повинен зв'язати локальний вебсервер із конкретною публічною веб-адресою (URL). Для реалізації тестового стенда на платформі українського реєстратора доменних імен NIC.UA було успішно зареєстровано доменне ім'я amotors.pp.ua [1]. Статус домену в панелі підтверджує його активність та готовність до подальших налаштувань (рис. 3.5).

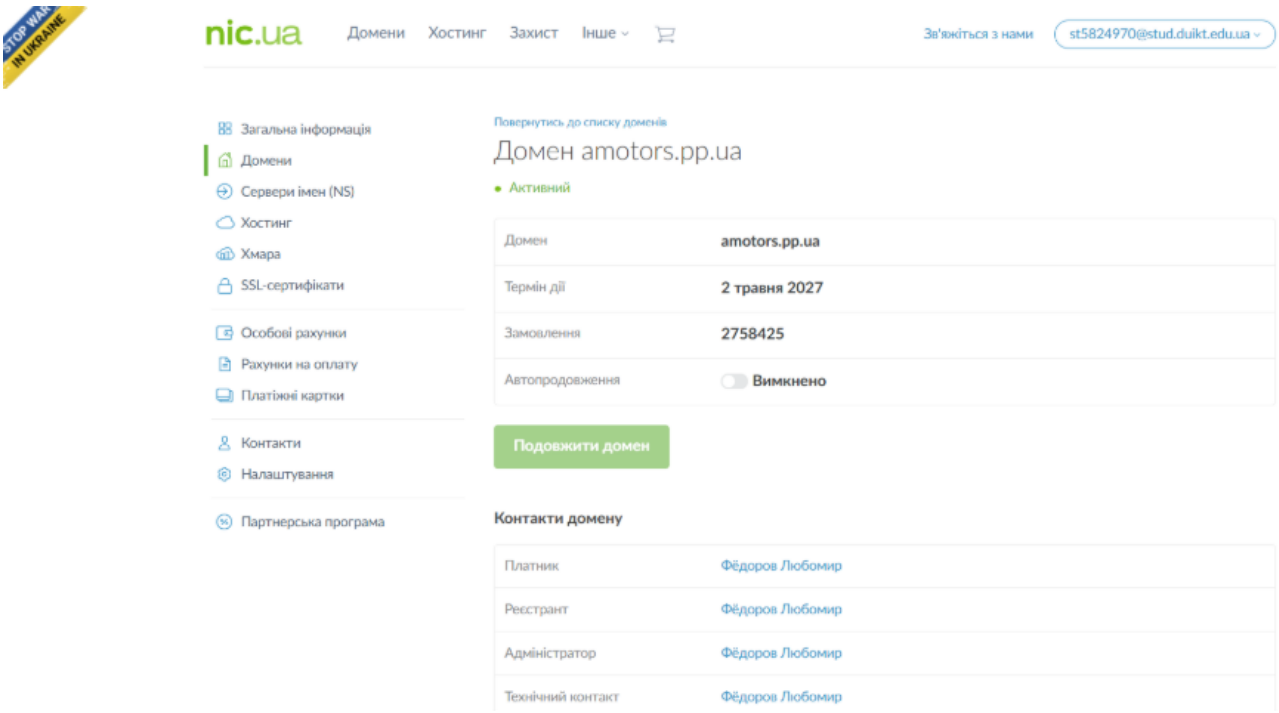


Рисунок 3.5 – Реєстрація корпоративного доменного імені в панелі управління реєстратора

Наступним кроком після реєстрації є підготовка до передачі управління DNS-зоною до інфраструктури Cloudflare. Традиційні сервери імен реєстратора не мають вбудованих інструментів динамічного захисту та швидкого оновлення записів, необхідних для архітектури Zero Trust. Після додавання зареєстрованого домену до облікового запису Cloudflare, платформа автоматично генерує унікальні Anycast NS-сервери (у даному випадку jorge.ns.cloudflare.com та tricia.ns.cloudflare.com), які необхідно використати для переделегування (рис. 3.6).

Отримані адреси серверів імен вносяться у відповідні налаштування на стороні реєстратора NIC.UA (через опцію «Власні сервери імен»). Таке переделегування дозволяє Cloudflare повністю перехопити управління маршрутизацією запитів до домену amotors.pp.ua. Використання глобальної Anycast-мережі брокера забезпечує мінімальну затримку (latency) під час розв'язання DNS-імен для віддалених клієнтів компанії ТОВ «Арма Моторс», а також гарантує високу стійкість до DDoS-атак на рівні DNS-інфраструктури, запобігаючи спробам підміни IP-адрес (DNS spoofing) та отруєнню кешу.

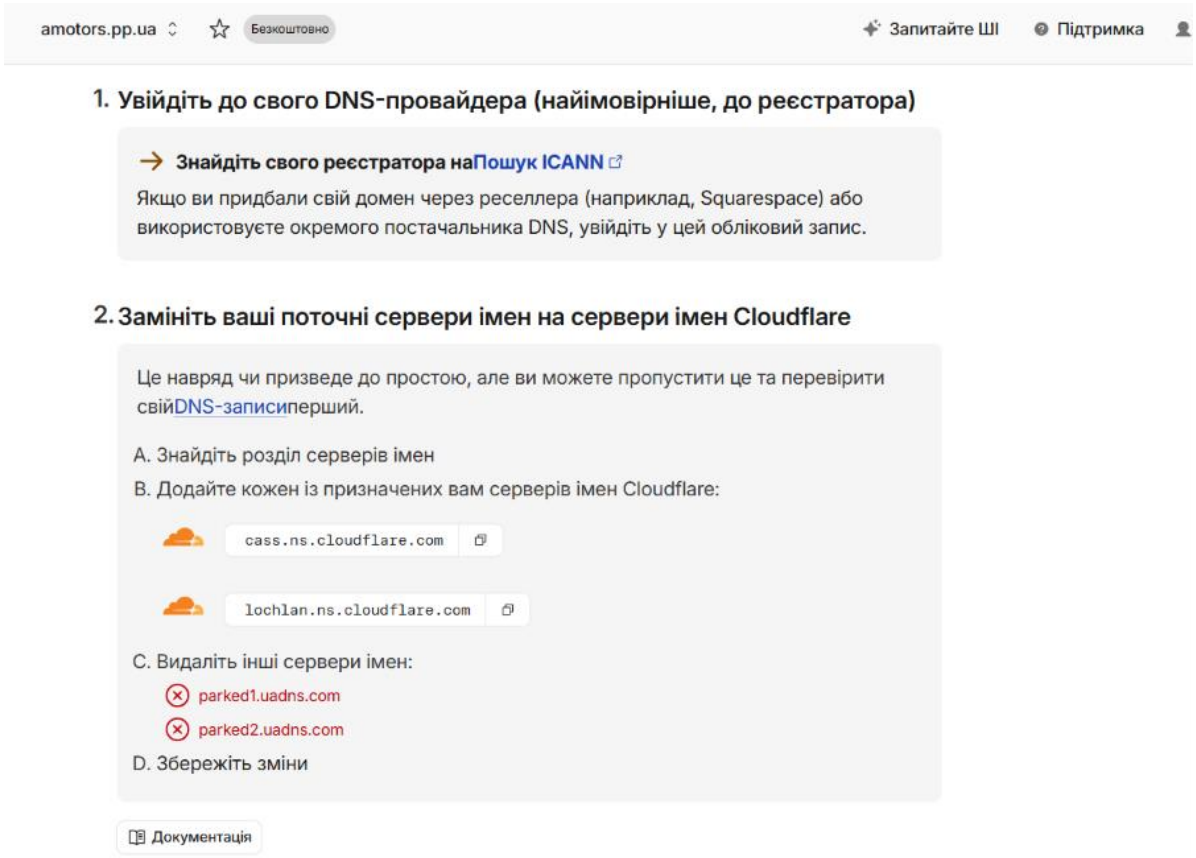


Рисунок 3.6 – Делегування управління доменом до інфраструктури Cloudflare

Процес оновлення глобальних DNS-записів у світовій мережі триває від кількох хвилин до кількох годин, після чого домен стає повністю активним і готовим до створення захищених тунелів.

Етап 3. Розгортання захищеного тунелю Cloudflare Tunnel. Реалізація парадигми невидимої мережі розпочалася з налаштування корпоративного середовища в панелі управління Cloudflare Zero Trust. Для маршрутизації авторизаційних запитів співробітників ТОВ «Арма Моторс» було створено унікальний ідентифікатор команди у вигляді субдомену amotors.cloudflareaccess.com [8]. Цей субдомен виступає єдиним центром єдиного входу (Single Sign-On), через який користувачі проходитимуть багатофакторну автентифікацію.

Після підготовки середовища авторизації було ініційовано створення нового захищеного тунелю (рис. 3.7). Тунелю було присвоєно ідентифікатор arma-motors-crm, який логічно відокремлює даний канал зв'язку від інших можливих сервісів

підприємства. На цьому етапі хмарний брокер генерує унікальний криптографічний токен, який знадобиться для подальшої автентифікації локального сервера.

