ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACK – acknowledge

AES – Advanced Encryption Standard

AH – Authentication Header

API – Application Programming Interface

APT – Advanced Persistent Threat

ASA – Adaptive Security Appliance

BYOD – Bring-Your-Own-Device

DES – Data Encryption Standard

DH – Diffie-Hellman

DMZs – Demilitarized Zones

DNS – Domain Name System

DOI – Domain of Interpretation

DPD – Dead Peer Detection

EDR – Endpoint Detection and Response

EMS – Enterprise Management Server

EPP – Endpoint Protection Platform

ESP – Encapsulation Security Payload

ETDR – Endpoint Threat Detection and Response

IaaS – Infrastructure as a Service

IKE – Internet Key Exchange

IPsec – Internet Protocol Security

LAN – Local Area Network

MD5 – Message-digest algorithm

MFA – Multi-Factor Authentication

MitM – Man-in-the-Middle

NAT – Network Address Translation

NGFW – Next-Generation Firewall

PaaS – Platform as a Service

PFS – Perfect Forward Secrecy

SHA – Secure Hash Algorithm

SIEM – Security Information and Event Monitoring

SSO – Single Sign-On

SSE – Cloud-Delivered Security Service Edge

UDP – User Datagram Protocol

UEM – Unified Endpoint Management

VPN – Virtual Private Network

ZT – Zero Trust

ZTA – Zero Trust Architecture

ZTNA – Zero Trust Network Acces

2FA – Two-Factor Authentication

3DES – Triple Data Encryption Standard

ВСТУП

Актуальність дослідження. Актуальність дослідження захисту віддаленої роботи працівників в сучасному світі необхідно розглядати в контексті швидкого розвитку технологій та поширення віддалених форматів роботи, наприклад через пандемії, психологічні або фізичні проблеми тощо. Віддалена робота створює нові виклики для безпеки та конфіденційності даних, а також вимагає нових стратегій захисту для забезпечення продуктивності та безпеки працівників.

Віртуальні приватні мережі (VPN) відіграють ключову роль у забезпеченні безпеки віддаленої роботи, забезпечуючи зашифроване з'єднання між пристроями працівників та корпоративною мережею. Це дозволяє запобігти несанкціонованому доступу до конфіденційної інформації та збільшує безпеку передачі даних через віддалені канали зв'язку.

Багатофакторна автентифікація (MFA) є ще одним важливим елементом безпеки віддаленої роботи, який додає додаткові шари захисту при вході в систему. Така система вимагає від працівника надати додатковий автентифікаційний фактор, наприклад такий як код, отриманий на мобільний пристрій. Це ускладнює заволодіння обліковими даними та зменшує ризик компрометації доступу до систем.

Обидва ці рішення дозволяють працівникам працювати віддалено, забезпечуючи відповідну безпеку та автентичність. Поєднуючи заходи захисту віддаленої роботи працівників із системами VPN та MFA, працівники можуть створити надійний захист від широкого спектру загроз кібербезпеці та покращити загальну безпеку.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів захисту віддаленої роботи працівників на базі FortiClient.

Об'єкт дослідження – захист віддаленої роботи працівників організації.

Предмет дослідження – методи та засоби захисту віддаленої роботи працівників організації на базі FortiClient.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту віддаленої роботи працівників організації на базі FortiClient.

Наукові завдання:

дослідити сутність проблеми захисту віддаленої роботи працівників організації;

проаналізувати основні підходи до захисту віддаленої роботи працівників організації;

проаналізувати існуючі рішення із захисту віддаленої роботи працівників організації;

проаналізувати методи та засоби захисту віддаленої роботи працівників організації на базі FortiClient;

запропонувати варіант системи захисту віддаленої роботи працівників організації на базі FortiClient;

розробити рекомендацій щодо застосування методів та засобів захисту віддаленої роботи працівників організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту віддаленої роботи працівників організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІДДАЛЕНОЇ РОБОТИ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми захисту віддаленої роботи працівників організації

Згідно звіту компанії Gartner [1] повідомляє, що 18% віддалених працівників не зацікавлені в поверненні в офіс, а 50% усіх працівників продовжуватимуть працювати віддалено ще довго після пандемії. Дані Управління Національної Статистики (Office for National Statistics) [2] за період з вересня 2022 року по січень 2023 року свідчать про те, що 44% працівників класифікуються як працівники, які працюють вдома або працюють за змішаною формою зайнятості.

