

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та рішення Zero Trust архітектури
для кіберзахисту корпоративних мереж»

Виконав: студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист
інформації»



Богдан ГЕРАСИМЕНКО

Керівник: професор кафедри КІ та КБ, д.т.н., доцент,



Володимир ВОРОТНИКОВ

Рецензент: завідувач кафедри КІ та КБ, к.т.н., доцент



Андрій ЄФІМЕНКО

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

06 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Герасименко Богдан Миколайович

Тема роботи: «Методи та рішення Zero Trust архітектури для кіберзахисту
корпоративних мереж»

затверджена Наказом університету від 06 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 29 грудня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Наукові джерела з методів впровадження політик Zero Trust;
2. Нормативно правові акти кібербезпеки щодо проектування корпоративних мереж;
3. Документація компанії Forrester.

Обладнання та програмне забезпечення:

1. Інструменти віртуалізації комп'ютерних мереж та робочих станцій GNS3, Oracle VirtualBox;
2. ОС Windows Server 2022;
3. Фреймворк моніторингу подій ElastAlertPro;

3. Фреймворк моніторингу подій ElastAlertPro;
4. Сервер RADIUS 19.2.1;
5. Модель безпеки Google BeyondCorp.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

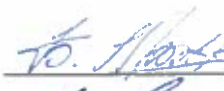
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор Фальковський	10.09.2025	10.09.2025
2	Ігор Фальковський	15.09.2025	15.09.2025
3	Ігор Фальковський	21.09.2025	21.09.2025

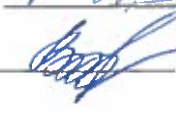
Студент  Богдан Герасименко

Керівник  Володимир ВОРОТНИКОВ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	10.09.2025	виконано
2	Формулювання робочого плану	08.10.2025	виконано
3	Пошук та аналіз актуальних джерел інформації	14.10.2025	виконано
4	Подання консультанту плану з метою перевірки	21.10.2025	виконано
5	Підготовка додаткових матеріалів	02.11.2025	виконано
6	Налаштування тестового середовища	24.11.2025	виконано
7	Налаштування стабільного функціонування мережного середовища	03.12.2025	виконано
8	Перевірка сценаріїв функціонування	15.12.2025	виконано
9	Оформлення роботи	21.12.2025	виконано
10	Підготовка до захисту	23.12.2025	виконано

Студент  Богдан Герасименко

Керівник  Володимир ВОРОТНИКОВ

АНОТАЦІЯ

Випускна кваліфікаційної робота II (другий) академічного (магістерського) рівня вищої освіти на тему «Впровадження Zero Trust архітектури для кіберзахисту корпоративних мереж» містить аналіз теоретичних рішень та практичних технологій для подальшого проектування системи з впровадженими методами захисту. Створено перелік програмно-апаратних рішень, цільових методів впровадження моделі Zero Trust для забезпечення належного рівня безпеки в корпоративних мережах;

Метою випускної кваліфікаційної роботи є детальне вивчення та ототожнення вибору та порівняння методів, технологій та аспектів проектування з використанням готових безкоштовних рішень та методів впровадження моделі Zero Trust в корпоративних мережах;

Обсяг пояснювальної записки складає 65 сторінок, 45 рисунків, 5 таблиць. Списку використаних джерел містить в собі 22 найменування, що розміщені на 2 сторінках.

Ключові слова: ZERO TRUST, AAA, КОРПОРАТИВНА КОМП'ЮТЕРНА МЕРЕЖА, КЛІЄНТ, АДМІНІСТРАТОР, АУТЕНТИФІКАЦІЯ.

ANNOTATION

The final qualification work of the II (two) academic (master's) level of higher education on the topic "Implementation of Zero Trust architecture for cyber protection of corporate networks" contains an analysis of theoretical solutions and practical technologies for further design of a system with implemented protection methods. A list of software and hardware solutions, targeted methods for implementing the Zero Trust model to ensure the proper level of security in corporate networks has been created;

The purpose of the final qualification work is to study in detail and identify the selection and comparison of methods, technologies and design aspects using ready-made free solutions and methods for implementing the Zero Trust model in corporate networks;

The volume of the explanatory note is 65 pages, 45 figures, 5 tables. The list of sources used contains 22 names, which are placed on 2 pages.

Keywords: ZERO TRUST, AAA, CORPORATE COMPUTER NETWORK, CLIENT, ADMINISTRATOR, AUTHENTICATION.

ВСТУП.....	9
 РОЗДІЛ 1 АНАЛІЗ ОБЛАСТІ ЗАСТОСУВАННЯ ТА ОБГРУНТУВАННЯ	
АКТУАЛЬНОСТІ ТЕМИ В УМОВАХ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ..	11
1.1 Актуальність теми роботи.....	11
1.2 Основні принципи методології Zero Trust	14
1.3 Політика безпеки, забезпечення дотримання політики безпеки та цілі Zero Trust	17
1.4 Постановка завдання дослідження	21
Висновки до розділу 1	23
 РОЗДІЛ 2 АНАЛІЗ ІНСТРУМЕНТІВ ВПРОВАДЖЕННЯ В КОРПОРАТИВНУ	
МЕРЕЖУ РІШЕННЯ ZERO TRUST.....	24
2.1 Впровадження архітектури Zero Trust	24
2.2 Застосування Google BeyondCorp як модель безпеки	28
2.3 Використання протоколу RADIUS.....	31
2.4 Привілейований доступ керування (PAM) як основа моделі Zero Trust	33
Висновки з розділу 2	37
 РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВПРОВАДЖЕННЯ ZERO TRUST	
АРХІТЕКТУРИ	38
3.1 Налаштування мережі впровадження правил Zero Trust.	38
3.2 Послідовність додавання нових користувачів у систему.....	42
Висновки з розділу 3	54
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	57
ДОДАТКИ	60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ZT – Zero Trust

НД – нульова довіра

ПЗ – програмне забезпечення

КТ – комп'ютерні технології

ПК – персональний комп'ютер

LAN – local area network

ОС – операційна система

PAM – Privileged Access Management

AAA – (Authentication, Authorization, and Accounting)

DLP – Data Loss Prevention

NGFW – Next-Generation Firewall

SAML – Security Assertion Markup Language

SSO – Single Sign-On

RADIUS – Remote Authentication Dial-In User Service

ВСТУП

Актуальність теми. В умовах стрімкого зростання масштабів розподілених систем, хмарних сервісів та віддаленої роботи старі моделі безпеки виявляються неефективними.

Вони не здатні запобігти загрозам, що виникають всередині мережі, таким як горизонтальне переміщення, а також не забезпечують належний захист API, мікросервісів та машинно-машинної взаємодії. Модель Zero Trust (ZTA) формує новий підхід до захисту, виходячи з принципу «нікому не довіряй без перевірки». Це означає обов'язкову аутентифікацію, авторизацію та безперервну перевірку кожного суб'єкта доступу до ресурсів, незалежно від їх розташування та приналежності.

Підтримка мікросегментації, принципу найменших привілеїв, адаптивного контролю доступу та глибокого моніторингу знижує ризики проникнення та прискорює виявлення загроз. Особливо гостро ця проблема проявляється в backend-інфраструктурі, де взаємодіють безліч сервісів, баз даних, API і CI/CD-конвеєрів. Тут уразливості можуть виникати не тільки із зовнішніх кордонів, але й усередині мережі, через скомпрометовані сервісні облікові записи або небезпечні з'єднання між мікросервісами.

Таким чином, аналіз та впровадження Zero Trust архітектури на рівні backend-інфраструктури є сьогоdnішнім імперативним завданням у забезпеченні кібербезпеки складних та динамічних ІТ-середовищ.

Метою кваліфікаційної роботи є реалізація методів та рішень Zero Trust архітектури для кіберзахисту корпоративних мереж. Робота націлена на створення продуманого практично реалізованого підходу впровадження та забезпечення безпеки в корпоративних мережах, де використовується велика кількість користувачів.

Об'єктом дослідження є процес впровадження, побудови та реалізації методів та рішень Zero Trust архітектури для кіберзахисту корпоративних мереж.

Предметом дослідження є доступні технології моделі Zero Trust для налаштування системи AAA, а саме протокол RADIUS, привілейований доступ керування RAM, перебудова процесів DevOps та SecOps та застосування готових рішень Google BeyondCorp як модель безпеки.

Задля досягнення поставленої мети необхідно провести аналіз матеріально-технічного підходу:

- Визначити ключеві об'єкти безпеки моделі Zero Trust;
- Проаналізувати ринок безкоштовних відкритих рішень;
- Підібрати рішення політик безпеки;
- Проектувати та налаштувати віртуальні комп'ютерні середовища;
- Визначити можливі моделі загроз;
- Поєднати всі компоненти середовища в одну єдину корпоративну систему.

У процесі виконання кваліфікаційної роботи було розроблено проект впровадження, побудови та реалізації методів та рішень Zero Trust архітектури для кіберзахисту корпоративних мереж.

РОЗДІЛ 1 АНАЛІЗ ОБЛАСТІ ЗАСТОСУВАННЯ ТА ОБГРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ В УМОВАХ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Актуальність теми роботи

В умовах стрімкого зростання масштабів розподілених систем, хмарних сервісів та віддаленої роботи старі моделі безпеки виявляються неефективними.

Сучасні комп'ютерні мережі займають перше місце в інфраструктурі кібербезпеки та інформаційних-технологіях, оскільки вони є засобом, за допомогою якого розподілені компоненти з'єднуються та взаємодіють один з одним. Саме з цієї причини головний принцип вимагає контролю та реєстрації мережевого трафіку. Системи Zero Trust – є актуальним рішенням забезпечення безпеки сучасних складних комп'ютерних систем. Зазвичай такі системи складаються з розподіленого набору вузлів забезпечення мережевого контролю. Важливо зазначити, що системи Zero Trust повномасштабно перевіряти та реєструвати метадані мережевого трафіку, але бути максимально логічні при перевірці вмісту мережевого трафіку через втрати обчислювальної потужності обладнання.

Отже, Zero Trust (нульова довіра) – це цілісна модель захисту мережевих, прикладних та інформаційних ресурсів, з забезпеченням моделі політики з контролем доступу. Досить велика кількість підприємства мають набір ІТ-інструментів та інструментів безпеки, встановлених у своїх середовищах, але нульова довіра (Zero Trust) вимагає, щоб вони розглядалися та працювали цілісно, з ідентичністю в центрі уваги, та з можливістю застосовувати політики, залежні від атрибутів та контексту, в усьомусередовищі.

У 2010 році аналітик незалежної компанії «Forrester» Джон Кіндерваг запровадив термін «Zero Trust» (Нульова Довіра) в офіційному документі «No More Chewy Centers: Introducing The Zero Trust Model Of Information Security». У документі були зібрані ідеї, які обговорювалися в галузі.

Компанія Forrester випустила свою початкову модель Zero Trust. пропонує всебічну модель, яка ставить дані в центр уваги, як показано на рисунку 1.1. Це відображає переконання Forrester, що вибухове зростання обсягів даних як у локальних, так і в хмарних середовищах є центром того, що потрібно захистити. Навколишні елементи — робочі навантаження, мережі, пристрої та люди — є каналами до даних і тому також потребують захисту.

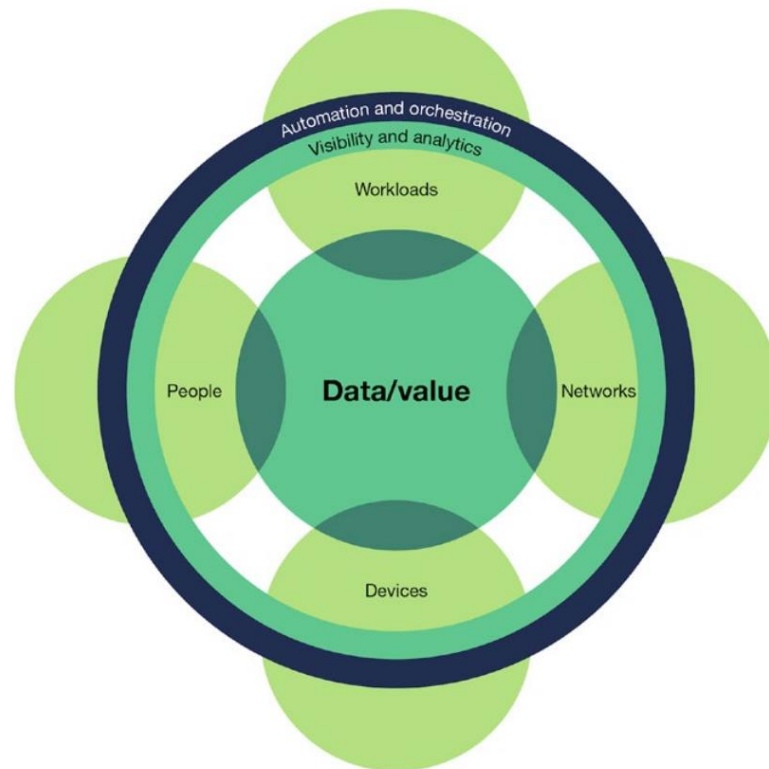


Рисунок 1.1 – Концепція моделі Zero Trust від компанії Forrester.

Дані є центром моделі ZT, вони включають класифікацію, сегментацію та захист даних, що є основою вимог до підтримки моделі нульової довіри. Крім того, запобігання втраті даних (DLP) має бути частиною архітектури нульової довіри та пов'язане з моделлю політики з можливістю застосовувати політики контекстного доступу, де це можливо.

Модель ZT в першу чергу орієнтована на сегментацію мережі — як з точки зору користувача, так і сервера — для забезпечення кращої безпеки на основі атрибутів, орієнтованих на ідентифікацію. Важливо перевірити, що підприємства мають багато існуючих компонентів, які створюють цілісну

інфраструктуру мережевої безпеки. Наприклад брандмауери наступного покоління (NGFW), брандмауери веб-додатків (WAF), рішення для контролю доступу до мережі (NAC) та системи захисту від вторгнень (IPS).

Ролеві та атрибутні системи керування доступом – це зрозумілі моделі в рамках IAM, а Zero Trust дозволяє використовувати їх ефективніше в інфраструктурі підприємства. Багатофакторна автентифікація (MFA) – це ще одна вимога, яка є важливою для підтримки Zero Trust. Нарешті, єдиний вхід (SSO) – з використанням сучасних відкритих стандартів, таких як SAML – є ще одним ключовим елементом у рамках «персонального» елементу. Як ви побачите в цій книзі, ми є рішучими прихильниками того, щоб зробити ідентифікацію центральною в кожному середовищі Zero Trust.

Також, робочі навантаження, згідно з визначенням Forrester, складаються з компонентів, що утворюють логічні функції, що керують інформаційно-комп'ютерною системою орієнтовану на клієнтів, так і в внутрішніх бізнес-користувачів — контейнерів, додатків, інфраструктурних процесів і т.д. Zero Trust (Нульова довіра) вимагає керування доступом до робочих навантажень на основі метаданих, які послідовно застосовується в гібридних середовищах.

Вони не здатні запобігти загрозам, що виникають всередині мережі, таким як горизонтальне переміщення, а також не забезпечують належний захист API, мікросервісів та машинно-машинної взаємодії. Модель Zero Trust (ZTA) формує новий підхід до захисту, виходячи з принципу «нікому не довіряй без перевірки». Це означає обов'язкову аутентифікацію, авторизацію та постійну перевірку кожного суб'єкта доступу до ресурсів, незалежно від їх розташування та приналежності.

Підтримка мікросегментації, принципу найменших привілеїв, адаптивного контролю доступу та глибокого моніторингу знижує ризики проникнення та прискорює виявлення загроз. Особливо гостро ця проблема

проявляється в backend-інфраструктурі, де взаємодіють безліч сервісів, баз даних, API і CI/CD-конвеєрів. Тут уразливості можуть виникати не тільки із зовнішніх кордонів, але й усередині мережі, через скомпрометовані сервісні облікові записи або небезпечні з'єднання між мікросервісами.

Без прозорості політики контролю та сегментації комп'ютерна мережа залишається відкритим полігоном без захисту. Таким чином, аналіз та впровадження Zero Trust архітектури на мережних рівнях є сьогоdnішнім імперативним завданням у забезпеченні кібербезпеки складних та динамічних ІТ-середовищ.

1.2 Основні принципи методології Zero Trust

Існують три основні принципи нульової довіри (ZT), які загально визнані та важливі. Початкова ідея принципів взята за основу зі статті «No More Chewy Centers», опублікованій компанією Forrester, що підтверджує їх доцільність при впровадженні ідей Zero Trust архітектури. На додаток до цих основних принципів, також додаються принципи, описані в документі NIST «Zero Trust Architecture». Що надає розширену інтерпретацію з точки зору сучасної галузі.

Головним принципом – є забезпечення безпечного доступу до всіх ресурсів, незалежно від місцезнаходження в системі. Це коротке твердження, яке охоплює кілька понять. По-перше, воно вимагає, щоб усі ресурси були включені до рішення Zero Trust. Також зобов'язує організації застосовувати цілісний підхід до Zero Trust та усунення ізольованих структур та бар'єрів, які завжди існують між інструментами безпеки та командами.

Другий принцип вимагає, щоб нульова довіра забезпечувала безпечний доступ ідентифікаторів до всіх ресурсів (даних, програм, робочих станцій, серверів) — незалежно від місцезнаходження ідентифікатора та незалежно від технології об'єкта інформаційно-комп'ютерної системи, до якого здійснюється доступ. Фактично цей принцип вимагає ліквідації традиційного корпоративного периметра та його заміни альтернативним, розширеним,

способом адміністрування. Це також означає, що мережевий трафік має бути зашифрований не лише під час його проходження через вразливі області ІКС. У такому разі, доступ має підлягати обов'язковій перевірці.

У разі застосування стратегії найменших привілеїв – необхідно забезпечити контроль доступу. Концепція мінімально привілейованого доступу до ресурсів не нова. Але дану концепцію було складно масштабно застосовувати до запровадження в комп'ютерних мережах старого типу. Особливо мереж які застосовували технологію DSL.

Найменшими привілеями необхідно керувати в різних місцях та різними типами ресурсів, як на мережевому, так і на прикладному рівні, використовуючи AAA. Історично склалося так, що рішення безпеки не могли подолати розрив між безпекою на рівні мережі та програми. Традиційно користувачі ПК отримували широкий доступ до мереж, а програми отримували лише контроль доступу з автентифікацією. Будь-хто в компанії міг отримати доступ до сторінки входу на фінансовому сервері. Але лише користувачі фінансового розділу мали облікові записи та паролі. Цього не достатньо для запеспечення достатнього рівню безпеки. Існує велика кількість відомих і критичних вразливостей, які не потребують автентифікації та можуть бути використані віддалено.

Наприклад, можливість надсилати мережеві пакети до системи є привілеєм. Якщо користувачі не мають права доступу до певної служби (наприклад, не мають облікових даних для SSH-підключення до сервера або для автентифікації у VPN), вони не зможуть мати можливість підключатися до цієї служби на мережевому рівні.

Перевірка та реєстрація всього трафіку. Комп'ютерні мережі є головним місцем в інфраструктурі безпеки та ІТ, оскільки вони є засобом розподілення компонентів з'єднання та спілкуються користувачів (обладнання).

Важливо зазначити, що системи нульової довіри повинні широко перевіряти та реєструвати метадані мережевого трафіку, але бути більш розсудливими при перевірці вмісту мережевого трафіку через витрати на обробку та зберігання.

З метою виконання умов впровадження технології Zero Trust, до інформації про мережевий трафік має бути додано ідентифікаційні дані, контекст пристроїв. Та в подальшому передано в брандмауери наступного покоління, інструменти мережевого моніторингу та SIEM, щоб покращити здатність приймання рішень щодо виявлення, оповіщення та реагування. А також регулярна підтримка засобів реагування на інциденти та інші оповіщення системи.

На рисунку 1.1 нижче представлена схема, що демонструє основні області контролю в концепції Zero Trust.