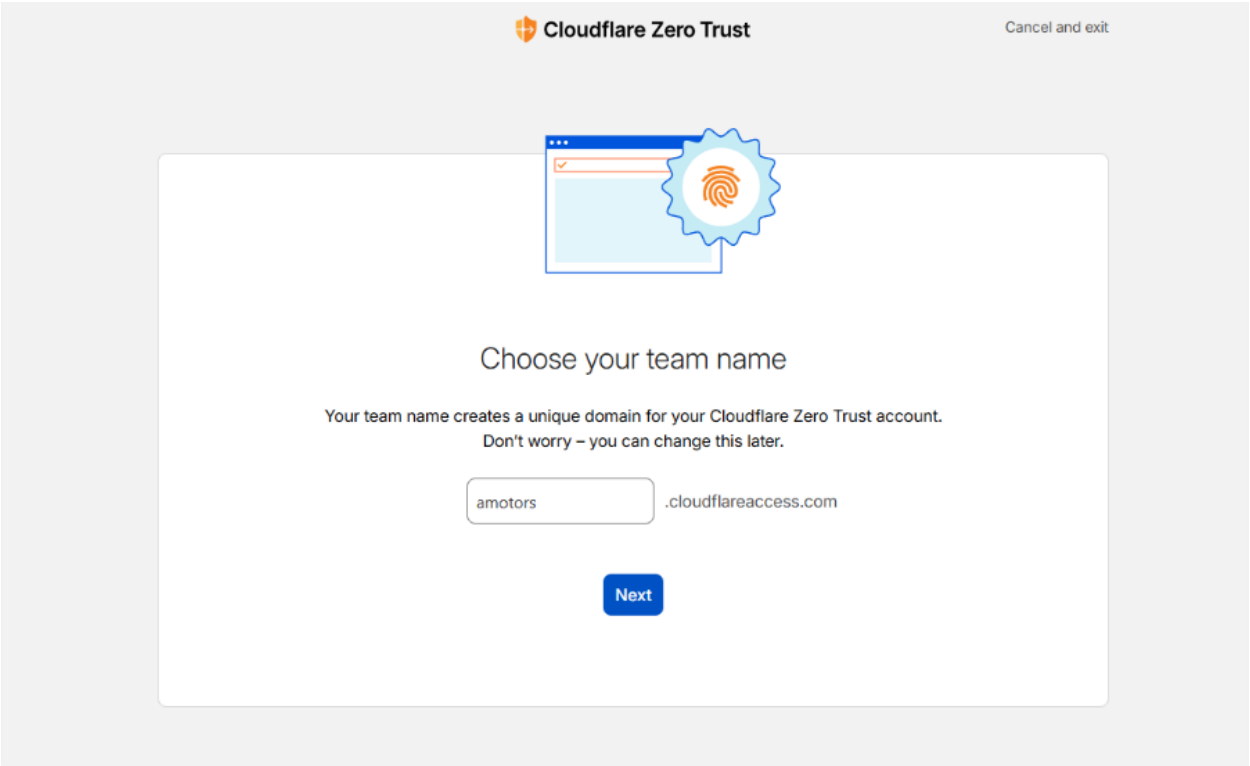


Рисунок 3.7 – Створення організації та ініціалізація тунелю в панелі Zero Trust

Для фізичного з'єднання цільового локального сервера з хмарною інфраструктурою необхідно встановити спеціального агента-посередника. Замість традиційного відкриття вхідних портів (port forwarding) на маршрутизаторі, архітектура Cloudflare використовує легкотривалий програмний демон cloudflared. На локальний сервер під управлінням ОС Ubuntu було завантажено відповідний інсталяційний пакет формату .deb з офіційного репозиторію.

Процес розгортання включав інсталяцію пакета та його реєстрацію як системної служби за допомогою згенерованого раніше токена авторизації (рис. 3.8). Використання токена гарантує, що лише цей конкретний сервер зможе підключитися до створеного тунелю. Після запуску служба cloudflared автоматично ініціює безпечні вихідні з'єднання (Outbound Connections) за протоколом HTTP/2 або QUIC до найближчих периферійних дата-центрів Anycast-мережі.

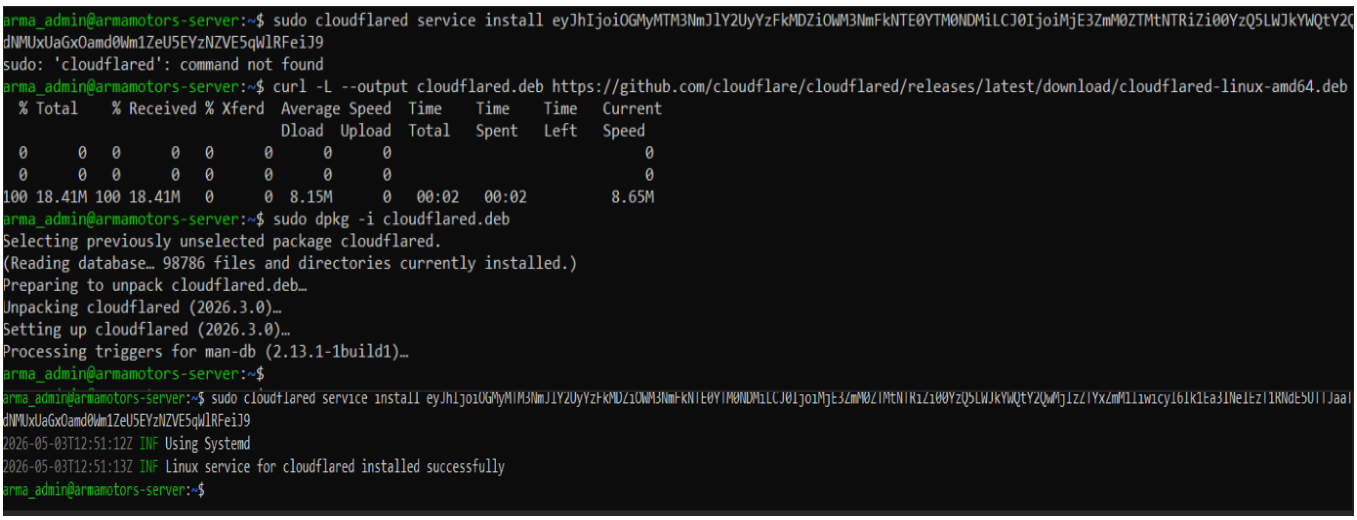


Рисунок 3.8 – Встановлення програмного демона конектора на локальному сервері

Успішне встановлення криптографічного з'єднання та синхронізація локального демона з глобальною мережею відображається в хмарній консолі керування. Зміна статусу тунелю на стан «HEALTHY» (рис. 3.9) свідчить про те, що маршрутизація працює коректно і сервер повністю готовий до обробки цільового трафіку.

З цього моменту локальний сервер отримав високозахищений канал зв'язку з інтернетом, залишаючись при цьому абсолютно невидимим для зовнішніх мережевих сканерів та хакерських ботнетів, оскільки всі вхідні порти на апаратному міжмережевому екрані підприємства залишаються закритими.