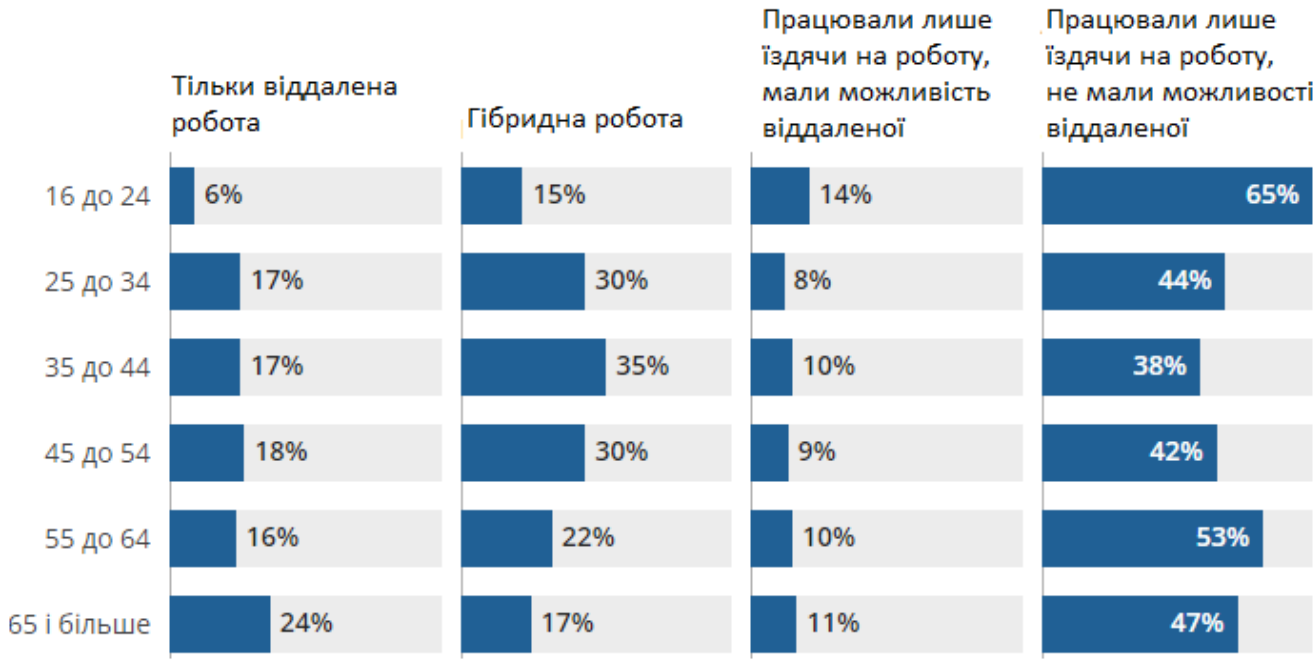

Рис. 1.1. Дані Управління Національної Статистики працюючих за період з вересня 2022 року по січень 2023 року [2]

Однак цей перехід до віддаленої роботи несе в собі безліч ризиків кібербезпеки, до яких організаціям і працівникам слід бути пильними. Фактично, з початку пандемії кількість кібератак на віддалених працівників зросла на 238%. Виходить збільшення кількості віддалених працівників збільшує ризики такої

роботи.