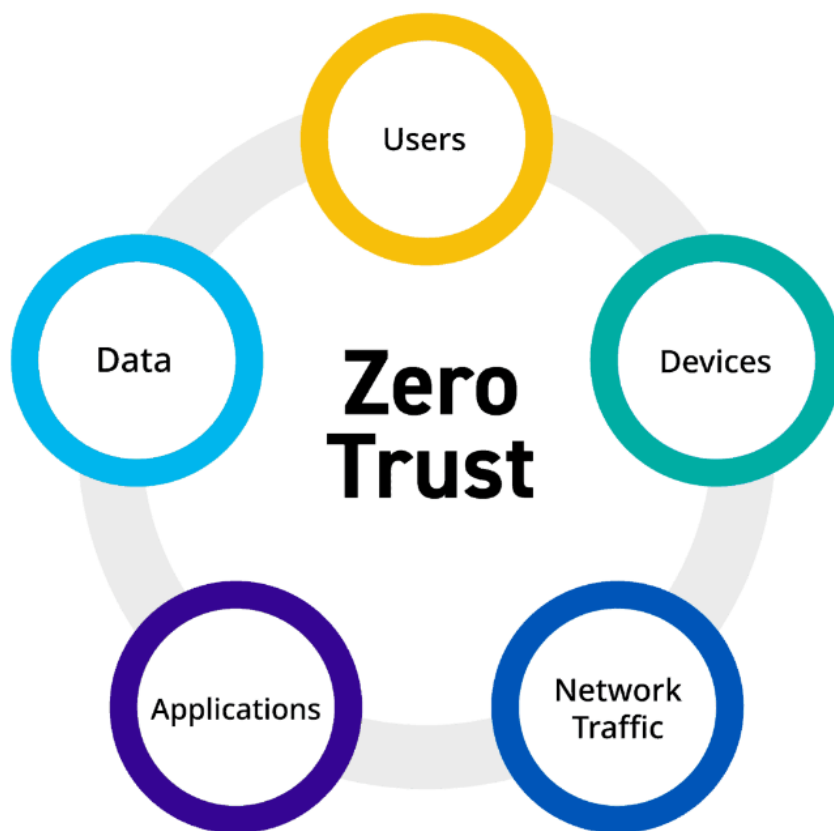


Рисунок 1.2 – Ключові компоненти Zero Trust архітектури.

NIST виділяє сім основоположних принципів:

1. Devices – кожен ресурс розглядається як потенційно незахищений.
2. Data – всі комунікації шифруються.
3. Applications – доступ надається на основі сесії динамічного контролю.
4. Users – політики доступу формуються з урахуванням поведінкових і контекстних факторів.
5. Network Traffic – регулярний моніторинг цілісності та стану активів.

1.3 Політика безпеки, забезпечення дотримання політики безпеки та цілі Zero Trust

Управління ідентифікацією та доступом (IAM) – це широка галузь інформаційної безпеки, що охоплює як технічні, так і бізнес-процесні аспекти контролю доступу шляхом надання правильного доступу в потрібний час потрібній особі. У багатьох відношеннях ідентифікація – та достатньо добре керована програма управління ідентифікацією – є ключем до успіху з програмою Zero Trust. Zero Trust в своїй основі забезпечує орієнтований на ідентифікацію підхід до безпеки, і тому розуміння та управління ідентифікацією є неймовірно важливим фактором у будь-якій програмі Zero Trust. І все ж організації не повинні і не можуть вимагати від своїх команд з ідентифікації та систем досконалості, перш ніж розпочати налаштування Zero Trust.

Системи управління ідентифікацією повинні служити авторитетним джерелом інформації про ідентифікаційні дані (фізичні та нефізичні сутності) та використовуватися як основна система для багатьох технічних інтеграцій, а також бізнес-процесів. Це нелегко — сучасні підприємства є складними та можуть не мати єдиної централізованої системи ідентифікації. Це нормально, і це не слід розглядати як перешкоду для впровадження «Нульової довіри». Фактично, «Нульова довіра», за своєю природою як система накладання, може допомогти подолати розриви між кількома системами ідентифікації.

Кожна система управління ідентифікацією відрізняється, що базується на унікальній комбінації кожного підприємства та обраного ним набору технологій, системи управління ідентифікацією містять спільні елементи, зображені на рисунку 1.3.

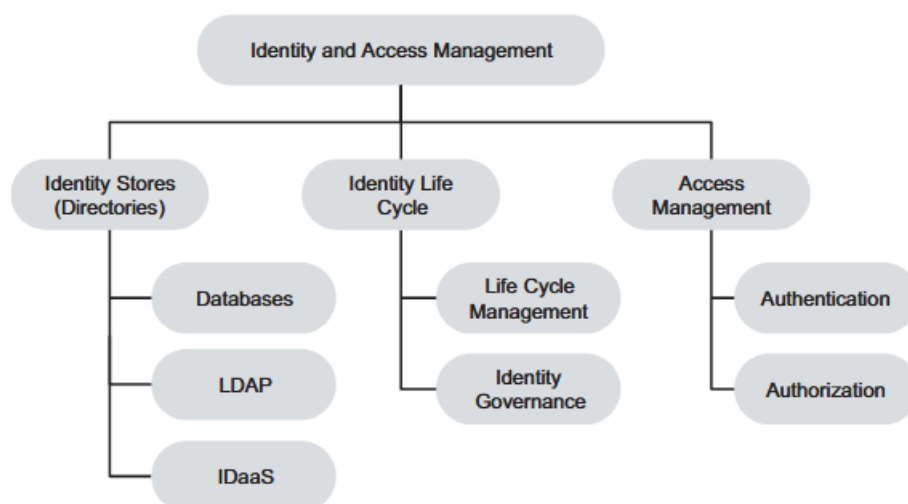


Рисунок 1.3 – Дерево структури IAM (Identity and Access Management).

Політики є основою Zero Trust — зрештою, її основними архітектурними компонентами є точки прийняття рішень щодо політик та точки виконання політик. Термін «політика» в англійській мові, звичайно, сильно перевантажений значеннями на багатьох різних рівнях. У нашому світі Zero Trust політики — це структури, створені організаціями для визначення того, яким ідентифікаторам дозволено отримувати доступ до яких ресурсів, за яких обставин.

В середовищі Zero Trust доступ можна отримати лише шляхом оцінки та призначення політики ідентифікатору, і цей доступ може бути забезпечений на рівні мережі або програми. Фактичні технічні засоби, політики яких визначаються та застосовуються, залежатимуть від продукту та впровадження, але концепції та компоненти є універсальними та мають бути поширеними в будь-якій системі Zero Trust. У документі NIST Zero Trust зазначається, що «політика – це набір правил доступу на основі атрибутів, які організація призначає суб’єкту, активу даних або програмі», і один з основних принципів

NIST полягає в тому, що доступ до ресурсів визначається динамічною політикою, включаючи спостережуваний стан ідентифікації клієнта, програми/сервісу та активу, що запитує, і може включати інші поведінкові та екологічні атрибути».

Отже, з робочого визначення Zero Trust повинна забезпечувати динамічне забезпечення виконання політик безпеки розширюючи деякі концепції в рамках системи нульової довіри NIST. Системи нульової довіри можуть бути майже нескінченними за широтою та глибиною, і важливо, щоб ви мали чітке уявлення про те, що слід і не слід включати, і що доцільно включити до моделі політики. Це необхідно для того, щоб ви могли почати визначати архітектуру та життєвий цикл політики безпеки, а також відповідний набір процесів та компонентів управління (таблиця 1.1).

Таблиця 1.1

Компоненти моделі політики Zero Trust (нульової довіри)

Компонент	Опис	Ключова вимога Zero Trust
Subject (Суб'єкт)	Сутності, які ініціюють дії (наприклад, користувачі або пристрої).	Суб'єкти мають бути автентифікованими ідентичностями.
Action (Дія)	Активність, яку виконує суб'єкт.	Повинна містити мережевий або прикладний компонент (або обидва).
Target (Ціль)	Об'єкт (ресурс), над яким виконується дія.	Бажано вузьке, а не широке визначення об'єкта.

Компонент	Опис	Ключова вимога Zero Trust
Condition (Умова)	Обставини, за яких суб'єкту дозволено виконати дію над ціллю.	Повинна ґрунтуватися на декількох типах атрибутів: суб'єкта, середовища та цілі.

Критерії суб'єкта використовуються для визначення набору ідентифікаційних осіб (суб'єктів), до яких застосовується ця політика. Суб'єкти, які можуть бути людьми або неособистісними об'єктами (NPE), повинні бути автентифікованими об'єктами та повинні існувати в деякій системі керування ідентифікацією. Суб'єкти мають багато атрибутів, пов'язаних з ними, отриманих з таких джерел, як їхня система автентифікації ідентифікації, профіль пристрої та мережева або геолокаційна інформація. Дані атрибути використовуються в критеріях суб'єкта для визначення того, чи слід призначити політику певній ідентичності. Навіть на основі цього короткого вступу має бути зрозуміло, що модель політики нульової довіри забезпечує контроль доступу на основі атрибутів (ABAC) багатьма способами.

Дії визначають фактичну активність, яку дана політика дозволяє суб'єкту виконувати. Вона повинна містити дію мережі або програми, і може містити обидві.

Цілі – це система або компонент, на які здійснюється дія. Вони можуть бути визначені статично (наприклад, з фіксованим ім'ям хоста або IP-адресою) або динамічно за допомогою атрибутів, таких як мітки чи теги гіпервізора або IaaS, які вирішуються під час виконання. Вони можуть бути вузько визначені (наприклад, окрема служба, що працює на одному сервері) або більш широко визначені (наприклад, доступ до класу серверів або підмережі). Умови диктують, коли суб'єкту дозволено фактично виконувати дію на цілі, і можуть включати широкий спектр обставин.

1.4 Постановка завдання дослідження

Метою кваліфікаційної роботи є впровадження методів та рішень Zero Trust архітектури для кіберзахисту корпоративних мереж з використанням безкоштовних відкритих рішень. Проект буде створено на базі віртуального програмного-апаратного середовища. В якому буде створена симуляція корпоративної мережі на основі готових рішень.

Побудова симульованої корпоративної мережі буде включати в собі наступні кроки:

- розробка віртуальної комп'ютерної корпоративної мережі за допомогою емулятора GNS3 та внутрішніми функціями програмного застосунку OracleVirtualBox;
- проектування топології мережі;
- налаштування та перевірка зв'язків з обладнанням;
- підготовка та впровадження Zero Trust моделі в мережу;
- розробка та налаштування кластеру, що імітуватиме контроль доступу в мережі;
- спроба здійснення несанкціонованого доступу;
- визначення та оцінка застосування правил моделі мережі Zero Trust, а також визначення ефективності можливостей використання у сучасних корпоративних мережах.

Дані принципи повинні поширюватися на такі області, як ідентифікація, пристрої, мережа, додатки, дані, з акцентом на спостережливість, автоматизацію та управління. Модель дозволяє організації поступово переходити від периметрового захисту до архітектури Zero Trust, розподіляючи витрати та зміни в часі.

У таблиці 1.2 представлені ключові особливості сучасної інфраструктури з зазначенням відповідних вимог до їх захисту в рамках моделі

Zero Trust. Кожна категорія інфраструктури супроводжується конкретними вразливостями та заходами захисту, заснованими на принципах

Таблиця 1.2

Порівняльний аналіз особливостей інфраструктури та вимог до її безпеки в контексті Zero Trust

Компонент інфраструктури	Ключові особливості	Вразливості та загрози	Zero Trust вимоги та заходи безпеки
Мікросервіси	Децентралізовані, масштабовані сервіси, які працюють незалежно	Lateral movement при компрометації одного сервісу, слабка авторизація між сервісами	Microsegmentation, сервісна автентифікація (mTLS), суворі політики доступу між сервісами
API-інтерфейси	Зовнішні та внутрішні точки входу в логіку застосунку	Атаки типу injection, DoS, несанкціонований доступ	API gateway з авторизацією, аудит, rate limiting, контроль вмісту запитів
CI/CD пайплайн	Автоматизовані процеси тестування	Supply chain атаки, інжекція шкідливого коду, неправомірний доступ до секретів	Підписані збірки, Zero Trust до агентів, управління доступом до секретів через Vault
Бази даних	Центри зберігання чутливих і операційних даних	Витік даних, не-санкціонований SQL-доступ, слабе шифрування	Контроль доступу на основі ролей і контексту (ABAC), шифрування даних у стані спокою та в русі, постійний аудит
Компонент backend-інфраструктури	Ключові особливості	Уразливості та загрози	Zero Trust вимоги та заходи безпеки
Черги повідомлень (Kafka, RabbitMQ)	Асинхронна взаємодія сервісів, високе навантаження	Несанкціонована підписка або публікація, витік метаданих	Аутентифікація клієнтів, TLS, суворі ACL та контроль тем
Внутрішні мережі/Service Mesh	Підмережі, що з'єднують мікросервіси, включаючи east-west трафік	Відсутність шифрування, недостатня сегментація	Використання сервісної сітки (наприклад, Istio) впровадження політики безпеки, end-to-end шифрування

DevOps-оточення	Високий рівень прав у розробників та автоматизації	Компрометація секретів, помилка конфігурації, зловживання правами	Принцип найменших привілеїв (PoLP), моніторинг дій, управління доступом на основі атрибутів
-----------------	--	---	---

Висновки до розділу 1

У ході підготовки було проаналізовано актуальні документи компанії «Forrester». А саме документ «No More Chewy Centers: Introducing The Zero Trust Model Of Information Security», статтю «No More Chewy Centers» та документ NIST «Zero Trust Architecture». У результаті чого зумів отримати розширену інтерпретацію впровадження технології Zero Trust (Нульової довіри) з точки зору сучасної галузі інформаційних технологій.

У результаті аналізу специфіки моделі мережі Zero Trust було сформоване уявлення про основні принципи роботи, умови безпеки, головні політики доступу.

Встановлено, що доступ до ресурсів визначається динамічною політикою, включаючи спостережуваний стан ідентифікації клієнта, програми/сервісу та активного середовища і може включати інші атрибути доступу.

Визначено необхідність впровадження політики Zero Trust в сучасних корпоративних мережах з подальшим забезпеченням систематизованого адміністрування мережі.

РОЗДІЛ 2 АНАЛІЗ ІНСТРУМЕНТІВ ВПРОВАДЖЕННЯ В КОРПОРАТИВНУ МЕРЕЖУ РІШЕННЯ ZERO TRUST

2.1 Впровадження архітектури Zero Trust

Впровадження Zero Trust архітектури в backend-інфраструктуру є одним з найбільш актуальних завдань сучасної кібербезпеки. В умовах, коли мікросервісні системи, API, CI/CD-конвеєри та хмарні середовища стають стандартом, традиційні моделі периметрової безпеки вже не можуть забезпечувати належний рівень захисту.

Zero Trust пропонує інший підхід: кожний компонент інфраструктури вважається потенційно ненадійним, незалежно від його розташування в мережі, і вимагає перевірки при кожному зверненні. Одним з ключових інструментів реалізації Zero Trust в backend є сервісна сітка – програмний прошарок, що забезпечує безпечну маршрутизацію, шифрування та авторизацію трафіку між мікросервісами. Такі рішення, як Istio, Linkerd та Envoy, дозволяють впровадити обов'язкове взаємне TLS (mTLS) для всього east-west трафіку всередині кластера, забезпечуючи конфіденційність та перевірку автентичності всіх підключень.

Крім того, сервісна сітка забезпечує централізовану реалізацію політик безпеки, відмовостійкість та трасування запитів, що відповідає принципам Zero Trust. Для підтвердження ідентичності сервісів використовується SPIFFE/SPIRE – система управління машинною ідентичністю, розроблена для автоматичної видачі короткоживучих X.509-сертифікатів. Вона дозволяє кожному мікросервісу отримати криптографічно перевіряєму унікальну ідентичність та взаємодіяти лише з перевіреними сервісами. Це критично важливо для побудови Zero Trust-середовищ, особливо в хмарних та гібридних середовищах, де традиційні методи управління доступом незастосовні. На додаток до сервісної сітки та SPIRE необхідно реалізувати динамічні політики авторизації. Одним з рішень в цій області є Open Policy Agent (OPA) – інструмент, який дозволяє централізовано управляти доступом до ресурсів на

основі атрибутів 60 (ABAC).

Це означає, що кожне звернення до сервісу аналізується за безліччю параметрів: ідентичність користувача, пристрій, геолокація, контекст сесії, рівень ризику. Такий підхід дозволяє реалізувати принцип мінімальних привілеїв і запобігає несанкціонованому доступу навіть при компрометації окремих компонентів.

Особливу увагу в Zero Trust для backend також приділяється захисту CI/CD пайплайнів і секретів інфраструктури. Впровадження рішень на кшталт HashiCorpVault дозволяє організувати безпечне зберігання ключів, токенів, паролів і сертифікатів. Vault забезпечує суворий контроль доступу, веде аудит всіх операцій, а також може динамічно видавати секрети і відкликати їх при необхідності. Це мінімізує ймовірність витоків і полегшує дотримання комплаєнсу.

Таблиця 1.3 ілюструє, які компоненти backend-інфраструктури потребують захисту і як саме реалізується Zero Trust на кожному рівні.

Таблиця 1.3

Реалізація Zero Trust в компонентах backend-інфраструктури

Компонент	Загрози та вразливості	Механізми Zero Trust
Мікросервіси	Lateral movement, підміна трафіку	mTLS, Istio, SPIRE, microsegmentation
API	Ін'єкції, несанкціонований доступ	API Gateway, OPA, RBAC/ABAC
CI/CD пайплайн	Supply chain атаки, вразливі образи	Підпис збірок, Vault, GitOps-перевірки
Секрети та конфігурації	Витік конфіденційної інформації	HashiCorp Vault, audit, dynamic secrets
Бази даних	Витік даних, надмірні привілеї	Шифрування, токенізація, політичний доступ
Внутрішній трафік	Перехоплення, DNS spoofing, ARP spoofing	Сервісна сітка, mutual TLS, ACL на рівні мережі

Також важливе впровадження моніторингу та логування в реальному часі. У моделі Zero Trust невід'ємною частиною є системи observ-ability – такі як Prometheus, Grafana, Fluentd, OpenTelemetry. Вони

дозволяють відстежувати поведінку кожного компонента backend-інфраструктури, виявляти відхилення від норми та оперативно реагувати на можливі атаки. Саме постійний аналіз контексту дає можливість автоматичної адаптації політик безпеки.

Таблиця 1.4 містить огляд найбільш поширених і надійних інструментів і технологій, що застосовуються для побудови Zero Trust в backend-середовищі. Вказані основні функції кожного рішення, його роль в архітектурі та область застосування. Всі технології визнані галузевими стандартами і використовуються в реальних корпоративних інфраструктурах для забезпечення мікросегментації, шифрування, ідентифікації, авторизації, управління секретами і спостережуваності.

Таблиця 1.4

Ключові інструменти та технології для реалізації Zero Trust архітектури в backend-інфраструктурі

Інструмент / технологія	Призначення в Zero Trust архітектурі	Основні функції та особливості
Istio (Service Mesh)	Забезпечення безпечного мережевого зв'язку між мікросервісами	mTLS, авторизація, маршрутизація, аудит трафіку, політики доступу, телеметрія ступа, телеметрія
Envoy Proxy	Мережевий проксі для сервісної сітки та API	Інспекція та контроль мережевого трафіку, впровадження політик, підтримка SPIFFE
SPIFFE / SPIRE	Управління машинною ідентичністю	Автоматична видача ідентифікаторів та X.509-сертифікатів та X.509-сертифікатів для сервісів
Open Policy Agent (OPA)	Центральне управління авторизацією	Реалізація політик доступу на основі атрибутів (ABAC), інтеграція з Kubernetes, Envoy, Istio
HashiCorp Vault	Управління секретами та доступом до конфіденційних даних	Динамічна видача токенів і сертифікатів, контроль доступу, аудит, інтеграція з CI/CD
Kubernetes Network Policies	Сегментація трафіку між подами/сервісами в кластері	Реалізація deny-by-default, контроль east-west трафіку
API Gateway (Kong, Ambassador, Istio Gateway)	Контроль вхідного трафіку до API	Rate-limiting, перевірка токенів, маршрутизація, авторизація, логування
Prometheus + Grafana	Моніторинг та візуалізація стану інфраструктури	Збір метрик, алерти, дашборди, телеметрія компонентів Zero Trust

Fluentd / Loki / ELK Stack	Логування подій, інцидентів	Централізований збір логів, аналіз аномалій, передача даних в SIEM
Cert-Manager	Автоматизація управління TLS-сертифікатами	Інтеграція з SPIRE/Vault, підтримка ACME/Let's Encrypt, Kubernetes-native

Впровадження Zero Trust архітектури в backend-інфраструктуру пов'язане з рядом об'єктивних труднощів, обумовлених як технічними, так і організаційними факторами:

1. Складність інтеграції з існуючою архітектурою – особливо в монолітних або гібридних системах.
2. Зростання витрат на впровадження нових інструментів (service mesh, системи авторизації, observability).
3. Нестача кваліфікованих фахівців, здатних грамотно спроектувати та підтримувати Zero Trust.
4. Опір всередині команд – зміна парадигми безпеки вимагає навчання та перебудови процесів DevOps та SecOps.