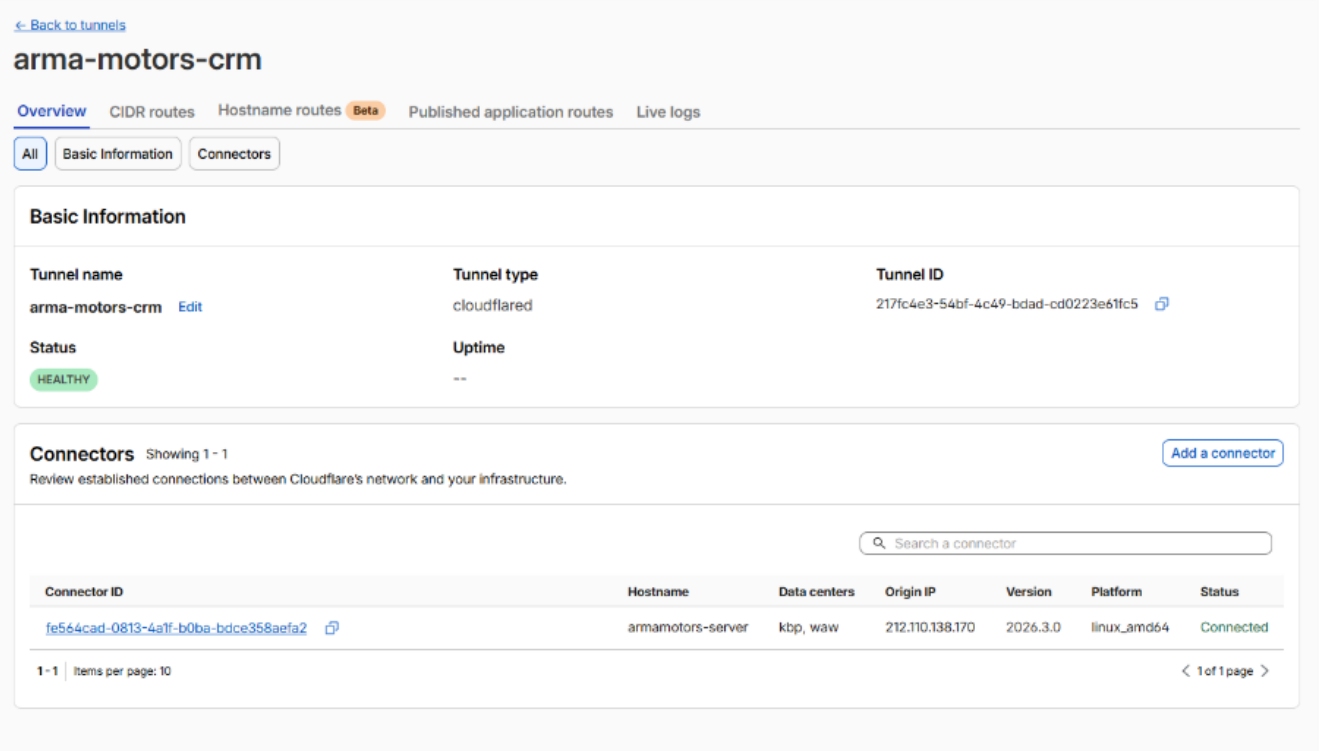


Рисунок 3.9 – Моніторинг статусу захищеного тунелю в панелі керування Cloudflare

Етап 4. Налаштування маршрутизації та політик мікросегментації. Після успішної активації вихідного тунелю наступним кроком є конфігурація маршрутизації на рівні хмарного брокера (Public Hostname). Оскільки локальний вебсервер Nginx не має зовнішньої IP-адреси, системі Cloudflare було вказано перенаправляти всі вхідні запити, що надходять на публічну адресу crm.amotors.pp.ua, безпосередньо через створений тунель до локальної служби http://localhost:80. Такий підхід (рис. 3.10) реалізує концепцію мікросегментації: користувач отримує доступ виключно до одного конкретного вебдодатка, не маючи фізичної видимості інших серверів чи портів у корпоративній мережі.

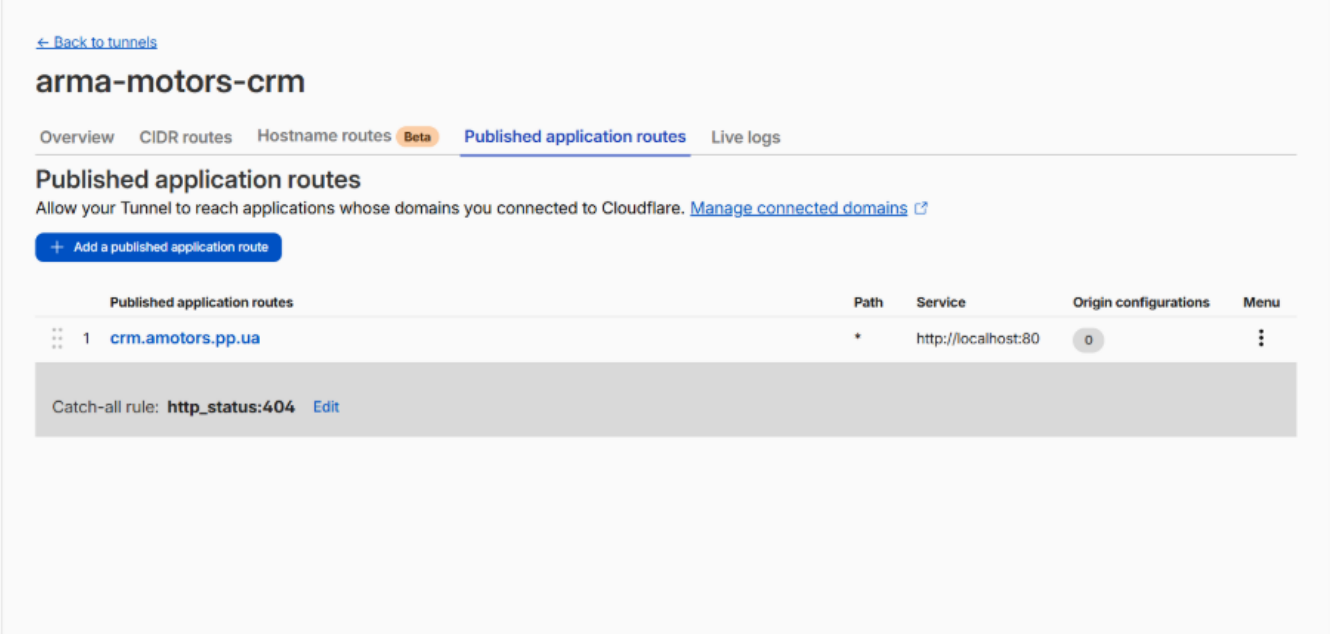


Рисунок 3.10 – Налаштування маршрутизації трафіку до локального веб сервера

Базова маршрутизація не захищає ресурс від несанкціонованого доступу. Згідно з парадигмою Zero Trust, ідентифікації лише самого користувача недостатньо – система повинна довіряти ще й пристрою. Для цього в налаштуваннях платформи було створено профіль перевірки стану безпеки кінцевої точки (Device Posture). Було обрано правило, яке через встановлений клієнт Cloudflare WARP збирає телеметрію з операційної системи та перевіряє наявність увімкненого міжмережевого екрана (Windows Firewall) на комп'ютері користувача (рис. 3.11).

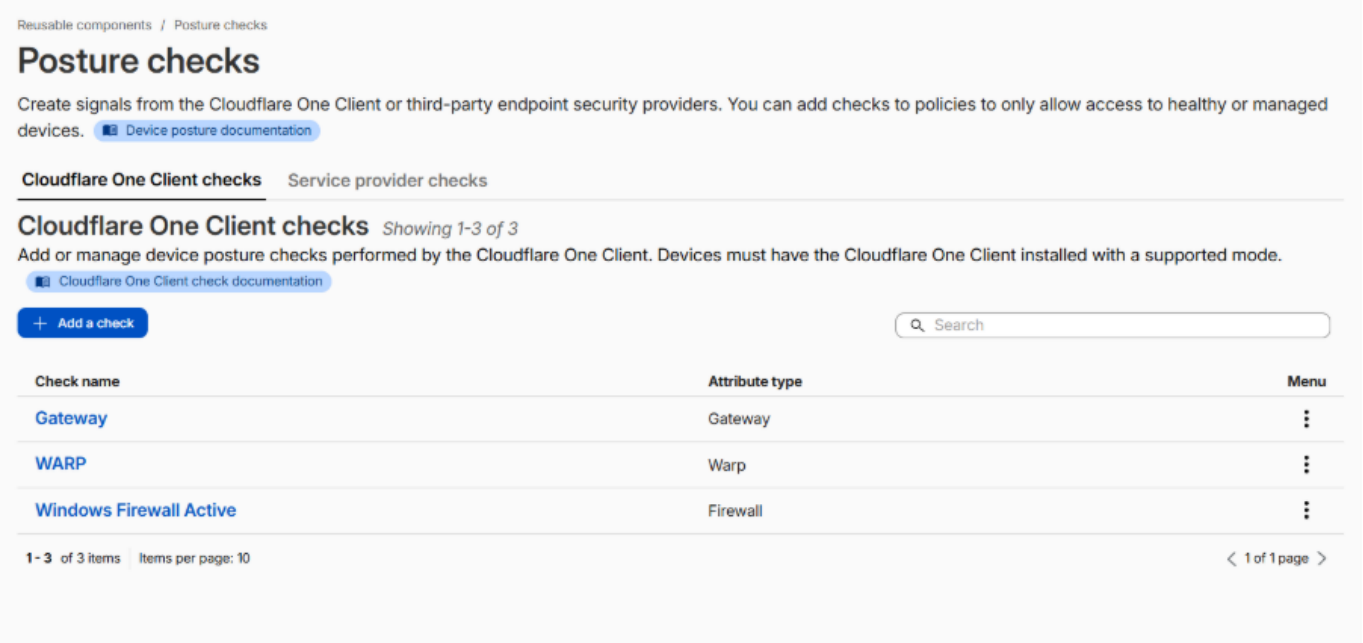


Рисунок 3.11 – Створення критерію перевірки стану захищеності кінцевого пристрою

Фінальним кроком етапу стало створення комплексної політики доступу (Access Policy), яка зв'язує маршрут і правила безпеки в єдиний логічний ланцюг. Для надійного захисту корпоративної CRM-системи конфігурація політики об'єднала перевірку особи та стану обладнання на основі булевої логіки (рис. 3.12).