Дискусія про те, чи становлять віддалені працівники більший ризик для кібербезпеки, ніж їхні колеги в офісі, триває. Але зловмисники не перебірливі: вони використовують вразливості і націлюються на співробітників, які нічого не підозрюють, незалежно від їхнього місцезнаходження. За даними Statista [3], 72% організацій висловлюють значне занепокоєння щодо ризиків онлайн-безпеки, з якими стикаються їхні віддалені співробітники.

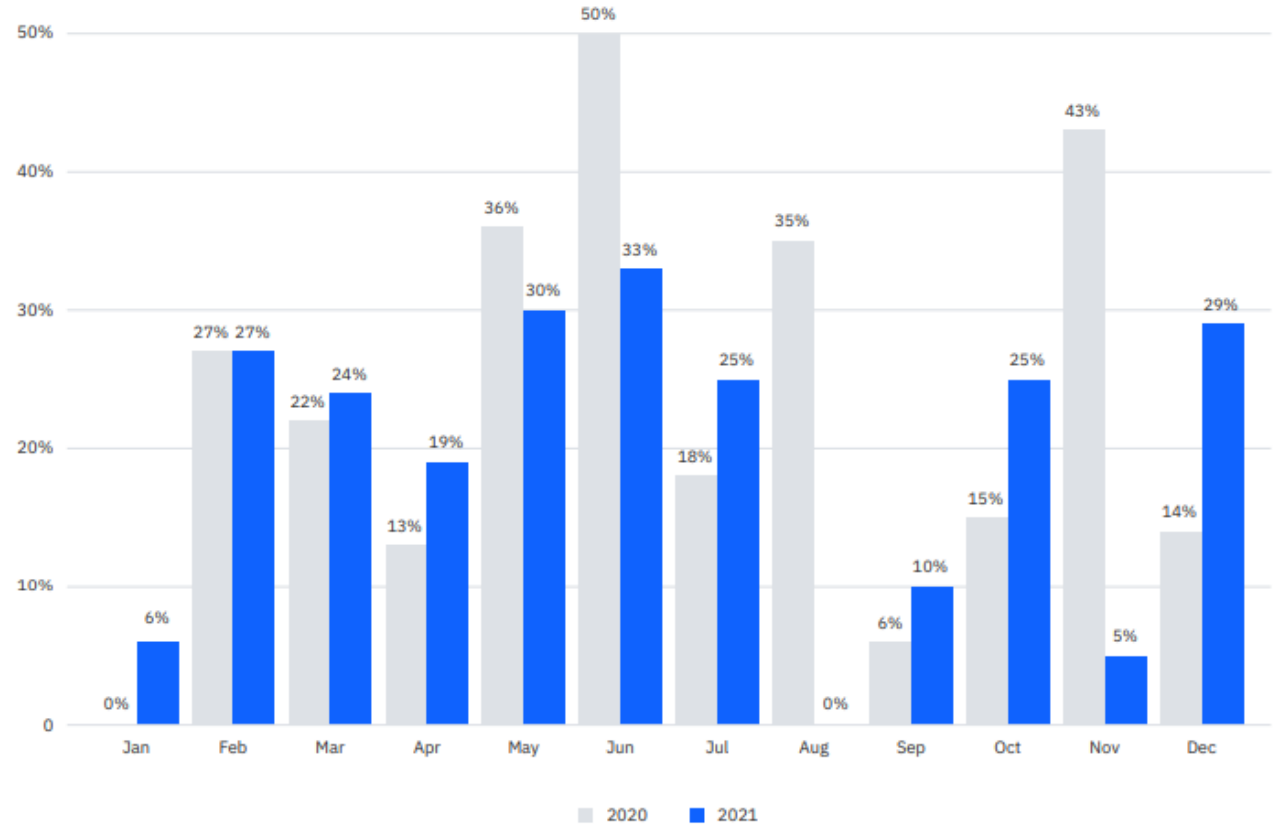

Рис. 1.2. Відсоток реагувань на інциденті, які були пов'язані з програмами-вимагачами, за місяцями, 2020 р. проти 2021 р. [4]