Продуктивні накладні витрати – шифрування трафіку, постійна перевірка доступу можуть знижувати загальну продуктивність систем. Перспективи розвитку Zero Trust архітектури в backend-інфраструктурі пов'язані з автоматизацією управління доступом та адаптацією до нових ІТ-реалій. Одним з ключових напрямків стає використання машинного навчання та поведінкового аналізу для динамічної оцінки ризиків та автоматичного регулювання прав доступу. Це дозволить швидше реагувати на аномалії та потенційні загрози без участі людини.

Zero Trust активно розвивається в сторону глибокої інтеграції з хмарними та edge-середовищами, включаючи IoT-пристрої. Це вимагає розширення механізмів контролю ідентичності, шифрування і сегментації в розподілених середовищах. Велика увага приділяється стандартизації: документи NIST, CISA та архітектура BeyondCorp стають основою для одноманітного впровадження підходів у різних галузях. Платформи та

інструменти також змінюються: все більше рішень спочатку проектуються з підтримкою Zero Trust – сервісні сітки, Kubernetes, API-шлюзи та системи управління секретами тепер інтегрують контроль доступу та шифрування «з коробки». Особливе значення набуває управління машинною ідентичністю, оскільки саме сервіси, а не тільки користувачі, взаємодіють в масштабованих backend-системах. У сукупності дані заходи спрямовані на створення більш гнучкої, адаптивної та самокерованої моделі кіберзахисту.

2.2 Застосування Google BeyondCorp як модель безпеки

BeyondCorp – це внутрішня назва Google ініціативи з трансформації мережевої безпеки, є визначним досягненням, яке має значний вплив на галузь. Google створив свою внутрішню архітектуру безпеки та забезпечив контроль доступу до мережі для десятків тисяч користувачів, але й публічно задокументував це в серії USENIX.

Компанія Google створила та впровадила складну систему Zero Trust протягом кількох років у великих масштабах. За їх словами, вони створили «нову модель, яка відмовляється від привілейованої корпоративної мережі. Натомість доступ залежить виключно від пристрою та облікових даних користувача, незалежно від мережевого розташування користувача. Весь доступ до корпоративних ресурсів повністю автентифікований, повністю авторизований та зашифрований на основі стану пристрою та облікових даних користувача.

Кінцевим результатом є те, що корпоративна мережа не надає жодного невід’ємного доступу — весь доступ надається на основі ідентифікації, пристрою та автентифікації на основі надійних джерел даних про пристрої та ідентифікацію. Компанія Google змінили невід’ємні атрибути в мережі доступ до всіх внутрішніх програм здійснюється через систему BeyondCorp, незалежно від того, чи користувач знаходиться в офісі чи працює віддалено. Google також систематизували дозволи доступу лише з керованих пристроїв. Таким чином некеровані пристрої не мають доступу до внутрішніх програм та

секторів. Важливо також зазначити, що цей проект був зосереджений виключно на контролі доступу користувача до сервера, а не сервера до сервера.

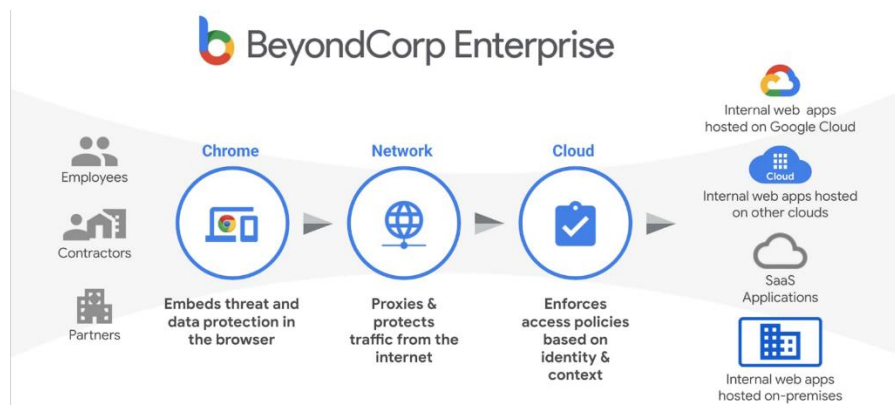


Рисунок 2.1 – Схема концепції Google BeyondCorp.

Такі складні рішення мають кілька наслідків для проектування корпоративних мереж. Зокрема, залежність від високоякісних даних про авторизацію користувачів. Тому для підтримки необхідно створювати складну базу даних інвентаризації пристроїв. Адміністратори корпоративної мережі повинні впроваджувати централізовану систему ідентифікації з SSO, яка видає короткочасні токени доступу. Така система управління ідентифікацією використовується для інформації про групи та ролі користувачів, надаючи всім рішення щодо політик ідентифікації. Система ідентифікації пов'язана з процесами управління персоналом, тому вона надійна та актуальна. Компоненти інфраструктури BeyondCorp показано на рисунку 2.2.

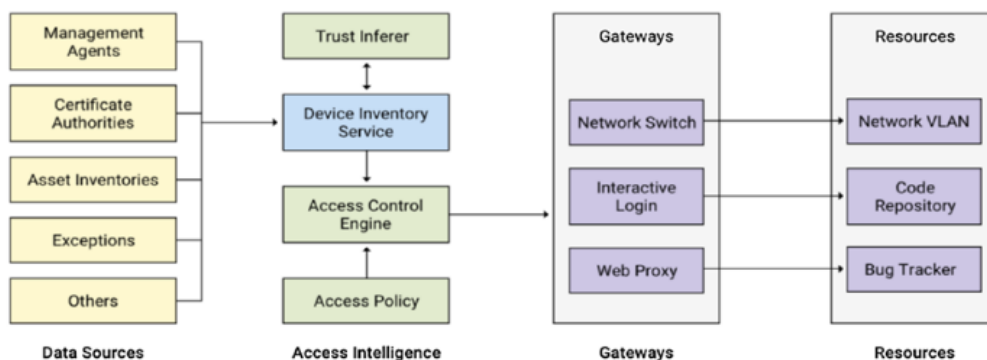


Рисунок 2.2 – Детальна схема роботи компонентів інфраструктури Google BeyondCorp.

Google застосував гібридний підхід до двох інших розділів. Фактично, їхні компоненти Access Intelligence утворюють точку прийняття рішень щодо політики (PDP), а інші шлюзи утворюють точку примусового виконання політики (PEP), проте механізм контролю доступу також технічно є частиною PEP. Інші компоненти мережі також можуть виступати в ролі PEP додатків, забезпечуючи повний доступ, залежно від додатка. Що детально продемонстровано на рисунку 2.3.

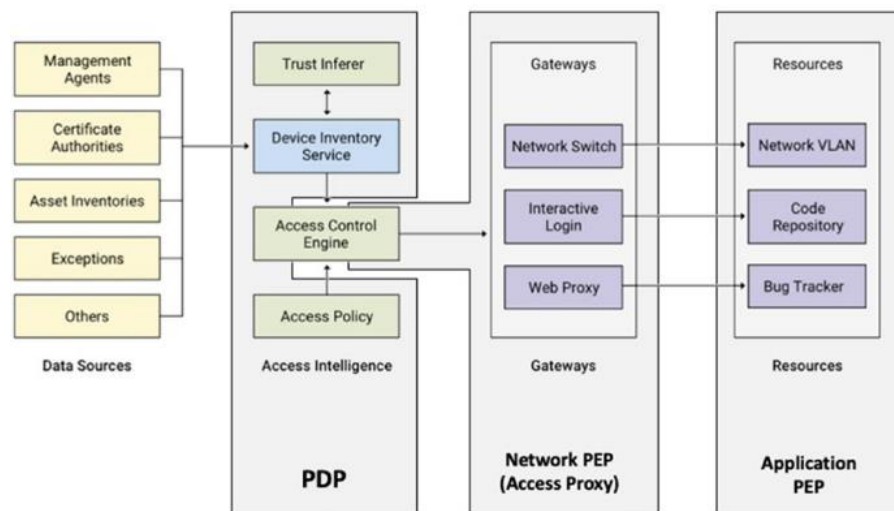


Рисунок 2.3 - Анотовані компоненти інфраструктури BeyondCorp.

Проксі-сервер доступу BeyondCorp (що складається зі шлюзів та частини механізму контролю доступу) діє як PEP, глобально доступний як для віддалених, так і для локальних користувачів. Система використовує кілька джерел даних для встановлення рівня довіри з динамічним застосуванням у проксі-сервері доступу.

Проксі-сервер доступу забезпечує дотримання правил на фронтенді, а авторизація застосовується на серверній частині (в межах дозволених ресурсів). Отже PEP програми пов'язані з політикою доступу або з джерелами даних, такими як IAM та іншими локальними системами контролю доступу до мережі використовують динамічне призначення VLAN на основі сертифікатів пристроїв. Щоб відрізнити керовані пристрої від некерованих. Це ефективний спосіб інтеграції NAC на базі 802.1x у мережу Zero Trust.

Google офіційно визнає, що BeyondCorp є складною та комплексною моделлю Zero Trust. Частково причиною цього був масштаб та складність, властиві організації Google.

BeyondCorp залишається доступною моделлю нульової довіри для використання якої розроблені для забезпечення цих переваг. Очікується, що Google продовжуватиме впроваджувати інновації та додавати нові можливості до власної комерційної пропозиції. Тому я розглядаю дану пропозицію як частину оцінки впровадження моделі Zero Trust.

2.3 Використання протоколу RADIUS

RADIUS – це ще один з AAA протоколів, що маштабно використовується. Це аббревіатура від Remote Authentication Dial-In User Service (служба віддаленої автентифікації користувачів з комутованим доступом). Спочатку він був створений для забезпечення автентифікації, авторизації та обліку (AAA), що по суті є попередниками сучасного управління ідентифікацією. Хоча термін AAA сьогодні не так широко використовується, ці теми явно є частиною сучасних основних ініціатив у сфері ідентифікації та безпеки.

RADIUS досі широко використовується на практиці. Як частина кількох офіційних стандартів IETF (RFC), він підтримується багатьма постачальниками та пропонує сумісність між компонентами різних постачальників. RADIUS має просту модель, за якою клієнт RADIUS (зазвичай називається «сервером доступу до мережі») взаємодіє безпосередньо із сервером RADIUS для виконання автентифікації від імені користувача. RADIUS повертатиме лише підтвердження або відхилення (можливо, після додаткового запиту, що активує MFA). RADIUS може використовуватися для надання контексту ідентифікації через розширення протоколу. Це продемонстровано на таблиці 2.1.

Контекст ідентифікації протоколу RADIUS

Version	Message Length
RPE	Command-Code
Vendor ID	
Hop-by-Hop Identifier	
End-to-End Identifier	
AVPs	

Передача інформації між користувачем RADIUS і на сервері автентифікуються за допомогою спільного секретного ключа, який ніколи не надсилається через мережу. Крім того, паролі користувачів системи RADIUS шифруються, щоб запобігти їх швидкому розшифровуванню зломисниками за допомогою перехоплення трафіку (рисунок 2.2).

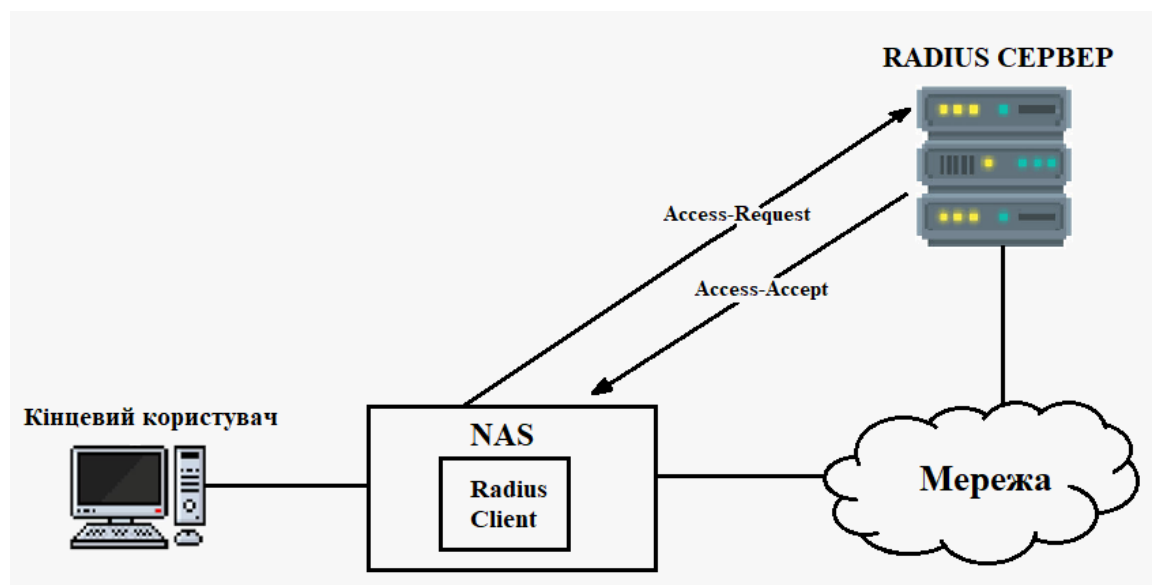


Рисунок 2.2 – Умовна схема роботи протоколу RADIUS в умовах застосування Zero Trust моделі.

Однак, RADIUS підтримує механізми автентифікації на основі стандартів, а не лише імені користувача та пароля, і його здатність робити це, продовжила термін служби даного протоколу. Фактично, багато сучасних постачальників ідентифікаційних протоколів пропонують API або шлюзи RADIUS, що дозволяє інтегрувати старіші програми або інфраструктуру в ці новіші платформи. Завдяки такому підходу старіші системи можуть використовувати новіші підходи до багатофакторної автентифікації або безпарольної автентифікації, які підтримуються на сучасних платформах ідентифікації, і які можуть бути викликані RADIUS.

2.4 Привілейований доступ керування (PAM) як основа моделі Zero Trust

Privileged Access Management (PAM) або Привілейований доступ керування – це частина системи індустрії IT-безпеки, яка контролює привілейованих користувачів (системних адміністраторів), які отримують доступ до систем або ресурсів, за допомогою набору функцій та процесів безпеки. PAM може бути використаний для контролю доступу до будь-якої системи, але зазвичай застосовується лише до важливих ресурсів, таких як контролери домену та виробничі сервери. Безпека Zero Trust, базується на передумові, що її слід використовувати для захисту всіх систем, але цінні системи зазвичай також захищені PAM. Що є розумним рішенням для корпоративних мереж Zero Trust.

Рішення PAM розвивалися та розширювалися разом із розвитком ринку та сьогодні пропонують функції, зосереджені на зберіганні паролів, обміні секретів та управлінні сесіями. Хоча PAM зазвичай автентифікує користувачів за допомогою постачальників корпоративної ідентифікації часто може використовувати членство в групах для контролю доступу, ми вважаємо, що має сенс класифікувати ці рішення як такі, що враховують ідентифікацію, а не як такі, що орієнтовані на ідентифікацію. Цю відмінність необхідно розуміти, оскільки рішення PAM може виглядати певним чином як система

Zero Trust, і воно може навіть надавати деякі можливості, подібні до PER, але не може вважатися рішенням Zero Trust саме по собі. Ми повернемося до цієї теми наприкінці цього розділу, але спочатку давайте розглянемо три основні функції, які зазвичай надаються PAM.

Рішення PAM розширені зберіганням та керуванням відносно користувачів до підтримки ширшого набору можливостей керування паролями. Паролі не обмежуються довжиною, вони можуть включати будь-який тип інформації, необхідної для прямого чи опосередкованого захисту систем.

Нижче наведено приклади елементів (рисунок 2.3), відмінних від паролів, які можуть зберігатися в рішенні для обміну в мережі:

- Хеші
- Сертифікати
- Інформація про орендаря хмари
- Ключі API
- Інформація про сховище бази даних
- Персональна інформація
- Інформація про SSH-з'єднання

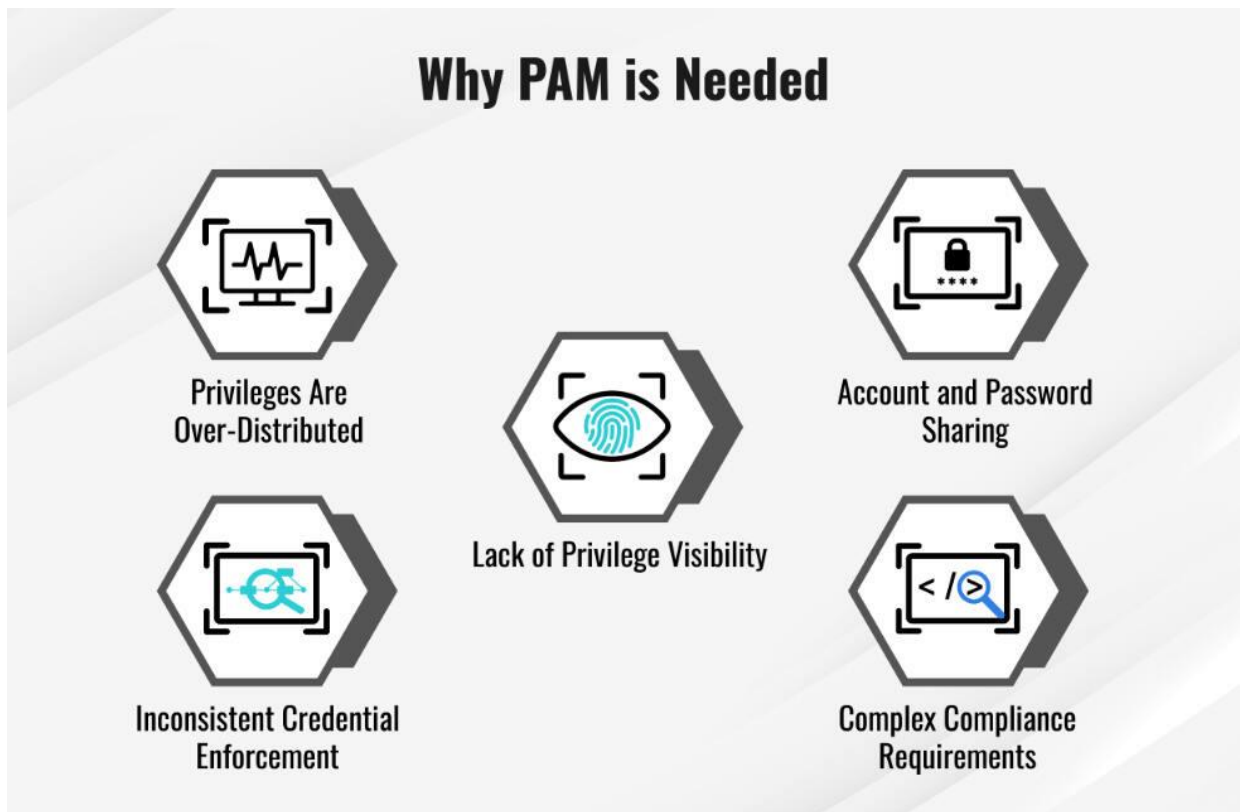


Рисунок 2.3 – Перелік всіх атрибутів системи PAM.

Спільним для всіх пунктів є необхідність надійного зберігання конфіденційної інформації таким чином, щоб вона була доступна лише автентифікованим та авторизованим особам і зберігала цілісність її даних (тобто не могла бути підроблена). Системи управління паролями повинні підтримувати доступ як користувачів, так і систем безпечним та аудитованим способом.

Окрім технічних переваг управління паролями, існують також додаткові переваги, зокрема, робочі процеси та процеси, що використовуються для зберігання та отримання доступу до паролів користувачів. Наявність середовища розташування та безпечного зберігання надає адміністраторам корпоративних мереж можливість уникнути застосування додаткових серверів зберігання облікових даних. Таким чином, зменшуючи ризик їх крадіжки або втрати.

На рисунку 2.4 продемонстровано один із способів розгортання PAM-рішення з централізованим сервером політик та розподіленим набором PAM-

агентів. У даному прикладі, організація вирішила використовувати своє РАМ-рішення як альтернативу іншим.

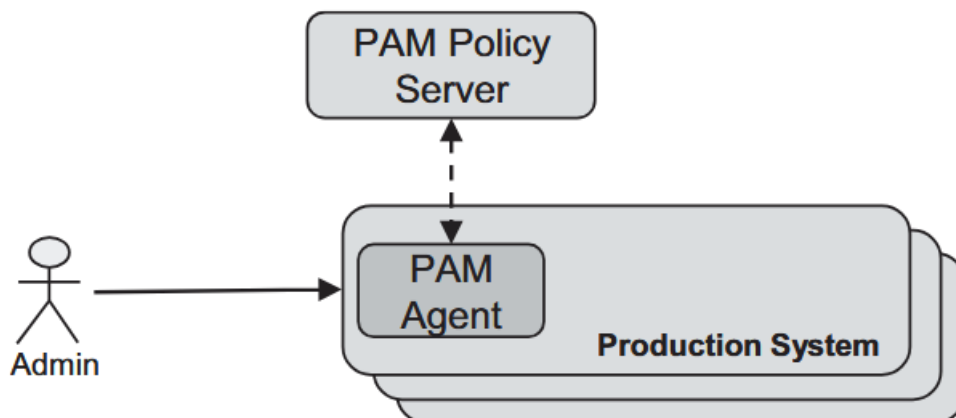


Рисунок 2.4 – РАМ, що забезпечує контроль доступу через управління сеансами

У контексті застосування РАМ як модель Zero Trust. Найпростіший і найлегший підхід — захистити доступ до самого РАМ-сервера, розмістивши його за РЕР, як показано на рисунку 2.5.

