МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему

«Система кіберзахисту інформаційно-телекомунікаційних систем комерційного підприємства для забезпечення віддаленої роботи користувачів»

Завідувач

випускової кафедри **Любчак В.О.**

Керівник роботи **Кальченко В.В.**

Студентки групи КБ-81-0 **Коломієць Н.О.**

СУМИ 2022

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____

Зав. кафедрою Любчак В.О.

“_____” _____2022 р.

ЗАВДАННЯ

до випускної роботи

Студентки четвертого курсу, групи КБ-81-0 спеціальності «Кібербезпека» денної форми навчання Коломієць Надії Олександрівни.

Тема: «Система кіберзахисту інформаційно-телекомунікаційних систем комерційного підприємства для забезпечення віддаленої роботи користувачів»

Затверджена наказом по СумДУ

№_____ від _____2021 р.

Зміст пояснювальної записки: 1) Аналіз предметної області 2) Методи кіберзахисту інформації при організації віддаленого доступу до інформаційно-телекомунікаційних систем 3) Розробка комплексного підходу до забезпечення кіберзахисту інформаційно-телекомунікаційної системи комерційного підприємства для забезпечення віддаленої роботи користувачів.

Дата видачі завдання “_____”_____2022 р.

Керівник випускної роботи _____ Кальченко В.В.

Завдання прийняла до виконання _____ Коломієць Н.О.

РЕФЕРАТ

Записка: 70 стор., 50 рис., 13 джерел.

Мета роботи — аналіз методів кіберзахисту інформаційно-комунікаційної системи комерційного підприємства та їх практичне застосування.

Об'єкт дослідження — система кіберзахисту інформаційно-комунікаційної системи комерційного підприємства.

Предмет дослідження – сукупність методів та заходів програмно-технічного характеру, які дозволять забезпечити кіберзахист інформаційно-комунікаційної системи при організації віддаленої роботи користувачів.

Методи дослідження — методи та технології оцінки кіберзахищеності інформаційно-комунікаційних систем.

Результати — проаналізовано сучасні методи, програмні та апаратні засоби для організації захищеної роботи інформаційно-комунікаційної системи комерційного підприємства, запропоновано комплексний підхід до забезпечення кіберзахисту клієнтської та серверної частини інформаційно-комунікаційної системи комерційного підприємства при організації віддаленої роботи користувачів.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, КІБЕРЗАХИСТ, КІБЕРБЕЗПЕКА, ВІДДАЛЕНИЙ ДОСТУП, ВІДДАЛЕНИЙ РОБОЧИЙ СТІЛ, КОМЕРЦІЙНЕ ПІДПРИЄМСТВО, REMOTE DESKTOP PROTOCOL, WINDOWS

ЗМІСТ

ВСТУП

Праця є невід'ємним атрибутом повсякденності будь якого дорослого чоловіка чи жінки і займає визначну роль у житті кожної людини. Адже джерело доходу являє собою ключ до можливостей, як всередині компанії так і за її межами.

Події останніх декількох років, а саме епідемії та війни заставили людство переглянути підходи до організації трудового процесу. Віддалений формат роботи дозволив людям виконувати певні операції не знаходячись фізично на своєму робочому місці.

Проте нові можливості створили нові кіберзагрози для інформаційно-комунікаційних систем підприємств. Кожен день наймогутніші та найбільші технологічні компанії стикаються з проблемами кібербезпеки. При цьому технічний рівень кібератак постійно удосконалюється, а кіберзлочинці знаходять все більш і більш витончені способи здійснення цих атак. Всі ці причини заставляють підприємства впроваджувати нові системи кіберзахисту та підходи до забезпечення до інформаційної безпеки в цілому.

Масовий та спішний перехід компаній на віддалені режими роботи суттєво загострив проблеми інформаційної безпеки. Більшість компаній вперше зіткнулися з таким завданням, тому перехід на віддалену роботу викликав у них чимало складнощів. Причини переходу на віддалену роботу – породили безліч загроз і можливостей для кібератак, багато із них спричинені різними факторами, зокрема найнебезпечнішим – людським.

Варто відзначити ймовірність витоків даних і поширення шкідливого ПЗ, оскільки багато співробітників підключаються до мережі організації з використанням особистих ПК. У період дистанційної роботи захист особистих пристроїв співробітників став актуальним як ніколи раніше.

Ще один небезпечний варіант - персональний комп'ютер зі застарілою операційною системою або піратською версією ОС, яка не оновлюється. Багато користувачів будинку не стежать за оновленням прошивки роутерів,

використовуючи стандартні паролі та в більшості випадків не використовують ліцензійні антивірусні засоби. Вони ж, як правило, найбільш схильні до фішингових компаній зловмисників з використанням соціальної інженерії.

Наступний фактор ризику – масове використання громадських хмарних послуг. Далеко не всі компанії придбали комерційні підписки, а використання безкоштовної персональної підписки, що часто не гарантує ні збереження даних, ні їх конфіденційності.

Віддалений доступ підвищує попит технології багатофакторної автентифікації. Така автентифікація з використанням сертифікатів, токенів (фізичних/програмних) та з вірно налаштованими груповими політиками Active Directory вирішує проблему несанкціонованого доступу до інформації.

Стандартна пара логін-пароль вже давно вважається небезпечною, особливо під час автентифікації на корпоративному ресурсі, доступному з Інтернету. У той же час VPN не завжди зручний для звичайних користувачів, тому IT-служби забезпечують можливість співробітникам звертатися до корпоративних сервісів без VPN, що потребує більш надійної автентифікації, що дозволяє працювати як з ОС, так і з мобільних пристроїв.

Правильне визначення методів організації роботи та якісне налаштування віддаленого робочого доступу – є запорукою безпеки інформації та будь-яких даних компанії. Отже тема даної роботи повністю відображає рівень її актуальності.

1. АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІДДАЛЕНОЇ РОБОТИ КОРИСТУВАЧІВ В КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

1.1 Роль RDS в операційній системі Windows Server

Служби віддаленого робочого столу (RDS) — це загальний термін для функцій Microsoft Windows Server, які дозволяють користувачам віддалено отримувати доступ до графічних робочих столів і програм Windows.

Користувачі можуть отримати доступ до настільних комп'ютерів і програм, також відомих як Microsoft RemoteApp, з різних типів клієнтських програм і пристроїв, у тому числі пристроїв, що не є Windows, за допомогою протоколу віддаленого робочого столу (RDP) Microsoft.

IT може реалізувати служби віддаленого робочого столу, використовуючи кілька екземплярів Windows Server, які виконують різні ролі.

Основною роллю робочого навантаження, в якій розміщуються робочі столи та програми Windows, є хост сеансів віддаленого робочого стола (RDSH). RDSH містить можливості спільного доступу на основі сеансів, які дозволяють кільком користувачам одночасно отримувати доступ до робочих столів і програм на одному екземплярі Windows Server.

Ролі інфраструктури служб віддаленого робочого столу, реалізовані в Windows Server, включають посередника підключення до RD, шлюз RD, ліцензування RD і веб-доступ до RD.

Служби віддаленого робочого столу доступні в Windows Server 2019, однак деякі функції обмежені. Windows Server Desktop Experience і RDSH не включають нові функції, такі як Microsoft Cortana, Microsoft Store і додаток і служби Xbox. Крім того, RDSH 2019 не підтримуватиме Office 365 Pro Plus і замість цього використовуватиме лише Office 2019 perpetual.

Вузол сеансів віддалених робочих столів розміщує програми на основі сеансів та робочі столи, до яких ви надали користувачам спільний доступ. Користувачі отримують доступ до цих робочих столів та програм за допомогою

одного з клієнтів віддаленого робочого столу для Windows, MacOS, iOS або Android. Користувачі також можуть підключатися за допомогою браузера, що підтримується, завдяки веб-клієнту.

Робочі столи та програми можна впорядкувати в один сервер вузла сеансів віддалених робочих столів або кілька; це звані колекції. Ви можете налаштувати ці колекції для конкретних груп користувачів у межах кожного клієнта. Наприклад, можна створити колекцію, де певна група користувачів має доступ до конкретних програм, але будь-який інший користувач, який не входить до групи, яку ви виділили, не зможе отримати доступ до цих програм.

Колекції можна розширювати, додаючи віртуальні машини сервера вузла сеансів віддалених робочих столів у ферму і призначаючи для кожної віртуальної машини вузла в колекції ту саму групу доступності. Це забезпечує більш високий рівень доступності колекції та збільшує її масштаб для підтримки кількох користувачів або програм з великим навантаженням на ресурси.

У більшості випадків кілька користувачів використовують один і той самий сервер вузла сеансів віддалених робочих столів, що дозволяє найефективніше витрачати ресурси Azure для вирішення розміщення робочих столів. У цій конфігурації користувачі повинні входити до колекції з неадміністративними обліковими записами. Ви також можете надати деяким користувачам повний адміністративний доступ до їхнього віддаленого робочого столу шляхом створення колекцій робочих столів з персональними сеансами.

Для подальшого налаштування робочих столів можна створити та надіслати віртуальний жорсткий диск з ОС Windows Server, який можна використовувати як шаблон для створення нових віртуальних машин вузла сеансів віддалених робочих столів. [1]

1.2 Організація віддаленого доступу в системі Linux

Linux Ubuntu Server – це безкоштовна серверна операційна система на базі ядра Linux. Ubuntu Server можна використовувати як платформу для Web-серверів, серверів баз даних, DNS-серверів, файлових серверів та інших типів серверів. Ubuntu дуже популярний дистрибутив Linux, у тому числі і серверний варіант, який активно використовується організаціями різних розмірів, за рахунок того, що головною особливістю Ubuntu Server, та й усіх серверних операційних систем на базі Linux, є надійність, продуктивність та безпека.

Найпопулярнішим способом віддаленої роботи на Linux є Remmina.

Remmina — це клієнт для віддаленого робочого столу, написаний на GTK,

щоб використовувати інші робочі столи віддалено, з крихітного екрана або великих моніторів.

Remmina підтримує декілька мережевих протоколів в інтегрованому та узгодженому інтерфейсі користувача. Нині підтримуються такі протоколи: X2Go, RDP (протокол віддаленого робочого столу), VNC (віртуальні мережеві обчислення) і SSH (безпечна оболонка/відкритий SSH).

Зовнішні плагіни також підтримуються для додавання нових протоколів і функцій. [2]

1.3 Використання Windows Server для дослідження

Існує безліч версій операційних систем від корпорації Microsoft, але розглянемо саме Windows Server, призначену для підтримки потужних серверів на великих підприємствах. Тим часом деякі користувачі іноді встановлюють таку систему на звичайні комп'ютери, оскільки вона має розширений функціонал у порівнянні зі звичайними випусками Windows, про що далі докладніше.

Однією з головних особливостей Windows Server є можливість створення домену Active Directory на її базі, що забезпечує високу стабільність роботи і рівень безпеки в такій мережі за умови грамотного адміністрування. Тобто

будь-яка окрема робоча станція не може сильно вплинути на швидкість роботи всередині домену, а всі важливі дані зберігаються на сервері з RAID-масивом, на якому регулярно робиться резервне копіювання.

Така схема використовується в багатьох організаціях, але з недавнього часу просунуті системні адміністратори все більше стали використовувати розподілені мережі, побудовані на блокчейні, в яких будь-які операції підтверджуються делегованою групою авторитетних вузлів. Тобто при цьому відпадає можливість порушення функціонування домену шляхом атаки одного сервера зловмисниками.

Веб-сервер(IIS) дозволяє повністю контролювати інтернет трафік, а також обмежувати доступ до певних ресурсів усім комп'ютерам або окремим користувачам.

Файлові служби застосовуються для створення файлових серверів, але тут слід зазначити, що у звичайних версіях Windows також існує можливість створення папок загального доступу, проте при цьому комп'ютер, на якому зберігаються файли, повинен бути обов'язково включений для нормальної роботи.

Служби друку та документів дають можливість підключати та налаштовувати мережеву копіювальну техніку.

Служби розгортання Windows використовуються для дистанційної установки операційної системи відразу на всі або кілька комп'ютерів.

Служби Windows Server Update Services дозволяють отримувати різні оновлення за розкладом, щоб розвантажити мережу у робочий час. [3]

Тому саме ця операційна система була обрана для дослідження.

2. АНАЛІЗ ІСНУЮЧИХ ТЕХНІЧНИХ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

2.1 SoftEther VPN

SoftEther VPN — це програмне забезпечення для VPN наступного покоління, яке забезпечує стабільність, гнучкість та можливість розширення та сумісне з усіма розширеними мережами, які створюють широку пропускну спроможність із високим навантаженням, що вимагається великим корпораціям та Інтернет-провайдерам, а також мережами для окремих осіб та будинків та мереж для малих та підприємства середнього розміру.

Тунелювання та інкапсуляція

VPN — це рішення для побудови віртуальної мережі. У VPN використовується техніка під назвою «тунелювання», яка дозволяє користувачам будувати віртуальну мережу між двома віддаленими точками існуючої публічної IP-мережі та вільно спілкуватися.

За допомогою технології тунелювання пакети, що передаються на фізичному середовищі зв'язку, такому як звичайний мережевий кабель або оптичне волокно, інкапсулюються як дані іншого протоколу, наприклад пакети TCP/IP, без безпосередньої передачі у фізичній мережі. Шифрування та електронний підпис можна додати одночасно під час інкапсуляції. Інкапсульовані дані передаються через сеанс, який називається «тунелем» між початковою та кінцевою точками зв'язку VPN. Інша сторона, яка отримує інкапсульовані дані, видаляє оригінальні пакети з капсул.

Коли має здійснюватися VPN-зв'язок, оскільки дані, що передаються між комп'ютером, який надсилає дані, і комп'ютером, який отримує дані, проходять через тунель, надсилаються інкапсульованими, незахищені дані ніколи не відкриваються в мережі.

Забезпечення безпеки переданих даних за допомогою шифрування

Однією з переваг використання VPN є підвищена безпека за допомогою шифрування.

IP-мережа, до якої може отримати доступ будь-хто, наприклад Інтернет, завжди піддається небезпеці підслуховування та маскування. Навіть якщо використовуються дорогі послуги передачі та інфраструктури, такі як виділені лінії або супутникові канали, лінії можуть бути фізично прослуховані, або дані можуть бути таємно переглянуті спеціалістами комунікаційної компанії зловмисно чи з цікавості, або можуть бути прослухововані та проаналізовані урядом, і т. д. При надсиланні та отриманні даних через таку глобальну мережу рекомендується, щоб дані були зашифровані якимось чином.

Безпека може бути значно підвищена за рахунок автоматичного шифрування зв'язку майже всіх програм за допомогою IP або Ethernet за допомогою VPN.

Краще підключення та незалежність від мережі

Іншою важливою перевагою використання VPN є те, що воно покращує підключення та забезпечує незалежність від мережі.

В публічних IP-мережах, таких як Інтернет, як правило, будь-який IP-пакет може бути переданий з комп'ютера з будь-якою IP-адресою на інший комп'ютер з будь-якою IP-адресою. Якщо дані мають передаватися через Інтернет, коли зв'язок має здійснюватися між клієнтським комп'ютером і комп'ютером-сервером, серверний комп'ютер може фактично отримувати пакети від іншого комп'ютера зі зловмисним наміром. Нині вразливі операційні системи та хробаки, які відкривають діри в безпеці програмного забезпечення для передачі та серверного програмного забезпечення в Інтернеті, поширюються, і існує ймовірність зараження. Оскільки комп'ютер, який

безпосередньо під'єднаний до Інтернету, є істотно небезпечним, не рекомендується, щоб комп'ютери, які обробляють важливі комунікаційні дані для бізнесу тощо, призначали прямі глобальні IP-адреси Інтернету та підключалися до Інтернету.

Замість виділеної лінії можна використовувати недороге підключення до Інтернету

Використовуючи структуру VPN, як описано раніше, без використання послуг виділеної лінії, які використовуються для стягнення високої плати за використання, з більш надійною безпекою, ніж служби виділеної лінії, зв'язок може здійснюватися між комп'ютерами будь-якої бази через Інтернет.

Використовуючи VPN, загальнодоступні мережі, за допомогою яких будь-які комп'ютери можуть вільно спілкуватися через IP Інтернет. Він може створити спеціалізовану віртуальну комунікаційну мережу компанії в цій мережі, а також безпечну та стабільну незалежну мережу, яку можна побудувати, не турбуючись про небезпеку Інтернету.

Труднощі проходження пристроїв мережевого шлюзу

Багато домашніх і бізнес-приватних мереж відокремлені від Інтернету мережевим шлюзом, таким як NAT (IP-маскарад), проксі-серверами та брандмауерами. Такими пристроями шлюзу можуть бути спеціальні пристрої (пристрої) або високопродуктивний комп'ютер під керуванням Linux тощо. Пристрій шлюзу виконує як функції безпеки, так і обмежує кількість фактичних Інтернет-адрес, необхідних для підключення приватної мережі до Інтернету.

Обмеження протоколу, який може спілкуватися в межах VPN

Багато звичайних протоколів VPN обмежені протоколом рівня 3 (рівень IP тощо) і, крім того, протоколом верхнього рівня (рівень TCP, прикладний рівень тощо), а зв'язок здійснюється за допомогою інкапсульованого тунелювання. Однак у цій системі протокол VPN не може бути призначений

для індивідуального спілкування через VPN з протоколами, які не відповідають вимогам.

Наприклад, у багатьох випадках застарілі протоколи, такі як спеціальний протокол керування, IPX/SPX і NetBEUI, які зараз використовуються обладнанням загального призначення, не можуть використовуватися через VPN, і важко передавати наявні системні комунікації за допомогою Інтернет VPN замість виділеної лінії.

Залежність від певної платформи

Для багатьох старих протоколів VPN існує проблема, якщо діапазон платформ, які підтримують різні протоколи VPN, не дуже широкий, і навіть якщо їх можна використовувати між кількома платформами, відмінності у відповідній реалізації призвели до проблем у практичному застосуванні в деяких випадків.

Крім того, деякі протоколи VPN вимагають апаратного забезпечення певних постачальників мережевих пристроїв і сумісності протоколів між постачальниками, які відмовилися.

Висока вартість, низька продуктивність

Ціна мережевих пристроїв і програмного забезпечення безпеки, як правило, надзвичайно висока, включаючи рішення мережевої безпеки, відмінні від рішень VPN. Проте, реально, продукти мережевої безпеки, що випускаються за високою ціною, часто не задовольняють вимогам до продуктивності та функцій.

Особливості SoftEther VPN

Великою перевагою SoftEther VPN є те, що він дуже просто долає обмеження старих рішень VPN.

SoftEther VPN здійснює інкапсуляцію та тунелювання на рівні 2, іншими словами Ethernet. Коли використовується SoftEther VPN, мережеві пристрої, такі як звичайні мережеві адаптери, комутаційний концентратор і комутація рівня 3, реалізуються програмно. Використовуючи SoftEther VPN, користувач створює дуже гнучкий, безпечний тунель на основі широко доступного та легкого протоколу TCP/IP.

Переваги створення віртуального Ethernet

На відміну від багатьох старих протоколів VPN, SoftEther VPN націлений на рівень 2 (Ethernet) для зв'язку VPN. Іншими словами, з VPN, націленим на старий рівень 3, інкапсульовані IP-пакети протікали через тунель. Але з SoftEther VPN, інкапсульовані пакети Ethernet будуть протікати через тунель.

Як згадувалося раніше, SoftEther VPN використовує протокол TCP/IP тільки для зв'язку VPN, і будь-які кадри Ethernet можна тунелювати. Коли здійснюється зв'язок VPN, SoftEther VPN шифрує всі дані за допомогою стандартного протоколу шифрування Інтернету, який називається безпечним рівнем сокетів (SSL). На даний момент системний адміністратор може використовувати будь-який алгоритм шифрування з алгоритму електронного підпису, який вибирає адміністратор.

Завдяки SoftEther VPN не лише шифрується зв'язок, але й підвищується безпека щодо автентифікації користувачів та серверної аутентифікації. SoftEther VPN підтримує автентифікацію користувачів за допомогою серверів RADIUS, які використовуються компаніями, домену NT / Active Directory та аутентифікації сертифікатів за допомогою X509 і RSA. Також підтримує деякі смарт-картки, які використовуються для цілей, які вважаються необхідними для високої безпеки.

Протокол, який використовувався для передачі пакетів зв'язку VPN і перевірок безпеки, таких як автентифікація користувача, що фактично протікає через фізичну IP-мережу під час зв'язку VPN, називається протоколом SoftEther

VPN. Протокол SoftEther VPN не тільки шифрує весь комунікаційний вміст за допомогою SSL, але він встановлює кілька одночасних з'єднань SSL, встановлених між VPN-сервером і VPN-клієнтом або з VPN Bridge. Крім того, змінюючи час на певний інтервал і повторно підключаючись, він може стабільно спілкуватися через деякі спеціальні мережеві пристрої, завдяки чому з'єднання TCP/IP, яке втрачено протягом певного інтервалу часу. Стабільний VPN-зв'язок також може здійснюватися за допомогою телефонних ліній з високою швидкістю втрат пакетів, деяких ADSL, PHS, бездротової локальної мережі тощо.

З SoftEther VPN програмне забезпечення VPN-сервера, VPN-клієнта тощо оснащено надзвичайно розширеними функціями. Наприклад, наведені нижче функції можна легко налаштувати та використовувати для обмеження зв'язку VPN, адміністрування мережі чи інших цілей.