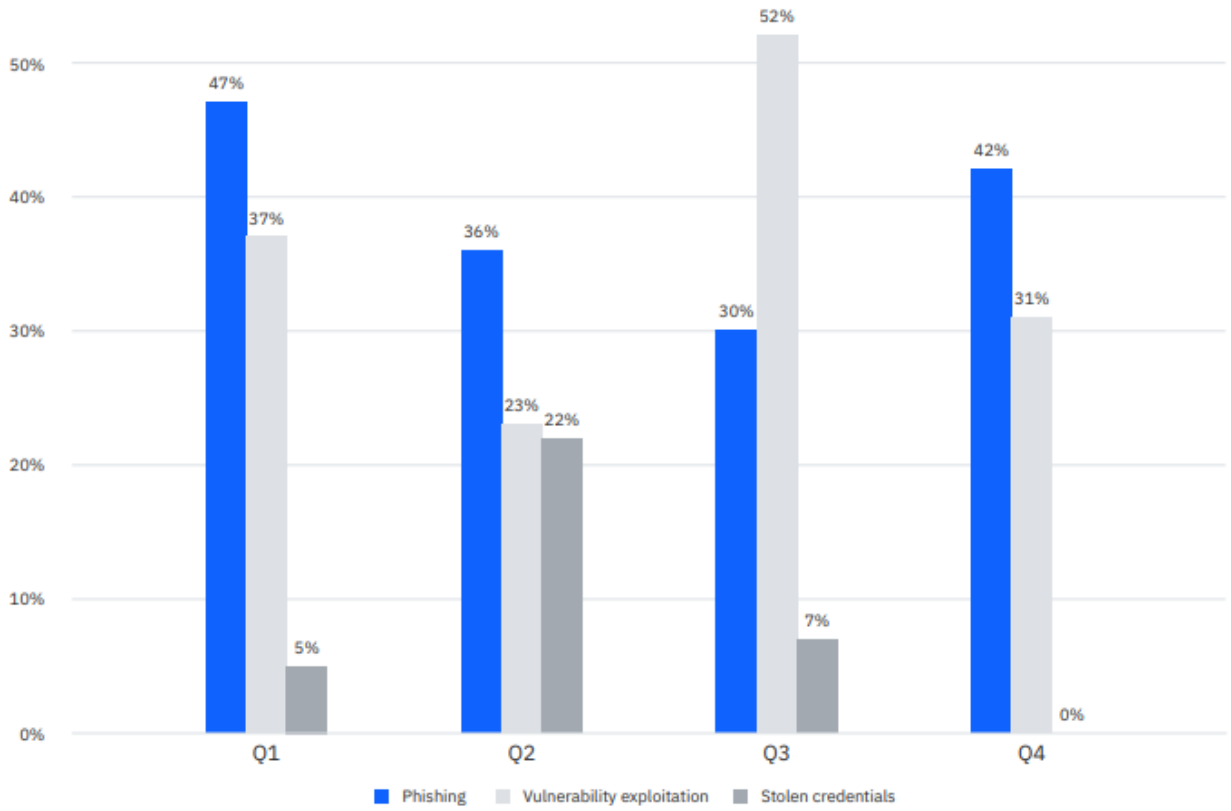

Рис. 1.3. Відсоток атак, пов'язаних з фішингом, використанням вразливостей та викрадених облікових даних, за кварталами, 2021 рік [4]

Фахівці з кібербезпеки вважають найбільшими загрозами кібербезпеці віддаленої роботи певний перелік “слабких місць”, враховуючи які можна значно покращити безпеку такої діяльності. Ось найпоширеніші ризики віддаленої роботи [5] (рис. 1.4):