Було налаштовано суворе правило, за яким доступ до застосунку надається виключно за умови одночасного виконання двох критеріїв: успішної автентифікації користувача через дозволену корпоративну електронну пошту (реалізовано через логічний оператор Include) ТА підтвердження безпечного стану пристрою з увімкненим брандмауером (реалізовано через логічний оператор Require). Якщо хоча б одна з умов не виконується, брокер миттєво блокує мережевий пакет ще на етапі хмарної периферії, не пропускаючи його до тунелю.

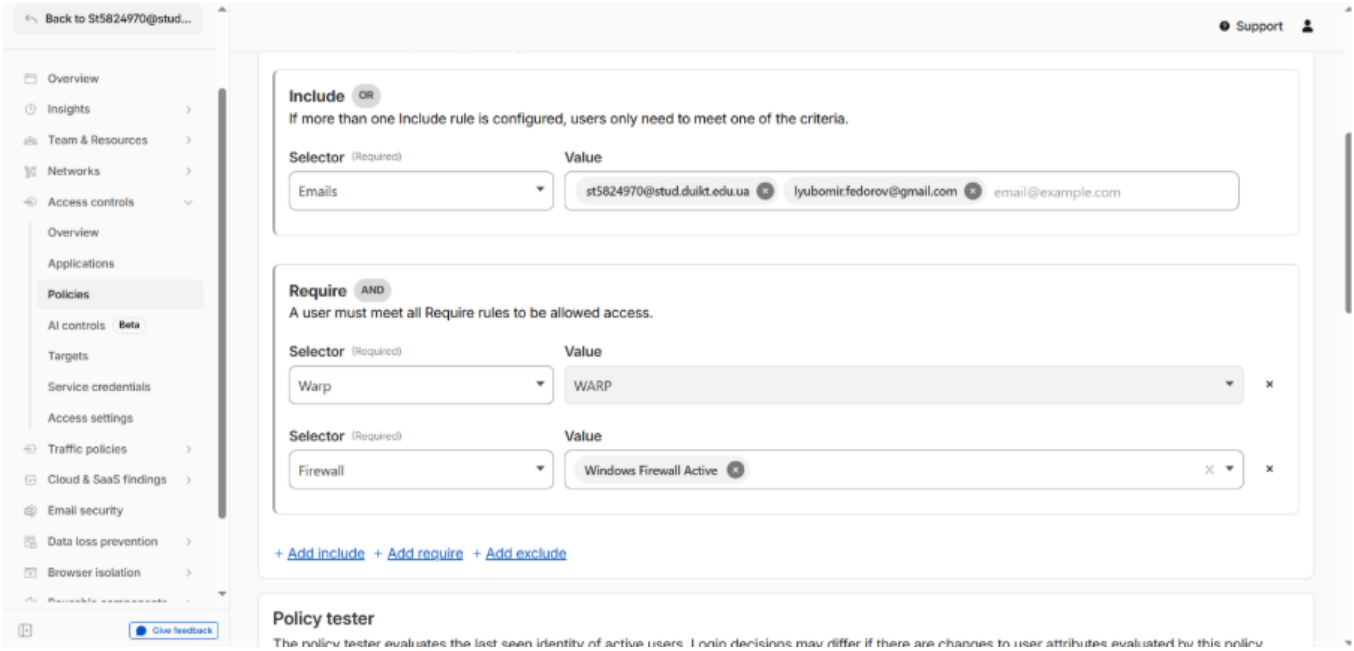


Рисунок 3.12 – Конфігурація комплексної політики доступу до корпоративного ресурсу

Етап 5. Експериментальна перевірка працездатності та механізмів Device Posture.

Практична перевірка розробленої архітектури Zero Trust проходила у кілька послідовних стадій для підтвердження коректної роботи всіх впроваджених рівнів захисту. На першій стадії користувач ініціював мережевий запит безпосередньо до захищеної адреси crm.amotors.pp.ua. Оскільки прямі звернення до вебсервера неможливі через відсутність відкритих портів, система автоматично перенаправила користувача на хмарний портал автентифікації Cloudflare Access. На цьому етапі (рис. 3.13) було успішно пройдено ідентифікацію особи за допомогою введення одноразового коду (OTP), надісланого на авторизовану корпоративну електронну скриньку.

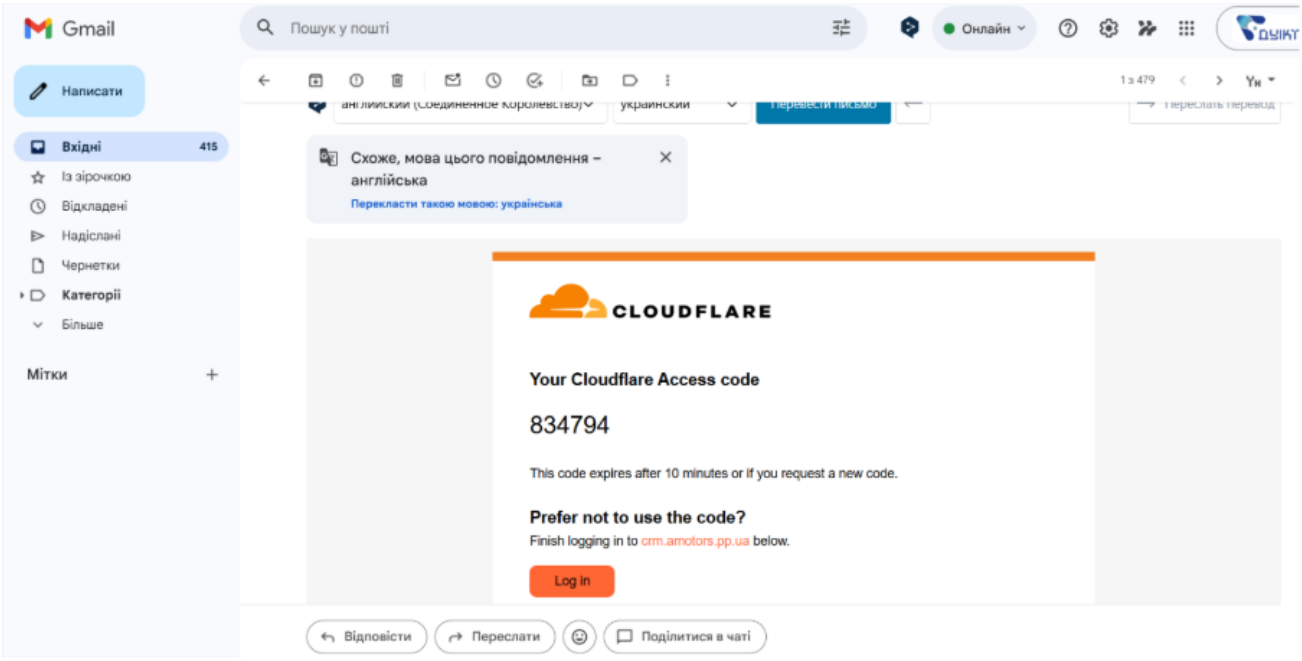


Рисунок 3.13 – Процес багатофакторної автентифікації користувача через електронну пошту

На другій стадії експерименту було проведено стрес-тестування механізму безперервного контролю стану пристрою (Device Posture). Для імітації компрометованого або вразливого комп'ютера на клієнтській машині було навмисно вимкнено системний брандмауер (Microsoft Defender Firewall). Незважаючи на те, що користувач мав дійсний токен поштової авторизації та активне зашифроване з'єднання через клієнт WARP, хмарний брокер миттєво відреагував на порушення комплексної політики безпеки. Запит було відхилено ще на етапі перевірки маршруту, а в браузері відобразилася сторінка блокування (рис. 3.14).