- Гнучка настройка параметрів зв'язку протоколу SoftEther VPN
- Реєстрація журналу операцій VPN або вмісту деяких пакетів
- Розширені функції безпеки
- Моніторинг зв'язку VPN
- Обробка великих середовищ за допомогою кластеризації
- Гнучка аутентифікація користувача
- Функція перемикання рівня 3, функція віртуального NAT і віртуального сервера DHCP
- Автоматизація адміністрування
- інші

SoftEther VPN наразі підтримує різні типи операційних систем і комбінацій ЦП, тому може працювати на різних платформах. За винятком кількох обмежень, SoftEther VPN працює однаково без залежності від типу процесора або платформи, наприклад Windows, Linux, FreeBSD, Solaris і Mac OS X.

Програмний код SoftEther VPN написаний на дуже взаємозамінному C і запрограмований так, щоб не залежати від певної операційної системи. SoftEther VPN наразі підтримує операційне середовище, зазначене в Специфікаціях, але в майбутньому буде підтримувати ще більше операційних систем і апаратного забезпечення процесора. Також полегшує інтеграцію мережевих пристроїв, таких як маршрутизатори та брандмауери.

SoftEther VPN, які працюють у різних середовищах, також можуть бути надійно з'єднані один з одним через Інтернет. Таким чином, якщо ви створюєте VPN, що використовує SoftEther VPN, коли кількість систем або пристроїв, які підтримують SoftEther VPN, збільшиться, здатність взаємного підключення буде технічно підтримуватися з системами. [4]

2.2 Firewall

Firewall є програмно-апаратним або програмним комплексом, який відстежує мережеві пакети, блокує або дозволяє їх проходження. У фільтрації трафіку брандмауер спирається на встановлені параметри найчастіше їх називають правилами мережевого екрану.

Сучасні міжмережові екрани (далі МЕ) розміщуються на периферії мережі, обмежують транзит трафіку, встановлення небажаних з'єднань та подібні дії за рахунок засобів фільтрації та аутентифікації.

Головне завдання МЕ – це фільтрація трафіку між зонами мережі. Він може використовуватися для розмежування прав доступу до мережі, захисту від сканування мережі компанії, проведення мережевих атак. Простіше кажучи, міжмережевий екран - це один із пристроїв, за допомогою якого забезпечується мережна безпека компанії.

Функції міжмережевого екрану

Уявимо, що ваша компанія обмінюється даними з одним із своїх підрозділів, при цьому ваші IP-адреси відомі. Зловмисник може спробувати

замаскувати свій трафік під дані офісу, але надіслати його з іншого IP. Брандмауер виявить заміну і не дасть йому потрапити всередину вашої мережі.

Захистит корпоративної мережі від DDoS-атак. Тобто ситуацій, коли зловмисники намагаються вивести з ладу ресурси компанії, надсилаючи їм безліч запитів із заражених пристроїв. Якщо система вміє розпізнавати такі атаки, вона формує певну закономірність і передає її брандмауер для подальшої фільтрації зловмисного трафіку.

Блокування передачі даних на невідому IP-адресу. Допустимо, співробітник фірми завантажив шкідливий файл і заразив свій комп'ютер, що призвело до витоку корпоративної інформації. При спробі вірусу передати інформацію на невідому IP-адресу, брандмауер автоматично зупинить це.

Правила МЕ

Мережний трафік, що проходить через брандмауер, зіставляється з правилами, щоб визначити, чи пропускати його.

Правило міжмережевого екрану складається з умови (IP-адреса, порт) та дії, яку необхідно застосувати до пакетів, що підходять під задану умову. До дій належать команди дозволити (accept), відхилити (reject) та відкинути (drop). Ці умови вказують МЕ, що саме потрібно зробити з трафіком:

- дозволити - пропустити трафік;
- відхилити - не пропускати трафік, а користувачеві видати повідомлення помилку «недоступно»;
- відкинути — заблокувати передачу і не видавати повідомлення у відповідь.

Типи міжмережевих екранів

Апаратний МЕ – це, як правило, спеціальне обладнання, складові якого (процесори, плати тощо) спроектовані спеціально для обробки трафіку.

Працює на спеціальному ПЗ – це необхідно для збільшення продуктивності обладнання. Прикладами апаратного міжмережевого екрану є такі пристрої, як Cisco ASA, FortiGate, Cisco FirePower, UserGate та інші.

Апаратні МЕ потужніші в порівнянні з програмними, проте це впливає на вартість рішень. Нерідко вона в рази вища, ніж у програмних аналогів.

Програмний МЕ – це програмне забезпечення, яке встановлюється на пристрої, реальні або віртуальні.

Через такий міжмережевий екран перенаправляється весь трафік усередину робочої мережі. До програмних належать брандмауер у Windows та iptables у Linux.

Програмні МЕ, як правило, дешевші і можуть встановлюватися не тільки на межах мережі, а й на робочих станціях користувачів. З основних недоліків - нижча пропускна здатність і складність налаштування в ряді випадків.

Міжмережевий екран з контролем стану сеансів аналізує всю активність користувачів від початку і до кінця - кожної встановленої сесії користувача. На основі цих даних він визначає типову та нетипову поведінку користувача. Якщо поведінка у рамках сесії здалася йому нетиповою, МЕ може заблокувати трафік.

Unified threat management, або універсальний шлюз безпеки

Такі міжмережеві екрани включають антивірус, брандмауер, спамфільтр, VPN і систему IDS/IPS (системи виявлення і запобігання вторгнень), контроль сеансів.

Основна перевага цієї технології в тому, що адміністратор працює не з парком різних пристроїв, а використовує єдине рішення. Це зручно, тому що виробник передбачає централізований інтерфейс управління службами, політиками, правилами, а також дає можливість більш тонкого налаштування обладнання.

У UTM-пристрій входять кілька видів процесорів:

- процесор загального призначення, або центральний процесор,
- процесор обробки даних,
- мережевий процесор,
- процесор обробки політик безпеки.

Процесор загального призначення нагадує процесор, встановлений у звичайному ПК. Він виконує основні операції на міжмережевому екрані. Інші види процесорів покликані знизити навантаження нього.

Процесор даних відповідає за обробку підозрілого трафіку та порівняння його з вивченими загрозами. Він прискорює обчислення, що відбуваються на рівні додатків, а також виконує завдання антивірусу та служб запобігання вторгненням.

Мережевий процесор призначений високошвидкісної обробки мережевих потоків. Основне завдання полягає в аналізі пакетів та блоків даних, трансляції мережевих адрес, маршрутизації мережевого трафіку та його шифруванні.

Процесор обробки політик безпеки відповідає за виконання завдань антивірусу та служб запобігання вторгненням. Також він розвантажує процесор загального призначення, опрацьовуючи складні обчислювальні завдання.

Антивірус. Забезпечує захист від вірусів та шпигунського ПЗ у реальному часі, визначає та нейтралізує шкідливість на різних платформах

Фільтрування по URL, або веб-фільтр, — можливість блокування доступу до сайтів або інших веб-застосунків за ключовим словом в адресі.

Інспектування SSL. Дозволяє міжмережевому екрану нового покоління встановлювати SSL-сесію з клієнтом та сервером. Завдяки цьому існує можливість переглядати шифрований трафік та застосовувати до нього політики безпеки.

Антиспам – функція, яка дозволяє захистити корпоративних користувачів від фішингових та небажаних листів

Application Control. Використовується для обмеження доступу до програм, їх функцій або цілих категорій програм. Все це задіяє функції відстеження стану програм, запущених користувачем, як реального часу.

Web Application Firewall — сукупність правил та політик, спрямованих на запобігання атакам на веб-додатки

Аутентифікація користувачів — це можливість настроювати індивідуальні правила під кожного користувача або групу.

Sandboxing. Метод, при якому файл автоматично поміщається в ізольоване середовище для тестування, або так звану пісочницю. У ній можна ініціалізувати виконання підозрілої програми або перехід URL, який зловмисник може прикріпити до листа. Пісочниця створює безпечне місце для встановлення та виконання програми, не наражаючи на небезпеку решту системи.

Ізольований захист дуже ефективний у роботі з так званими загрозами нульового дня. Це загрози, які раніше були помічені чи відповідають жодному відомому шкідливому ПЗ. Незважаючи на те, що звичайні фільтри електронної пошти можуть сканувати електронні листи для виявлення шкідливих відправників, типів файлів та URL-адрес, загрози нульового дня виникають постійно. Традиційні засоби фільтрації можуть пропустити.

Основною функцією класичного брандмауера є відстеження та фільтрація трафіку на мережевому та транспортному рівнях моделі OSI. На відміну від нього проксі-сервер встановлює зв'язок між клієнтом та сервером, тим самим дозволяючи проводити перевірку на прикладному рівні, фільтрувати запити на підключення тощо.

Найчастіше проксі-сервер є доповненням до стандартного міжмережевого екрану, а міжмережові екрани нового покоління вже включають всі функції проксі-сервера. [5]

2.3 BitLocker

Шифрування диска BitLocker або BitLocker — це функція безпеки та шифрування Microsoft Windows, яка включена в деякі нові версії Windows. BitLocker дозволяє користувачам шифрувати все на диску, на якому встановлено Windows, захищаючи ці дані від крадіжки або несанкціонованого доступу.

Microsoft BitLocker покращує захист файлів і системи, пом'якшуючи несанкціонований доступ до даних. Він використовує алгоритм Advanced Encryption Standard із 128- або 256-бітними ключами. BitLocker поєднує в собі процес шифрування на диску та спеціальні методи керування ключами.

BitLocker використовує спеціалізований чіп, який називається Trusted Platform Module (TPM). TPM зберігає ключі шифрування Рівеста-Шаміра-Адлемана, специфічні для хост-системи для апаратної автентифікації. TPM встановлюється оригінальним виробником комп'ютера і працює з BitLocker для захисту даних користувача.

На додаток до TPM, BitLocker також може блокувати процес запуску, доки користувач не введе PIN-код або не вставить знімний пристрій, як-от флеш-накопичувач, який має ключ запуску. BitLocker також створює ключ відновлення для жорсткого диска користувача — на випадок, якщо користувач забуде або втратить свій пароль.

Комп'ютери, на яких не встановлено TPM, все ще можуть використовувати BitLocker для шифрування дисків ОС Windows. Але для цієї реалізації потрібен ключ запуску USB, щоб увімкнути комп'ютер або вийти з

режиму глибокого сну. Однак Microsoft стверджує, що перевірка цілісності системи перед запуском є більшою, коли BitLocker поєднується з TPM.

Засоби перегляду паролів відновлення BitLocker і інструменти шифрування диска BitLocker — це два додаткові інструменти, які використовуються для керування BitLocker. Засіб перегляду паролів відновлення BitLocker дозволяє користувачам знаходити паролі відновлення BitLocker, резервні копії яких створені в доменних службах Active Directory (AD). Цей інструмент використовується для відновлення даних, що зберігаються на вже зашифрованому диску. Інструменти шифрування дисків BitLocker — це комбінація інструментів командного рядка, командлетів BitLocker для Windows PowerShell, а також manage-bde і repair-bde. Repair-bde, наприклад, використовується під час спроб аварійного відновлення, коли диски, захищені BitLocker, неможливо розблокувати звичайним шляхом або за допомогою консолі відновлення. Інструмент командного рядка Manage-bde вмикає або вимикає BitLocker. Вимкнення BitLocker розшифрує всі файли на диску, коли ці дані більше не потребують захисту.

BitLocker увімкнено за замовчуванням. Але якщо його вимкнено, користувач може перейти до рядка пошуку Windows і знайти Керування BitLocker. Якщо на пристрої встановлено BitLocker, він відображатиметься на панелі керування, а одним із варіантів є увімкнення BitLocker. Інші варіанти включають захист від призупинення, створення резервної копії ключа відновлення та вимкнення BitLocker.

Після ввімкнення BitLocker Windows починає перевірку системних налаштувань. Користувач повинен створити пароль, який потрібен щоразу, коли він отримує доступ до свого ПК або диска. Потім користувач вибирає параметри ключа відновлення. Після натискання «Далі» користувач може вибрати, яку частину свого диска він бажає зашифрувати. Параметри двотомного шифрування полягають у шифруванні лише використаного

дискового простору або шифрування всього диска. Шифрування використовуваного дискового простору стосується лише дискового простору, який містить дані, тоді як шифрування всього диска означає, що весь обсяг сховища, включаючи вільний простір, зашифровано.

Натиснувши це, користувач може запустити перевірку системи BitLocker, яка гарантує, що BitLocker може отримати доступ до ключів відновлення та шифрування до того, як щось буде зашифровано. Після перевірки системи майстер шифрування диска BitLocker перезавантажує комп'ютер, щоб почати процес шифрування кінцевої точки. Захист вмикається лише після входу користувача та реєстрації пристрою в домені AD.

Щоб розшифрувати та вимкнути BitLocker, користувачу слід шукати Керування BitLocker на панелі пошуку Windows, вибрати опцію, що з'явиться, а потім вимкнути BitLocker; розпочнеться процес розшифровки даних.

Ключ відновлення BitLocker — це 48-значний цифровий пароль, який використовується для розблокування системи користувача, коли BitLocker виявляє можливу спробу несанкціонованого доступу. Ключ служить додатковим заходом безпеки для захисту даних користувача. Windows також може запитати ключ відновлення BitLocker, якщо в апаратне, програмне або мікропрограмне забезпечення системи внесено зміни.

Якщо ключ відновлення втрачено, єдиний варіант — перевстановити Windows. Щоб уникнути цього, резервні копії ключів відновлення BitLocker можна створити в таких місцях:

- Обліковий запис Microsoft користувача. Якщо користувач увійде в обліковий запис Microsoft на іншому пристрої, він зможе переглянути свій ключ звідти.
- Флешка USB. USB-флеш-накопичувач може зберігати ключ, який можна вставити в заблокований ПК, щоб розблокувати його. Якщо ключ

зберігається як текстовий файл, користувач може підключити його до іншого ПК, щоб прочитати пароль.

- Обліковий запис користувача Microsoft Azure Active Directory (AD). Ключ може зберігатися в більшому обліковому записі Azure AD, пов'язаному з пристроєм користувача.
- Система системного адміністратора. Системний адміністратор може мати ключ відновлення, якщо пристрій користувача підключено до домену.
- Володіння користувача. Користувач, можливо, роздрукував або написав код на папері. [6]

2.4 RDP Defender

Коли ваш сервер Windows доступний і загальнодоступний в Інтернеті, на нього постійно нападають хакери, мережеві сканери та роботи грубої сили, які намагаються вкрасти вашу ідентифікацію, щоб отримати доступ до ваших особистих даних або взяти під контроль ваш комп'ютер. Щоб ефективно протистояти цій загрозі, вам потрібно встановити антишпигунське програмне забезпечення.

Як правило, в системі безпеки Windows є недолік, який дозволяє шкідливому програмному забезпеченню стежити за вашими з'єднаннями. Ці різноманітні шпигунські програми в Інтернеті дуже небезпечні для вашого сервера. Кожного разу, коли ви підключаєтеся, існує ризик того, що одне або кілька потенційно шкідливих програм буде встановлено на вашому комп'ютері без вашого відома. Це може статися, наприклад, коли ви завантажуєте веб-сторінку або клацаєте по рекламі, підозрілому вкладеному файлу в листі тощо.

Їх мета: збирати та передавати інформацію про середовище, де вони працюють. Це означає ваш комп'ютер, ноутбук, сервер, мобільний телефон тощо. Деякі з них використовуються як профайлери для збору даних для націлювання на електронну пошту. Це може заразити вашу машину й запустити

її в будь-який час неочікуваним чином, сповільнюючи продуктивність, впливаючи на споживання ЦП та пропускної спроможності.

Звісно, Windows пропонує власний Захисник, «Захисник Windows», який використовує як запобіжні, так і виправляючі методи, щоб захистити вас: попереджаючи про небажані програми, які намагаються встановити, і надає інструменти аналізу, щоб виявити їх на вашому комп'ютері та дозволити вам очистити його.

Крім того, цей ризик особливо високий, коли ви відкриваєте сеанс RDS: роботи сканують відкриті порти та намагаються вкрасти вашу ідентифікацію, щоб увійти. Кожну хвилину від сотень до тисяч комбінацій, які використовують поточні логіни та словники паролів, автоматично перевіряються. на вашому сервері через зовнішні IP-адреси.

RDP Defender, антишпигунське програмне забезпечення, встановлене на вашому комп'ютері, буде автоматично активовано щоразу, коли ви відкриваєте з'єднання RDS, і блокуватиме будь-яку атаку.

RDP Defender ефективно захищає в режимі реального часу ваш сервер RDS або ваш ПК, відстежуючи невдалі спроби входу в Windows і автоматично додаючи в чорний список IP-адреси, що порушують правила після кількох збоїв. [7]

2.5 Mikrotik

Mikrotkls Ltd – це торгова марка продуктивного підприємства Латвії, що виготовляє та продає на ринку різні маршрутизатори, операційне обладнання та інше обладнання. Заснували компанію в далекому 1995 році, головною метою якої, була робота з продажу мережевого обладнання на міжнародних торгових майданчиках. На період 2007 року компанія мала у своєму розпорядженні штат, що складається з понад 70 співробітників.

Mikrotik – складається із заліза, під загальним найменуванням RouterBoard, та операційної системи RouterOS.

Плюси mikrotik

- Ціна. У цьому співвідношенні Mikrotik немає конкурентів. Молодші моделі мають функціонал старших (RouterOS), а ціна як у «домашніх роутерів».
- Можливості. TP-Link, Dlink, Zyxell, Linksys і.т.д просто не правильно порівнювати тому що це роутери а mikrotik це повноцінний маршрутизатор який можна порівняти з Linux або Cisco. (для розуміння у mikrotik немає wan порту та lan портів тобто будь-який порт може бути будь-яким залежить від того як ви налаштуєте bridge та маршрутизацію)
- Високонадійна та стабільна робота. При проведенні тестуючих аналізів і відповідно при правильному налаштуванні, Mikrotik здатний працювати тривалий час, і при цьому зовсім не доставляти жодних проблем. Ще важливою деталлю є наявність скриптової мови, яка допомагає в налаштуваннях при будь-якій проблемі, а також наявності WatchDog (System → Watchdog прим. Якщо 8.8.8.8 не пінгується більше 5 хвилин перевантажуємо роутер.), що дозволяє уникати проблем із зайвими зависаннями роутера. Якщо вибрати собі надійне заземлення, а також ДБЖ, то можна уникнути більшу частину проблемних ситуацій. Варто відзначити, що на різних форумах дуже часто можна зустріти пости, повідомлені лагам і перебоям у роботі роутера, однак, на своєму досвіді я з цим не стикався (крім власних косяків).
- Оновлення, документація. Для отримання детальної інформації про якесь оновлення, досить просто зайти на офіційний сайт вікіпедії, де знаходяться всі прошивки. Примітно, що для скачування зовсім не потрібно бути авторизованим або зареєстрованим, на відміну від того ж Cisco, де отримання інформації - це ціла проблема (необхідний статус сертифікації і так далі).

- Скрізь використовується RouterOS. Що дозволяє доступ до швидкої зміни обладнання, відновлення на інше залізо, а також передача (або просто пропозиція у вигляді поради) іншим користувачам. (Тут є невеликий нюанс при зміні заліза з відмінною версією ОС або різною кількістю портів доведеться доналаштовувати ручками, але це не порівняти з налаштуванням всього з нуля.)
- Віртуалізація. Можливість підняти RouterOS на x86 (як на реально потужній залізці так і в Hyper-v). І завдяки переносимості конфігурації, ви можете розгорнути mikrotik будь-де.

Мінуси mikrotik

- Для реально безперебійної роботи mikrotik все-таки не призначений, тут потрібні кластери, але це не так складно організувати через тугішу віртуалізацію, але все-таки це трохи інше.
- Також мінус у тому випадку, коли є необхідність шифрування за ГОСТом
- Важко налаштувати для людини, що абсолютно не розуміє в мережах. Mikrotik пристрій для системного адміністратора.
- Вузька популярність марки (і відповідно поширення). Цей мінус важливий не лише для фахівців високого рівня, але й для користувачів. Наприклад, якщо RouterOS мало затребуваний, відповідно і його фахівці мало кому цікаві. І інша сторона, якщо фірма, що користується ОС, втратить на час свого адміна, то знайти йому заміну для вирішення питання про вхід з ладу системи дуже важко.
- На молодших моделях слабкий Wi-Fi. Великий функціонал, але сама роздача вайфа слабка.
- Немає «корпоративної» техпідтримки та гарантії.

Останнім часом все частіше зустрічаємося з брутфорсом (Brute force – метод злому облікових записів за допомогою підбору паролів до них). Найчастіше атака йде стандартні сервіси і, відповідно, стандартні порти. Наприклад:

SSH - TCP 22 port

PPTP - TCP 1723 port, GRE (не має порт)

L2TP - UDP 1701, 4500, 500 ports

RDP - TCP 3389 port

VNC-TCP 5900 port

Якщо ви використовуєте складні паролі, підібрати їх буде нелегко. Тому основна проблема, що виникає під час брутфорсу, це падіння швидкості мережі. Часто це саме "швидкість інтернету". На інтерфейс маршрутизатора, що входить, надходить велика кількість пакетів з високою швидкістю, канал забивається, і "корисні" пакети проходять з меншою швидкістю, ніж хотілося б.