- шахрайство по електронній пошті – фішингові стратегії є найбільшою кіберзагрозою для віддалених працівників. Фішингові схеми - це коли особа або організація маскується під легітимне джерело, зазвичай електронну пошту, щоб обманом змусити жертву надати приватні облікові дані або конфіденційну інформацію. Ця інформація потім може бути використана для злому облікових записів, крадіжки конфіденційної інформації, шахрайства з особистими даними тощо. Фішингові електронні листи стають дедалі складнішими для працівників виявляти;
- послаблення контролю безпеки – численні існуючі рівні кіберзахисту не будуть застосовуватися до віддалених співробітників. Працівники, які раптово забирають свої робочі пристрої додому, виявляються позбавленими

захисту, оскільки вони замінюють офісну мережу домашнім Wi-Fi;

- кібератаки на інфраструктуру віддаленої роботи – розгортання нової інфраструктури не тільки посилює існуючі методи контролю, але й створює нові ризики. Команди безпеки повинні бути напоготові на випадок атак грубої сили та атак на стороні сервера. Крім того, захист від DDoS-атак стане життєво важливим. Це буде перший випадок для багатьох організацій, коли DDoS-атака може зруйнувати їхній бізнес, перешкоджаючи віддаленим працівникам отримати доступ до Інтернет-послуг;
- доступ до конфіденційних даних через незахищені мережі Wi-Fi – через незахищені громадські мережі Wi-Fi співробітники можуть підключитися до домашньої бездротової мережі або отримати доступ до своїх корпоративних акаунтів. Зловмисники можуть легко підглядати за їхніми з'єднаннями та збирати конфіденційні дані. Наприклад, кіберзлочинці можуть зловити та вкрасти дані, надіслані звичайним текстом у незашифрованому вигляді;
- розширення атак – зі збільшенням кількості людей, які працюють віддалено, підприємства просто мають більше кінцевих точок, мереж і програмного забезпечення для захисту, що значно збільшує обсяг роботи для IT-відділів, які часто бувають перевантажені;
- особисті пристрої, що використовуються для роботи – багато працівників передають файли між робочим і особистим комп'ютерами під час роботи з дому, що викликає занепокоєння. Крім того, в останні роки стала популярною практика, відома як "Принеси свій власний пристрій" або політика BYOD, яка дозволяє працівникам використовувати свої власні пристрої на роботі;
- проблема громадських місць – вавіть якщо кібербезпека знаходиться в центрі нашої уваги,не можна повністю ігнорувати фізичну безпеку, коли мова йде про конфіденційну інформацію. Наприклад, є співробітники, які можуть голосно розмовляти по телефону під час роботи в громадських місцях, виставляти екран свого ноутбука на загальний огляд у кафе або навіть залишати свої пристрої без нагляду;

- слабкі паролі – часто працівники намагаються захистити свої облікові записи слабкими паролями, що стає потенційно великою загрозою для працівника та його конфіденційних даних. Повторні паролі - ще один поширений небезпечний прийом, який використовують кіберзлочинці. Після того, як вони зламають пароль до одного облікового запису, вони намагатимуться отримати доступ до інших облікових записів, використовуючи той самий пароль. Працівники, які повторюють паролі, особливо в особистих і робочих акаунтах, піддаються більшому ризику стати жертвами кібератаки;
- практика незашифрованого обміну файлами – працівники щодня можут обмінюватись великою кількістю приватних даних, від інформації про клієнтські рахунки до файлів тощо, що ,наприклад, компанія не може дозволити собі не захистити цю інформацію від викрадення кіберзлочинцями. Перехоплення конфіденційної інформації компанії може призвести до шахрайства з персональними даними, атак з вимогою викупу, крадіжок тощо;
- неправильні конфігурації хмарних технологій – хмара є важливою технологією для віддаленої роботи, хоча вона також пов'язана з певними ризиками. Неправильні конфігурації, особливо ті, що пов'язані з доступом, становлять один з таких ризиків. Компанії можуть випадково надати користувачам занадто великий доступ або не впровадити контроль доступу;
- злом веб-камери – коли співробітники працюють з дому, вони часто беруть участь у телеконференціях і відеодзвінках, які вимагають від них використання веб-камери. На жаль, хитрі кіберзлочинці можуть легко і незаконно отримати доступ до їхньої веб-камери, порушуючи їхню приватність. Ще гірше, якщо вдома розкидані конфіденційні документи, зловмисники можуть побачити їх, перехопивши їхню веб-камеру;
- загрози скрізь – ризики для безпеки віддаленої роботи існують скрізь! Перехід на віддалену роботу є благословенням для зловмисників. Однак є інструменти та механізми, що зможуть надати відповідний захист для віддаленої роботи.