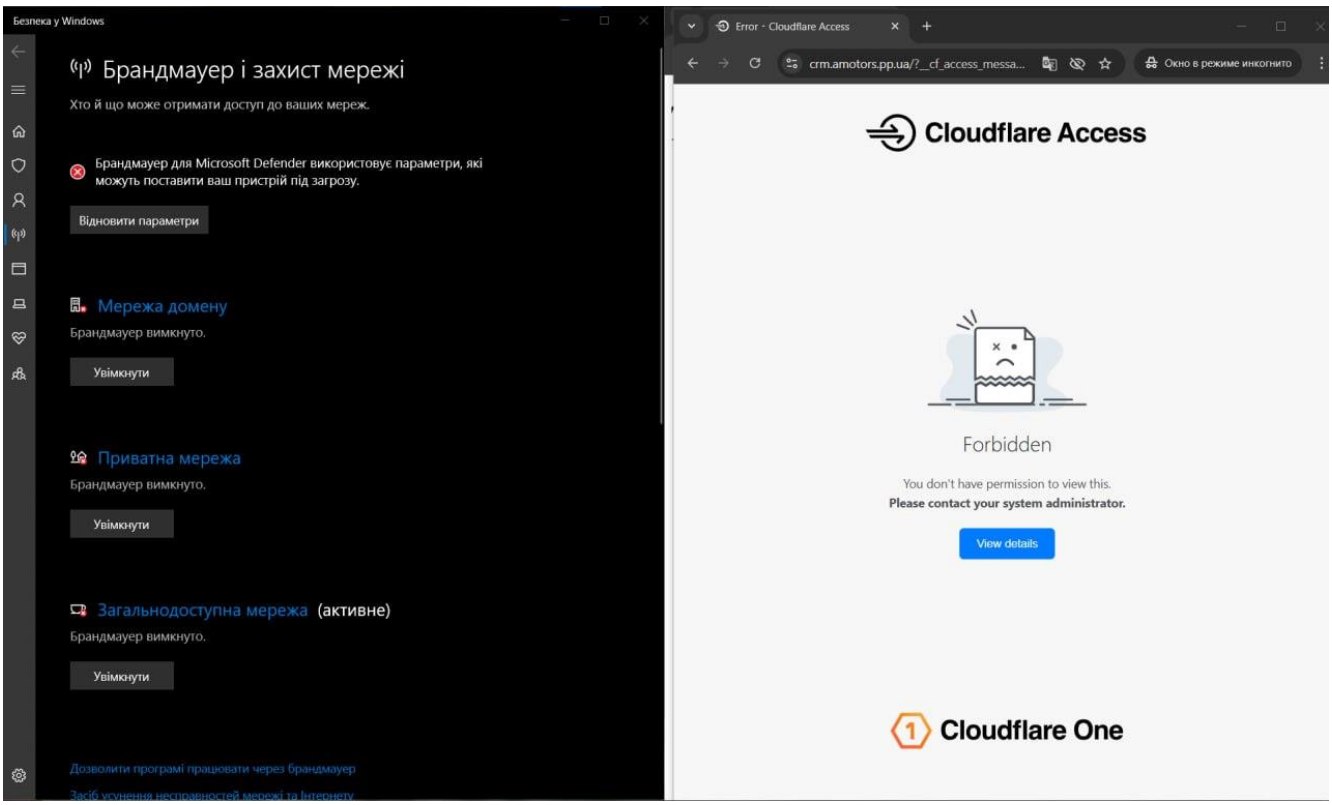


Рисунок 3.14 – Блокування доступу до ресурсу через невідповідність пристрою політиці безпеки

На третій стадії експерименту було проведено повторне тестування системи після усунення штучно створеної вразливості. Системний міжмережевий екран операційної системи Windows було знову переведено в активний стан. Встановлений на пристрої клієнт Cloudflare WARP автоматично зафіксував ці зміни на рівні ОС та негайно передав оновлену телеметрію до центру управління Zero Trust.

Отримавши актуальні дані, політика доступу перерахувала булеву логіку операторів перевірки (ідентичність підтверджено + пристрій захищено). Після цього система задовольнила всі критерії безпеки і надала користувачу повноцінний прозорий доступ до захищеної корпоративної вебсторінки управління клієнтами (рис. 3.15).

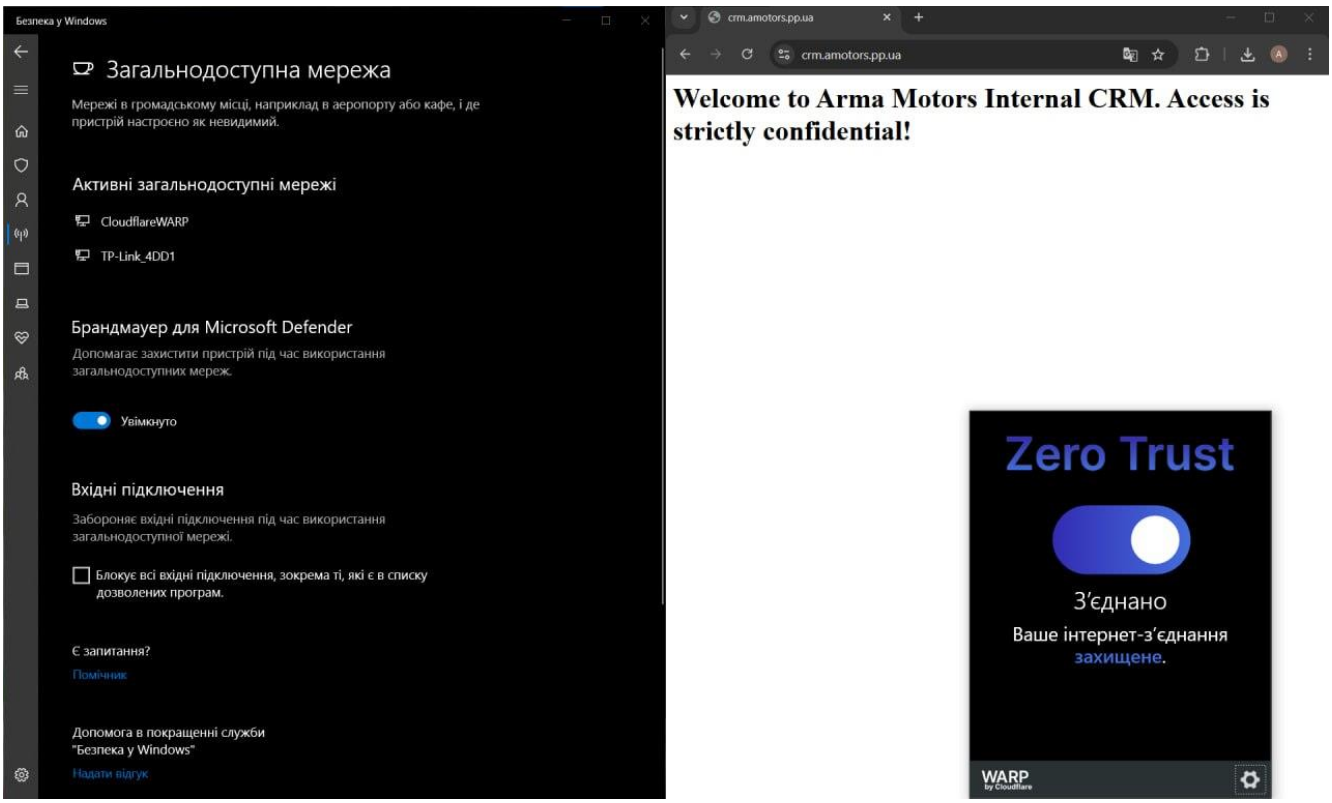


Рисунок 3.15 – Успішне підключення до цільового ресурсу після активації засобів захисту операційної системи

Результати експериментального тестування беззаперечно підтверджують ефективність розробленої архітектури для ТОВ «Арма Моторс». Система функціонує в повній відповідності до парадигми нульової довіри: вона повністю відмовляється від поняття довіреної локальної мережі, приховує інфраструктуру від зовнішнього сканування та безперервно аналізує контекст кожного підключення, мінімізуючи ризики навіть у випадку викрадення облікових даних співробітника.

3.4. Оцінка ефективності запропонованого методу та розрахунок доцільності його практичного впровадження

Оцінка ефективності впровадження архітектури Zero Trust Network Access для підприємства базується на зіставленні потенційних фінансових втрат від реалізації кіберзагроз із вартістю розгортання запропонованої моделі безпеки. Для

максимально об'єктивного аналізу доцільно використати метод кількісної оцінки ризиків (Quantitative Risk Analysis), який дозволяє перевести технічні вразливості у фінансові показники [16].

Методика кількісної оцінки базується на розрахунку кількох ключових метрик. Очікуваний одиничний фінансовий збиток розраховується за формулою:

$$SLE = AV \times EF \tag{3.1}$$

де SLE – очікуваний фінансовий збиток від одного інциденту;

AV – загальна фінансова вартість інформаційного активу;

EF – фактор впливу, що позначає відсоток втрати вартості активу внаслідок одиничного інциденту безпеки.

Очікувані сумарні річні збитки розраховуються за формулою:

$$ALE = SLE \times ARO \tag{3.2}$$

де ALE – очікуваний сумарний річний збиток від конкретної загрози;

ARO – річна норма виникнення, тобто очікувана частота реалізації загрози протягом одного року.

Для проведення розрахунків необхідно визначити базові показники для ТОВ «Арма Моторс». Найбільш критичним активом підприємства є корпоративна CRM-система. Її вартість (AV) формується не лише з вартості програмного забезпечення та серверного обладнання, а насамперед з цінності клієнтської бази, історії транзакцій та потенційних штрафів за витік персональних даних. Експертна оцінка вартості цього активу для великого дилерського центру становить орієнтовно 2 000 000 грн.

У межах традиційної периметральної архітектури з відкритими портами VPN ймовірність успішної атаки (наприклад, проникнення вірусу-шифрувальника) є високою. У випадку реалізації такої загрози система стає недоступною на час

відновлення (в середньому від 2 до 3 робочих днів). Враховуючи простій відділу продажу, сервісу та репутаційні втрати, фактор впливу (EF) оцінюється у 40% [11].