Також варто зазначити, що багато серверів і маршрутизаторів ведуть логи спроб авторизації. Якщо цих спроб тисячі, то розмір логів може досягати декількох десятків гігабайт. Це призводить до підвищеного навантаження на дискову підсистему та швидкої витрати місця.

Для захисту від брутфорс-атаки на SSH - TCP 22 port і PPTP - TCP 1723 port (наприклад взяті стандартні порти) потрібно блокувати ip-адреси всіх, хто спробує встановити чотири з'єднання поспіль з інтервалом менше однієї хвилини.

Це може бути реалізовано таким чином:

- При першому підключенні SSH додаємо ip-адресу в список ssh_stage1, якщо менш ніж через одну хвилину приходить ще один запит на підключення, додаємо в список ssh_stage2 і т.д.
- Після списку ssh_stage3 слідує список blacklist.

- Для підключень по PPTP така ж логіка, тільки міняється назва списків на pptp_stage1 - pptp_stage3. Для списку ip-адрес blacklist створюється правило блокування в Firewall. [8]

3. РОЗРОБКА МЕТОДІВ ТА ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ ДО ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Поняття кіберзахисту та його методів

Кіберзахист – це механізм захисту комп'ютерних мереж, який включає реагування на дії та захист критично важливої інфраструктури, а також забезпечення інформацією для організацій, державних установ та інших можливих мереж. Кіберзахист спрямований на запобігання, виявлення та своєчасне реагування на атаки чи погрози, так що жодна інфраструктура чи інформація не будуть підроблені. Зі збільшенням обсягу і складності кібератак кіберзахист стає необхідним більшості організацій як захисту конфіденційної інформації, так захисту активів.

При розумінні конкретного середовища кіберзахист аналізує різні загрози, можливі для цього середовища. Потім він допомагає у розробці та реалізації стратегій, необхідних для протидії зловмисним атакам чи загрозам. У кіберзахист залучено широкий спектр різноманітних видів діяльності для захисту відповідного об'єкта, а також для швидкого реагування на ландшафт загроз. Це може включати зниження привабливості середовища для можливих зловмисників, розуміння критичних положень та конфіденційної інформації, вживання профілактичних заходів для забезпечення того, щоб атаки були дорогими, можливість виявлення атак та можливості реагування та реагування. Кіберзахист також проводить технічний аналіз, щоб визначити шляхи та області, на які можуть націлити зловмисники.

Кіберзахист забезпечує таку необхідну гарантію для запуску процесів та дій, не турбуючись про загрози. Це допомагає у підвищенні ефективності використання стратегії та ресурсів безпеки. Кіберзахист також допомагає підвищити ефективність ресурсів безпеки та витрати на безпеку, особливо у критичних місцях.

Як було згадано, кіберзахист працює комплексно, маючи під собою безліч методів для забезпечення безпеки інформації та будь-яких інших активів компанії, які знаходяться на електронних носіях.

Розглянемо комплекс підходів до захисту, як фізичну підготовку компанії до віддаленої роботи, так і програмні рішення. [9]

3.2 Фізичне забезпечення кіберзахисту

Проектування серверного приміщення має проводитися з урахуванням низки факторів: навантаження на мережу та кількість мережевих підключень, необхідна потужність, контроль кімнатної температури та вентиляція, фізична безпека, а також захист від пожежі та надзвичайних ситуацій.

Серверні кімнати мають суттєві відмінності від двох інших варіантів розміщення даних та робочого навантаження - у центрах обробки даних та мікро-датацентрах.

Центри обробки даних можна розглядати як будівлю, що складається з великої кількості виділених серверних кімнат. Однак на практиці центри обробки даних відрізняються від звичайних серверних кімнат мережевою пропускною здатністю. Якщо серверна кімната має досить невелике навантаження на мережу, необхідну для однієї організації, центр обробки даних може підтримувати кілька організацій, що складаються з тисяч або мільйонів підключених користувачів одночасно. Тому їм потрібне відповідне обладнання.

Мікро-датацентри ближче до концепції звичайних серверних кімнат, однак вони використовуються як виділені портативні юніти, які можуть бути легко використані для масштабування бізнесу. Завдяки можливості швидкого розгортання мікродатацентри підходять для масштабування обчислювальних потужностей у віддалених областях, для забезпечення стабільної роботи серверного обладнання під час стихійних лих, а також вони здатні забезпечити

тимчасову потужність при переміщенні робочих навантажень між дата-центрами.

Організація серверної кімнати

На етапі проектування серверної кімнати слід звернути особливу увагу на наступні моменти: розташування та розмір кімнати, обладнання, захист від пожежі та охолодження. На цьому етапі важливо оцінити масштаб майбутньої ІТ-інфраструктури та залежно від орієнтовних технічних потреб спроектувати, якою має бути серверна кімната та яким чином можна буде максимально ефективно використати виділений простір.

Якщо залишити простоювати занадто велику частину простору навіть з урахуванням можливого масштабування, це може спричинити зайві витрати, у той час як надмірне використання простору може підвищити ризики, які можуть призвести до величезних витрат або навіть інцидентів.

Технічне обладнання кімнати включають облаштування звукоізолюючих стін, спеціальних дверей для доступу до обладнання, антистатичні підлоги для запобігання електростатичних розрядів, а також обладнання для забезпечення температурного режиму.

Підготовка обладнання включає розрахунок необхідної щільності потужності, що вимірюється у ватах на квадратний метр або в кіловатах на стійку, а також пошук і установку обладнання - антисейсмічні опори і кріплення, заземлення електроенергії для серверних стійок, зазор для приміщень, необхідних для забезпечення мобільності обладнання.

Протипожежні заходи включають використання нерідких протипожежних систем та відповідне прокладання обладнання для серверних кімнат, особливо якщо кабелі проходять через стелю або підлогу.

Система охолодження включає встановлення стельових повітроводів, які подають охолоджене повітря до найбільш гарячих точок.

обслуговування серверних кімнат

Великий серверний зал Серверні кімнати повинні бути не тільки обладнані належним чином, але й підтримуватися. Для цього існує ряд стандартних робочих процедур, включаючи встановлення нового обладнання та утилізації несправного або застарілого. Ось лише деякі рекомендації щодо кращих практик, які слід розглянути та запозичити при обслуговуванні серверної кімнати:

Встановлення сервера. Установка повинна проводитися за наявності резервних джерел живлення, використання сертифікованих кабелів з урахуванням розподілу ваги шляхом розміщення більш важких конфігурацій на нижніх полицях, зниження довжини кабелю, які не перевищують допустимий радіус вигину.

Проектування схем мережі. Комутатори та інше мережеве обладнання повинні бути розташовані логічно, щоб звести до мінімуму довжину кабелів, а критично важливі системи, що потребують резервування, повинні мати додаткові комутатори та маршрутизатори, підключені до резервних джерел живлення.

Видалення сервера. Усі кабелі та серверне обладнання повинні бути видалені та належним чином марковані перед утилізацією, а база даних активів має бути оновлена, щоб відобразити видалення сервера.

Аварійне реагування. Повинна бути визначена та введена в дію політика дій у надзвичайних ситуаціях, а також відпрацьовано процедури реагування на надзвичайні ситуації. На випадок таких ситуацій мають бути передбачені правила з наявністю дома аварійних комплектів і вогнегасників.

Розробка політик. Повинні бути розроблені документи, що описують усі політики та процедури, які мають переглядатися та оновлюватися щороку.

Управління інструментами та обладнанням. Повинен вестись облік інвентаризації. Повинні бути встановлені процедури обліку обладнання та інструментів та його технічного обслуговування.

Розміщення серверного обладнання

Варіантів дизайну серверної кімнати безліч. У міру збільшення користувальницького попиту на обчислювальні потужності та розвитку технологій поряд із цим зростанням на ринку, як і раніше, з'являтимуться нові постачальники та технологічні пропозиції, що охоплюють загальні та спеціалізовані рішення для серверних кімнат.

Потужність: резервування та розподіл

Параметри енергосистеми спрямовані на захист критичних систем від стрибків напруги за збереження безперервної роботи сервера. Вони охоплюють системи аварійного резервного живлення, розподілення електроенергії та моніторингу потужності. Загальні вимоги до серверної включають:

Блоки розподілу живлення у стійці. Ці блоки мають кілька розеток живлення для розподілу електроенергії між декількома пристроями та мають форм-фактори, що підходять практично для будь-якої серверної стійки. Зазвичай блоки розподілу включають захист від перенапруги, а більш просунуті моделі пропонують вимірювання потужності та дистанційне керування потужністю.

Джерело безперебійного живлення - ДБЖ, відомий як система резервного живлення, забезпечує буфер між основним живленням та серверними пристроями. У разі відключення електроенергії ці блоки забезпечують електроживлення, доки не включиться основне електропостачання або альтернативне джерело.

Програмне забезпечення моніторингу енергоспоживання. В організаціях, де час простою є серйозною проблемою, використання інтелектуальних пристроїв rPDU, датчиків та програмного забезпечення для моніторингу центрів обробки даних необхідно для оптимізації операцій та забезпечення безперервності бізнесу.

Контроль температури

Для невеликих серверних кімнат може бути достатньо охолодження за допомогою системи комфортного охолодження будівлі, але для більших або щільних приміщень може знадобитися більш точне керування температурним режимом з використанням рішень для охолодження, розроблених спеціально для важливих IT-обладнань.

У випадку високопродуктивних обчислювальних додатків, найбільш прийнятним рішенням можуть бути системи рідинного охолодження.

Системи пожежогасіння

Для невеликого серверного приміщення може не знадобитися власна система пожежогасіння. Страховики, як правило, можуть дати рекомендації залежно від розміру приміщення та потужності.

Якщо потрібна пожежогасіння, у приміщенні може знадобитися автоматичний або ручний вогнегасник.

Автоматизована система, що використовує технологію PAFSS, є економічним рішенням для однієї або декількох серверних стійок. Він складається з агента під тиском у каністрі, що знаходиться поруч зі стійками, та розподільчого шланга всередині шафи. Шланг розплавиться за максимальної температури нагрівання, щоб випустити вогнегасну речовину в шафу.

Системи моніторингу

моніторинг серверної кімнати Слід також приділити увагу моніторингу. Температура та вологість у серверній кімнаті зазвичай є контрольованими факторами довкілля.

У кімнаті має бути встановлений базовий блок моніторингу з відповідними датчиками. Якщо вони отримують показання, що виходять за межі попередньо встановленого порогу, система моніторингу середовища може бути настроєна на надсилання попереджень до попередньо визначеного списку розсилки електронною поштою та SMS.

Інші фактори навколишнього середовища, які можна контролювати, включають витік води, дим та вогонь, а також безпеку приміщення та проникнення в серверну шафу.

Камери визначення руху також можуть бути встановлені та підключені до відповідної системи моніторингу навколишнього середовища для забезпечення відеозапису з камер відеоспостереження після та до події, а також двостороннього зв'язку в серверній кімнаті.

Щодо легко створити спеціалізований простір для розміщення IT-серверів та мережевих пристроїв. Практики проектування та будівництва відповідають вимогам великих серверних та центрів обробки даних, які масштабуються відповідно до проектних та бюджетних вимог. Рекомендується провести попередній аналіз майданчика для виявлення проблем, які необхідно вирішити під час встановлення та які можуть вплинути на загальну вартість та успіх проекту.

Типові проблеми включають навантаження на електричний ланцюг, придатність стін і перегородок, прокладання кабелів, прокладання охолодних труб, де розмістити теплообмінник і як обслуговувати серверну кімнату. [10]

3.3 Програмне забезпечення кіберзахисту

Налаштування ролі RDP та встановлення ліцензій служби віддалених робочих столів

1. Встановлення ролі RDP на Windows Server

Встановлення ролі RDP на сервер Windows відбувається в два етапи: спочатку встановлюється служба віддаленого робочого столу, а потім визначається сервер ліцензування.

1.1 У меню, у верхньому правому кутку, вибираємо «Управління» (Manage) → «Додати ролі та компоненти» (Add Roles and Features):

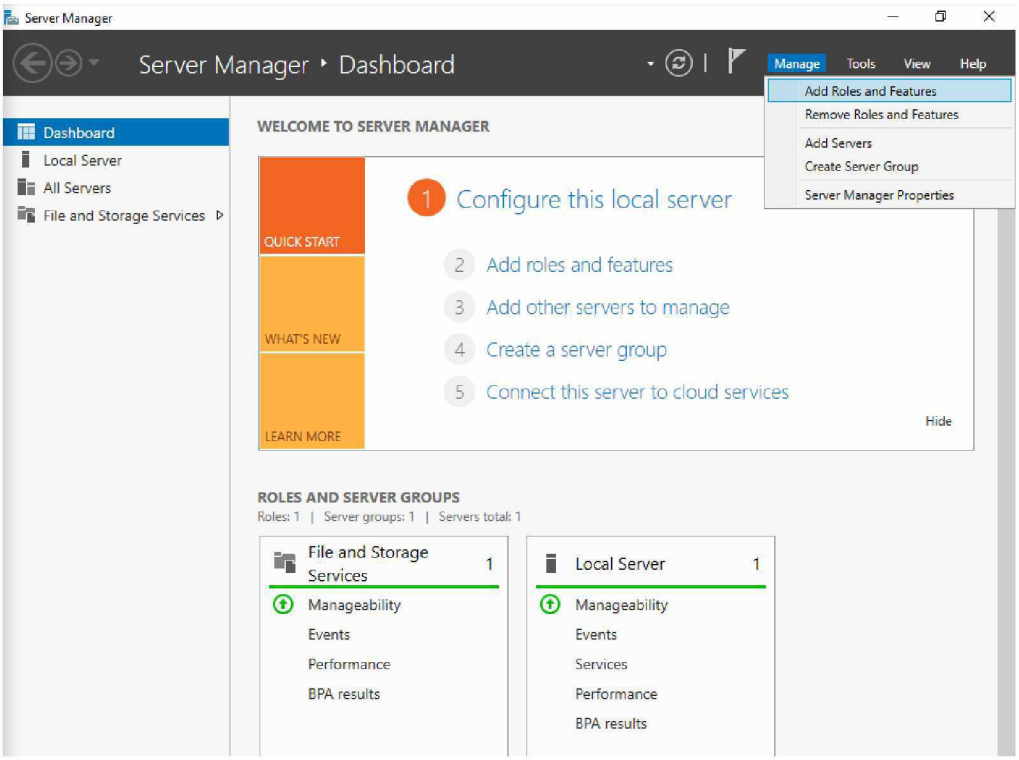

Рисунок 1.1 – Додавання ролей та компонентів

1.2 Залишаємо перемикач на «Встановлення ролей і компонентів» (Role-based or features-based installation):

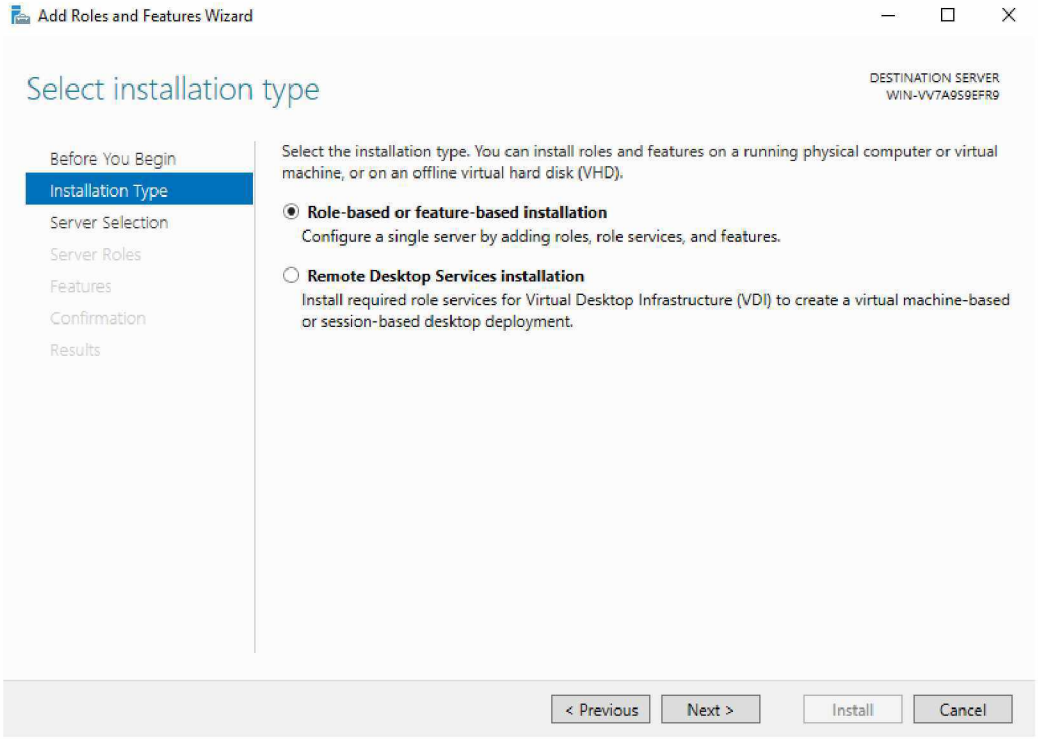

Рисунок 1.2 – Встановлення ролей та компонентів

1.3 Вибираємо той сервер із пулу серверів, на який буде встановлено службу терміналів;

1.4 Відзначаємо роль «Служби віддалених робочих столів» (Remote Desktop Services) у списку ролей. Компоненти залишаємо у тому вигляді, як вони є;

1.5 Далі необхідно вибрати встановлювані служби ролей. Нам знадобиться «Ліцензування віддалених робочих столів» (Remote Desktop Licensing) та «Вузол сеансів віддалених робочих столів» (Remote Desktop Session Host).

1.6 Погоджуємося на встановлення додаткових компонентів, натиснувши на «Додати компоненти» (Add Features) у майстрі:

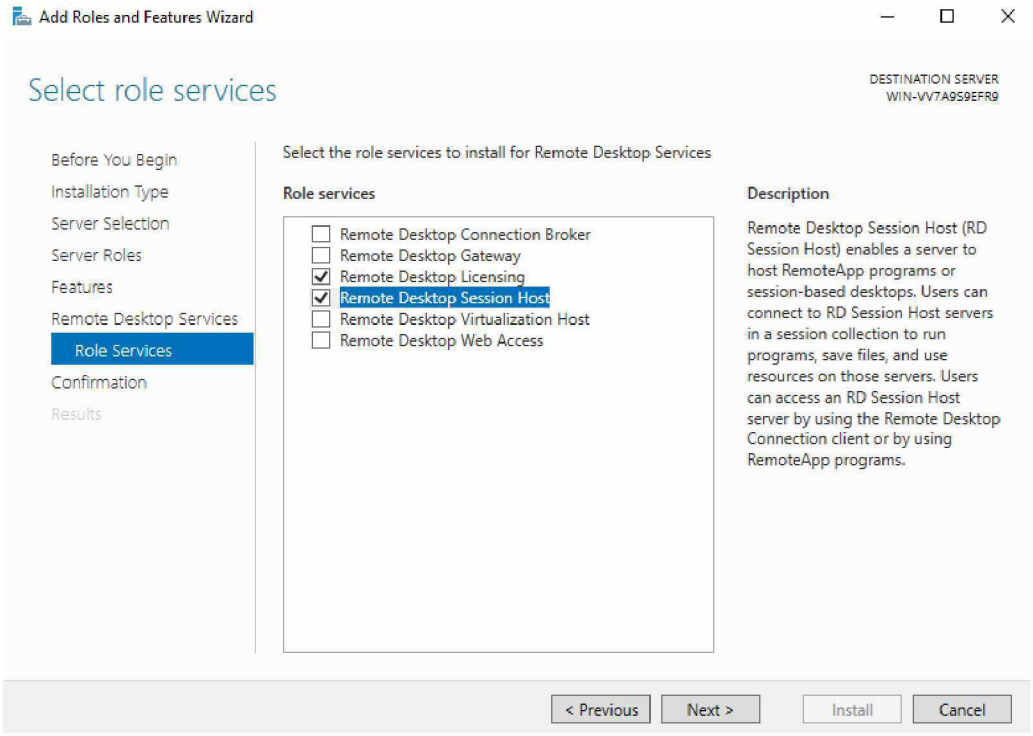

Рисунок 1.6 – Необхідні служби ролей

1.7 Усі параметри встановлення ролі визначено. На останній сторінці встановлюємо прапорець «Автоматичний перезапуск кінцевого сервера, якщо потрібно» (Restart the destination server automatically if required) , підтверджуємо вибір натиснувши «Так» (Yes) у вікні і натисніть «Встановити» (Install) для запуску установки служби;

1.8 Якщо все пройшло добре, після перезавантаження, на екрані буде повідомлення про успішне встановлення всіх вибраних служб та компонентів:

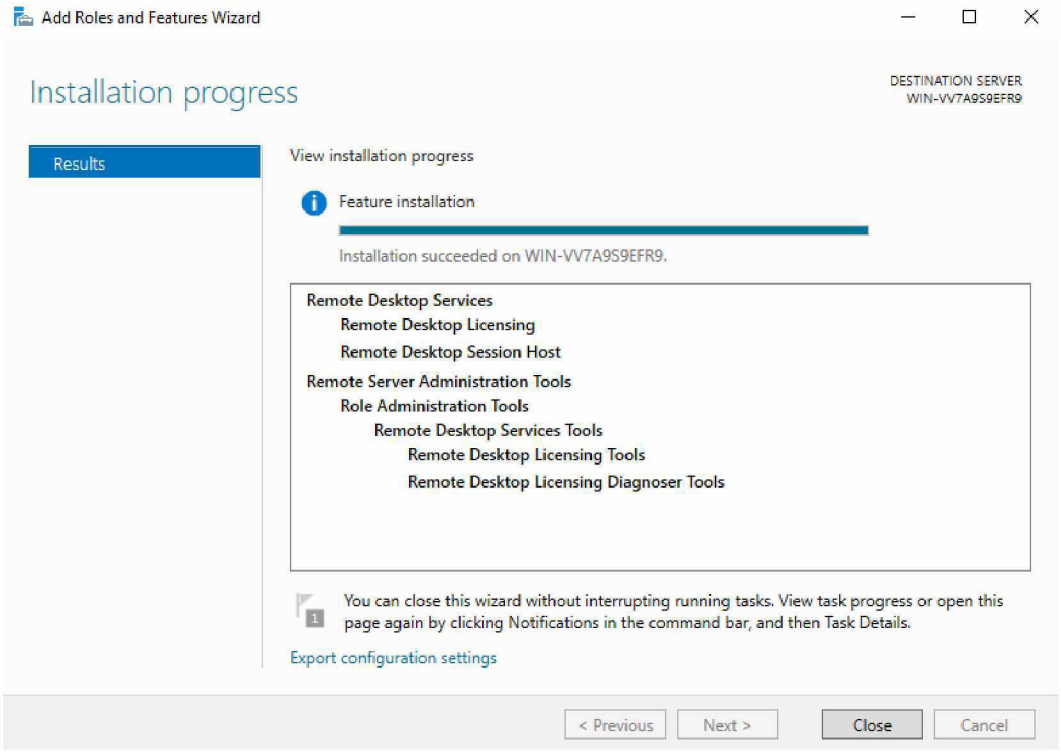

Рисунок 1.8 – Завершення роботи майстра

2. Визначення сервера ліцензування для служби віддалених робочих столів

2.1 Тепер запускаємо «Засіб діагностики ліцензування віддалених робочих столів» (RD Licensing Diagnoser);

2.2 Доступних ліцензій поки що немає, оскільки не встановлено режим ліцензування для сервера вузла сеансів віддалених робочих столів:

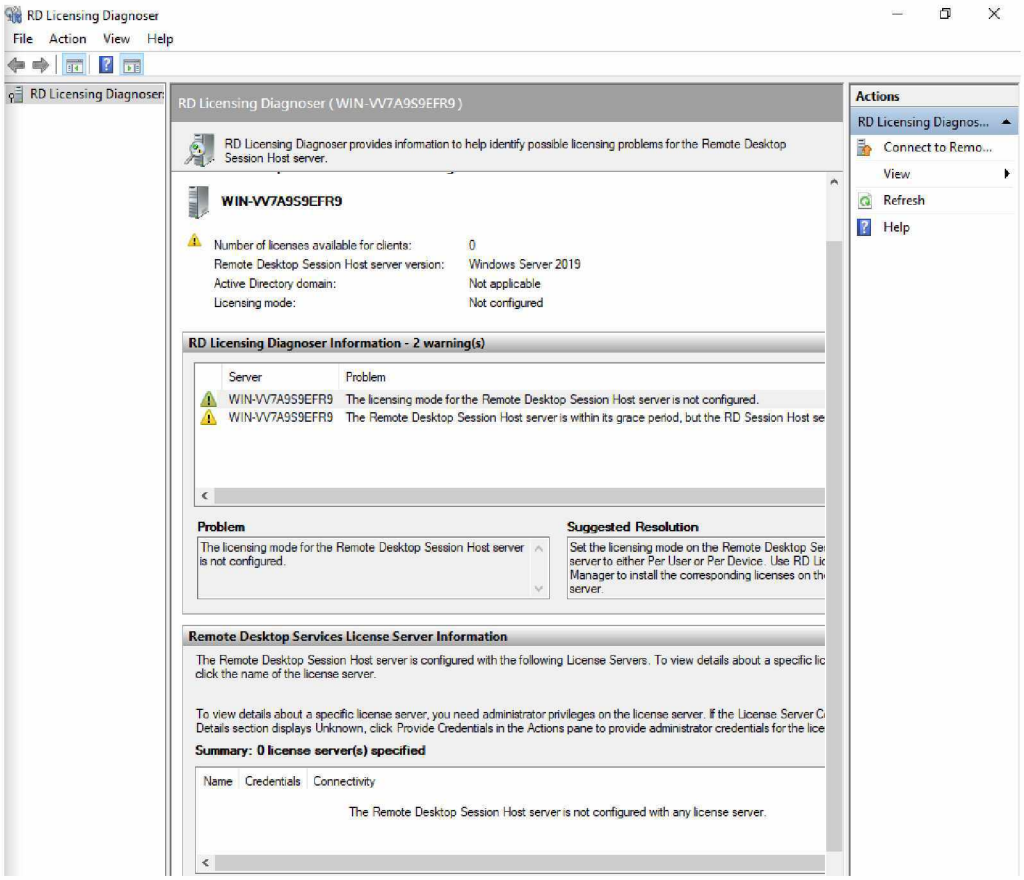

Рисунок 2.2 – Показ доступності ліцензій

2.3 Сервер ліцензування вказується тепер у локальних групових політиках. Для запуску редактора виконаємо команду *gpedit.msc;*

2.4 Відкриється редактор локальної групової політики. У дереві зліва розкриємо вкладки:

Конфігурація комп'ютера (Computer Configuration) → Адміністративні шаблони (Administrative Templates) → Компоненти Windows (Windows Components) → Служби віддалених робочих столів (Remote Desktop Services)

→ Вузол сеансів віддалених робочих столів (Remote Desktop Session Host) → Ліцензування (Licensing).

Відкриємо параметри «Використовувати вказані сервери ліцензування віддалених робочих столів» (Use the specified Remote Desktop license servers), клацнувши двічі на відповідному рядку;

2.5 У вікні редагування параметрів політики переставляємо перемикач у положення «Увімкнено» (Enabled). Потім потрібно визначити сервер ліцензування для служби віддалених робочих столів. Вказуємо мережеве ім'я або IP-адресу сервера ліцензій та натискаємо «ОК»:

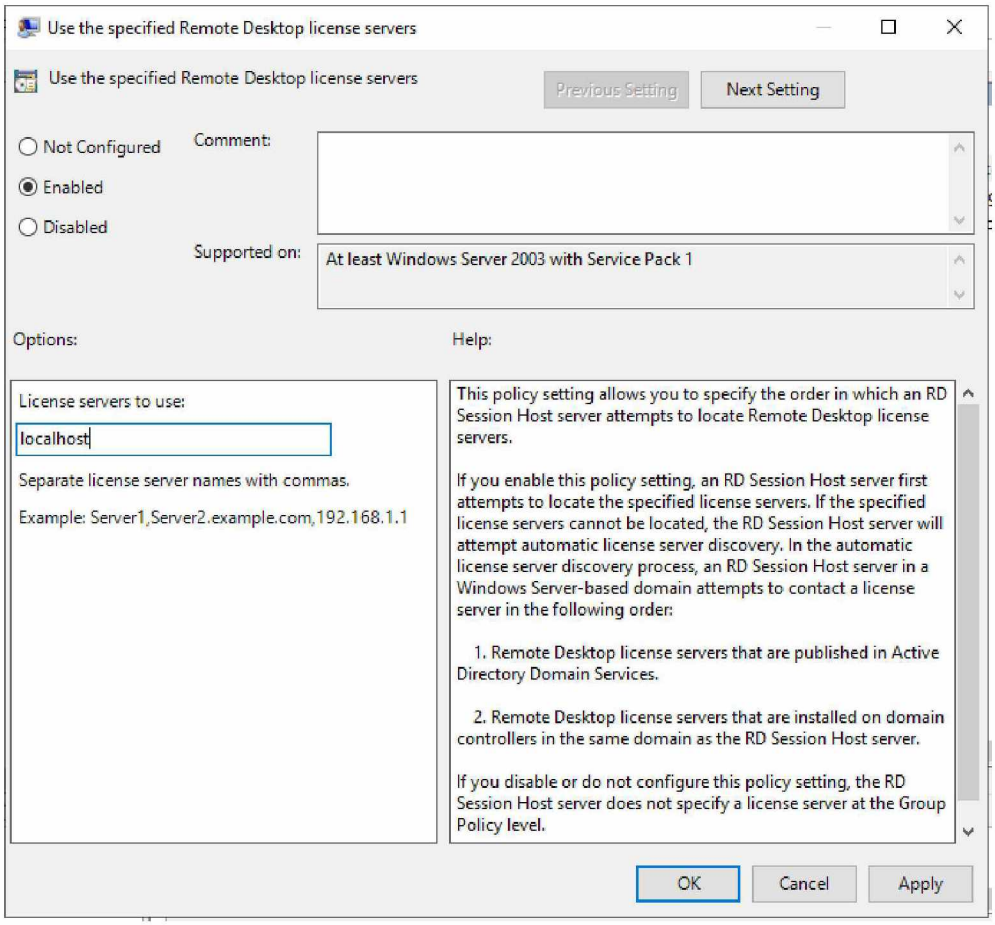

Рисунок 2.5 – Сервер ліцензування

2.6 Далі змінюємо параметри політики «Задати режим ліцензування віддалених робочих столів» (Set the Remote licensing mode). Також встановлюємо перемикач у положення «Увімкнено» (Enabled) та вказуємо режим ліцензування для сервера вузла сеансів віддалених робочих столів. Можливі 2 варіанти:

- «На користувача» (Per User)
- «На пристрій» (Per Device)

Змінивши перелічені вище політики, закриваємо редактор;

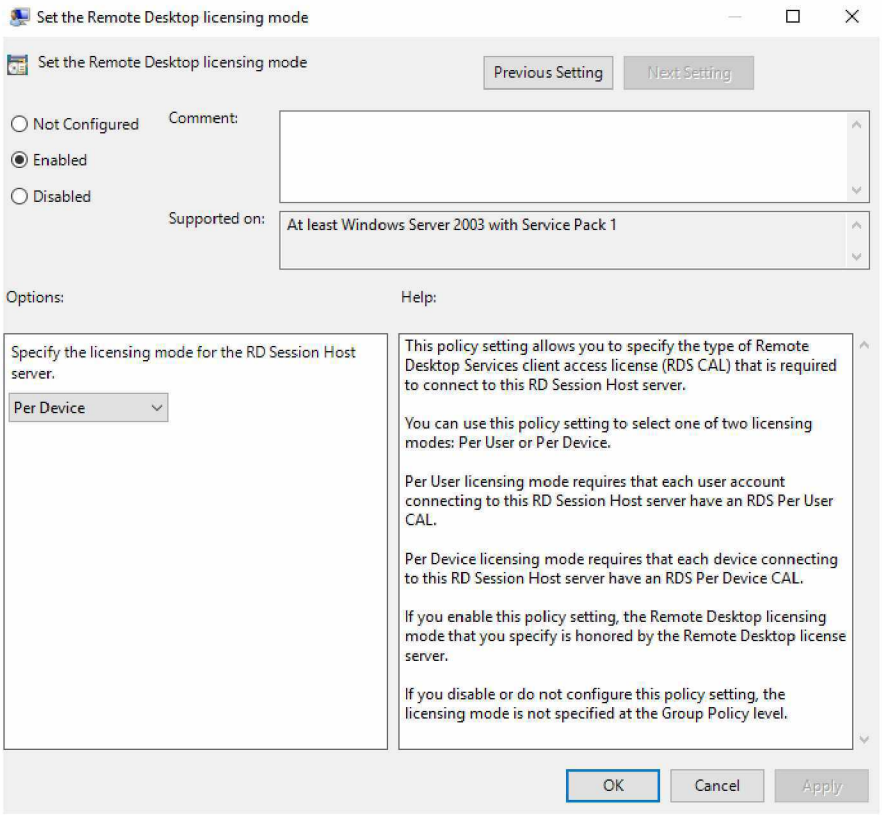

Рисунок 2.6 – Режим ліцензування для сервера

2.7 Повертаємося в оснастку «Засіб діагностики ліцензування віддалених робочих столів» (RD Licensing Diagnoser) і бачимо нову помилку, що вказує на те, що сервер ліцензування вказано, але не ввімкнено;

2.8 Для запуску сервера ліцензування переходимо до «Диспетчера ліцензування віддалених робочих столів» (RD Licensing Manager);

2.9 Тут показаний сервер ліцензування зі статусом «Не активовано» (Not Activated). Для активації клацаємо по ньому правою кнопкою миші та в контекстному меню вибираємо «Активувати сервер» (Activate Server):

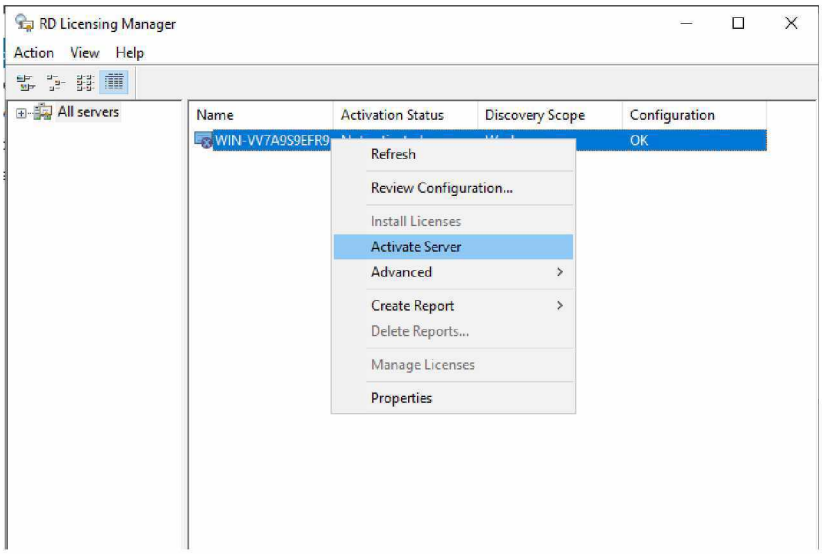

Рисунок 2.9 – Активація сервера ліцензування

2.10 Запуститься Майстер активації сервера:

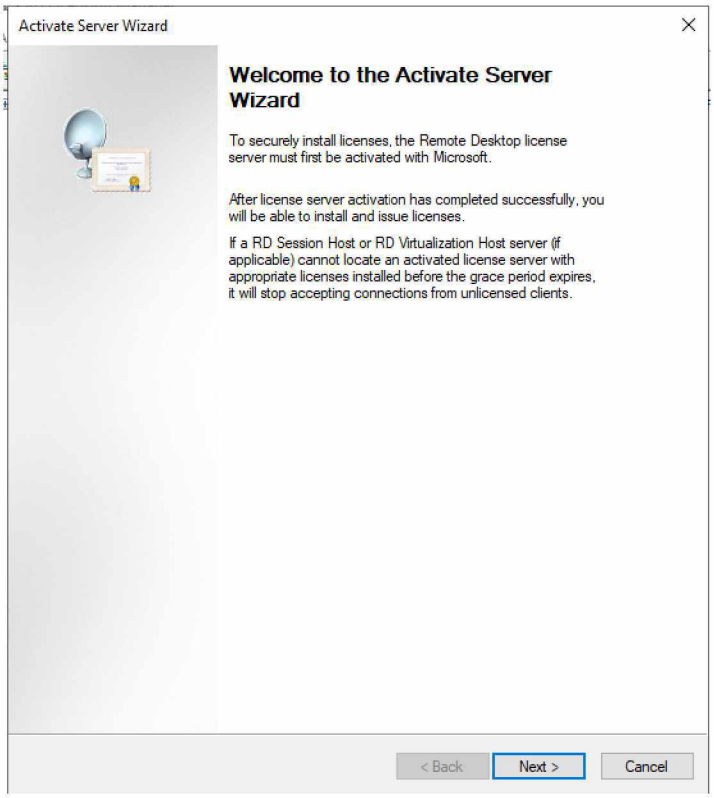

Рисунок 2.10 – Майстер активації сервера

2.11 Потім вибираємо метод підключення («Авто» (Automatic connection) - за замовчуванням);

2.12 Вводимо відомості про організацію (ці поля обов'язкові для заповнення):

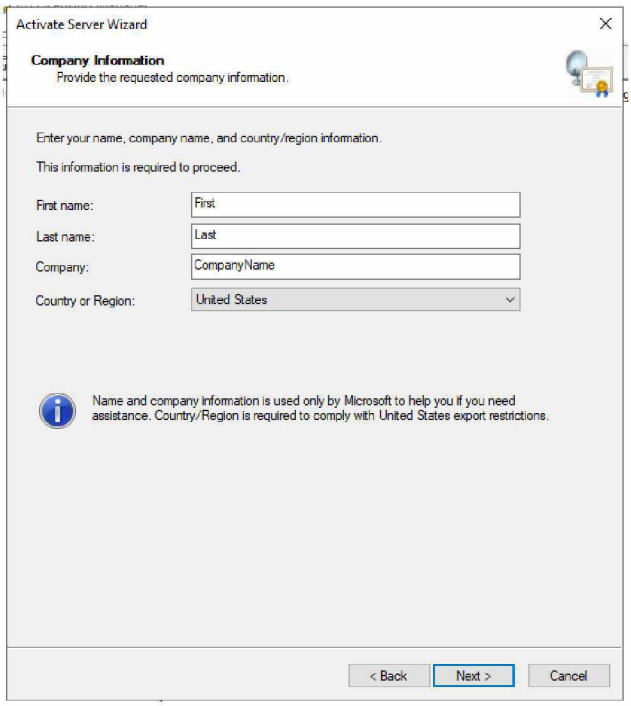

Рисунок 2.12 – Відомості про організацію

2.13 Вводимо додаткові відомості про організацію:

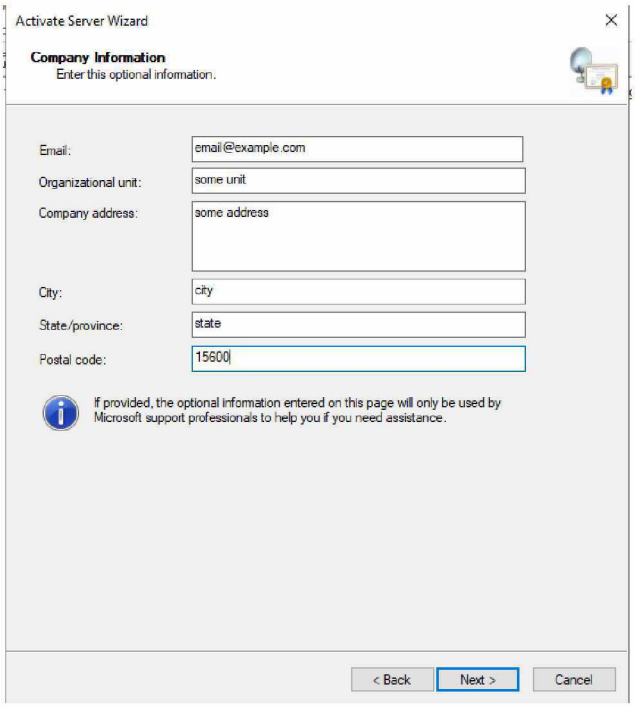

Рисунок 2.13 – Додаткові відомості

2.14 Сервер ліцензування активовано. Тепер потрібно встановити ліцензії. Для цього натискаємо «Далі» (Next), залишаючи позначку в чекбоксі «Запустити майстер установки ліцензій»:

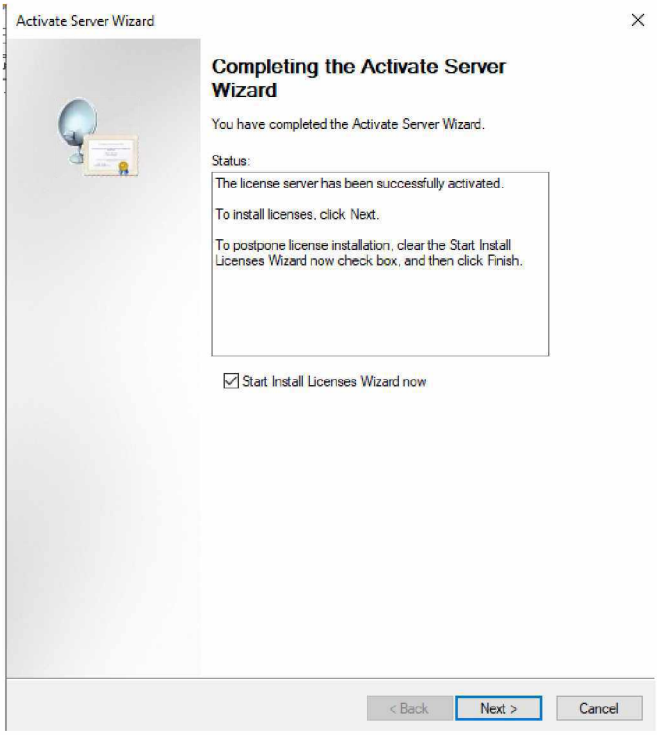

Рисунок 2.14 – Встановлення ліцензії

3. Встановлення ліцензій на сервер ліцензування служби віддалених робочих столів

3.1 Натискаємо «Далі» (Next) на початковій сторінці Майстра установки ліцензій:

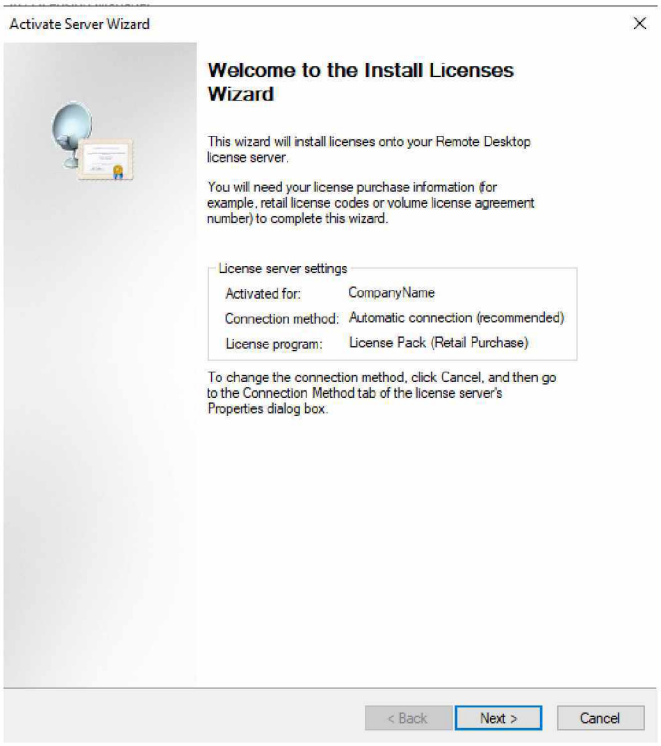

Рисунок 3.1 – Майстер установки ліцензій

3.2 Потім обираємо необхідну програму ліцензування:

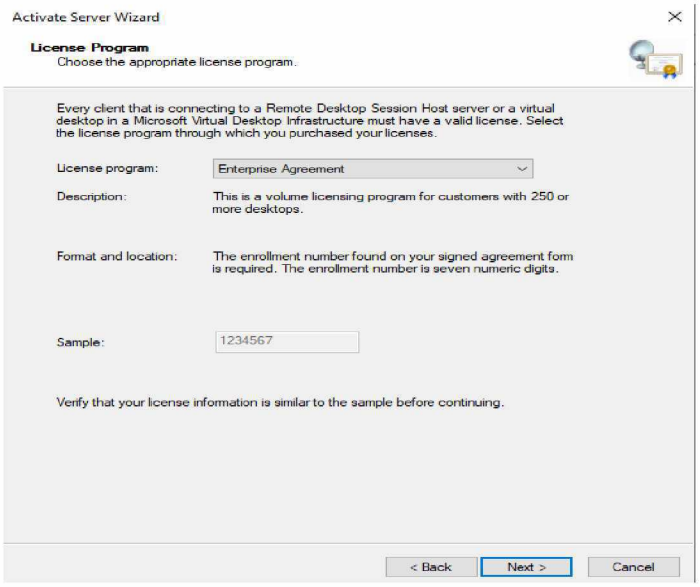

Рисунок 3.2 – Програма ліцензування

3.3 Вводимо номер угоди:

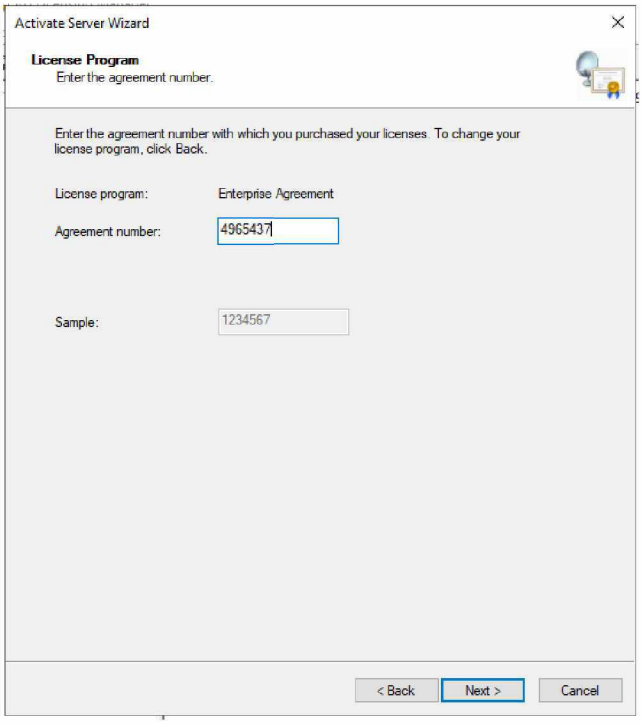

Рисунок 3.3 – Угода ліцензування

3.4 Вказуємо версію продукту, тип ліцензії та кількість ліцензій відповідно до програми ліцензування:

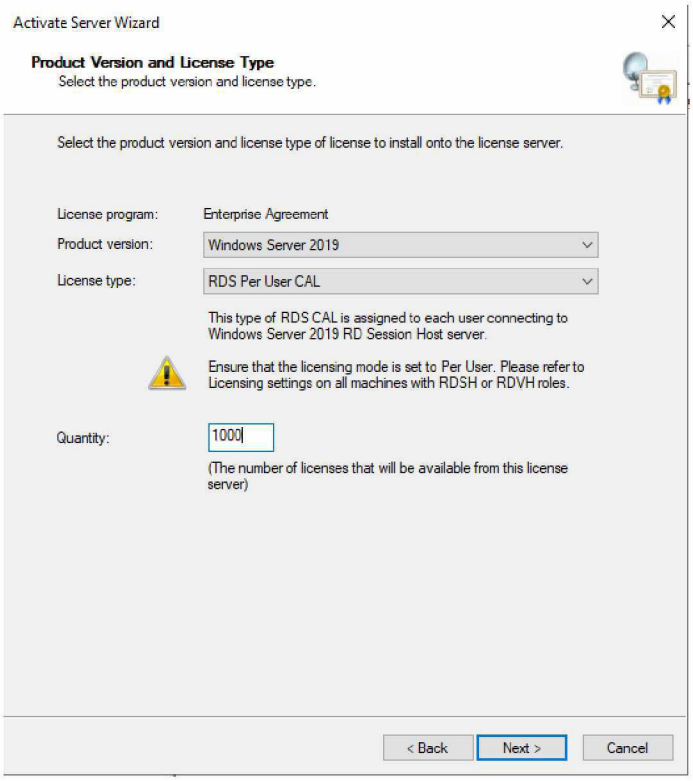

Рисунок 3.4 – Кількість потрібних ліцензій

3.5 Очікуємо завершення роботи майстра встановлення ліцензій з повідомленням про те, що запитані ліцензії успішно встановлені;

3.6 У диспетчері ліцензування переконуємось, що сервер працює, а також бачимо загальну та доступну кількість встановлених ліцензій:

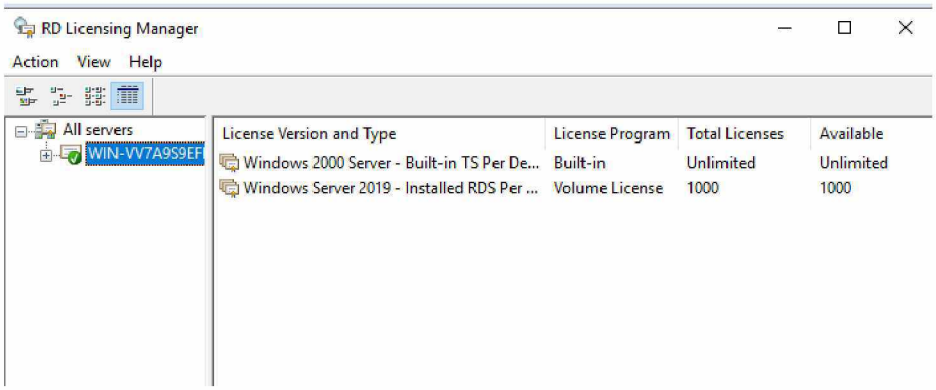

Рисунок 3.6 – Дієздатність серверу та кількість ліцензій

3.7 Повертаємося до «Засобу діагностики ліцензування віддалених робочих столів» (RD Licensing Diagnoser) і бачимо, що помилок немає:

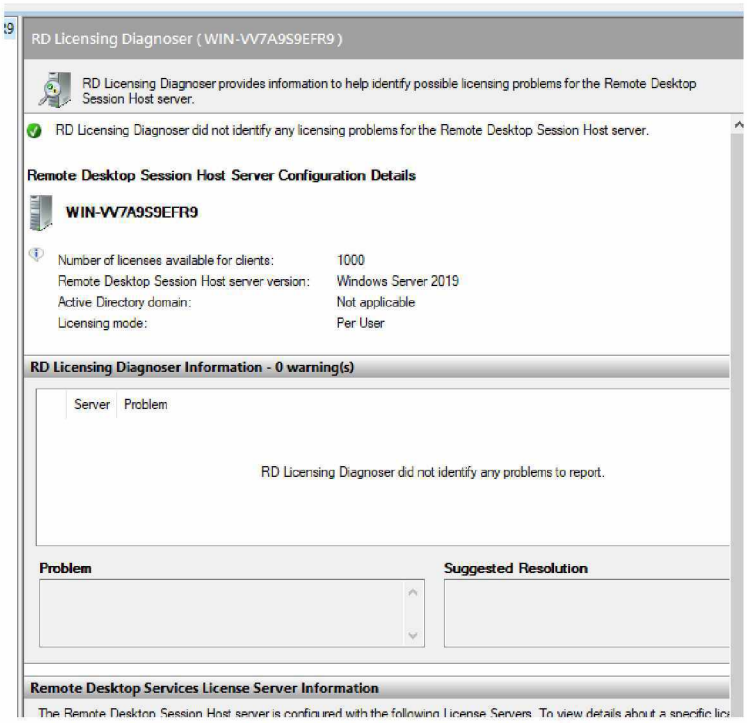

Рисунок 3.7 – Перевірка роботи сервера

Захист RDP підключення

1. Заміна стандартного порту RDP

Зазвичай для віддаленого з'єднання застосовується протокол TCP 3389, однак у деяких випадках виникає потреба в його зміні - наприклад, може вимагати політика безпеки.

1.1 Для того щоб замінити порт, необхідно здійснити редагування реєстру операційної системи. Редагування реєстру здійснюється за допомогою програми-редактора, запустити яку можна запустити, надрукувавши в консолі PowerShell команду regedit.

Потім у редакторі потрібно знайти розділ RDP-Tcp, зробити це можна, пройшовши такий шлях:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

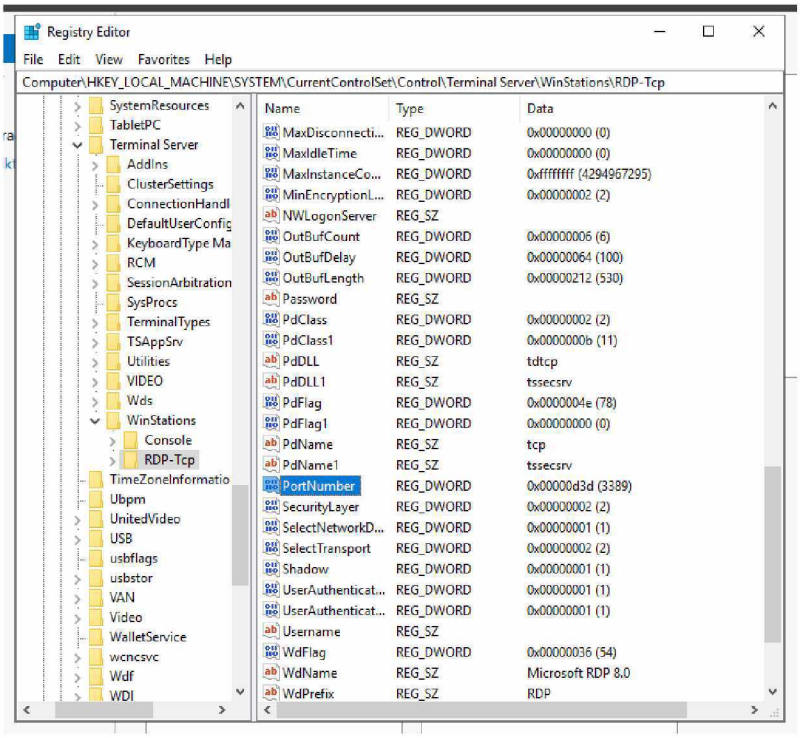

Рисунок 1.1 – Редагування реєстру

1.2 У ньому потрібно знайти елемент PortNumber. Далі слід перейти в десятковий (Decimal) формат введення та задати новий порт для підключення за протоколом RDP:

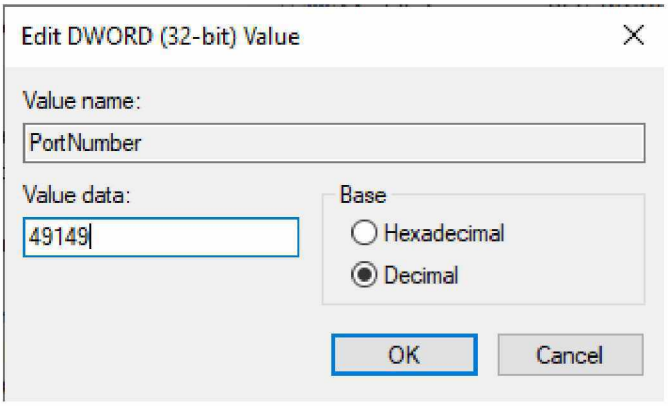

Рисунок 1.2 – Новий порт підключення RDP

При виборі нового порту для підключення необхідно пам'ятати, що існує кілька категорій портів у розбивці за їх номерами:

Номери від 0 до 10213 – відомі порти, які призначаються та контролюються організацією IANA (Internet Assigned Numbers Authority). Як правило, їх використовують різні системні програми ОС.

Порти від 1024 до 49151 - зареєстровані порти, що призначаються IANA. Їх дозволяється використовуватиме вирішення приватних завдань.

Номери портів від 49152 до 65535 - динамічні (приватні) порти, які можуть використовуватись будь-якими програмами або процесами для вирішення робочих завдань.

Після зміни порту для віддаленого підключення необхідно відкрити його в налаштуваннях міжмережевого екрана, інакше спроби зовнішнього з'єднання блокуватимуться.

1.3 Для цього потрібно скористатися оснащенням керуванням Брандмаеур Windows у режимі підвищеної безпеки (Windows Firewall with Advanced Security). У ній потрібно вибрати пункт «Правила для вхідних підключень», натиснути на цей пункт правою кнопкою миші і вибрати «Створити правило»:

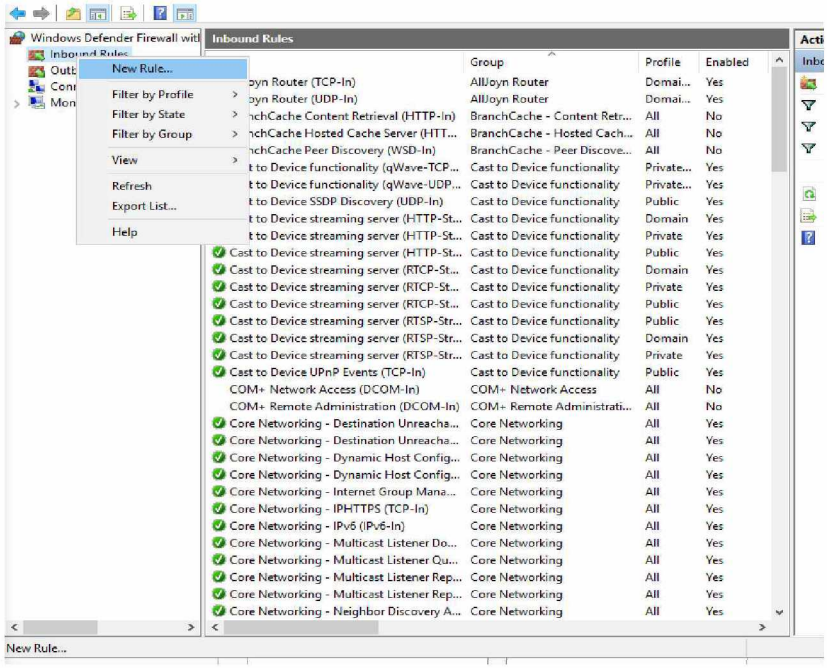

Рисунок 1.3 – Правила для вхідних підключень

1.4 Ми будемо створювати правило для порту.

Потрібно вибрати тип протоколу (TCP або UDP) та вказати порт, який ми задавали під час редагування реєстру:

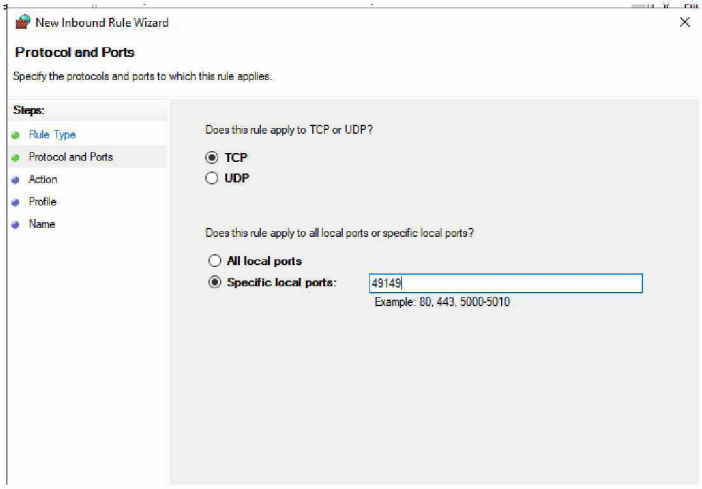

Рисунок 1.4 – Створення правила для порту

1.5 На наступному етапі необхідно вибрати тип дії, який визначає правило. У нашому випадку необхідно дозволити підключення за допомогою вказаного порту:

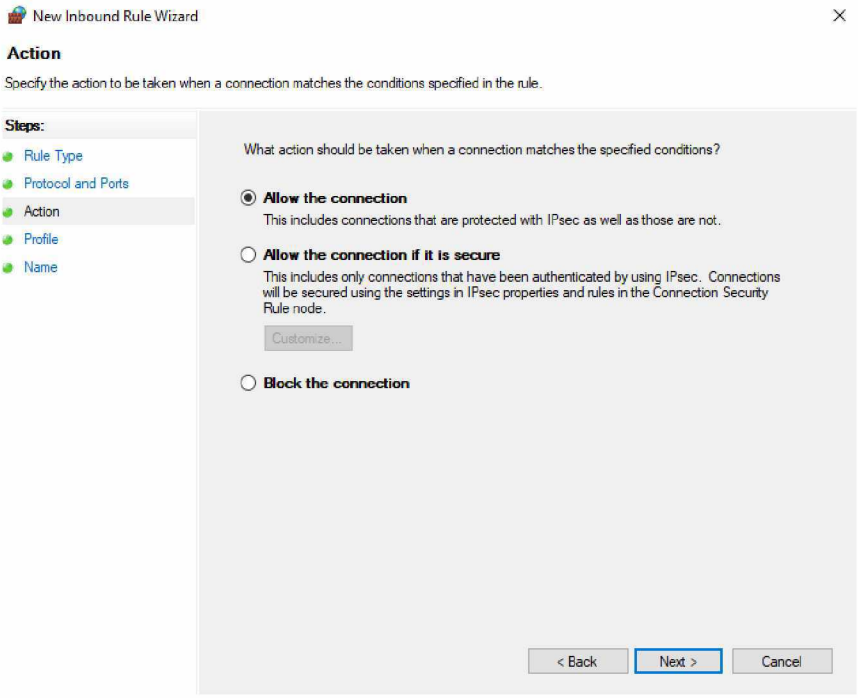

Рисунок 1.5 – Тип дії, який визначає правило

1.6 Далі необхідно вказати область дії правила - воно залежить від того, де працює сервер (у робочій групі, домені або приватному доступі):

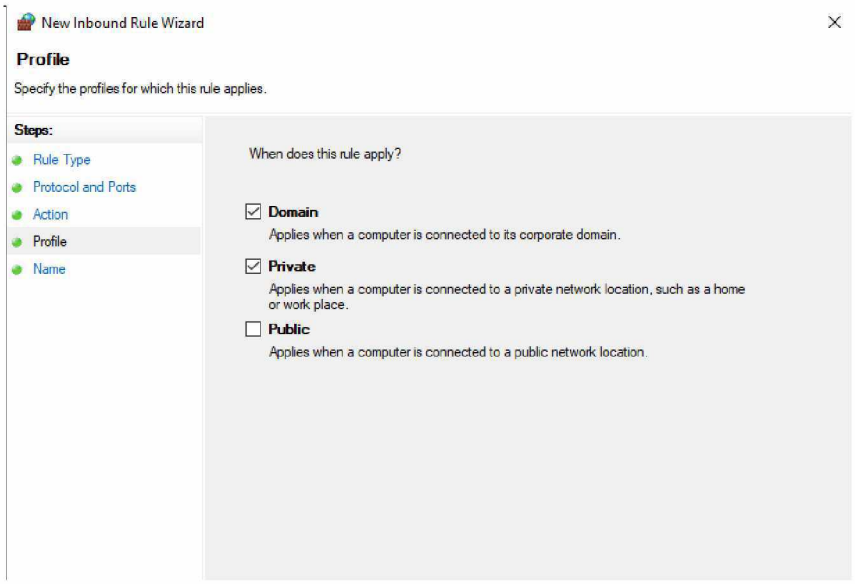

Рисунок 1.6 – Область дії правила

1.7 Потім потрібно вибрати ім'я для правила (рекомендується вибирати його таким чином, щоб потім правило легко дізнатися серед інших):

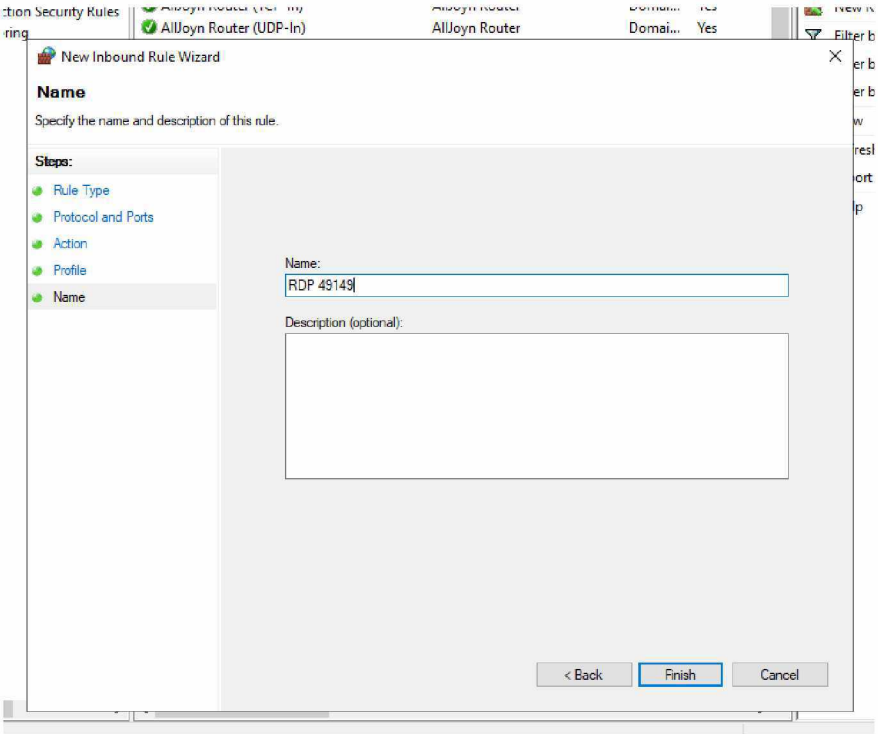

Рисунок 1.7 – Ім’я правила

Після цього необхідно перезавантажити сервер.