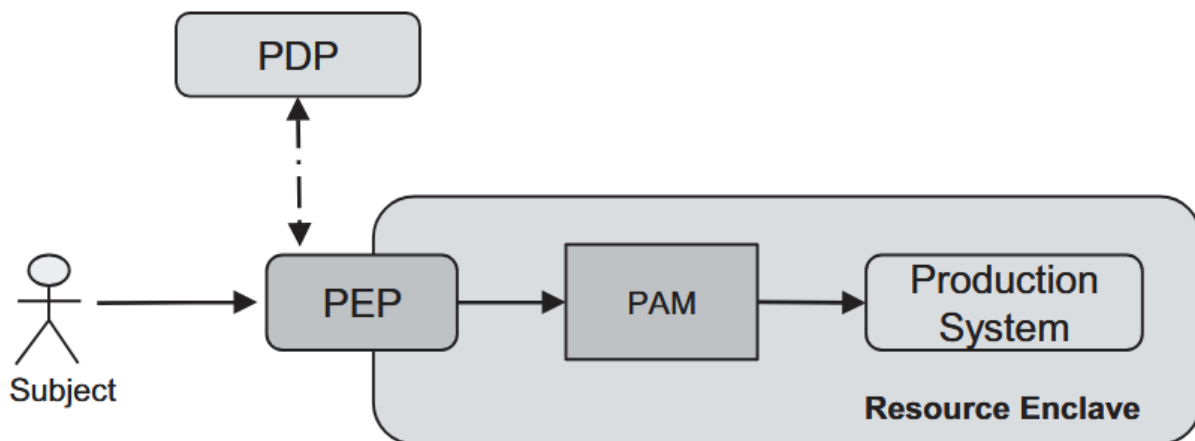


Рисунок 2.5 – Умовна схема розгортання РАМ сервера.

У даному сценарії РАМ-рішення є захищеним ресурсом в моделі Zero Trust. Хоча це не складне рішення, але воно підвищує безпеку корпоративної мережі, запобігаючи доступу до нього неавторизованим користувачам або пристроям. Це продумана практика безпеки — зрештою, якщо РАМ-сервер

містить головні паролі системи. Він перетворюється в бажану мішень для кіберзлочинців.

Система РАМ – надає необхідні функції керування паролями та доступом, Що допомагає підтримувати вимоги мережної безпеки, відповідності та аудиту. Але інтеграція РАМ з платформою Zero Trust може підвищити цінність обох систем, і організації, які використовують РАМ, повинні надати пріоритет захисту самого сервера РАМ. Вони також можуть розглянути способи, за допомогою яких ці два рішення можуть обмінюватися інформацією, щоб приймати кращі рішення щодо доступу разом, хоча це, ймовірно, буде максимально продуманим варіантом використання.

Висновки з розділу 2

У другому розділі було створено обліковий запис на платформі Springer Nature Link з метою проведення аналізу допоміжних середовищ розширення моделі Zero Trust. Отримана інформація, про протоколи подібні протоколу RADIUS та системи РЕР, РАМ. Кожен протокол з даної сфери застосування було розглянуто детально з поглибленим вивченням всіх аспектів кібербезпеки в цілому. Таким чином були детально представлені сервіси розширеного захисту даних.

В ході вивчення теоретичних матеріалів було встановлено, що наявність середовища РЕР надає адміністраторам корпоративних мереж можливість уникнути застосування додаткових серверів зберігання облікових даних. Таким чином, зменшуючи ризик їх крадіжки або втрати. Але також було встановлено, що наявність РАМ-сервера, що зберігає головні паролі системи перетворює його в головну мішень для взлому.

Розділ 2 (два) сформулював чітке практичне уявлення налаштування, створення та підбору допоміжних протоколів для розробки корпоративної мережі з впровадженою технологією Zero Trust, що буде реалізовуватись та розгортатись в наступному розділі.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВПРОВАДЖЕННЯ ZERO TRUST АРХІТЕКТУРИ

3.1 Налаштування мережі впровадження правил Zero Trust.

Зображена на рисунку 3.1 розробка схеми адресації пристроїв мережі. Було враховано, що перша IP адреса мережі стає шлюзом VirtualBox Nat Network та DNS для доступу до глобальної мережі інтернет.

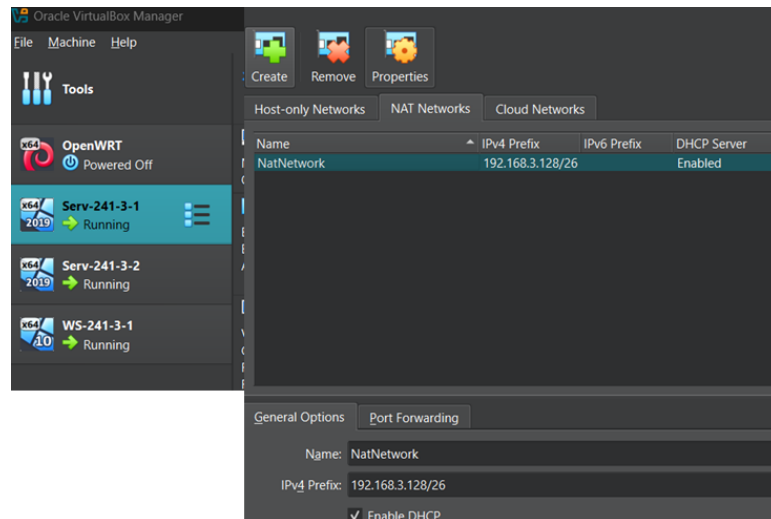


Рисунок 3.1 – Налаштування внутрішньої мережі в середовищі Oracle VirtualBox.

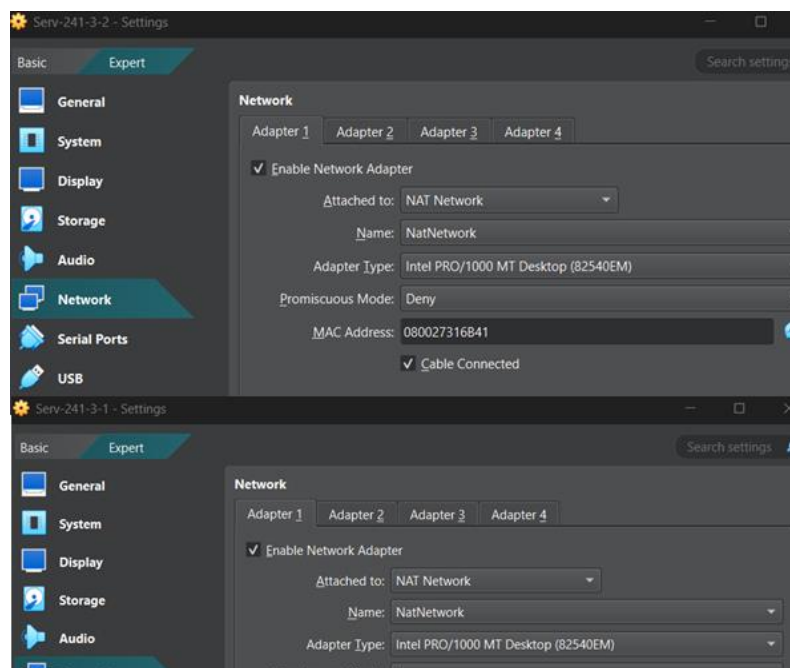


Рисунок 3.2 – Зміна адаптера на сервері (аналогічно на всіх ВМ мережі)

Наступним кроком згідно таблиці необхідно кожній робочій станції та серверу отримати робочу IP-адресу, що показано на рисунку 3.3.

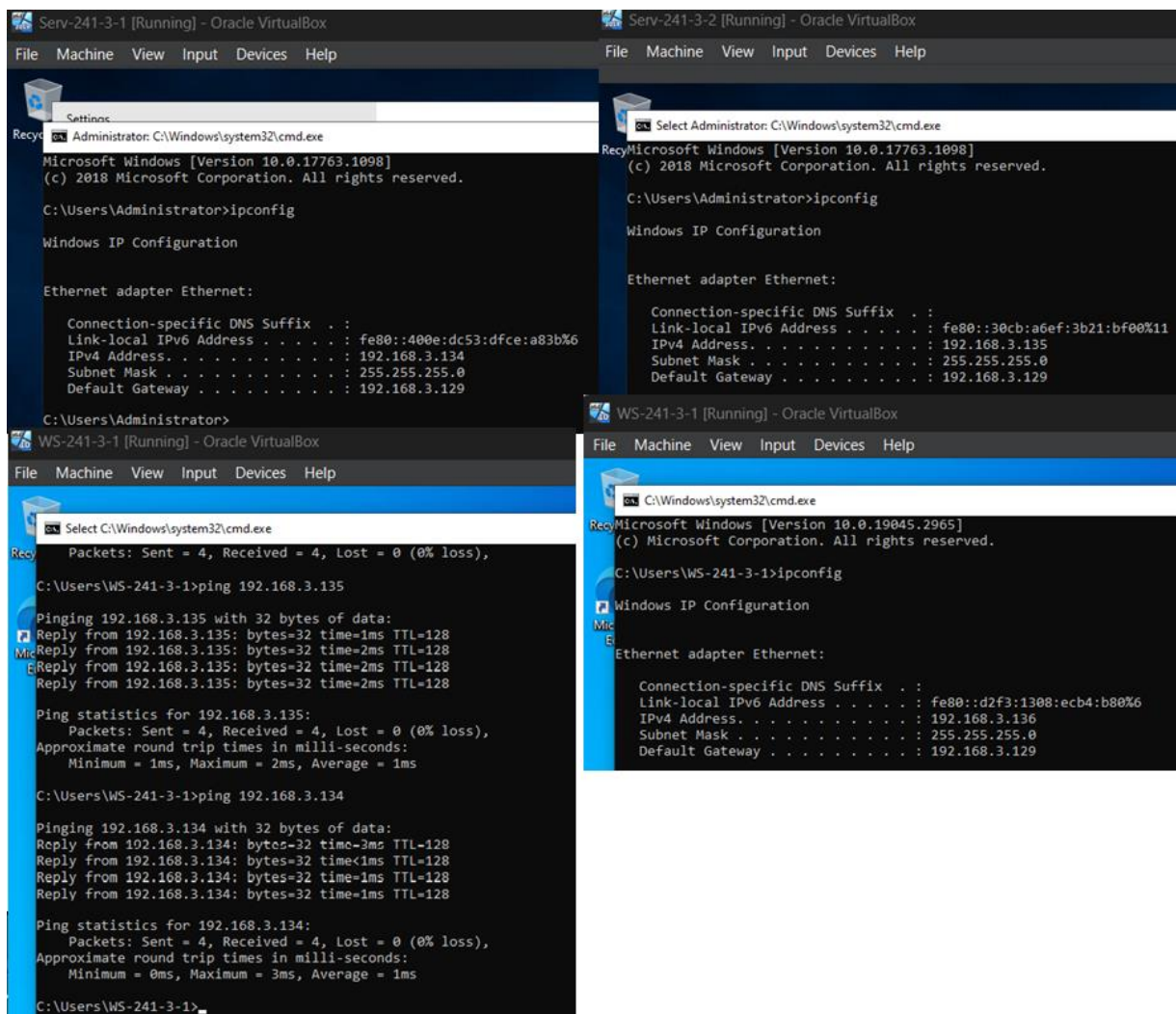


Рисунок 3.3 – Отримання IP-адрес в середовищі WindowsServer та подальша перевірка зв'язку.

Засобами PowerShell на сервері Serv-241-3-1 було встановлено Active Directory, а сервер Serv-241-3-2 додано до домену та надано йому роль додаткового контролера домену. Ім'я домену верхнього рівня – herasymenko.net. На сервері Serv-G-N-2 також було встановлено роль Active Directory Domain Services засобами PowerShell. Зображено на рисунках 3.4, 3.5, 3.6.

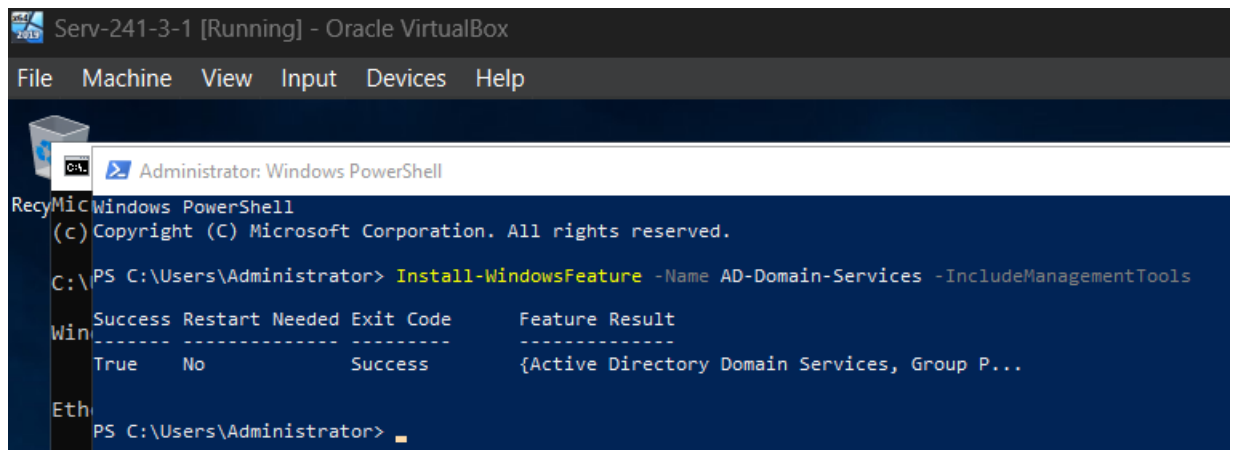


Рисунок 3.4 – Встановлення AD на перший контролер домену.

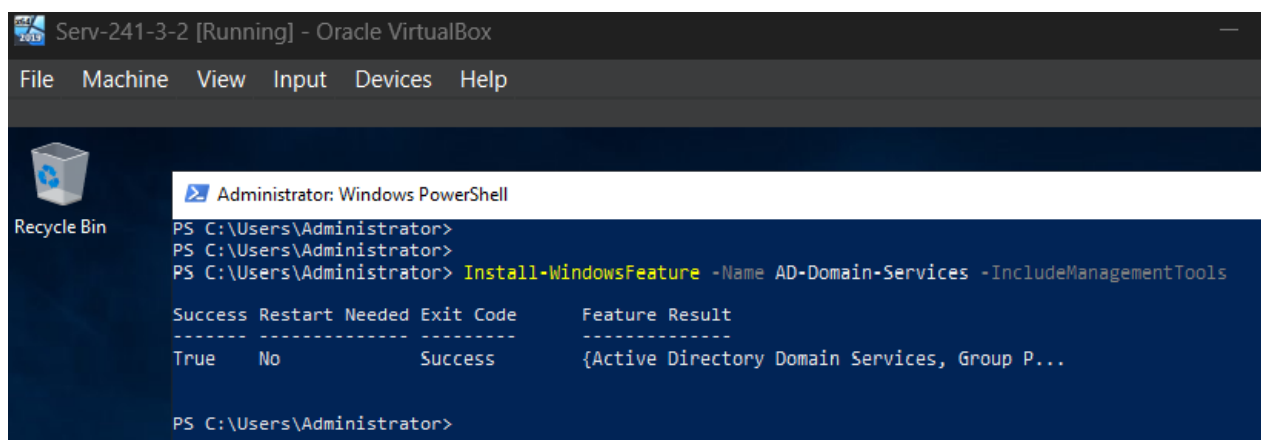


Рисунок 3.5 – Встановлення AD на другий контролер домену.

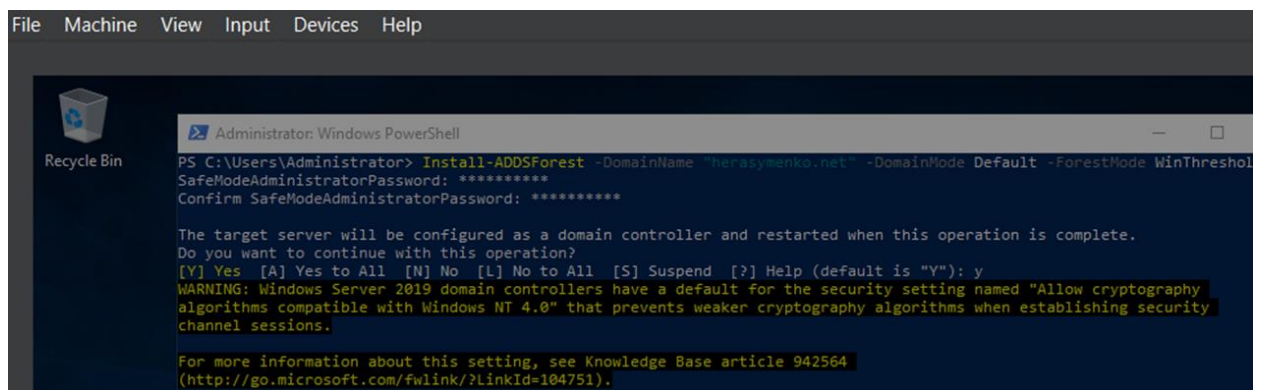


Рисунок 3.6 – Створення домену на першому контролері домену.

На наступному кроці (рисунок 3.7) видно встановлені контролери домену.

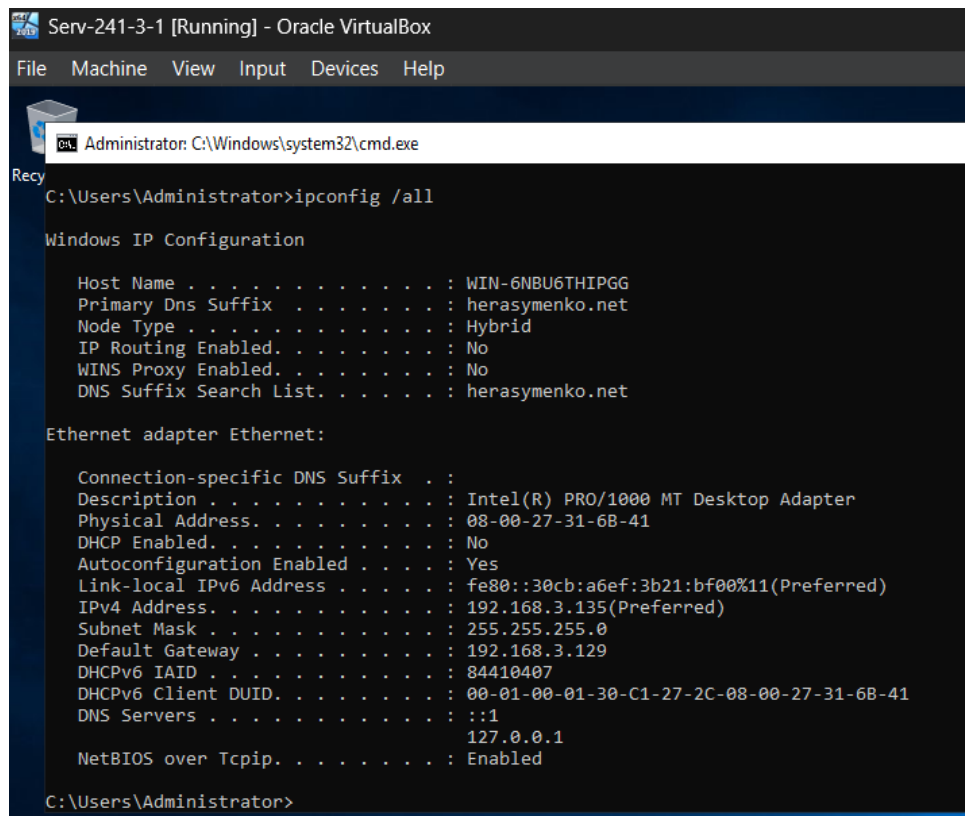


Рисунок 3.7 – Перевірка конфігурації контроллер

На рисунку 3.8 було додано нового користувача.