Розрахуємо очікуваний одиничний збиток (SLE) для діючої інфраструктури:

$$SLE = 2\,000\,000 \times 0{,}4 = 800\,000(\text{грн})$$

Через постійне автоматизоване сканування відкритих портів шлюзу та відсутність перевірки стану кінцевих пристроїв (Device Posture), ймовірність успішної атаки на класичний VPN становить щонайменше 1 раз на 2 роки [24]. Відповідно, показник ARO дорівнює 0,5.

Розрахуємо річний очікуваний збиток (ALE) до впровадження нової системи:

$$ALE_{\text{базовий}} = 800\,000 \times 0{,}5 = 400\,000(\text{грн/рік})$$

Впровадження розробленого методу мікросегментації на базі екосистеми Cloudflare якісно змінює рівень ризику. Переведення головного маршрутизатора в режим повного блокування вхідних запитів зводить площу зовнішньої атаки до нуля. Обов'язкова перевірка наявності активного локального міжмережевого екрана та багатофакторна автентифікація нейтралізують загрози викрадення паролів. Завдяки цим заходам річна ймовірність успішної атаки (ARO) знижується до 0,05 (орієнтовно 1 раз на 20 років).

Розрахуємо новий річний очікуваний збиток (ALE) після міграції на архітектуру Zero Trust:

$$ALE_{\text{новий}} = 800\,000 \times 0.05 = 40\,000(\text{грн/рік})$$

Для визначення економічної ефективності необхідно врахувати витрати на впровадження рішення. Важливою перевагою обраної платформи Cloudflare Zero Trust є відсутність плати за ліцензії для команд чисельністю до 50 осіб, що повністю покриває потреби цільової групи ТОВ «Арма Моторс». Відповідно, єдиними

витратами є оплата праці системного адміністратора на проєктування, розгортання та тестування системи. Орієнтовні трудовитрати становлять 40 робочих годин за середньою ставкою 500 грн/год [2]. Таким чином, вартість впровадження (С) дорівнює 20 000 грн.

Фінальним етапом є розрахунок показника повернення інвестицій у безпеку – ROSI (Return on Security Investment). Оцінка здійснюється за формулою [16]:

$$ROSI = \left(\frac{(ALE_{\text{базовий}} - ALE_{\text{новий}}) - \text{C}}{\text{C}} \right) \times 100\% \qquad (3.3)$$

де ALE(базовий) – очікуваний річний збиток до впровадження системи захисту;

ALE(новий) – очікуваний річний збиток після впровадження системи захисту;

С – вартість впровадження заходів безпеки.

Проведемо підстановку значень:

$$ROSI = \left(\frac{400\,000 - 40\,000 - 20\,000}{20\,000} \right) \times 100\% = 1700\%$$

Для наочності результати розрахунків зведено у таблицю 3.2 і зображено на діаграмі (рис. 3.16).

Таблиця 3.2

Порівняльна оцінка ризиків та ефективності рішень безпеки

Показник	**Традиційна архітектура (VPN)**	**Архітектура Zero Trust (Cloudflare)**
Вартість активу (AV)	2 000 000 грн	2 000 000 грн
Фактор впливу (EF)	40% (0,4)	40% (0,4)

Показник	Традиційна архітектура (VPN)	Архітектура Zero Trust (Cloudflare)
Очікуваний одиничний збиток (SLE)	800 000 грн	800 000 грн
Річна ймовірність інциденту (ARO)	0,5	0,05
Очікуваний річний збиток (ALE)	**400 000 грн**	**40 000 грн**
Вартість впровадження захисту (C)	-	20 000 грн
ROSI (Повернення інвестицій)	-	**1700%**

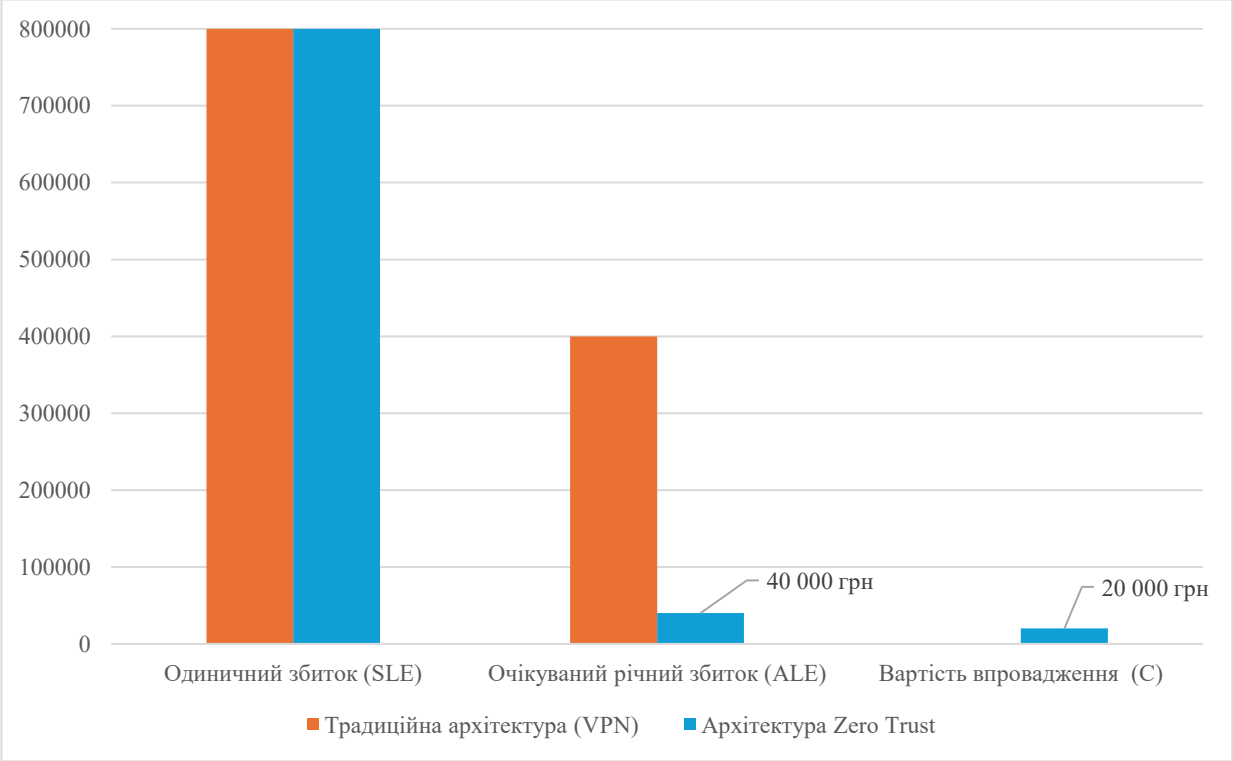


Рисунок 3.16 – Порівняльна діаграма показників економічного ризику та витрат на інформаційну безпеку

Таким чином, розрахунок доцільності математично доводить, що практичне впровадження розробленого методу володіє надзвичайно високим показником повернення інвестицій. Витративши лише 20000 грн на оплату налаштувань, підприємство заощаджує в середньому 360000 грн щороку за рахунок уникнення потенційних кіберінцидентів. ТОВ «Арма Моторс» отримує сучасний ешелонований комплекс захисту критично важливих корпоративних даних без необхідності закупівлі дороговартісного апаратного забезпечення [3,9], що робить запропонований алгоритм оптимальним та беззаперечно обґрунтованим рішенням.

ВИСНОВКИ

У кваліфікаційній роботі розглянуто актуальна проблема підвищення рівня захисту корпоративної мережі підприємства. Виконано проєктування та впровадження архітектури нульової довіри.

За результатами проведеної роботи були сформульовані такі висновки:

1. Проведений аналіз актуального ландшафту кіберзагроз та доведено що традиційна VPN-архітектура втратила свою надійність через відкриті порти та системну вразливість до програм-вимагачів.

2. Було обґрунтовано доцільність впровадження концепції Zero Trust Network Access. Сформовано архітектурну модель безпеки для цільового підприємства ТОВ «Арма Моторс», яка базується на принципах мікросегментації, безперервної верифікації суб'єктів та приховуванні ресурсів підприємства за хмарним брокером доступу.

3. Здійснено проєктування та розгортання захищеної інфраструктури на базі екосистеми Cloudflare. Зв'язок із локальними серверами здійснюється виключно через ізольовані вихідні тунелі. Це дозволило перевести апаратний міжмережевий екран підприємства в режим повного блокування вхідних з'єднань, що звело площу зовнішньої атаки до нуля.

4. Налаштовано гранулярні політики контролю доступу. Багатофакторна автентифікація через єдиний центр входу поєднана з безперервним моніторингом кінцевих пристроїв. Експеримент довів дієвість підходу – відключення працівником локального брандмауера миттєво ініціює автоматичне блокування сесії.

5. Розрахована економічна ефективність запропонованого рішення з використанням методики кількісної оцінки ризиків. Розрахунки показали що впровадження розробленої архітектури знижує річну ймовірність успішної кібератаки до 0,05. Очікувані фінансові збитки зменшуються вдесятеро: із 400 000 до 40 000 гривень на рік. Показник повернення

інвестицій у безпеку становить 1700 %, що підтверджує високу фінансову доцільність впровадження системи для захисту комерційної таємниці та клієнтських баз даних ТОВ «Арма Моторс».