2. Шифрування

2.1 Відкриваємо gpedit.msc. Заходимо в Конфігурація комп'ютера → Адміністративні шаблони → Компоненти Windows → Служби віддалених робочих столів → Безпека. Встановлюємо параметр «Вимагати використання спеціального рівня безпеки для віддалених підключень за методом RDP» у значення «Увімкнено» та Рівень безпеки на значення «SSL»:

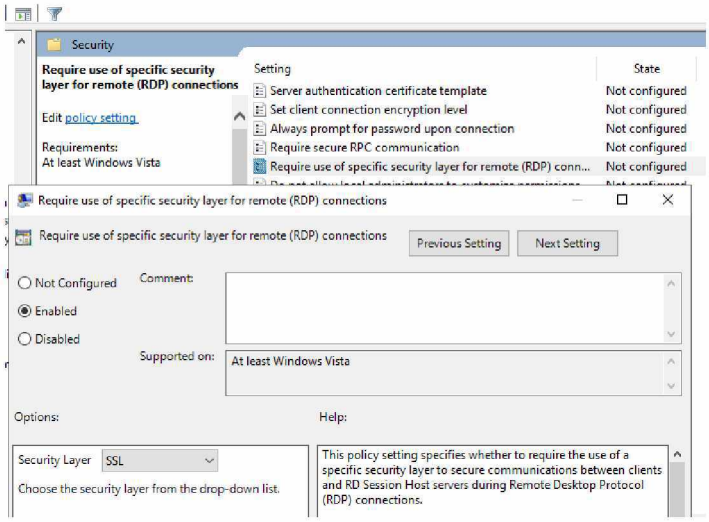

Рисунок 2.1 – Параметр використання спеціального рівня безпеки RDP

2.2 Тепер нам потрібно зробити так, щоб застосовувалися лише стійкі алгоритми шифрування. В цій же гілці відкриваємо параметр «Встановити рівень шифрування для клієнтських підключень» (Set client connection encryption level). Вмикаємо та обираємо «Високий» (High Level) рівень.

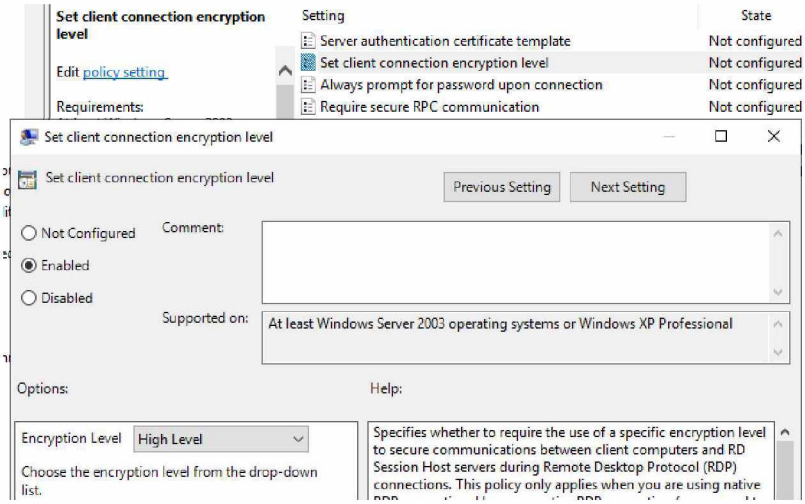

Рисунок 2.2 – Параметр шифрування для клієнтських підключень

2.3 Але це ще не межа. Найбільший рівень шифрування забезпечується стандартом FIPS 140-1.

Щоб увімкнути використання FIPS 140-1, потрібно в цьому ж оснащенні піти в Конфігурація комп'ютера → Конфігурація Windows → Параметри безпеки → Локальні політики → Параметри безпеки. Шукаємо параметр «Системна криптографія: використовувати FIPS-сумісні алгоритми для шифрування, хешування та підписування» і вмикаємо його.

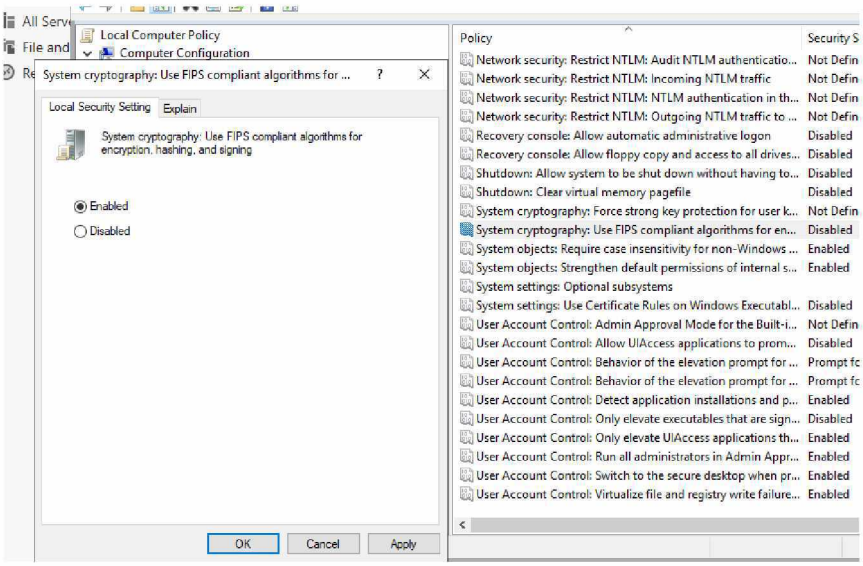

Рисунок 2.3 – FIPS-сумісні алгоритми для шифрування

2.4 І на завершення обов'язково вмикаємо параметр «Вимагати безпечне RPC-підключення» на шляху Конфігурація комп'ютера → Адміністративні шаблони → Компоненти Windows → Служби віддалених робочих столів → Безпека.

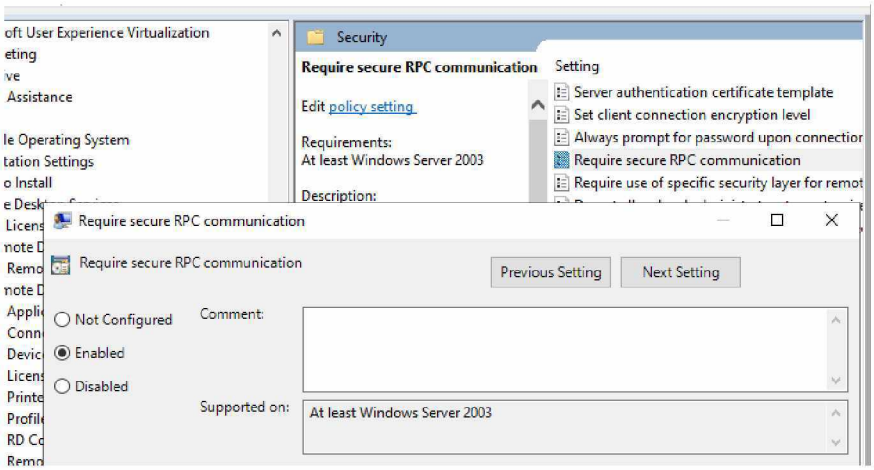

Рисунок 2.4 – Параметр безпечного RPC-підключення

3. Мережева автентифікація (NLA)

За замовчуванням, ви можете підключитися по RDP не вводячи логін та пароль і побачити Welcome-скрін віддаленого робочого столу, де вже від вас попросять залогінитися. Це зовсім не безпечно в тому плані, що такий віддалений комп’ютер легко піддається DDoS-атакам.

3.1 В гілці Конфігурація комп'ютера → Адміністративні шаблони → Компоненти Windows → Служби віддалених робочих столів → Безпека вмикаємо параметр «Вимагати автентифікації користувача для віддалених підключень шляхом перевірки автентичності на рівні мережі»:

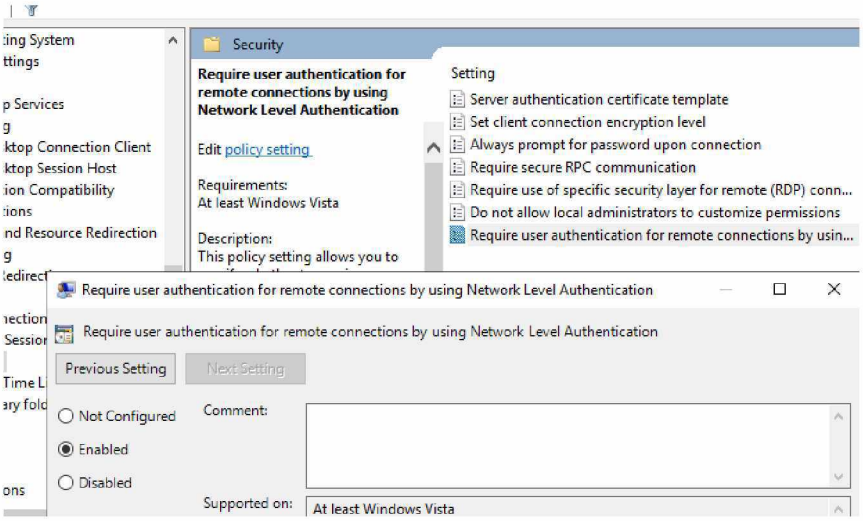

Рисунок 3.1 – Налаштування автентифікації

4. Зміна імені облікового запису

Обліковий запис Адміністратор не призначений для постійної роботи із системою, а лише для випадків, коли потрібно встановити програму, або налаштувати інші критичні для роботи системи компоненти.

4.1 Виконайте Пуск → Управління Комп'ютером (compmgmt.msc) → Enter;

4.2 У вікні розгорніть Управління комп'ютером (Computer Menagement)→ Локальні користувачі та групи (Local Users and Groups) → Користувачі (Users):

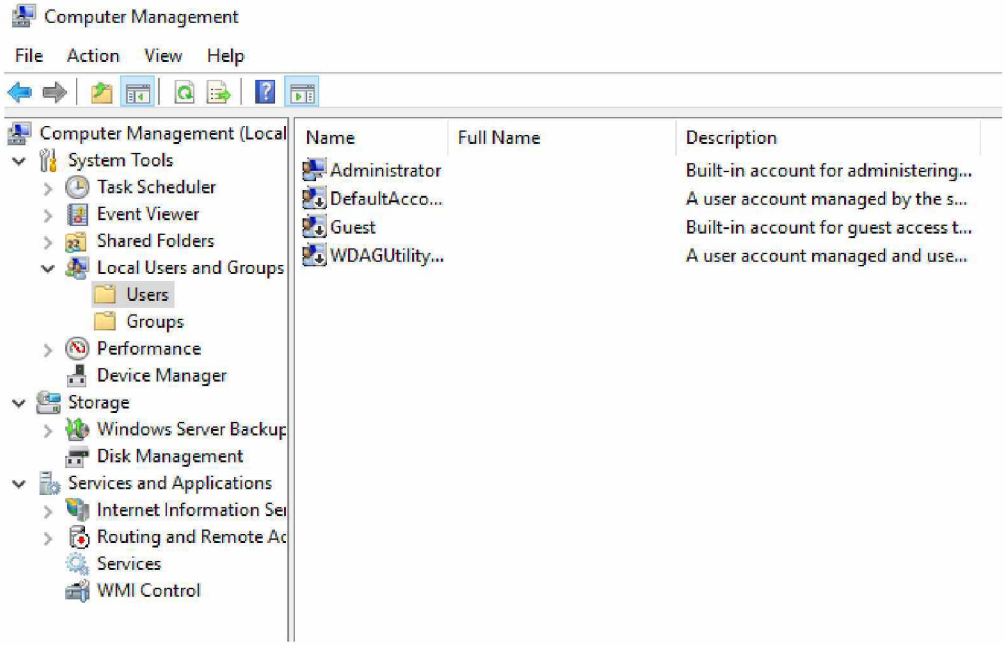

Рисунок 4.2 – Користувачі сервера

4.3 Виберіть користувача Administrator, натисніть клавішу F2 та перейменуйте:

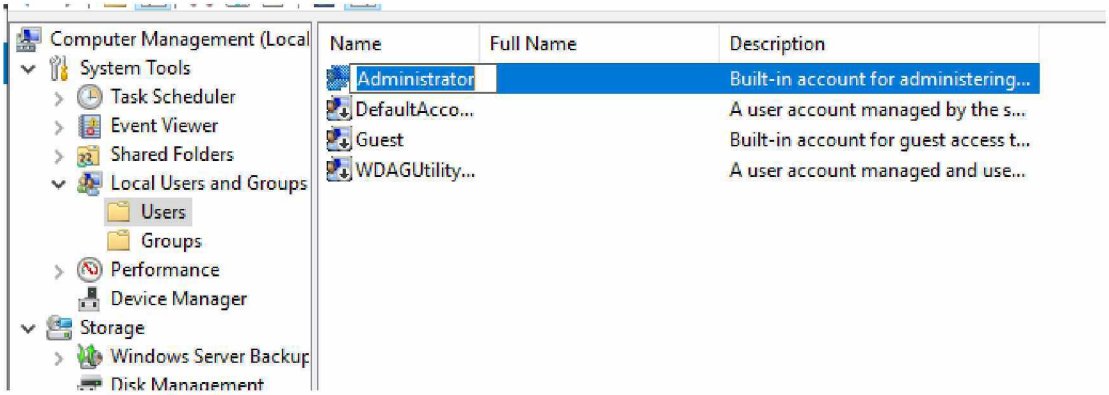

Рисунок 4.3 – Перейменування користувача

4.4 Введіть нове ім'я та збережіть зміни, натиснувши клавішу Enter:

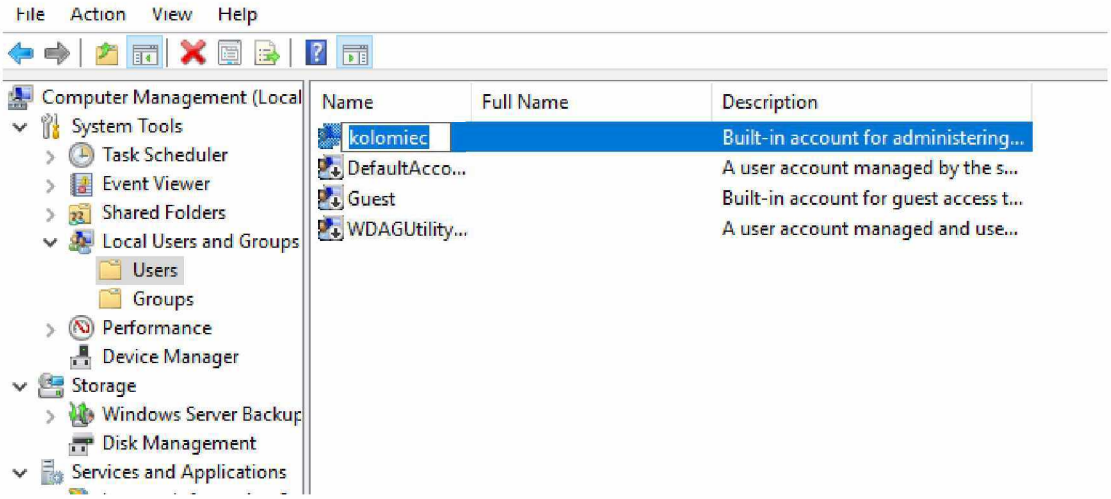

Рисунок 4.4 – Нове ім’я користувача

5. Блокування облікового запису

В операційних системах Microsoft Windows для забезпечення надійного рівня безпеки можна автоматично блокувати обліковий запис користувача, якщо він багаторазово ввів неправильний пароль.

З основних причин блокування можна виділити:

- Підбір пароля, так званий брутфорс, що в результаті призводить до блокування;
- Після зміни пароля у користувача залишилися старі підключення WIFI на комп'ютері або телефоні зі старими обліковими даними, які намагаються автоматично підключитися до сервісів компанії;
- Як і у випадку з WIFI, у користувача після зміни пароля можуть бути закешовані, старі паролі в доступах до мережних куль, Outlook календарів та інших програм, які одного разу попросили ввести логін та пароль;
- Іноді бувають завдання у планувальнику Windows, які запускалися від імені користувача, а не системи;
- Збережені паролі у браузерах
- Служби, що працюють з піддоменного облікового запису

5.1 Відкриваємо редактор групової політики та клацаємо правим кліком миші з політики «Default Domain Policy», з контекстного меню виберемо пункт «Змінити» (Edit):

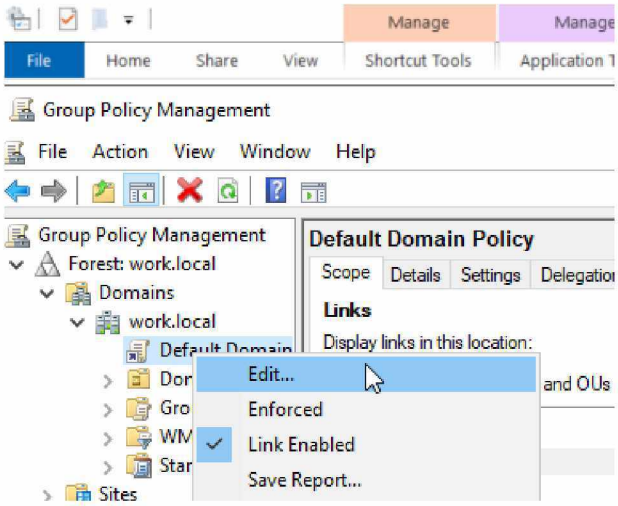

Рисунок 5.1 – Редагування політики

5.2 Переходимо до Конфігурація комп'ютера → Політики → Конфігурація Windows → Параметри безпеки → Політики облікових записів → Політики блокування облікових записів (Computer Configuration → Windows Settings → Security Settings → Account Policy → Account Lockout Policy):

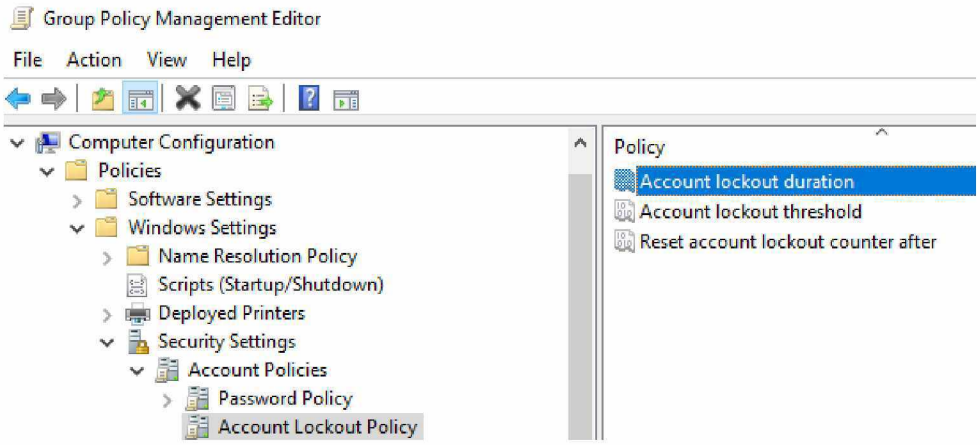

Рисунок 5.2 – Політики облікових записів

5.3 У політиці є три пункти:

1) Час до скидання лічильника блокування (Reset account lockout counter after);
2) Порогове значення блокування (Account lockout threshold);
3) Тривалість блокування облікового запису (Account lockout duration).