Рис. 1.4. Найпоширеніші ризики віддаленої роботи [5]

Враховуючи усі вищеперераховані ризики може здатися, що віддалена робота несе за собою тільки небезпеку як для компаній, так і для працівників, які на ці компанії можуть працювати, і що такий режим роботи не є вартим уваги, але ці думки є до тих пір поки не починають розглядатися практичні методи захисту віддаленої роботи працівників, створена безпека яких є не гірша за аналоги виїзної безпеки роботи працівників.

1.2. Аналіз підходів до захисту віддаленої роботи працівників організації

Зі зростанням кількості віддалених працівників зростає і кількість кібератак, що є взаємопов'язаними чинниками. Розуміння найкращих практик для віддалених працівників стає критично важливим у світі зростаючих загроз. Існує багато підходів до захисту віддаленої роботи працівників, кожен з яких має свої переваги та недоліки. Нижче буде наведено найкращі практики боротьби з ризиками безпеки віддаленої роботи:

- MFA/2FA (багатофакторна автентифікація/двофакторна автентифікація) – за даними Zipdo [6], 50% компаній дозволяють віддаленим працівникам отримувати доступ до IT-мережі організації без будь-якої багатофакторної автентифікації. Впроваджуючи MFA/2FA у всіх системах та облікових записах, дозволить забезпечити додатковий рівень безпеки, вимагаючи від віддалених працівників надати кілька форм перевірки (наприклад, пароль і тимчасовий код) перед отриманням доступу, що значно посилює захист від несанкціонованого доступу та слугуватиме слугуватиме додатковим рівнем безпеки. Чим більше таких рівнів, тим менший ризик того, що кіберзлочинці отримають доступ до ваших чутливих систем;
- використання менеджера паролів – окрім багатофакторної автентифікації, що стосується паролів, потрібно заохочувати віддалених працівників використовувати надійний менеджер паролів. Ці інструменти генерують надійні, унікальні паролі для кожного облікового запису, надійно зберігають їх і автоматично вводять за потреби. Це мінімізує ризик слабких паролів або повторного використання паролів і підвищує безпеку паролів. Таким чином, працівникам не потрібно буде запам'ятовувати всі різні паролі, які їм потрібно налаштувати для своїх робочих акаунтів;
- використання VPN (Віртуальної Приватної Мережі) – за даними Zipdo [6], лише 43% працівників використовують VPN під час віддаленої роботи. Забезпечте використання VPN для створення безпечних, зашифрованих з'єднань між віддаленими працівниками та ресурсами компанії. Це захищає

дані від перехоплення, маючи вирішальне значення, коли ваші співробітники підключаються до незахищених мереж, таких як точки доступу Wi-Fi, навіть коли вони працюють з дому. Рекомендується, щоб ваші співробітники використовували конкретний VPN, наприклад вашої компанії. Цей інструмент маршрутизує трафік через інтернет з приватної мережі вашої організації, забезпечуючи ще більший рівень безпеки. По суті, будь-хто, хто спробує перехопити зашифровані дані, не зможе їх прочитати. Таким чином, ваші співробітники зможуть підключатися до інтрамережі вашої компанії (якщо вона у вас є);