Таким чином, мета кваліфікаційної роботи досягнута, а всі поставлені завдання виконано в повному обсязі. Розроблена система готова до масштабування та використання в реальних умовах бізнесу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Офіційний сайт реєстратора доменних імен NIC.UA. *NIC.UA*. URL: https://nic.ua/ (дата звернення: 12.05.2026).
2. Статистика зарплат IT-спеціалістів в Україні. *DOU.ua*. URL: https://jobs.dou.ua/salaries/ (дата звернення: 16.05.2026).
3. Chen X., Feng W., Ge N., Zhang Y. Zero Trust Architecture for 6G Security. *IEEE Wireless Communications*. 2024. Vol. 31, no. 2. P. 112–119. URL: https://ieeexplore.ieee.org/document/10288499 (дата звернення: 19.05.2026).
4. Cisco Duo Editions Datasheet. *Cisco*. 2023. 8 p. URL: https://resources.duo.com/explore/assets/duo-editions-datasheet (дата звернення: 19.05.2026).
5. Configure Microsoft cloud services for the CISA Zero Trust Maturity Model. *Microsoft Learn*. URL: https://learn.microsoft.com/en-us/security/zero-trust/cisa-zero-trust-maturity-model-intro (дата звернення: 19.05.2026).
6. Cybersecurity and Infrastructure Security Agency (CISA). Zero Trust Maturity Model Version 2.0. *CISA*. 2023. 34 p. URL: https://www.cisa.gov/zero-trust-maturity-model (дата звернення: 19.05.2026).
7. Department of Defense (DoD). Zero Trust Strategy. *U.S. Department of Defense*. 2022. 28 p. URL: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf (дата звернення: 19.05.2026).
8. Designing ZTNA access policies. *Cloudflare Docs*. URL: https://developers.cloudflare.com/reference-architecture/design-guides/designing-ztna-access-policies/ (дата звернення: 19.05.2026).
9. Dhiman P. та ін. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors*. 2024. Vol. 24, no. 4. P. 1328–1350. URL: https://doi.org/10.3390/s24041328 (дата звернення: 19.05.2026).

10. ENISA Threat Landscape 2024. *European Union Agency for Cybersecurity*. 2024. 154 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 19.05.2026).

11. IBM Security. Cost of a Data Breach Report 2025. *IBM*. 2025. 78 p**.** URL: https://www.ibm.com/reports/data-breach (дата звернення: 19.05.2026).

12. Lee S., Huh J.-H., Woo H. Security System Design and Verification for Zero Trust Architecture. *Electronics*. 2025. Vol. 14, no. 4. P**.** 643–660. URL: https://doi.org/10.3390/electronics14040643 (дата звернення: 19.05.2026).

13. Manage Zero Trust Application. *Perimeter 81 Support*. URL: https://support.perimeter81.com/docs/manage-zero-trust-application (дата звернення: 19.05.2026).

14. National Cybersecurity Center of Excellence (NCCoE). Implementing a Zero Trust Architecture (NIST SP 1800-35). *National Institute of Standards and Technology*. 2022. 248 p**.** URL: https://csrc.nist.gov/pubs/sp/1800/35/final (дата звернення: 19.05.2026).

15. Nginx security headers. *Ploi.cloud*. URL: https://ploi.cloud/documentation/security/nginx-security-headers (дата звернення: 19.05.2026).

16. Return On Security Investment. *ENISA*. 2012. 24 p**.** URL: https://www.enisa.europa.eu/sites/default/files/publications/Return%20On%20Security%20Investment.pdf (дата звернення: 19.05.2026).

17. Sasada T., Taenaka Y., Kadobayashi Y., Fall D. Web-Biometrics for User Authenticity Verification in Zero Trust Access Control. *IEEE Access*. 2024. Vol. 12. P. 45012–45025. URL: https://ieeexplore.ieee.org/document/10555260/ (дата звернення: 19.05.2026).

18. Syrotynskyi R., Tyshyk I., Kochan O., Sokolov V., Skladannyi P. Methodology of network infrastructure analysis as part of migration to zero-trust architecture. *CEUR Workshop Proceedings*. 2024. Vol. 3800. **P.** 45–56. URL: https://ceur-ws.org/Vol-3800/short3.pdf (дата звернення: 19.05.2026).

19. ThreatLabz 2025 VPN Report: Why 81% of Organizations Plan to Adopt Zero Trust by 2026. *Zscaler Blog*. 2025. URL: https://www.zscaler.com/blogs/security-research/threatlabz-2025-vpn-report-why-81-organizations-plan-adopt-zero-trust-2026 (дата звернення: 19.05.2026).

20. Universal ZTNA / Zscaler Private Access. *Zscaler Help*. URL: https://help.zscaler.com/zpa/universal-ztna-zscaler-private-access-private-service-edge (дата звернення: 19.05.2026).

21. VPN and its impact on cybersecurity. *ITorakular*. 2024. URL: https://itorakul.com.ua/en/vpn-cybersecurity/ (дата звернення: 19.05.2026).

22. Will VPN Security Vulnerabilities Accelerate ZTNA Adoption? *Akamai*. 2024. URL: https://www.akamai.com/blog/security/will-vpn-security-vulnerabilities-accelerate-ztna-adoption (дата звернення: 19.05.2026).

23. Zero Trust Architecture and Prospects for its Implementation in the Government Sector of Ukraine. *Science and Defense*. 2024. № 1. **С. 45–52**. URL: https://digest.mil.knu.ua/en/article/view/9607 (дата звернення: 19.05.2026).

24. Zscaler ThreatLabz. The Big Idea: VPNs Are No Longer the Backbone of Secure Access (2025 VPN Risk Report). *Zscaler*. 2025. 40 p. URL: https://www.zscaler.com/learn/2025-vpn-risk-report (дата звернення: 19.05.2026).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)

Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

Виконав:

Студент групи ІСД-42
Любомир ФЕДОРОВ

Керівник:

PhD, доцент каф. ІСТ
Дмитро КОЗЛОВ

Київ 2026

ОБ'ЄКТ, ПРЕДМЕТ ТА МЕТА ДОСЛІДЖЕННЯ

ОБ'ЄКТ ДОСЛІДЖЕННЯ

Процес забезпечення інформаційної безпеки корпоративних інфраструктур в умовах віддаленого та гібридного режимів роботи.

ПРЕДМЕТ ДОСЛІДЖЕННЯ

Методи та технологічні засоби побудови архітектури ZTNA на прикладі платформи Cloudflare для захисту внутрішніх сервісів.

МЕТА РОБОТИ

Підвищення рівня безпеки мережі ТОВ «Арма Моторс» шляхом проєктування та впровадження архітектури Zero Trust Network Access.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

ГІБРИДНА РОБОТА

Масовий перехід на віддалений доступ повністю розмив класичний мережевий периметр підприємств.

КРАХ VPN МОДЕЛІ

Традиційні засоби «замок та рів» базуються на помилковій надмірній довірі після автентифікації.

КРИТИЧНІСТЬ ДАНИХ

Для ТОВ «Арма Моторс» CRM-система містить конфіденційні дані клієнтів з високою комерційною цінністю.

ВИКОНАНІ ЗАВДАННЯ ДОСЛІДЖЕННЯ

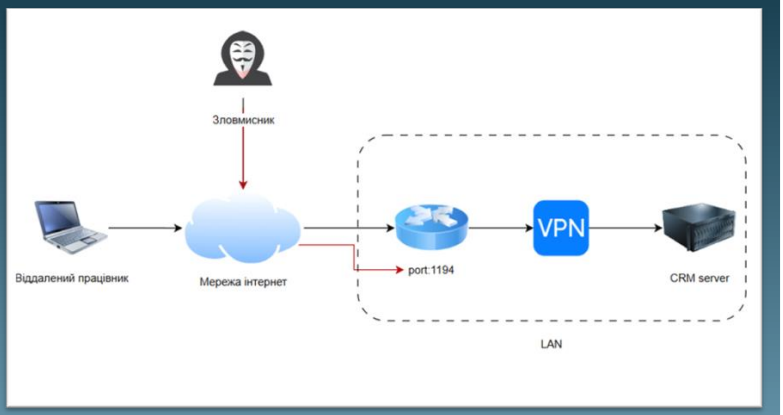
- **Аналіз загроз:** Виявлено вразливості традиційних VPN-мереж та ризики відкритих вхідних портів.
- **Теорія:** Вивчено стандарти NIST та CISA щодо побудови систем нульової довіри.
- **Проєктування:** Розроблено нову топологію мережі та 5-етапний алгоритм безшовної міграції сервісів.
- **Реалізація:** Створено технічний стенд на базі Cloudflare та Nginx для перевірки механізмів Device Posture.
- **Економічне обґрунтування:** Розраховано коефіцієнт ROSI та оцінено зниження ризиків.