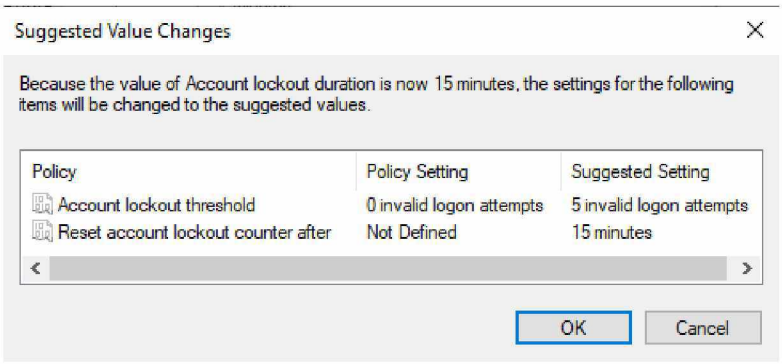

Рисунок 5.3 – Налаштована політика блокування користувача

4. Захист підключення з'єднання з допомогою VPN

VPN-підключення є універсальним рішенням для захисту персональної внутрішньо-корпоративної інформації для власників бізнесу, які не можуть дозволити установку дорогого ПЗ. На ринку подібного сервісу представлені послуги у різних цінових категоріях, є хороші безкоштовні та платні версії, що відрізняються набором функцій, рівнями потужності. Також є прості у використанні сервіси, з якими зможуть звертатися рядові співробітники, адміністратори, тому власнику не доведеться проводити спеціальне навчання або наймати штат штату для налагодження vpn-з'єднання.

6.1 Установка сервера повинна виконуватись під обліком з правами адміністратора (Запуск від імені Адміністратора).

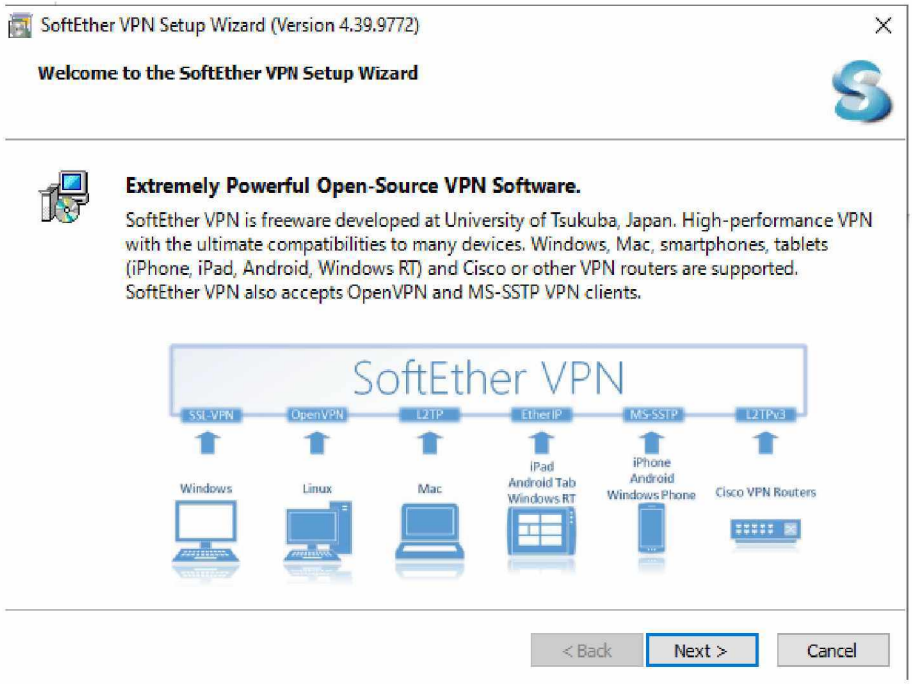

Рисунок 6.1 – Вікно встановлення програми

6.2 Після натискання кнопки Далі потрібно вибрати встановлюваний компонент – SoftEther VPN Server.

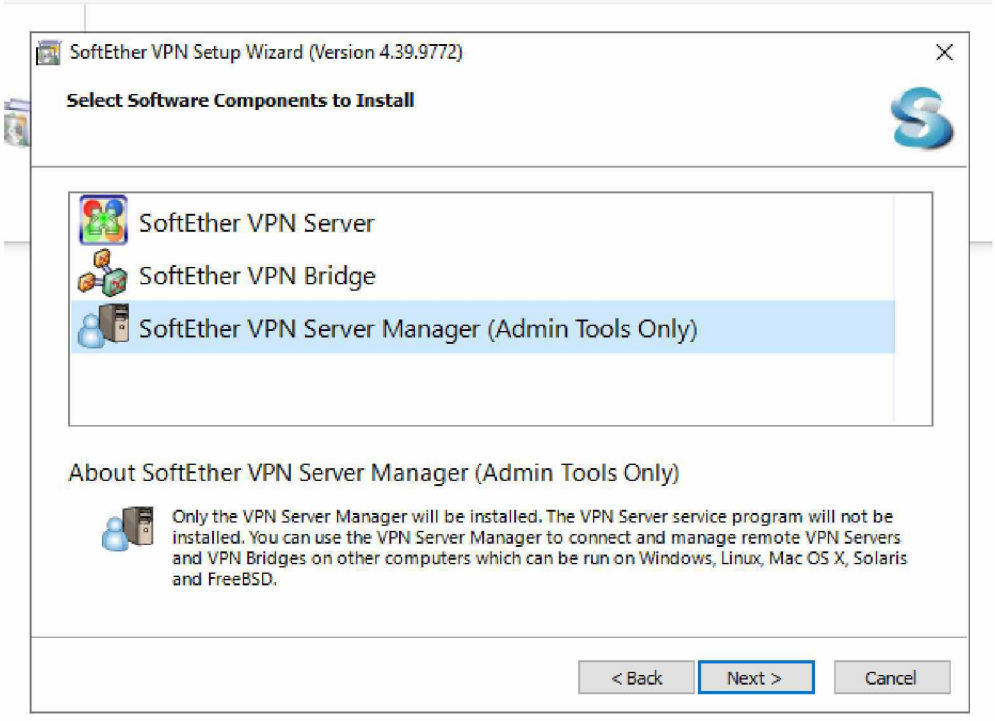

Рисунок 6.2 – Встановлення серверу

6.3 Далі необхідно обрати режими використання SoftEther VPN Server:

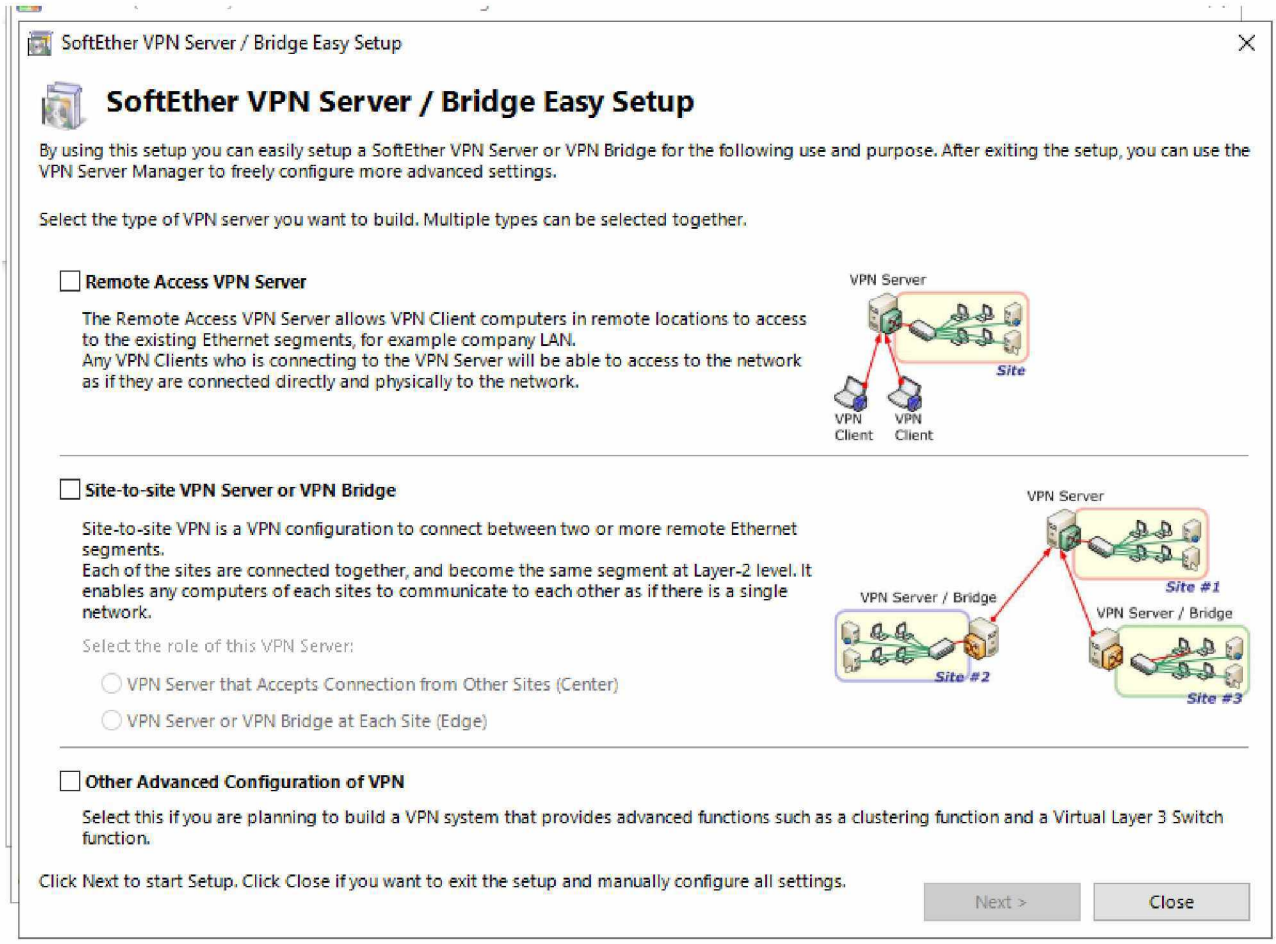

Рисунок 6.3 – Режими користування

6.4 Віртуальний концентратор (хаб, Virtual Hub) функціонує аналогічно реальному та забезпечує зв'язок всіх підключених до сервера клієнтів між собою. Для географічно рознесених клієнтів забезпечується використання протоколів загального доступу, бази даних, ігрових серверів тощо. так само, як вони знаходяться в єдиній локальній мережі. Іншими словами, сервер SoftEher VPN створює віртуальні провідні з'єднання та віртуальні концентратори для всіх підключених до нього клієнтів. Концентраторів може бути кілька та їх імена повинні відрізнятися:

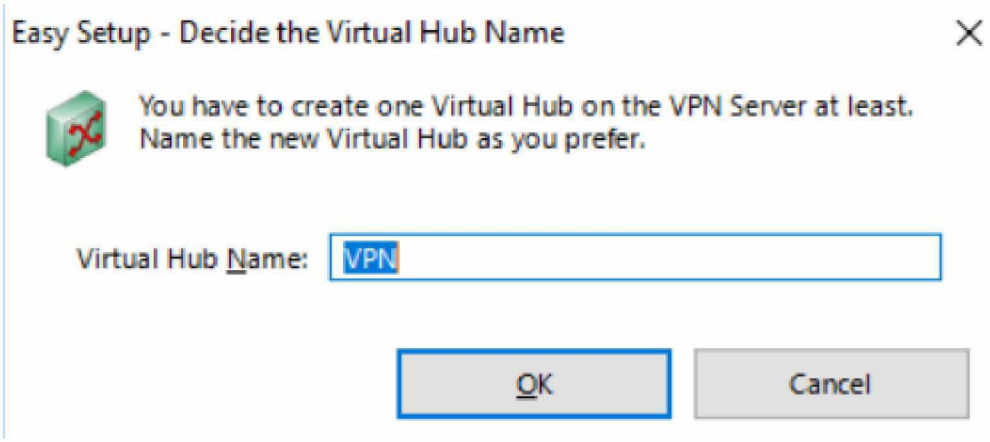

Рисунок 6.4 – Ім’я віртуального концентратора

6.5 На наступному кроці можна і, як правило, навіть потрібно налаштувати динамічний DNS для даного VPN сервера:

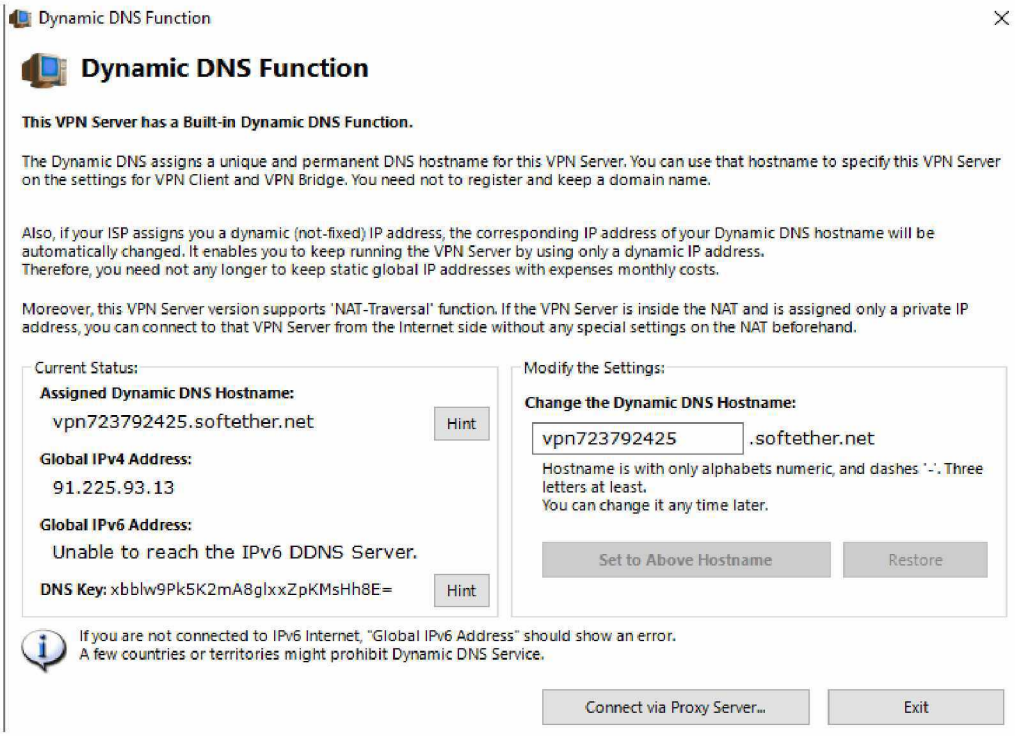

Рисунок 6.5 – динамічний DNS

6.6 Також, у будь-який момент часу можна налаштувати віртуальну приватну мережу з використанням хмарної служби VPN Azure Cloud, створеної в рамках проекту SoftEther VPN:

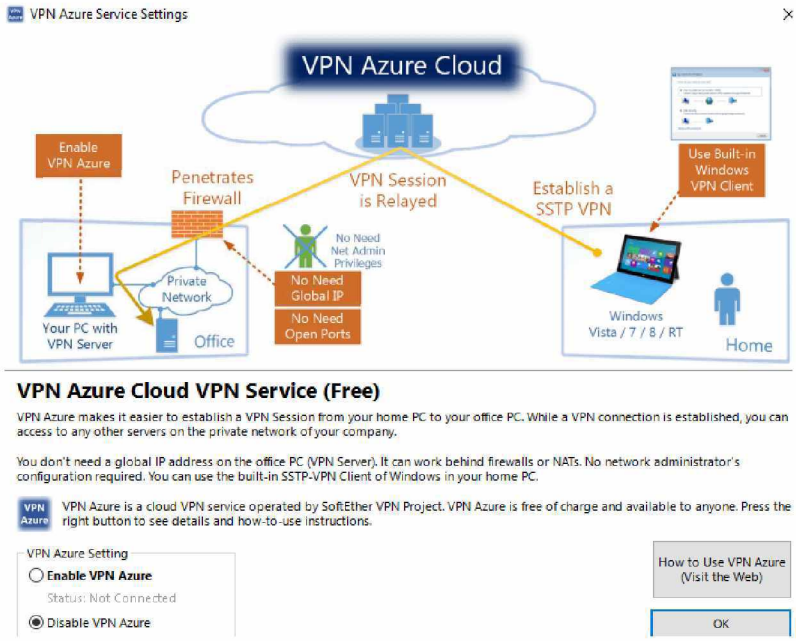

Рисунок 6.6 – Налаштування Azure

6.7 Наступним кроком необхідно створити користувачів сервера SoftEther VPN. Створення користувачів можна виконати у будь-який момент часу, підключившись до сервера та обравши режим керування віртуальним концентратором – Manage Virtual Hub:

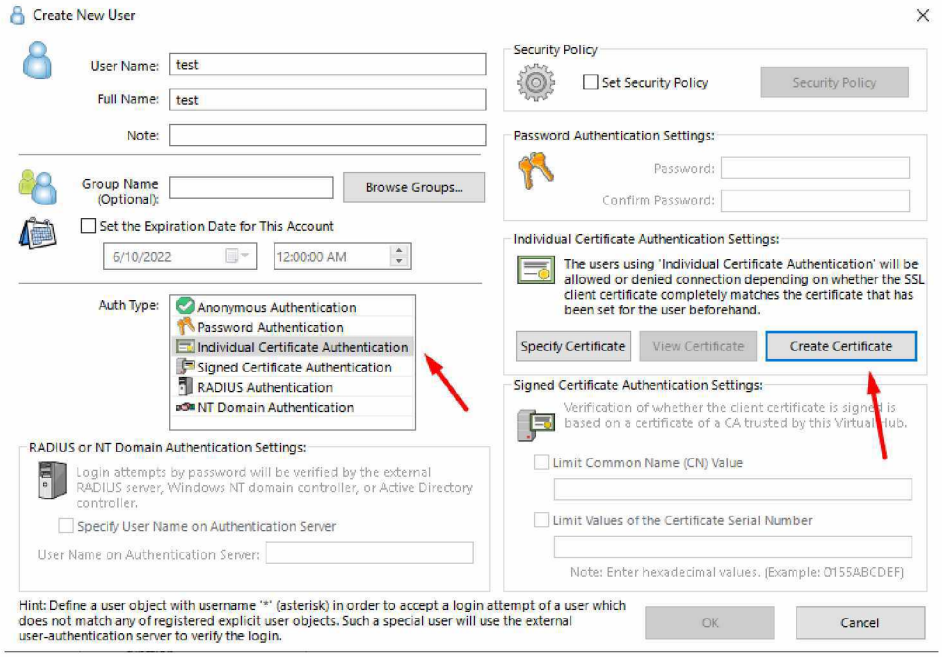

Рисунок 6.7 – Створення нового користувача

6.8 Після створення користувача створюється самопідписаний сертифікат, якого цілком достатньо визначення достовірності користувача, що підключається до серверу VPN. Після натискання Ok буде запропоновано зберегти створений сертифікат:

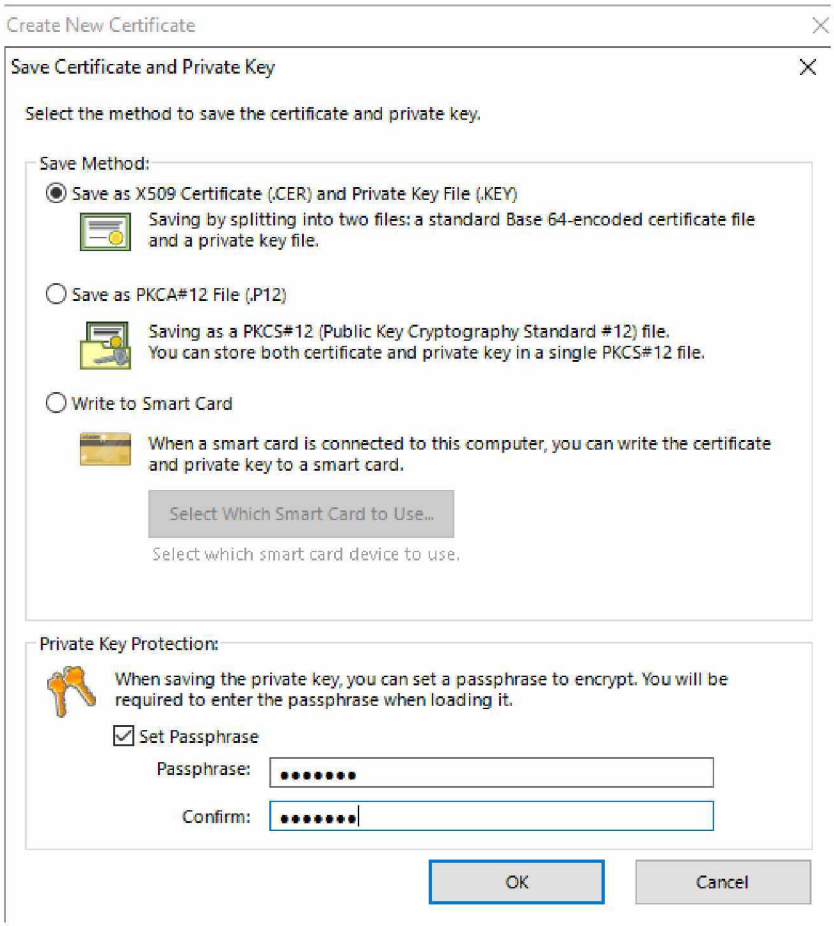

Рисунок 6.8 – Створення сертифікату

6.9 Установка клієнта виконується за замовчуванням. Після встановлення та запуску SoftEther VPN Client Manager потрібно створити віртуальний мережний адаптер і нове VPN-підключення. Можна відразу натиснути кнопку додавання нового підключення – Add VPN Connection, і необхідні елементи будуть створені в процесі додавання;