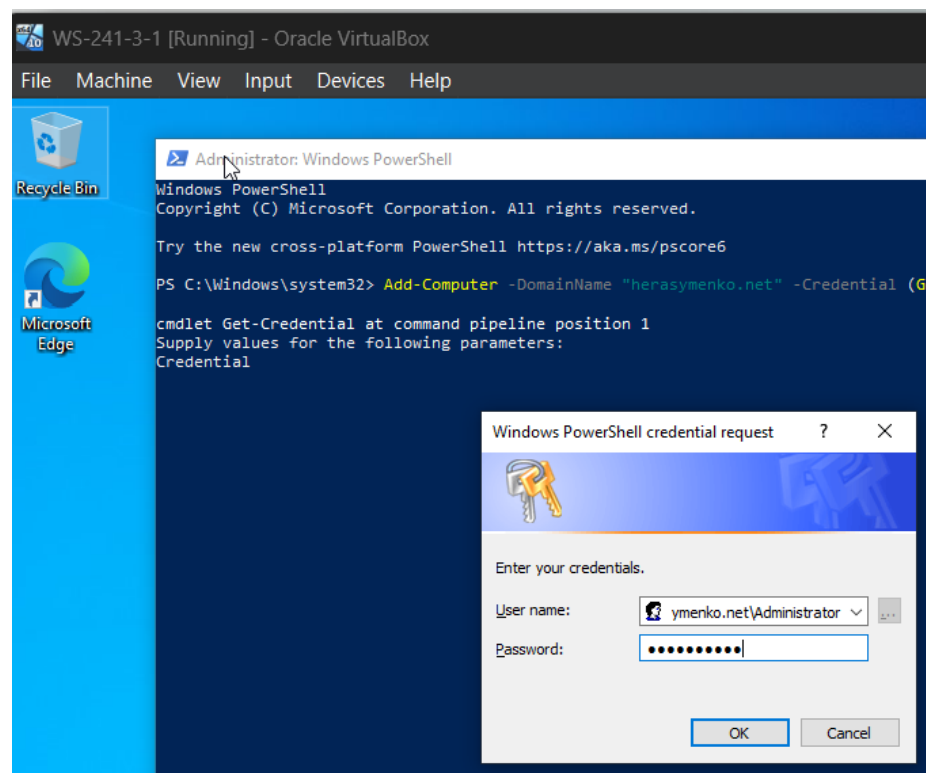


Рисунок 3.8 – Автентифікація нового користувача.

З метою збереження рекомендованих налаштувань безпеки Windows Server 2019 необхідно заборонити на серверах внутрішній істр ipv4 трафік (рисунок 3.9).

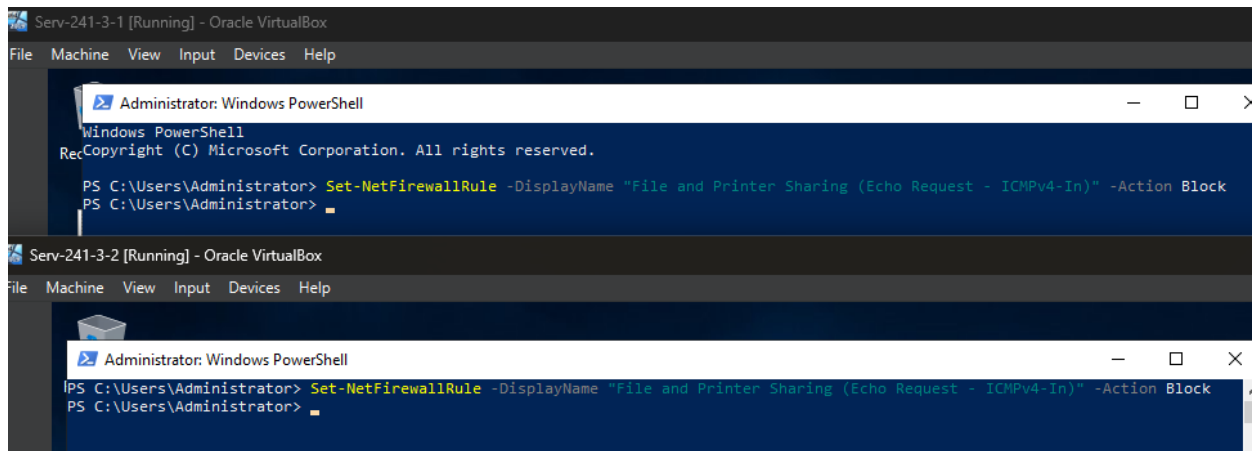


Рисунок 3.9 – Заборона вхідного істр v4 трафіку на обох контролерах домену.

З метою збереження налаштувань контролера домену необхідно перезавантажити систему (рисунок 3.10).

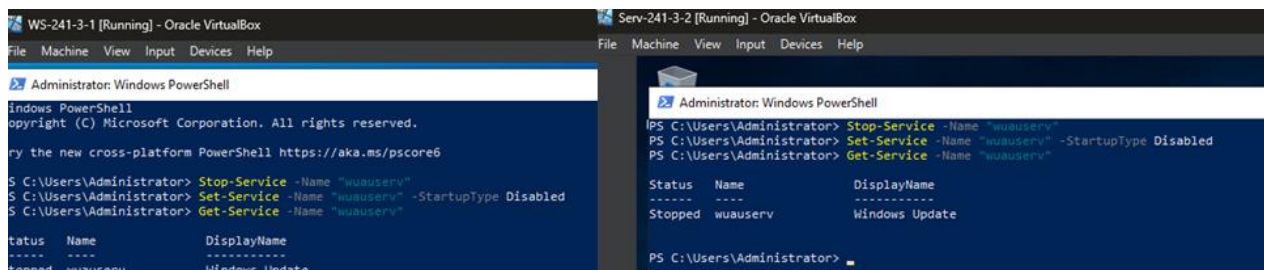


Рисунок 3.10 – Оновлені дані.

3.2 Послідовність додавання нових користувачів у систему

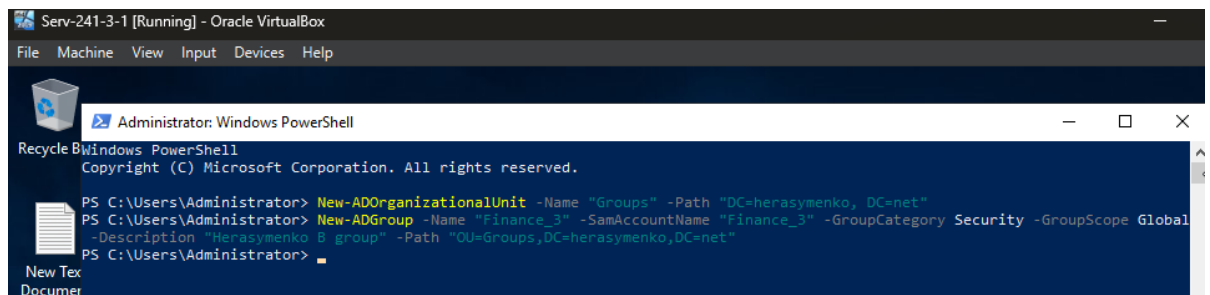
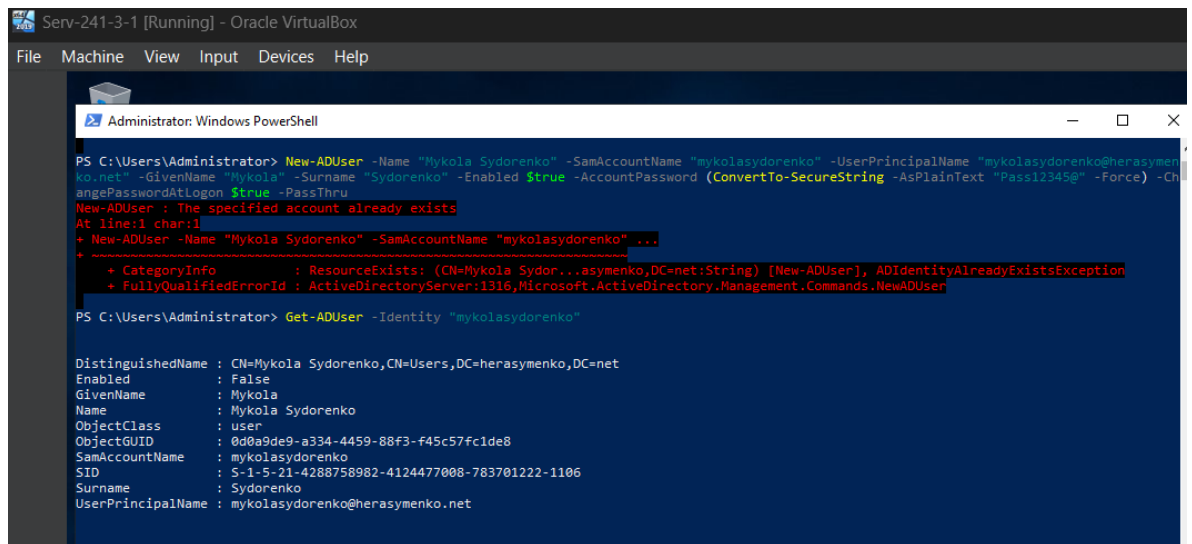


Рисунок 3.11 – Створення нової групи користувачів.



```
Serv-241-3-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

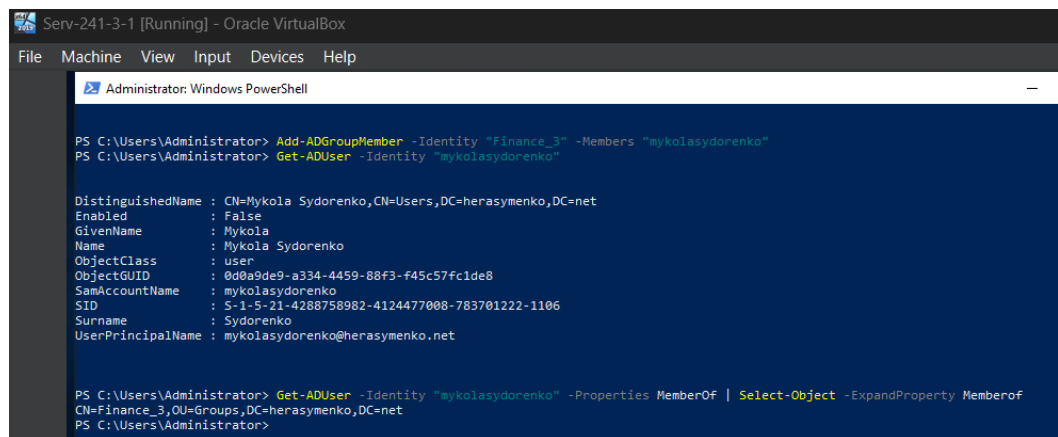
Administrator: Windows PowerShell

PS C:\Users\Administrator> New-ADUser -Name "Mykola Sydorenko" -SamAccountName "mykolasydorenko" -UserPrincipalName "mykolasydorenko@herasymenko.net" -GivenName "Mykola" -Surname "Sydorenko" -Enabled $true -AccountPassword (ConvertTo-SecureString "Pass123456" -AsPlainText -Force) -ChangePasswordAtLogon $true -PassThru
New-ADUser : The specified account already exists
At line:1 char:1
+ New-ADUser -Name "Mykola Sydorenko" -SamAccountName "mykolasydorenko" ...
+ ~~~~~
+ CategoryInfo          : ResourceExists: (CN=Mykola Sydor...asymenko,DC=net:String) [New-ADUser], ADIdentityAlreadyExistsException
+ FullyQualifiedErrorId : ActiveDirectoryServer:1316,Microsoft.ActiveDirectory.Management.Commands.NewADUser

PS C:\Users\Administrator> Get-ADUser -Identity "mykolasydorenko"

DistinguishedName : CN=Mykola Sydorenko,CN=Users,DC=herasymenko,DC=net
Enabled            : False
GivenName         : Mykola
Name              : Mykola Sydorenko
ObjectClass       : user
ObjectGUID        : 0d0a9de9-a334-4459-88f3-f45c57fc1de8
SamAccountName    : mykolasydorenko
SID               : S-1-5-21-4288758982-4124477008-783701222-1106
Surname           : Sydorenko
UserPrincipalName : mykolasydorenko@herasymenko.net
```

Рисунок 3.12 – Виника проблема з паролем але користувач створився.



```
Serv-241-3-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

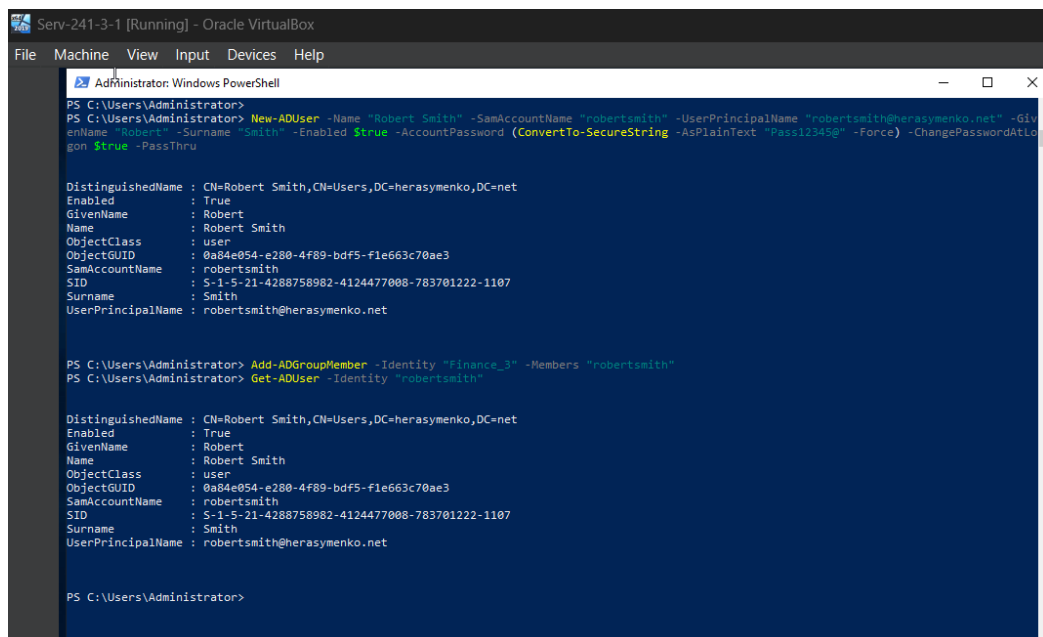
Administrator: Windows PowerShell

PS C:\Users\Administrator> Add-ADGroupMember -Identity "Finance_3" -Members "mykolasydorenko"
PS C:\Users\Administrator> Get-ADUser -Identity "mykolasydorenko"

DistinguishedName : CN=Mykola Sydorenko,CN=Users,DC=herasymenko,DC=net
Enabled            : False
GivenName         : Mykola
Name              : Mykola Sydorenko
ObjectClass       : user
ObjectGUID        : 0d0a9de9-a334-4459-88f3-f45c57fc1de8
SamAccountName    : mykolasydorenko
SID               : S-1-5-21-4288758982-4124477008-783701222-1106
Surname           : Sydorenko
UserPrincipalName : mykolasydorenko@herasymenko.net

PS C:\Users\Administrator> Get-ADUser -Identity "mykolasydorenko" -Properties MemberOf | Select-Object -ExpandProperty MemberOf
CN=Finance_3,OU=Groups,DC=herasymenko,DC=net
PS C:\Users\Administrator>
```

Рисунок 3.13 – Створення першого користувача.



```
Serv-241-3-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Administrator: Windows PowerShell

PS C:\Users\Administrator> New-ADUser -Name "Robert Smith" -SamAccountName "robertsmith" -UserPrincipalName "robertsmith@herasymenko.net" -GivenName "Robert" -Surname "Smith" -Enabled $true -AccountPassword (ConvertTo-SecureString "Pass123456" -AsPlainText -Force) -ChangePasswordAtLogon $true -PassThru

DistinguishedName : CN=Robert Smith,CN=Users,DC=herasymenko,DC=net
Enabled            : True
GivenName         : Robert
Name              : Robert Smith
ObjectClass       : user
ObjectGUID        : 0a84e054-e280-4f89-bdf5-f1e663c70ae3
SamAccountName    : robertsmith
SID               : S-1-5-21-4288758982-4124477008-783701222-1107
Surname           : Smith
UserPrincipalName : robertsmith@herasymenko.net

PS C:\Users\Administrator> Add-ADGroupMember -Identity "Finance_3" -Members "robertsmith"
PS C:\Users\Administrator> Get-ADUser -Identity "robertsmith"

DistinguishedName : CN=Robert Smith,CN=Users,DC=herasymenko,DC=net
Enabled            : True
GivenName         : Robert
Name              : Robert Smith
ObjectClass       : user
ObjectGUID        : 0a84e054-e280-4f89-bdf5-f1e663c70ae3
SamAccountName    : robertsmith
SID               : S-1-5-21-4288758982-4124477008-783701222-1107
Surname           : Smith
UserPrincipalName : robertsmith@herasymenko.net