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПОТОЧНОЇ АРХІТЕКТУРИ

Відкриті вхідні порти: Шлюз постійно очікує запити ззовні, стаючи ціллю для сканерів.

Надмірна довіра: Після авторизації користувач бачить увесь сегмент локальної мережі.

Відсутність контролю хоста: Заражений домашній ПК безперешкодно передає шкідливий трафік у тунель.



АЛГОРИТМ ВПРОВАДЖЕННЯ МОДЕЛІ ZTNA

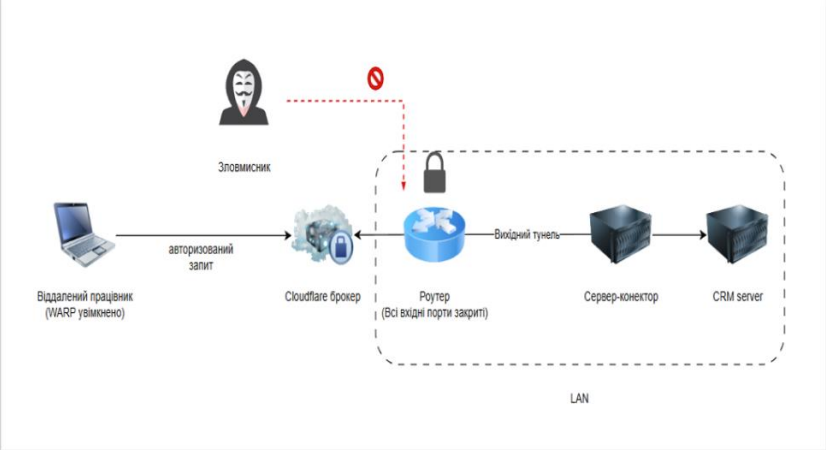
1. Аудит: Інвентаризація активів та CRM
2. Проєктування: Розробка ролевих політик ідентифікації та формалізація матриці управління доступом
3. Розгортання: Встановлення служби cloudflared для ініціації безпечних вихідних з'єднань до хмарного брокера
4. Інтеграція: Підключення IdP-провайдерів та розгортання агента WARP для моніторингу стану кінцевих точок.
5. Ізоляція: Переключення трафіку в тунель та повне блокування відкритих вхідних портів на маршрутизаторі.

ТЕХНІЧНА АРХІТЕКТУРА: CLOUDFLARE TUNNEL

Конектор cloudflared самостійно будує вихідний зашифрований маршрут назовні.

Роутер підприємства повністю блокує всі вхідні пакети з інтернету.

Інфраструктура ховається від автоматизованого сканування шкідливими ботнетами.

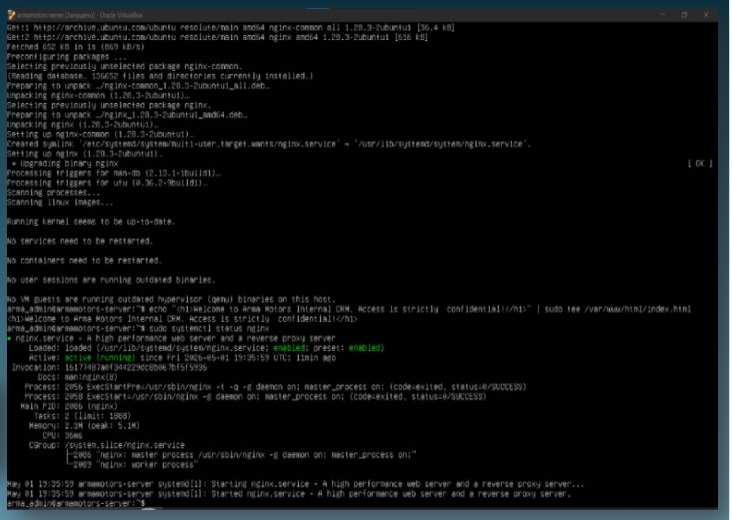


КОНФІГУРАЦІЯ СЕРВЕРА ТА ВЕБСЕРВЕРА NGINX

Цільову CRM-систему розгорнуто на базі ОС **Ubuntu Server** за допомогою пакета **Nginx**.

Служба прив'язана виключно до внутрішнього локального інтерфейсу, унеможливлюючи прямий обхід хмарного брокера.

```
listen 80;
server_name crm.amotors.pp.ua;
access_log /var/log/nginx/crm_access.log;
```



МАТРИЦЯ УПРАВЛІННЯ ДОСТУПОМ

Група користувачів	Критерії автентифікації	Вимоги до стану пристрою	Дія системи
Адміністратори	IdP + MFA (OTP код)	Клієнт активний, FW + Антивірус	Дозволити
Менеджери CRM	IdP + Робочий час	Клієнт активний, FW увімкнено	Дозволити
Сервісний персонал	Успішна автентифікація	Будь-який стан пристрою	Заблокувати
Невідомі сканери	Відсутня	Відсутній клієнт шифрування	Ігнорувати

ПОЛІТИКИ ДОСТУПУ ТА DEVICE POSTURE

CLOUDFLARE ACCESS

Перевіряє автентичність користувача через одноразові коди авторизації.

АГЕНТ WARP

Безперервно збирає та передає в хмару телеметрію захищеності операційної системи.

ЛОГІЧНІ ОПЕРАТОРИ

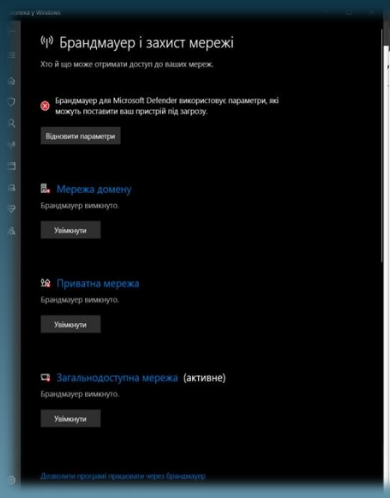
Поєднання умов **Include** ідентифікація пошти та **Require** активний Firewall.

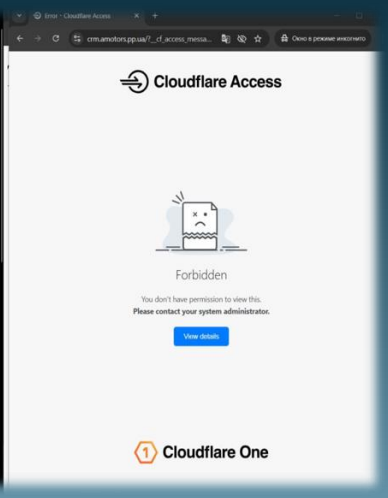
ЕКСПЕРИМЕНТАЛЬНЕ ТЕСТУВАННЯ БЕЗПЕКИ

Крок 1: Користувач підтверджує особу через OTP-код у корпоративній скриньці.

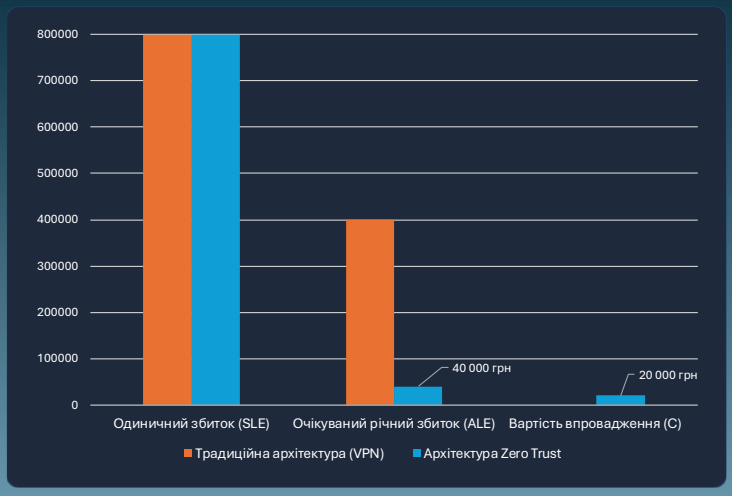
Крок 2: Навмисне відключення брандмауера Windows негайно фіксується агентом WARP, брокер миттєво видає статус **Forbidden**.

Крок 3: Активація захисту автоматично відновлює прозорий доступ до CRM.





ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ РОЗРОБКИ



Метрики кількісної оцінки:

Вартість активу: 2 000 000 грн

ALE (до модернізації): 400 000 грн/рік

ALE (після міграції): 40 000 грн/рік

Витрати на впровадження: 20 000 грн

ROSI = 1700%

ВИСНОВКИ

- Традиційні VPN з відкритими портами є критично вразливими до автоматизованих атак.
- Технологія Cloudflare Tunnel ліквідувала вхідні порти, забезпечивши невидимість мережі.
- Механізм Device Posture виключає несанкціонований доступ зі скомпрометованих пристроїв.
- Показник повернення інвестицій ROSI доводить абсолютну фінансову доцільність методу.

Апробація результатів