6.10 Тобто, перед додаванням нового підключення необхідно створити адаптер віртуальної мережі. Після натискання кнопки ”Так” розпочнеться діалог визначення параметрів адаптера Virtual Network Adapter:

Рисунок 6.10 – Адаптер віртуальної мережі

6.11 Можливе створення до 127 віртуальних адаптерів, імена яких мають відрізнятись. Створення адаптера займає деякий час і завершується його появою у нижній половині вікна:

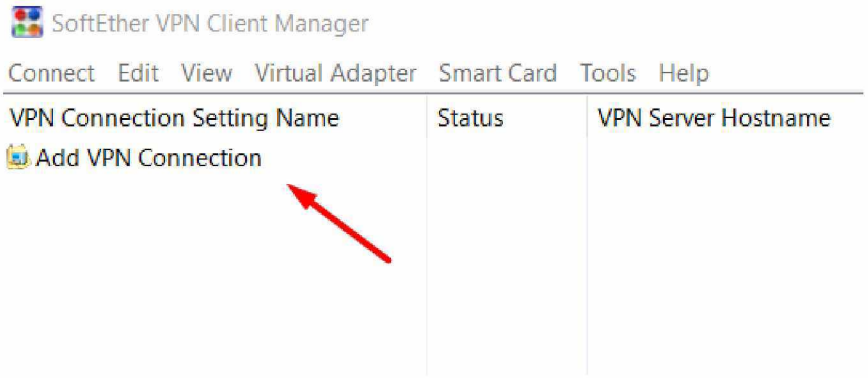

Рисунок 6.11 – Створення vpn з’єднання

6.12 Під час створення нового підключення можна скористатися комбінацією клавіш Ctrl+N:

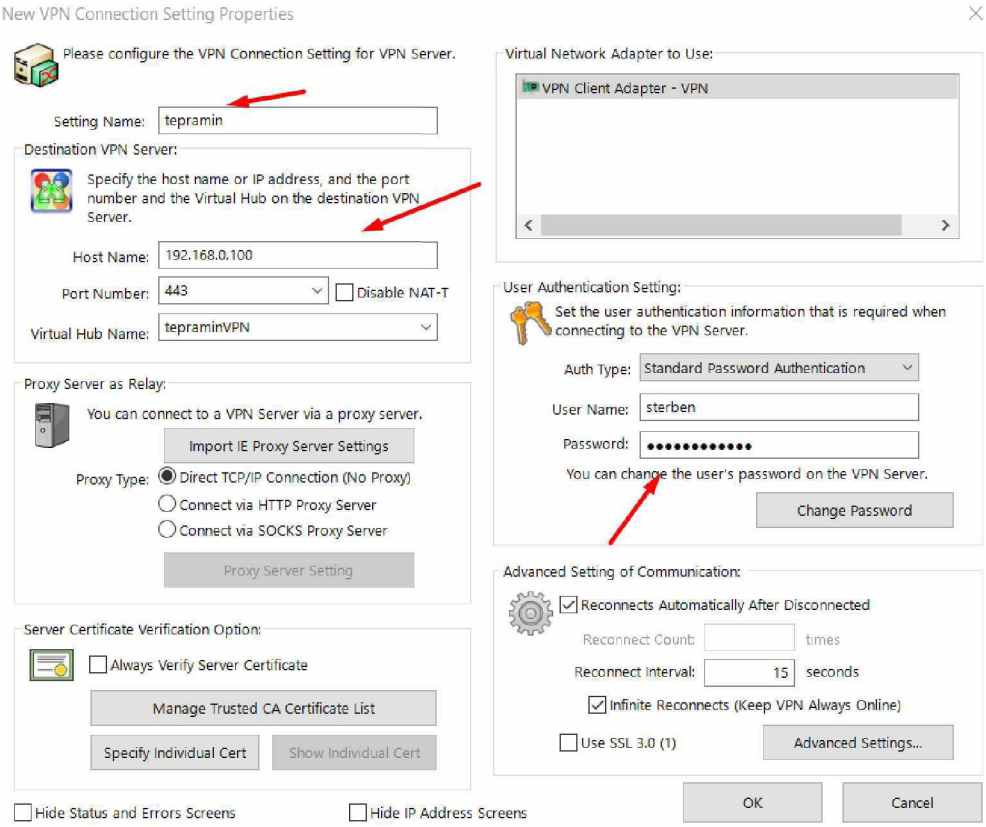

Рисунок 6.12 – Створення підключення

6.13 Після створення з'єднання можна здійснити підключення до сервера за допомогою пункту Connect контекстного меню, яке викликається правою кнопкою мишки на вибраному підключенні:

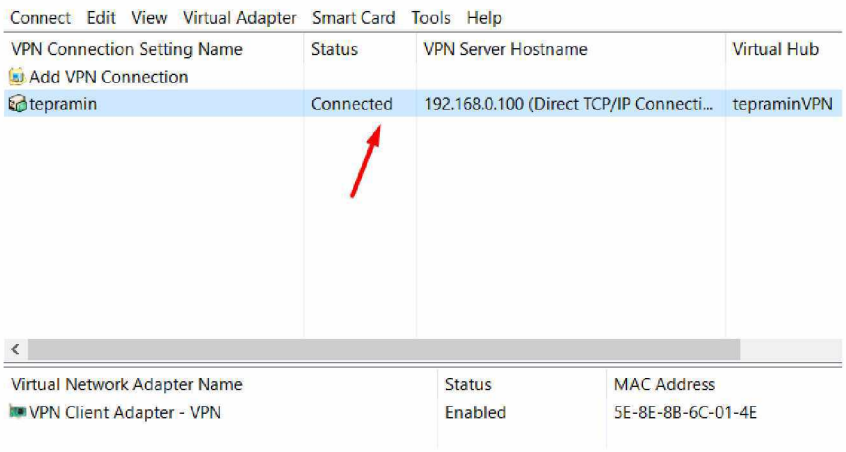

Рисунок 6.13 – Дієздатність підключення

5. RDP Defender для захисту від перебору паролів

Поки ваш сервер Windows є загальнодоступним, дуже висока ймовірність того, що хакери, мережні сканери або боти в якийсь момент спробують вгадати ваші облікові дані для входу.

Хоча вони можуть бути безуспішними, ці спроби можуть викликати навантаження на процесор і пропускну здатність, тому найкраще їх повністю заблокувати.

7.1 Встановлюємо та розгортаємо програму:

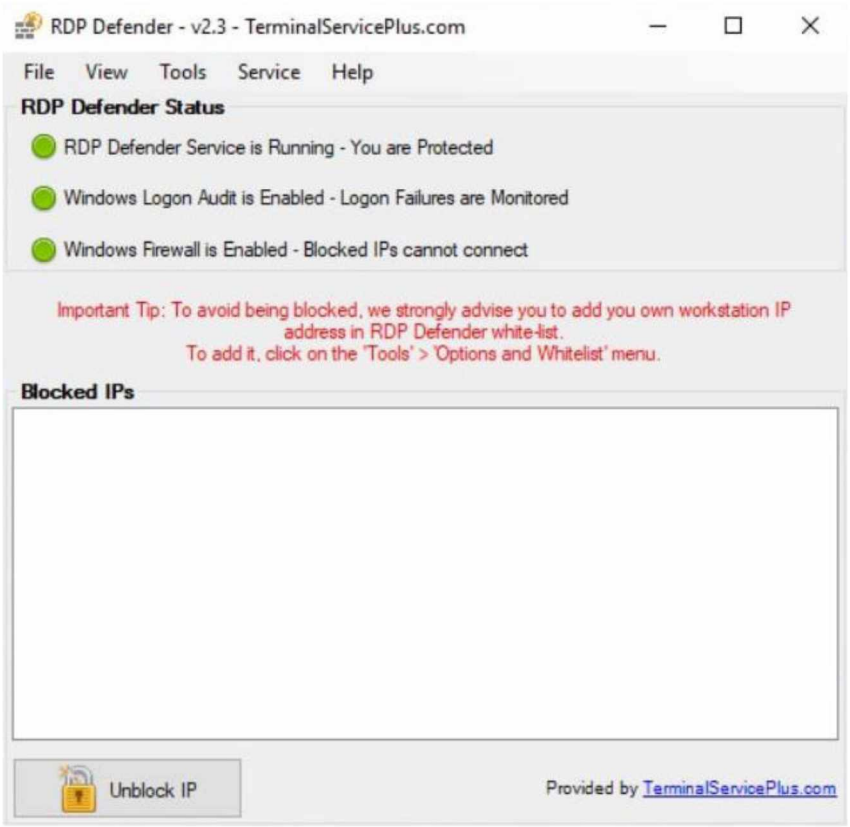

Рисунок 7.1 – Інтерфейс RDP Defender

7.2 Виставляємо мінімальну кількість спроб помилок підключень:

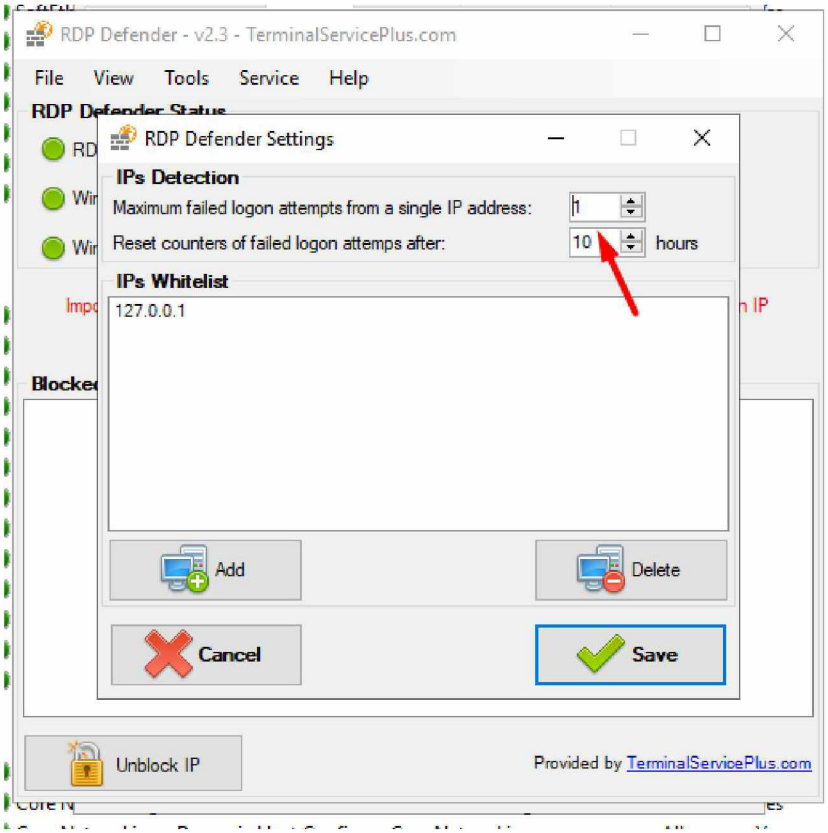

Рисунок 7.2 – Налаштування списку підключень

7.3 Робимо невірну спробу підключення до серверу, задля видимості дієздатності програми:

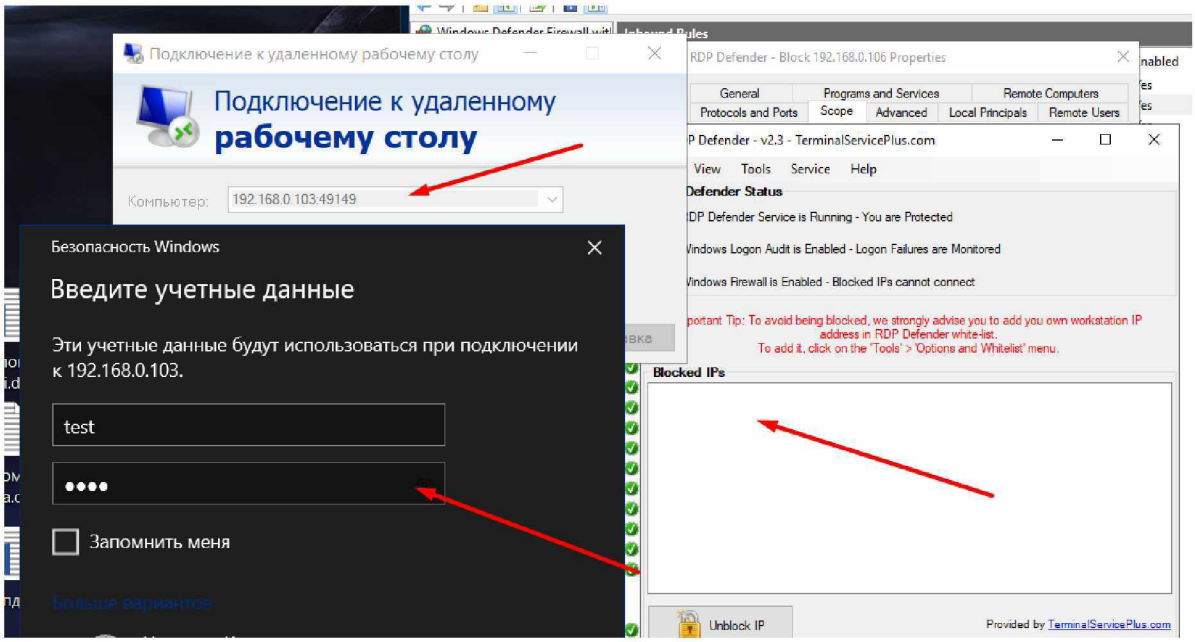

Рисунок 7.3 – Умисне помилкове підключення до серверу

7.4 Результат невірного підключення до серверу:

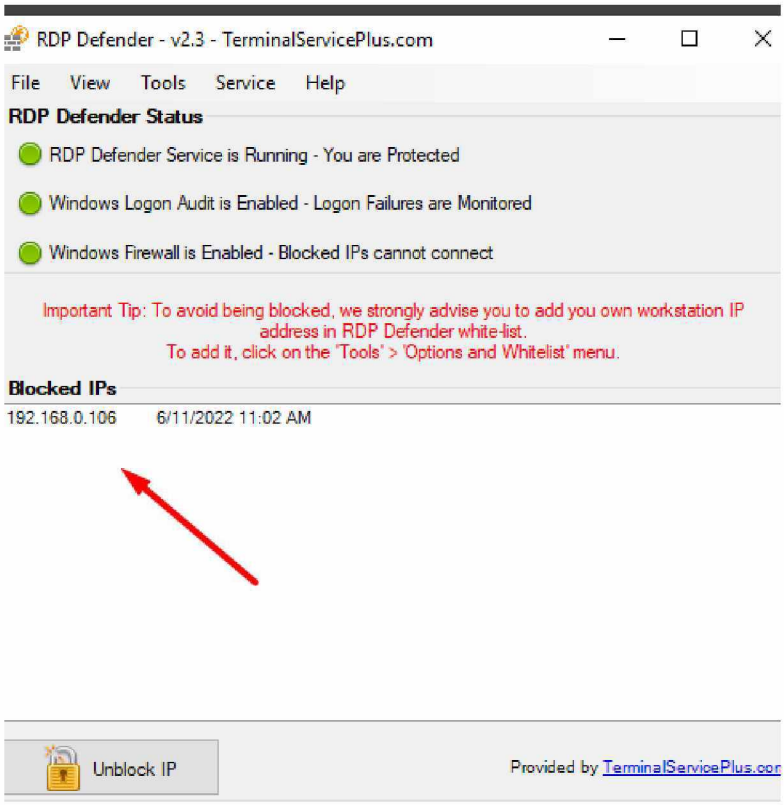

Рисунок 7.4 – IP адреса, яка потрапила в журнал

ВИСНОВОК

В результаті виконання кваліфікаційної роботи було проведено аналіз програмних засобів для забезпечення віддаленої роботи користувачів в комерційних підприємствах, зокрема розкриті теми ролі віддалених робочих столів в обраній операційній системі, розглянуто іншу систему для організації віддаленого доступу та пояснено, чому саме було обрано певний метод дослідження тематики.

Також висвітлено аналіз існуючих технічних рішень для забезпечення кіберзахисту інформаційно-комунікаційних систем, таких як SoftEther VPN, розглянуто систему Firewall, технологію шифрування BitLocker, програмне забезпечення RDP Defender та маршрутизатор Mikrotik.

Проведено розробку методів та підходів до забезпечення кіберзахисту віддаленого підключення до інформаційно-комунікаційної системи підприємства. А саме описано поняття кіберзахисту, його методів, оглянуте фізичне забезпечення кіберзахисту серверів підприємства та розроблений комплекс програмного забезпечення кібербезпеки. Серед них, налаштування ролі віддаленого доступу та встановлення ліцензій, а також методи захисту віддаленого підключення, такі як: заміна стандартного порту, шифрування даних, мережева автентифікація, зміна імені облікового запису та її блокування, у випадку невірно введеного паролю, створено віртуальну приватну мережу та забезпечено захист від підбору паролів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Roles of Remote Desktop Services [Electronic resource] // Developer tools, technical documentation and coding examples | Microsoft Docs. – Mode of access: https://docs.microsoft.com/ru-ru/windows-server/remote/remote-desktop-services/rds-roles (date of access: 01.06.2022);

2. Access a remote desktop | Ubuntu [Electronic resource] // Ubuntu. – Mode of access: https://ubuntu.com/tutorials/access-remote-desktop#1-overview (date of access: 01.06.2022);

3. cat /it/blog/sysadmin. Для чего нужна операционная система Windows Server? [Електронний ресурс] / cat /it/blog/sysadmin // – Режим доступу: https://vk.com/@it_blog_sysadm1n-dlya-chego-nuzhna-operacionnaya-sistema-windows-server (дата звернення: 04.06.2022);

4. SoftEther VPN project - softether VPN project [Electronic resource] // SoftEther VPN Project - SoftEther VPN Project. – Mode of access: https://www.softether.org/ (date of access: 04.06.2022);

5. Межсетевой экран: что такое и как работает - Блог компании Селектел [Електронний ресурс] // Блог компании Селектел. – Режим доступу: https://selectel.ru/blog/firewall/ (дата звернення: 04.06.2022);

6. Gillis A. S. What is BitLocker? Definition from SearchEnterpriseDesktop [Electronic resource] / Alexander S. Gillis // SearchEnterpriseDesktop. – Mode of access: https://www.techtarget.com/searchenterprisedesktop/definition/BitLocker (date of access: 08.06.2022);

7. Download RDP defender 2.4 [Electronic resource] // softpedia. – Mode of access: https://www.softpedia.com/get/Security/Security-Related/RDP-Defender.shtml (date of access: 08.06.2022);

8. MikroTik защита от брутфорса (Brute force) [Електронний ресурс] // itobereg.ru. – Режим доступу: https://itobereg.ru/mikrotik/mikrotik-brute-force-protection (дата звернення: 08.06.2022);

9. Как обеспечить информационную безопасность в компании: полное руководство от А до Я [Електронний ресурс] // Kickidler. – Режим доступу: https://www.kickidler.com/ru/info/kak-obespechit-informaczionnuyu-bezopasnost-v-kompanii.html (дата звернення: 10.06.2022);

10. Xelent. Какой должна быть серверная [Електронний ресурс] / Xelent // data center | Xelent. – Режим доступу: https://www.xelent.ru/blog/kakoy-dolzhna-byt-servernaya/ (дата звернення: 10.06.2022);

11. Установка роли RDP на сервер Windows - WIKI [Електронний ресурс] // WIKI. – Режим доступу: https://www.sim-networks.com/ru/wiki/remote-desktop-protocol-setup-to-windows (дата звернення: 14.05.2022);

12. Смена порта RDP по умолчанию в windows server 2012 | база знаний 1cloud.ru [Електронний ресурс] – Режим доступу: https://1cloud.ru/help/windows/ustanovka-novogo-porta-rdp-po-umolchaniju-v-windows-server-2012 (дата звернення: 17.05.2022);

13. Обеспечение безопасности windows server 2008/2012 | база знаний 1cloud [Електронний ресурс] // Облачный сервис для вашего бизнеса | 1cloud. – Режим доступу: https://1cloud.ru/help/windows/windowssecurity (дата звернення: 13.05.2022)