PS C:\Users\Administrator>
```

Рисунок 3.14 – Створення другого користувача.

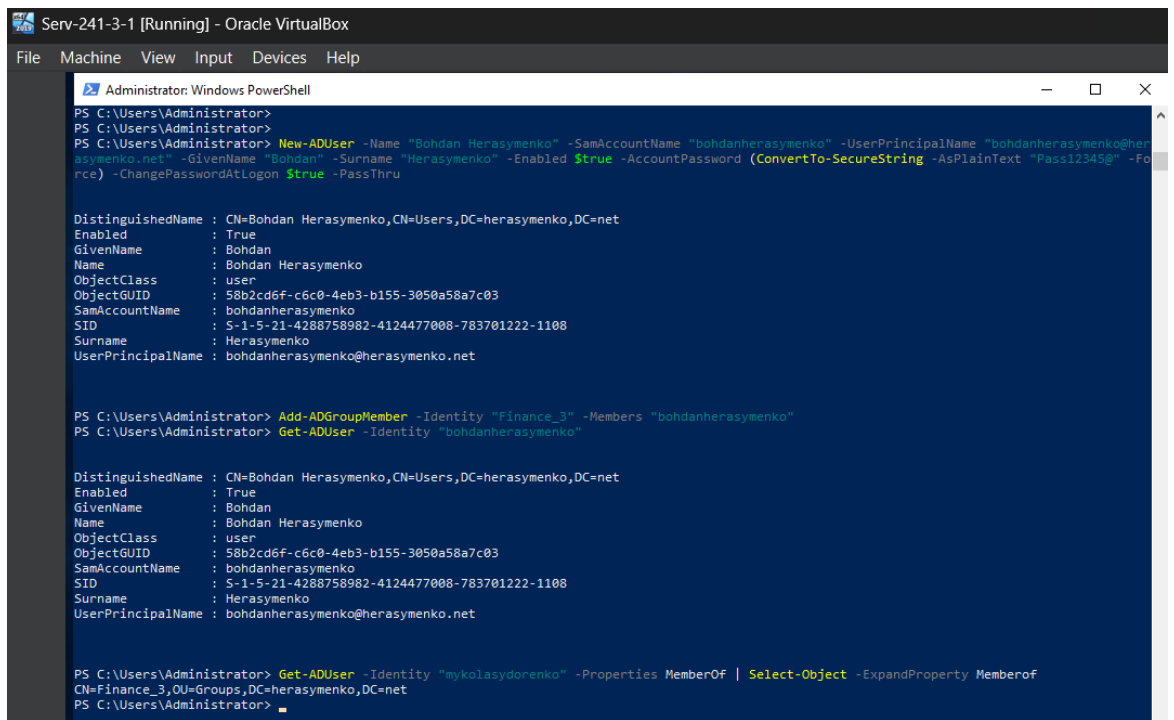


Рисунок 3.15 – Створення третього користувача.

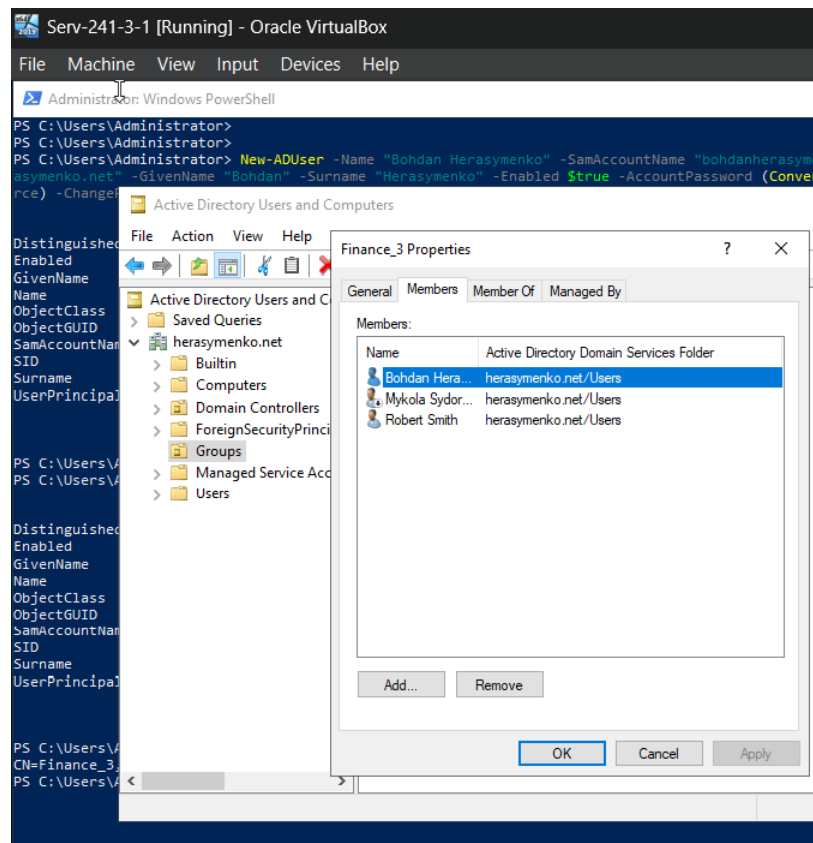
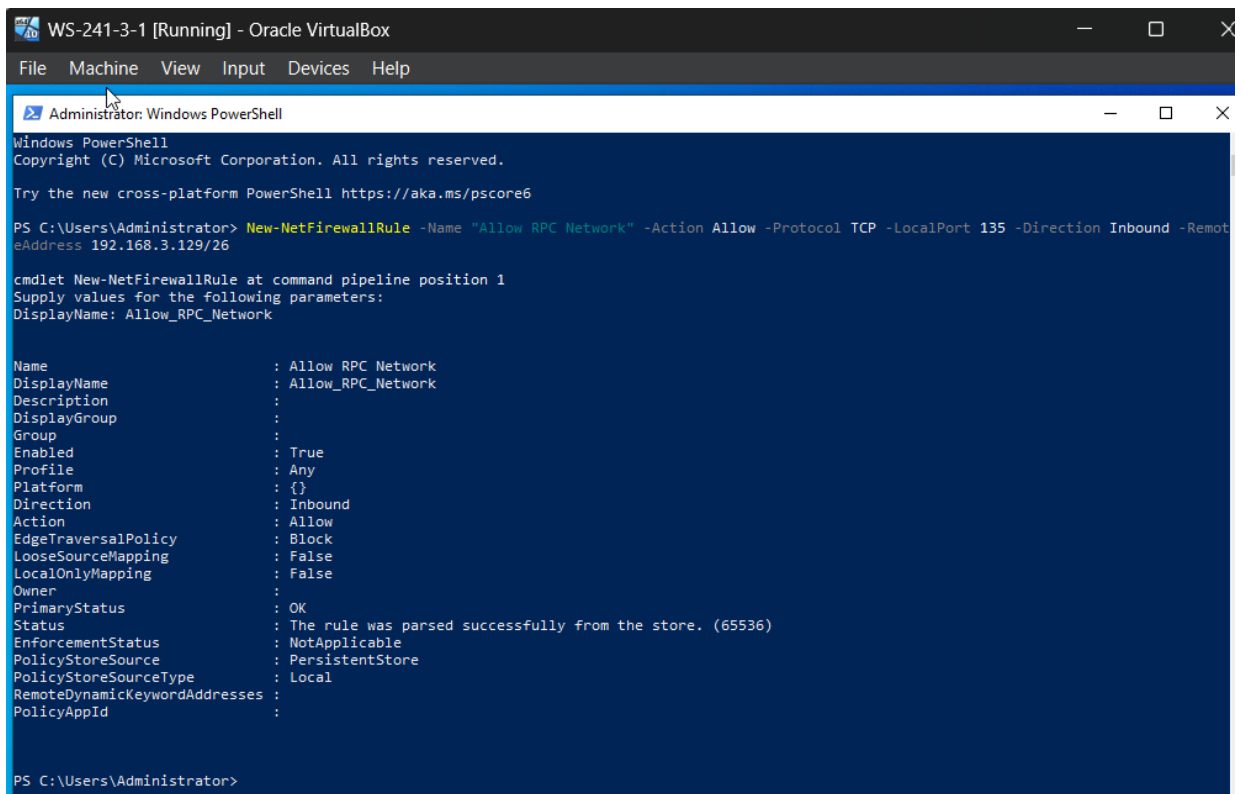


Рисунок 3.16 – Перегляд створених користувачів через GUI

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> rpcping -s Serv-241-3-2
Exception 1722 (0x000006BA)
Number of records is: 3
ProcessID is 3916
System Time is: 12/8/2025 6:39:23:225
Generating component is 18
Status is 0x6BA, 1722
Detection location is 1442
Flags is 0
NumberOfParameters is 1
Unicode string: Serv-241-3-2
ProcessID is 3916
System Time is: 12/8/2025 6:39:23:225
Generating component is 18
Status is 0x6BA, 1722
Detection location is 322
Flags is 0
NumberOfParameters is 0
ProcessID is 3916
System Time is: 12/8/2025 6:39:23:225
Generating component is 18
Status is 0x2AF9, 11001
Detection location is 320
Flags is 0
NumberOfParameters is 1
Unicode string: Serv-241-3-2
PS C:\Users\Administrator>

PS C:\Users\Administrator> rpcping -s Serv-241-3-1
Exception 1722 (0x000006BA)
Number of records is: 3
ProcessID is 2556
System Time is: 12/8/2025 6:38:17:57
Generating component is 18
Status is 0x6BA, 1722
Detection location is 1442
Flags is 0
NumberOfParameters is 1
Unicode string: Serv-241-3-1
ProcessID is 2556
System Time is: 12/8/2025 6:38:17:57
Generating component is 18
Status is 0x6BA, 1722
Detection location is 322
Flags is 0
NumberOfParameters is 0
ProcessID is 2556
System Time is: 12/8/2025 6:38:17:57
Generating component is 18
Status is 0x2AF9, 11001
Detection location is 320
Flags is 0
NumberOfParameters is 1
Unicode string: Serv-241-3-1
PS C:\Users\Administrator>
```

Рисунок 3.17 – Перевірка роботи RPC-серверів на DC та спроба отримання записів системного журналу Security з Serv-241-3-2 за його IP-адресою



```
WS-241-3-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Administrator> New-NetFirewallRule -Name "Allow RPC Network" -Action Allow -Protocol TCP -LocalPort 135 -Direction Inbound -Remot
eAddress 192.168.3.129/26

cmdlet New-NetFirewallRule at command pipeline position 1
Supply values for the following parameters:
DisplayName: Allow_RPC_Network

Name                : Allow RPC Network
DisplayName          : Allow_RPC_Network
Description          :
DisplayGroup         :
Group               :
Enabled              : True
Profile              : Any
Platform             : {}
Direction           : Inbound
Action               : Allow
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses :
PolicyAppId          :
```

Рисунок 3.18 – Створення правила «Allow RPC Network» на робочій станції

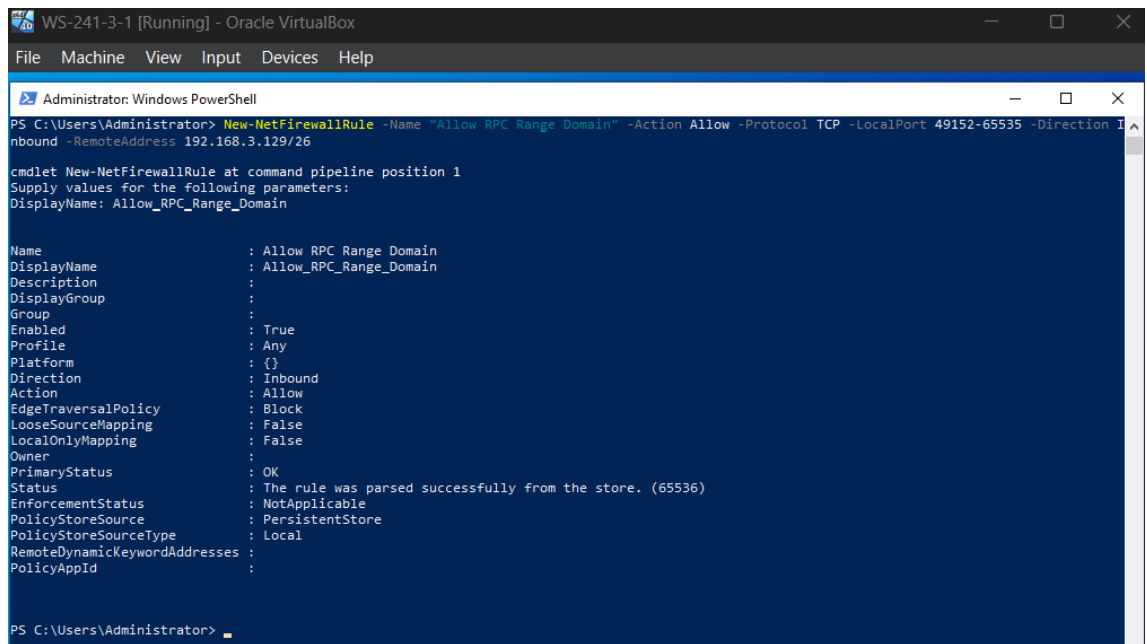


Рисунок 3.19 – Створення правила «Allow RPC Range Domain» на робочій станції

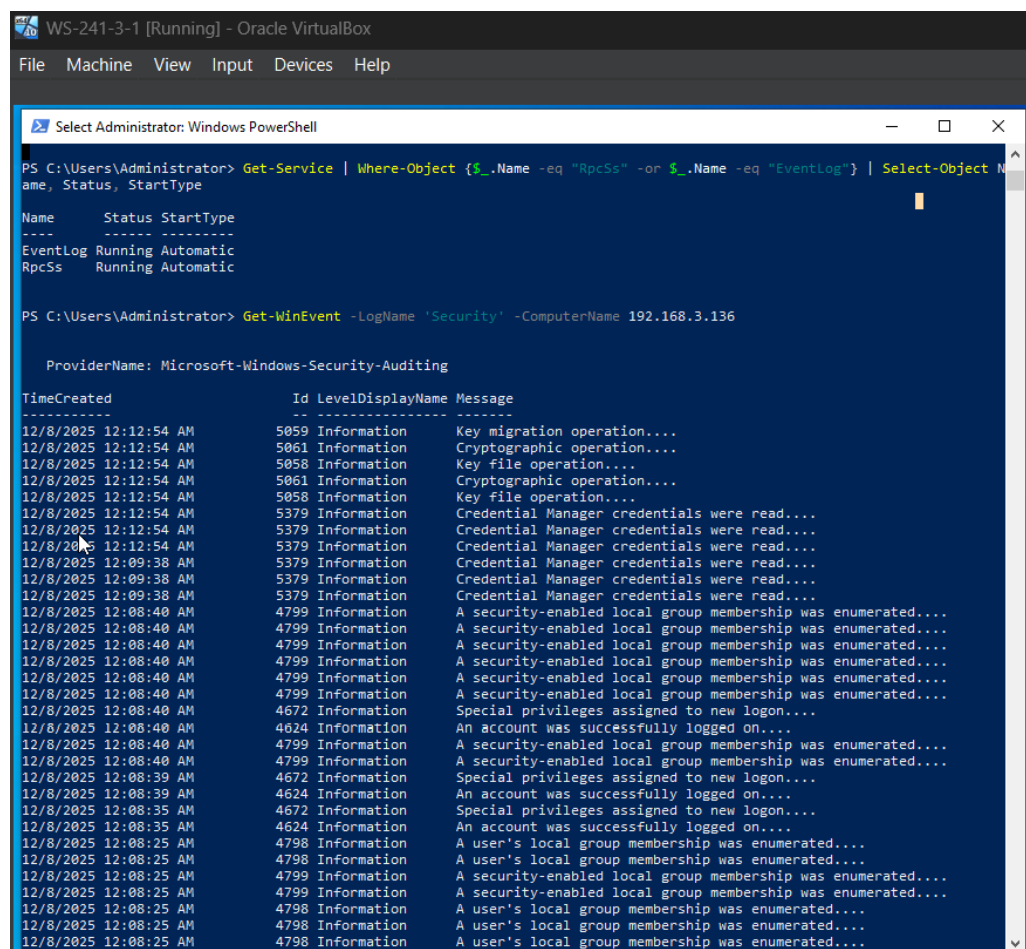


Рисунок 3.20 – Перевірка роботи RPC-серверу на робочій станції

Перевірка роботи RPC-серверу на контролерах домену (рисунок 3.21)

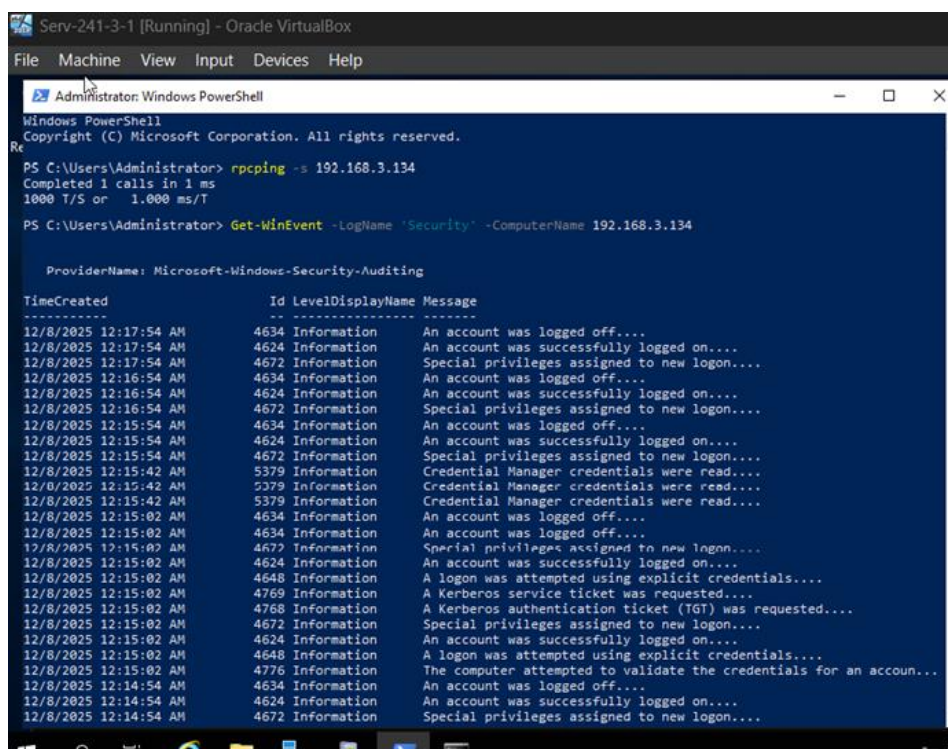


Рисунок 3.21 – Перевірка роботи RPC-серверу на контролері домену

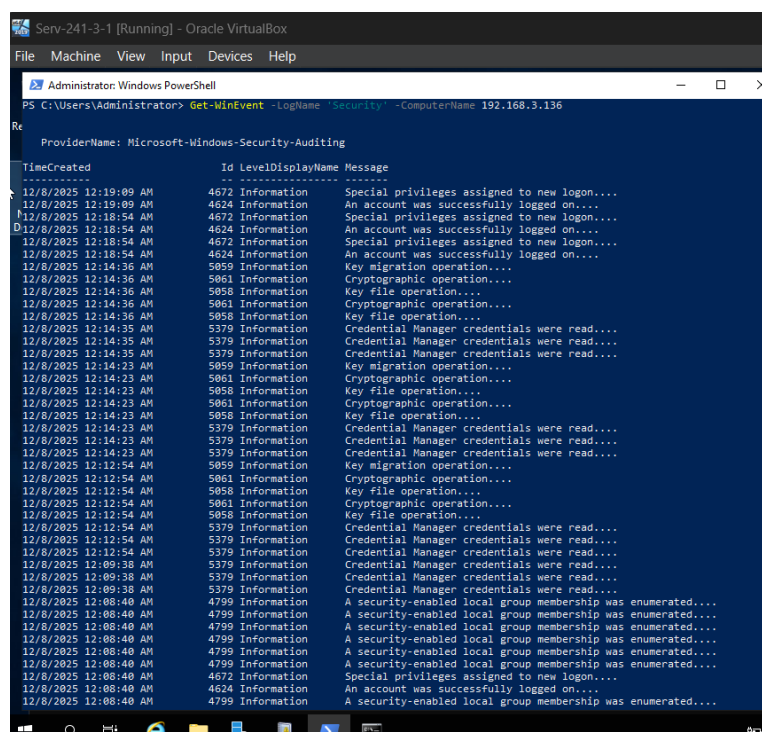


Рисунок 3.21 – Перевірка роботи RPC-серверу на робочій станції з контролеру домену

```
PS C:\Users\Administrator> Get-WinEvent -LogName System -ComputerName 192.168.3.136

ProviderName: LsaSrv
TimeCreated          Id LevelDisplayName Message
-----
12/8/2025 12:19:55 AM 6038 Warning      Microsoft Windows Server has detected that NTLM authentication i...

ProviderName: Microsoft-Windows-DistributedCOM
TimeCreated          Id LevelDisplayName Message
-----
12/8/2025 12:13:08 AM 10016 Warning      The machine-default permission settings do not grant Local Activ...

ProviderName: Service Control Manager
TimeCreated          Id LevelDisplayName Message
-----
12/8/2025 12:08:15 AM 7040 Information    The start type of the Windows Modules Installer service was chan...
12/8/2025 12:08:01 AM 7040 Information    The start type of the Windows Modules Installer service was chan...

ProviderName: Microsoft-Windows-Kernel-General
TimeCreated          Id LevelDisplayName Message
-----
12/8/2025 12:04:28 AM 1 Information     The system time has changed to [ 2025] -[ 12] -[ 08T08:04:28.75556340...
12/8/2025 12:04:28 AM 24 Information    The time zone information was refreshed with exit reason 0. Curr...
12/8/2025 12:04:28 AM 1 Information     The system time has changed to [ 2025] -[ 12] -[ 08T08:04:28.74929770...
12/8/2025 12:04:28 AM 24 Information    The time zone information was refreshed with exit reason 0. Curr...

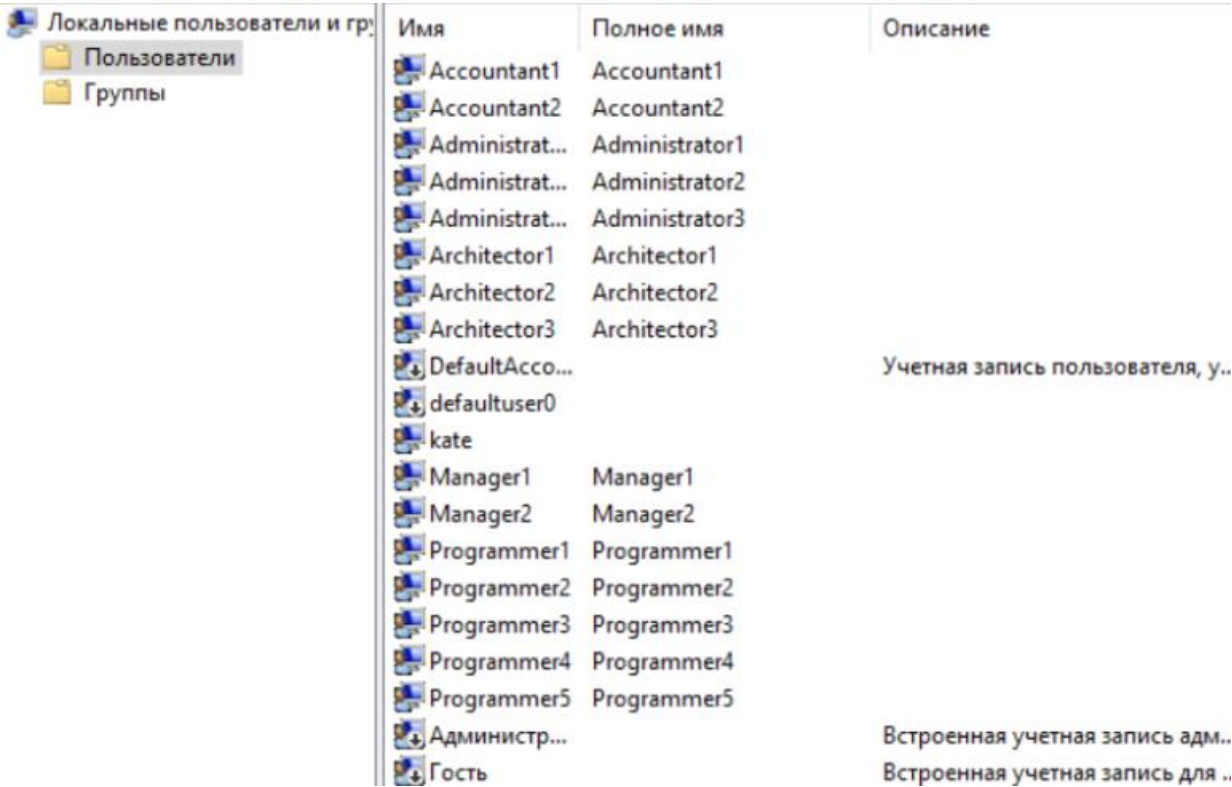
ProviderName: Microsoft-Windows-Kernel-Power
TimeCreated          Id LevelDisplayName Message
-----
12/8/2025 5:58:09 AM 105 Information    Power source change.

ProviderName: Microsoft-Windows-Time-Service
TimeCreated          Id LevelDisplayName Message
-----
12/8/2025 5:43:00 AM 50 Warning        The time service detected a time difference of greater than 5000...
```

Рисунок 3.22 – Спроба отримання записів з робочої станції на контролері домену.

Наступним кроком, для побудови повноцінних профілів користувачів є, додавання їх до існуючих груп, згідно з професійними інтересами. Для кожного з них, потрібно визначити до якої секції вони належать та додати до обраної групи. На рисунку зображено вигляд вікна користувачів після

внесення.



Локальные пользователи и группы

Имя	Полное имя	Описание
Accountant1	Accountant1	
Accountant2	Accountant2	
Administrat...	Administrator1	
Administrat...	Administrator2	
Administrat...	Administrator3	
Architector1	Architector1	
Architector2	Architector2	
Architector3	Architector3	
DefaultAcco...		Учетная запись пользователя, у...
defaultuser0		
kate		
Manager1	Manager1	
Manager2	Manager2	
Programmer1	Programmer1	
Programmer2	Programmer2	
Programmer3	Programmer3	
Programmer4	Programmer4	
Programmer5	Programmer5	
Администр...		Встроенная учетная запись адм..
Гость		Встроенная учетная запись для ..

Рисунок 3.23 – Вигляд вікна користувачів після внесення змін.

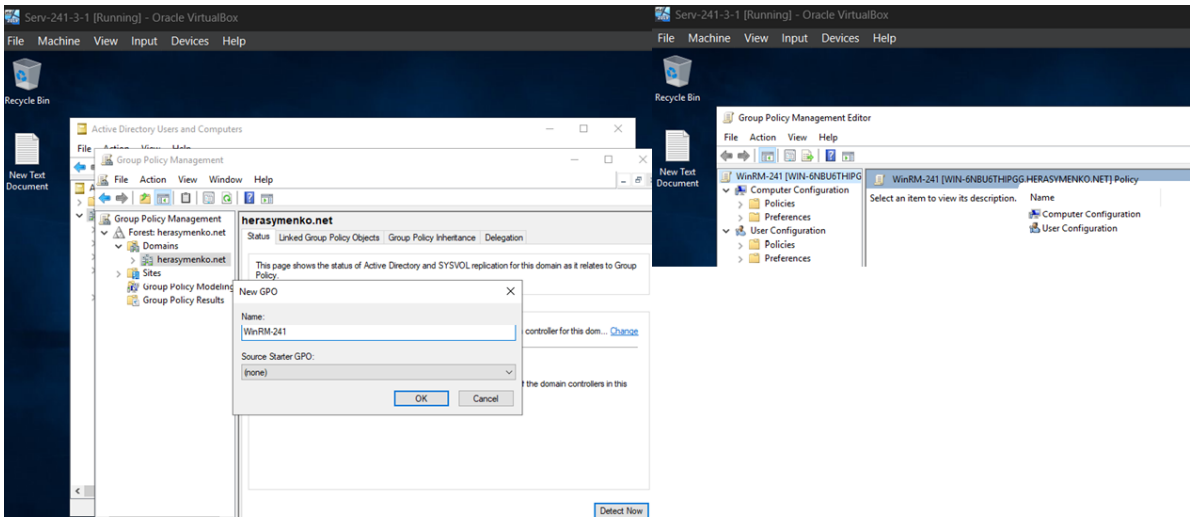


Рисунок 3.24 – Створення нової політики WinRM-241 у Group Policy Management Console.

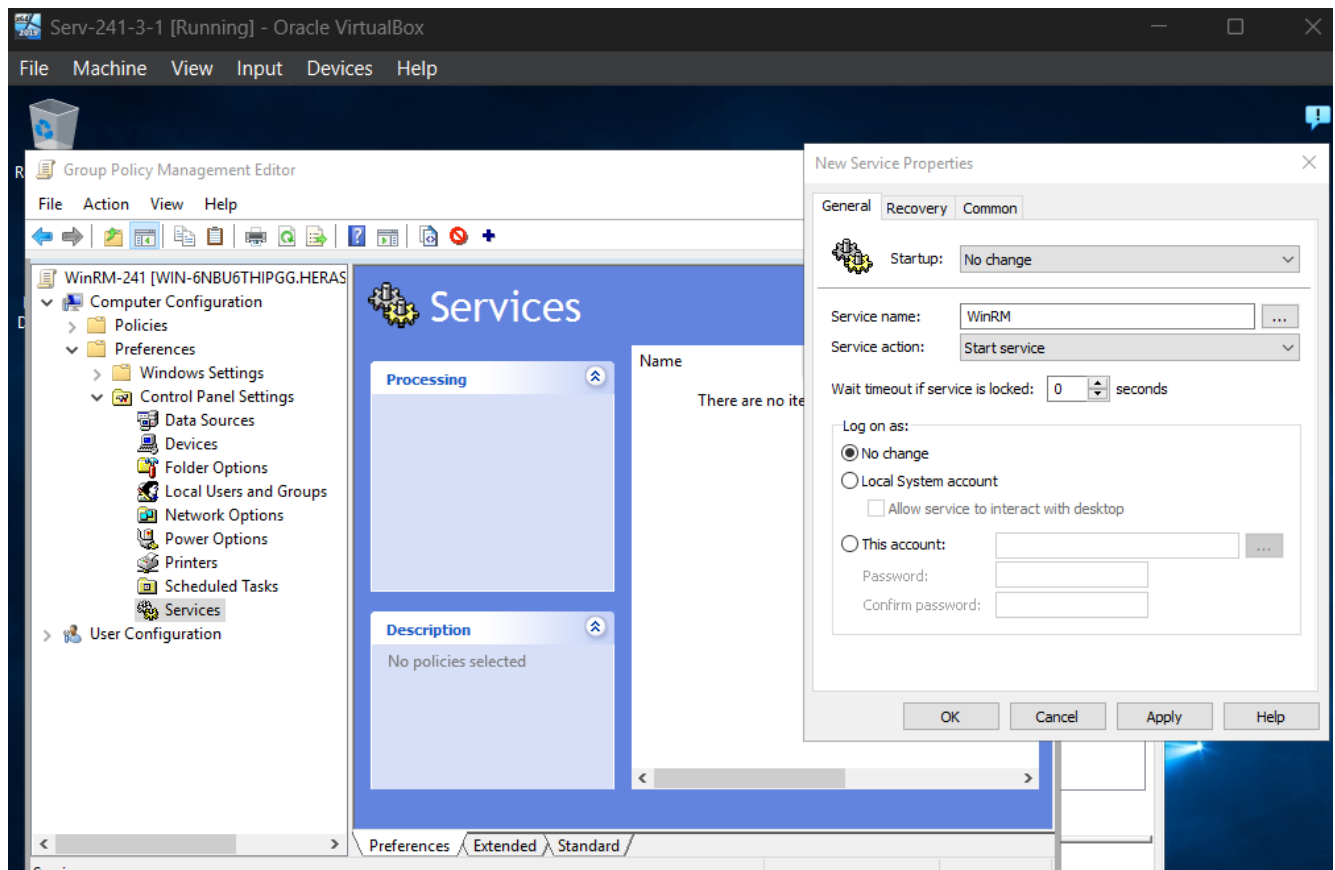


Рисунок 3.25 – Налаштування Recovery у політиці WinRM-22 у Group Policy Management.

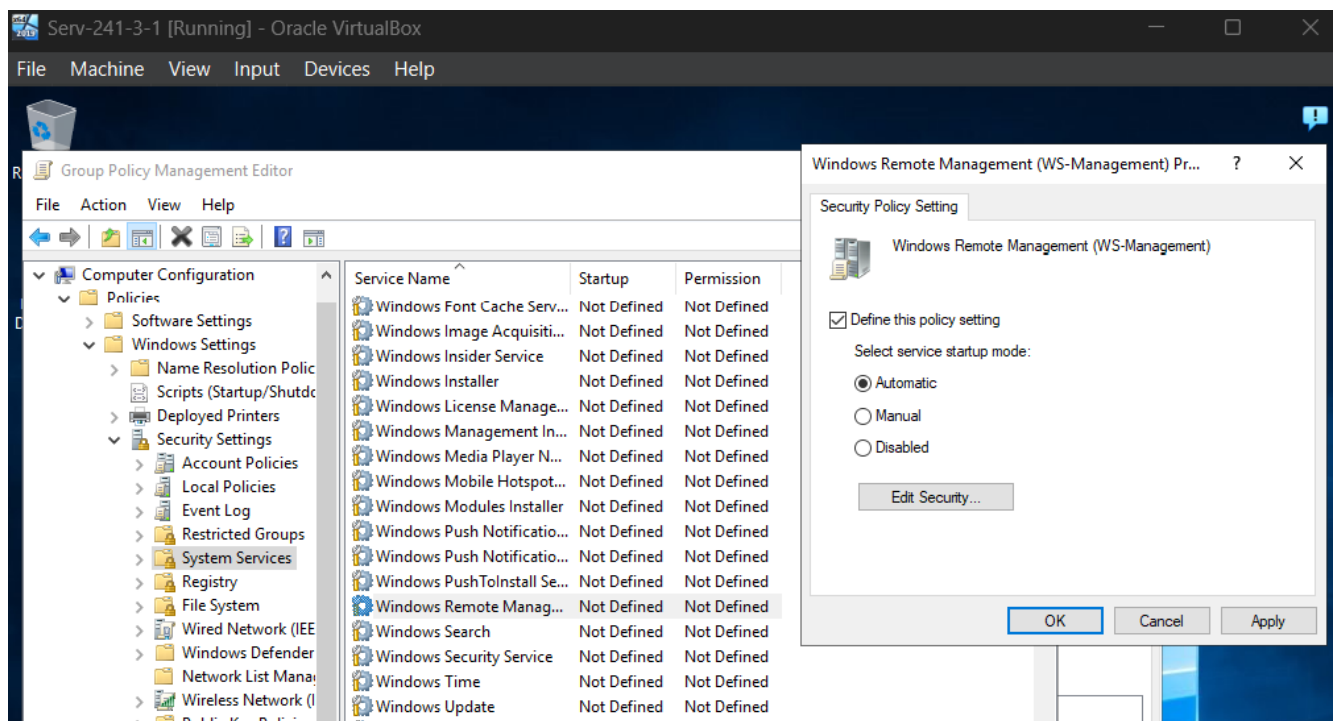


Рисунок 3.26 – Ввімкнення автоматичного режиму.

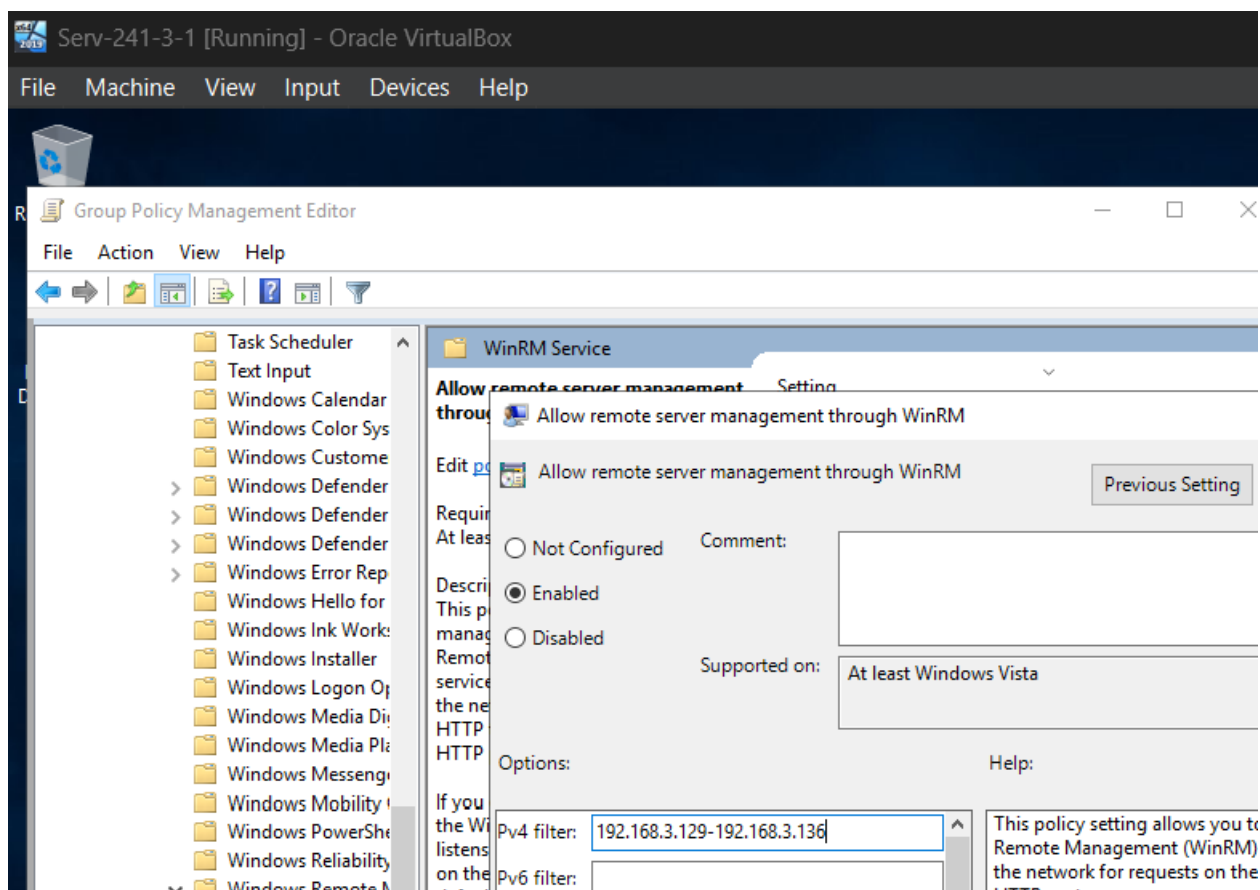


Рисунок 3.27 – Налаштування фільтра мереж у політиці WinRM-241.

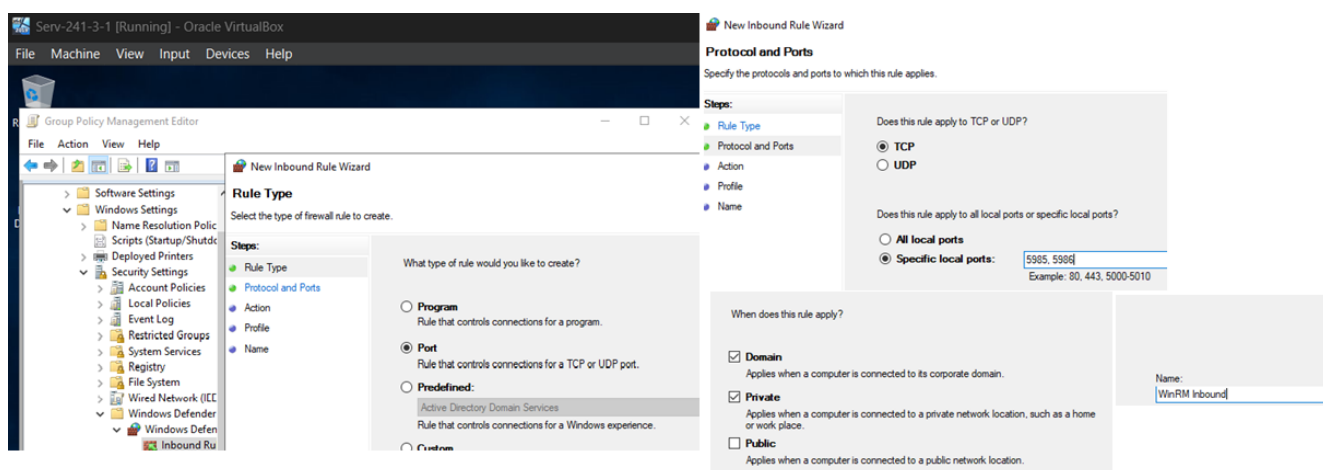


Рисунок 3.28 – Налаштування правил firewall у WinRM-241 у Group Policy Management.

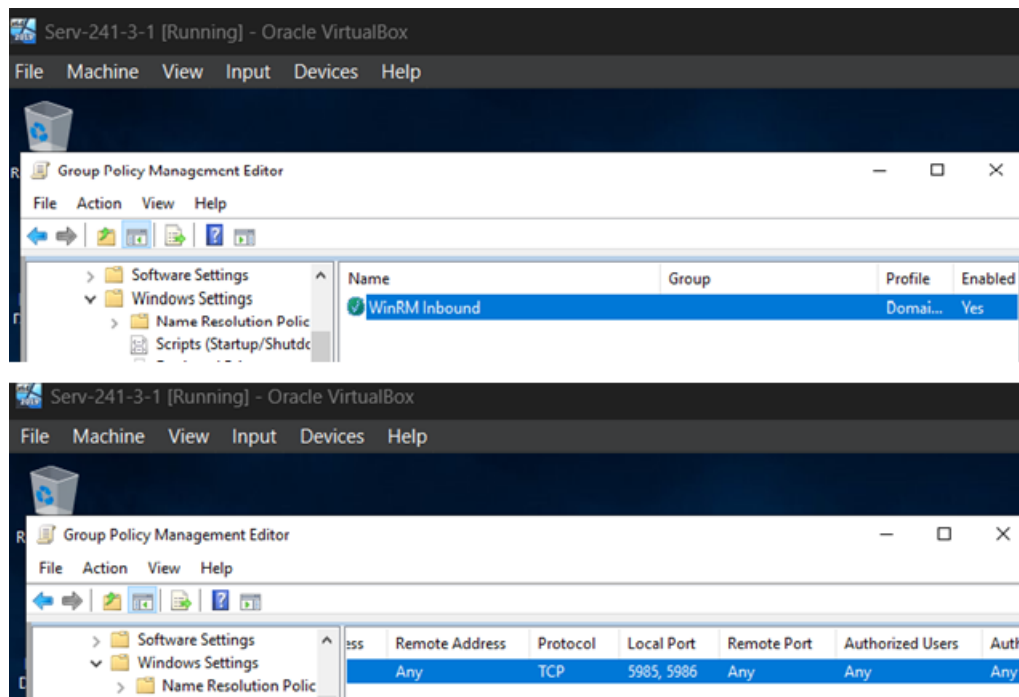


Рисунок 3.29 – Налаштування правил firewall у WinRM-241.

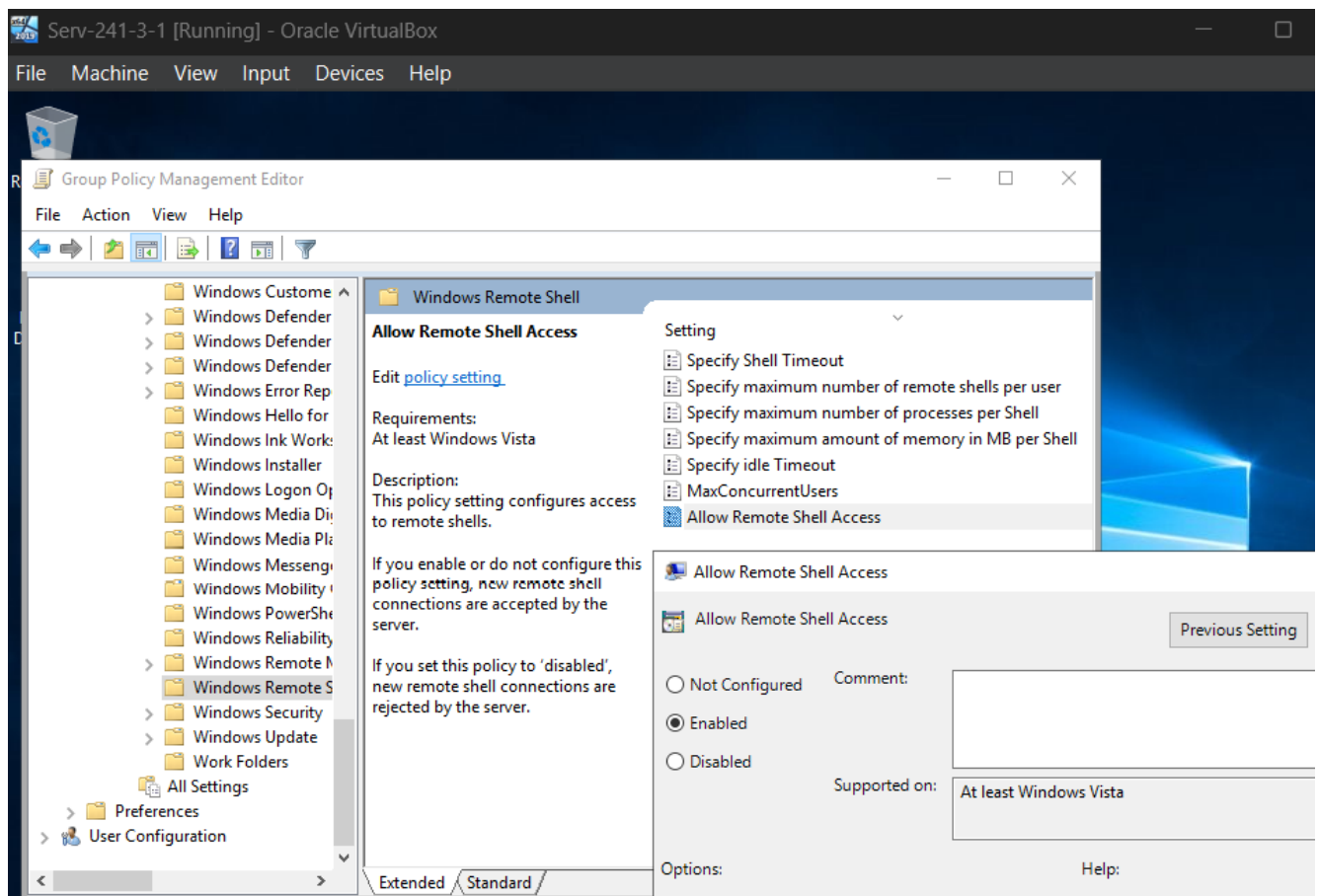


Рисунок 3.30 – Allow Remote Shell Access.

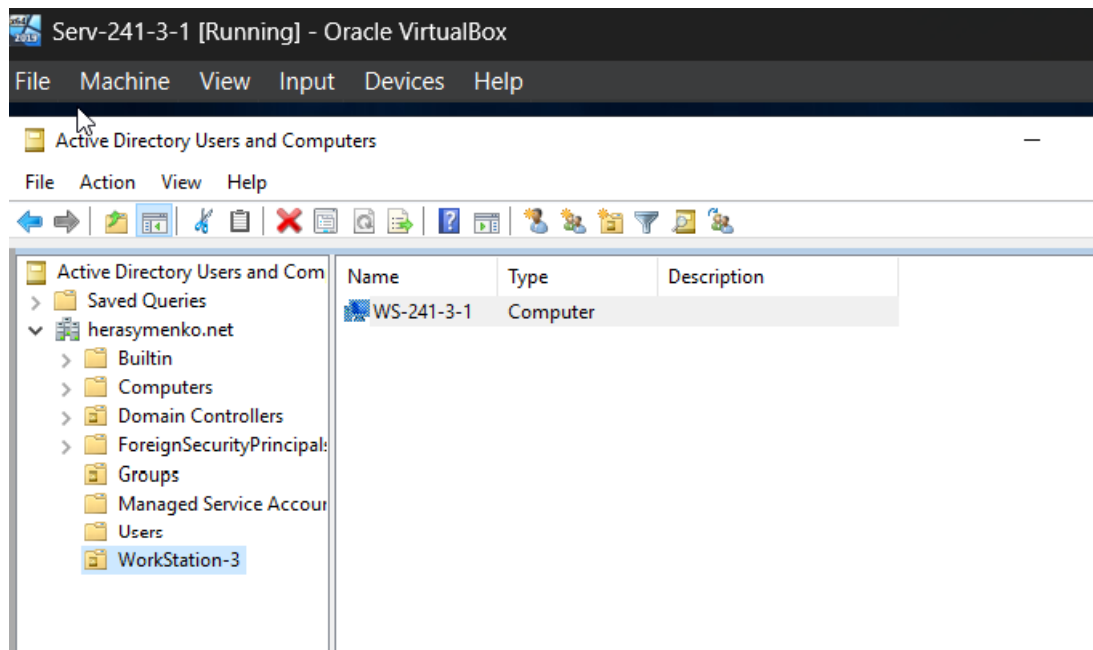


Рисунок 3.31 – Створений OU WorkStation-5 і переміщена робоча станція.

Для розмежування користувачів по відповідним групам, необхідно додати кожному з них членство в тій чи іншій групі, яка співпадає з його професійними інтересами.

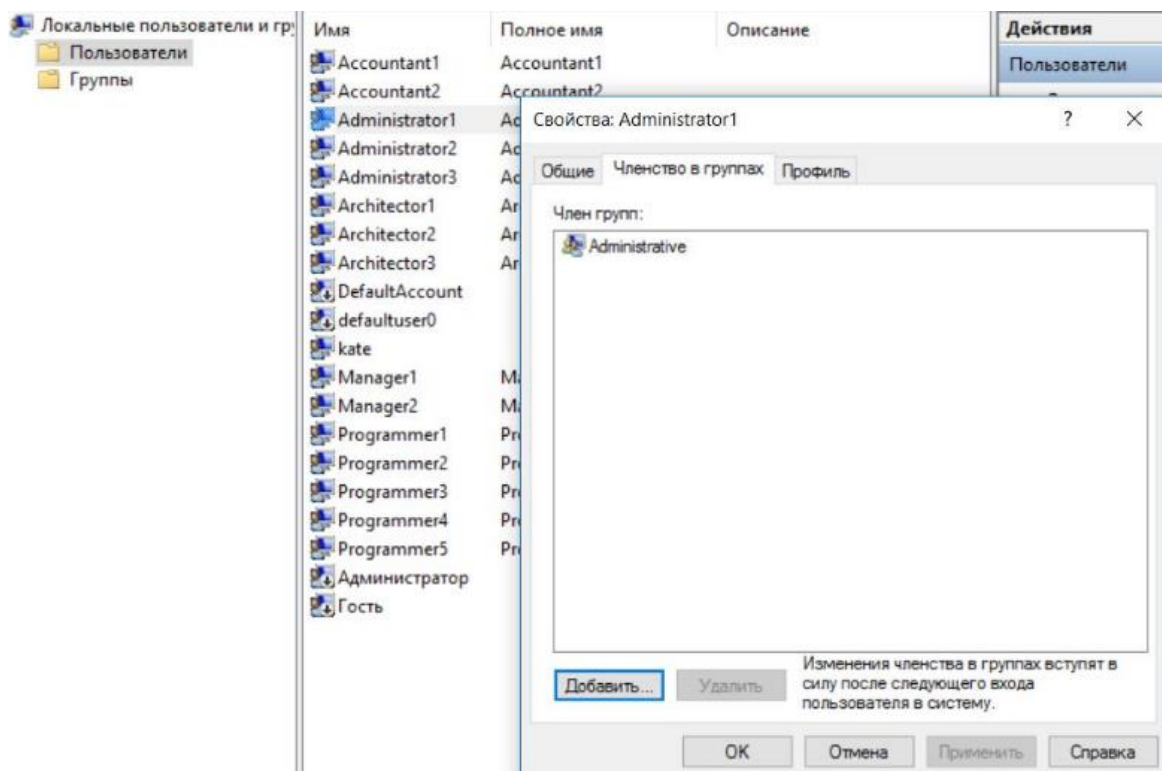


Рисунок 3.32 – Членство в групах користувача.

Для початку встановлення деяких заборон, необхідно відкрити перелік усіх можливостей редактору групової політики, саме в розділі 37 конфігурація користувача. При натисканні на обрану функцію, відображається її короткий опис для кращого розуміння функціональності. На рисунку нижче зображено вигляд вікна з функціями та можливостями групової політики.

Рисунок 3.33 – Вигляд вікна з функціями та можливостями групової політики.

Висновки з розділу 3

Обґрунтовано вибір технологічного стека, що включає в себе рішення класу ZTNA (Zero Trust Network Access). Що дало змогу не використовувати

традиційні VPN-шлюзи, та впроваджувати системи адаптивної автентифікації (РАМ). Це забезпечило перевірку не лише облікових даних користувача, а також стан безпеки кінцевого пристрою в режимі реального часу. Застосовано методи мікросегментації мережі, що дозволило значно обмежити можливість «переміщення» (lateral movement) злоумисника всередині комп'ютерної системи. Впровадження периметрів знизило залежність критичних корпоративних сервісів від несанкціонованого доступу. Також, проведено оцінку ефективності запропонованих рішень, яка допомогла знизити ризик несанкціонованого доступу до важливих даних.

ВИСНОВКИ

У ході виконання випускної кваліфікаційної роботи спроектовано наочну корпоративну комп'ютерну мережу. Комп'ютерну інфраструктуру реалізовано за допомогою емулятора комп'ютерних середовищ Oracle VirtualBox. Також було проаналізовано рішення проблеми безпеки та вразливості корпоративних мереж.

У першому розділі було сформовано теоретичні відомості щодо ідеї застосування методології Zero Trust. У першому підрозділі було розглянуто основи побудови та принцип функціонування принципів нульової довіри (Zero Trust). Було опрацьовано недоліки застосування методології у корпоративних мережах. Описано принципи функціонування комп'ютерних мереж з впровадженою системою Zero Trust. У результаті аналізу специфіки моделі мережі Zero Trust було сформоване уявлення про основні принципи роботи, умови безпеки, головні політики доступу. Встановлено, що доступ до ресурсів визначається динамічною політикою, включаючи спостережуваний стан ідентифікації клієнта, програми/сервісу та активного середовища і може включати інші атрибути доступу. Визначено необхідність впровадження політики Zero Trust в сучасних корпоративних мережах з подальшим забезпеченням систематизованого адміністрування мережі.

У другому розділі було створено обліковий запис на платформі Springer Nature Link з метою проведення аналізу допоміжних середовищ розширення моделі Zero Trust. Отримана інформація, про протоколи подібні протоколу RADIUS та системи RADIUS, RADIUS. Кожен протокол з даної сфери застосування було розглянуто детально з поглибленим вивченням всіх аспектів кібербезпеки в цілому. Таким чином були детально представлені сервіси розширеного захисту даних.

В ході вивчення теоретичних матеріалів було встановлено, що наявність середовища RADIUS надає адміністраторам корпоративних мереж можливість уникнути застосування додаткових серверів зберігання облікових даних.

Таким чином, зменшуючи ризик їх крадіжки або втрати. Але також було встановлено, що наявність РАМ-сервера, що зберігає головні паролі системи перетворює його в головну мішень для взлому.

Другий розділ сформулював чітке практичне уявлення налаштування, створення та підбору допоміжних протоколів для розробки корпоративної мережі з впровадженою технологією Zero Trust, що буде реалізовуватись та розгортатись в наступному розділі.

У третьому розділі здійснено вибір відповідного програмного продукту серверної інфраструктури обладнання мережі. Було налаштовано мережу у відповідності до проекту та перевірено правильність функціонування реалізованої технології. Було проведено практичну реалізацію та оцінку ефективності методів архітектури Zero Trustc (нульової довіри) для захисту корпоративної інфраструктури. Обґрунтовано вибір технологічного стека, що включає в себе рішення класу ZTNA (Zero Trust Network Access). Що дало змогу не використовувати традиційні VPN-шлюзи, та впроваджувати системи адаптивної автентифікації (РАМ). Це забезпечило перевірку не лише облікових даних користувача, а також стан безпеки кінцевого пристрою в режимі реального часу. Застосовано методи мікросегментації мережі, що дозволило значно обмежити можливість «переміщення» (lateral movement) зловмисника всередині комп'ютерної системи. Впровадження периметрів знизило залежність критичних корпоративних сервісів від несанкціонованого доступу. Також, проведено оцінку ефективності запропонованих рішень, яка допомогла знизити ризик несанкціонованого доступу до важливих даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gilman, E., & Barth, B.: Zero Trust Networks: Building Secure Systems in Untrusted Networks. O'Reilly Media, 2017. 205 с.
2. Garbis, J., & Chapman, J. W.: Zero Trust Security: An Enterprise Guide. Apress, 2021. 54 с.

3. Kindervag, J.: Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research, 2015. 355 с.
3. George Finney: Project Zero Trust, 2017. 197 с.
4. NIST Special Publication 800-207: Zero Trust Architecture, 2010. 81 с.
5. Cloud Security Alliance (CSA): Software-Defined Perimeter (SDP) Architecture Guide, 2018. 266 с.
6. Okta: The Ultimate Guide to Zero Trust, 2011. 115 с.
7. Palo Alto Networks: The Strategy to Stop Cyberattacks, 2016. 283 с.
8. Forrester Research: The Definition of Zero Trust, 2021. 217 с.
9. ACM Digital Library: Zero Trust Architecture Cloud Computing, 2022. 191 с.
10. C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS), 2015. 139 с.
11. Jason Garbis, Jerry W. Chapman Zero Trust Security An Enterprise Guide, 2021, 246 с.
12. Enterprise resource planning [Электронный ресурс] - Режим доступа: http://en.wikipedia.org/wiki/Enterprise_resource_plannin
13. List of ERP vendors [Электронный ресурс] - Режим доступа: http://en.wikipedia.org/wiki/List_of_ERP_vendors
14. ASP.NET Overview [Электронный ресурс] - Режим доступа: <http://msdn.microsoft.com/en-us/library/4w3ex9c2.aspx>
15. Overview of ADO.NET [Электронный ресурс] - Режим доступа: [http://msdn.microsoft.com/en-us/library/h43ks021\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/h43ks021(VS.71).aspx)
16. Silverlight Architecture [Электронный ресурс] - Режим доступа: [http://msdn.microsoft.com/en-us/library/bb404713\(VS.95\).aspx](http://msdn.microsoft.com/en-us/library/bb404713(VS.95).aspx)

17. WCF RIA Services [Электроний ресурс] - Режим доступа:
<http://www.silverlight.net/getstarted/riaservices/>
18. Microsoft Silverlight [Электроний ресурс] - Режим доступа:
http://en.wikipedia.org/wiki/Silverlight#Silverlight_4
19. Pollitt A., Sampat M. Kubernetes Security and Observability: A Holistic Approach to Securing and Troubleshooting Cloud Native Applications. O'Reilly Media, Incorporated, 2021. 165 с.
20. Binnie C., McCune R. Cloud Native Security. Wiley & Sons, Limited, John, 2021. 336 с.
21. Grasso L., Degioanni L. Practical Cloud Native Security with Falco: Risk and Threat Detection for Containers, Kubernetes, and Cloud. O'Reilly Media, Incorporated, 2022. 127 с.
22. Pollitt A., Sampat M. Kubernetes Security and Observability: A Holistic Approach to Securing and Troubleshooting Cloud Native Applications. O'Reilly Media, Incorporated, 2021. 165 с.

ДОДАТКИ

Конфігурації та лістинги пристроїв мережі

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#hostname SW-9-3-1
```

```
SW-9-3-1(config)#no ip domain-lookup
```

```
SW-9-3-1(config)#interface FastEthernet 0/3
```

```
SW-9-3-1(config-if)#description LINK-TO-SW-9-3-2
```

```
SW-9-3-1(config-if)#duplex half
```

```
SW-9-3-1(config-if)#speed 100
```

```
SW-9-3-1(config-if)#exit
```

```
SW-9-3-1(config)#exit
```

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#hostname SW-9-3-2
```

```
SW-9-3-2(config)#no ip domain-lookup
```

```
SW-9-3-2(config)#interface FastEthernet 0/24
```

```
SW-9-3-1(config-if)#description LINK-TO-SW-9-20-1
```

```
SW-9-3-1(config-if)#duplex half
```

```
SW-9-3-1(config-if)#speed 100
```

```
SW-9-3-1(config-if)#exit
```

```
SW-9-3-1(config)#exit
```

```
SW-9-3-2>enable
```

```
SW-9-3-2#configure terminal
```

```
SW-9-3-2(config)#interface FastEthernet 0/21
SW-9-3-2(config-if)#description LINK-TO-R-9-3-1
SW-9-3-2(config-if)#duplex full
SW-9-3-2(config-if)#speed 100
SW-9-3-2(config-if)#exit
SW-9-3-2(config)#exit
```

```
Router#enable
Router#configure terminal
Router(config)#hostname R-9-3-1
R-9-3-1(config)#interface FastEthernet 0/0
R-9-3-1(config-if)#description LINK-T0-SW-9-3-2
R-9-3-1(config-if)#duplex full
R-9-3-1(config-if)#speed 100
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
```

```
SW-9-3-1>enable
SW-9-3-1#clock set 11:06:10 may 05 2024
SW-9-3-1#configure terminal
SW-9-3-1 (config)#clock timezone EET 2
SW-9-3-1 (config)#clock summertime EET reccuring last Monday may 3:00 last
monday march 3:00
SW-9-3-1 (config)#banner motd
# Connection to SW-9-3-1#
```

```
SW-9-3-1>enable
```

```
SW-9-3-1#configure terminal
SW-9-3-1 (config)#service password-encryption
SW-9-3-1(config)#enable secret adminpass9
SW-9-3-1 (config)#line vty 0 4
SW-9-3-1 (config-line)#password adminpass1
SW-9-3-1 (config-line)#login
SW-9-3-1 (config-line)#transport input telnet
SW-9-3-1 (config-line)#logout-warning 30
SW-9-3-1 (config-line)#absolute-timeout 10
SW-9-3-1 (config-line)#logging synchronous
SW-9-3-1 (config-line)#exit
SW-9-3-1 (config)#exit
```

```
SW-9-3-2>enable
SW-9-3-2#clock set 10:50:30 may 03 2024
SW-9-3-2#configure terminal
SW-9-3-2(config)#clock timezone EET 2
SW-9-20-2(config)#clock summertime EET reccuring last Monday may 3:00 last
monday march 3:00
SW-9-3-2(config)#banner motd # Connection to SW-9-3-2#
```

```
SW-9-3-2>enable
SW-9-3-2#configure terminal
SW-9-3-2(config)#username admin20 privilege 15 secret adminpass20
SW-9-3-2(config)#username technic20 privilege 1 secret technicpass20
SW-9-3-2(config)#enable secret adminpass9
SW-9-3-2(config)#ip domain-name mynet.net
```

SW-9-3-2(config)#crypto key generate rsa general-keys modulus 1344

SW-9-3-2(config)#ip ssh version 1

SW-9-3-2(config)#line vty 0 4

SW-9-3-2(config-line)#login local

SW-9-3-2(config-line)#transport input ssh

SW-9-3-2(config-line)#transport output ssh

SW-9-3-2(config-line)#logout-warning 30

SW-9-3-2(config-line)#absolute-timeout 10

SW-9-3-2(config-line)#logging synchronous

SW-9-3-2(config-line)#exit

SW-9-3-2(config)#exit

SW-9-3-2>enable

SW-9-3-2#configure terminal

SW-9-3-2 (config)#login block-for 150 attempts 5 within 5

SW-9-3-2(config)#login delay 10

SW-9-3-2(config)#login on-failure log

SW-9-3-2(config)#login on-success log

SW-9-3-2(config)#ip ssh time-out 20

SW-9-3-2(config)#ip ssh authentication-retries 5

SW-9-3-2 (config)#ip ssh maxstartups 5

SW-9-3-2(config)#ip ssh logging events

SW-9-3-2(config)#exit

SW-9-3-2 #exit

R-9-3-1>enable

R-9-3-1#clock set 11:13:10 may 25 2024

R-9-3-1#configure terminal

R-9-3-1(config)#clock timezone EET 2

R-9-3-1 (config)#clock summertime EET reccuring last Monday may 3:00 last
monday march 3:00

R-9-3-1 (config)#banner motd

Connection to R-9-3-1#

Комутатор SW-9-3-1 (Інтерфейс vlan1)

MAC-адреса: 0019.AADB.56C0

Значення біту G/L змінюємо на 1: 00000010

Старший байт після зміни у шістнадцятковому форматі: 02₁₆

Формуємо номер вузла: 0219:AAFF:FEDB:56C0

Номер мережі: FE80:0000:0000:0000::

IP-адреса версії 6 має вигляд:

у основному форматі: FE80:0000:0000:0000:0219:AAFF:FEDB:56C0/64

у скороченому форматі: FE80::219:AAFF:FEDB:56C0/64