- впровадження політики безпеки Work-From-Home (для роботи з дому) – політика безпеки віддаленої роботи буде письмовою стратегією компанії, яка визначає всі правила та практики для всіх співробітників, які виконують свої обов'язки за межами фізичного офісу організації. Ці політики часто включають всі важливі аспекти онлайн-безпеки, наприклад чітке визначення того, які посади мають право на віддалену роботу; список інструментів та платформ, які вони повинні використовувати як віддалені працівники; надання працівникам інструкції щодо дій при перших ознаках компрометації акаунта, щоб у разі чого - працівники мали чіткі інструкції як діяти в таких ситуаціях;
- уникання публічного Wi-Fi – нагадування віддаленим працівникам про необхідність уникати публічних мереж Wi-Fi для виконання важливих робочих завдань також є формою додаткового захисту віддаленої роботи. Якщо публічний Wi-Fi необхідний, використання VPN стає ще більш важливим для додаткового захисту;
- зберігати робочі дані на робочих пристроях – необхідно заохочувати працівників чітко розмежовувати робочі та особисті дані на своїх пристроях. Це мінімізує ризик того, що окремі програми чи акаунти можуть скомпрометувати конфіденційну та/або корпоративну інформацію;
- блокування видимості того, що відбувається на робочих пристроях – віддалені працівники повинні облаштувати свої робочі місця так, щоб

сторонні особи не могли бачити їхні екрани. Це особливо важливо при роботі в громадських місцях;

- ніколи не залишати пристрої незаблокованими – автоматичне блокування та надійні, унікальні паролі або біометрична автентифікація підвищують загальний рівень безпеки;
- регулярне оновлення програмного забезпечення – як би це банально не було. Налаштування автоматичного оновлення програмного забезпечення не лише операційної системи, але й додатків та патчів безпеки є достатньо вдалим підходом захисту віддаленої роботи працівників організації. Регулярне оновлення пристроїв гарантує оперативне усунення вразливостей. Якщо це працівник компанії, замість того, щоб покладати на нього зобов’язаність пам’ятати та вчасно оновлювати ПО, краще внести інформацію про оновлення програмного забезпечення як обов'язкову для них у календарі та через внутрішні канали зв'язку;
- обережне надання спільного доступу до екрана – потрібно попереджувати віддалених працівників бути обережними, надаючи спільний доступ до екрана під час мережевих дзвінків або презентацій. Завжди перевіряти вміст, який буде відображатися, і обмежувати спільний доступ до екрана лише необхідним для цього працівникам;
- керування цифровим слідом та інформацією, якою працівник ділиться в соціальних мережах – співробітники повинні бути проінформовані про потенційні ризики, пов'язані з поширенням особистої або робочої інформації в соціальних мережах. Надмірне поширення може надати зловмисникам цінну інформацію для атак соціальної інженерії;
- застереження щодо веб-камери – необхідне заохочування використання чохлів для веб-камер або програмних засобів для вимкнення камери, коли вона не використовується. Злом веб-камери є реальною загрозою, тому віддаленим працівникам слід активно захищати свою конфіденційність;
- відстеження всіх віддалених з'єднань – команди безпеки повинні використовувати інструменти та практики для відстеження та моніторингу

всіх віддалених з'єднань. Повна видимість віддалених робочих середовищ необхідна для раннього виявлення загроз і реагування на них;

- пріоритезувати доступне навчання з кібербезпеки – на жаль, 30% віддалених працівників не отримують регулярного навчання від своїх роботодавців, а за даними Data Basix [7] , 44% працівників не проходять навчання з кібербезпеки щодо загроз роботи з дому. Забезпечення віддаленим працівникам легкий доступ до політик кібербезпеки, навчальних матеріалів та ресурсів сприяє постійному навчанню та підвищенню обізнаності, що в свою чергу надає працівникам бути в курсі останніх загроз та найкращих практик.

Розширюючи та послідовно впроваджуючи наведені вище найкращі практики, компанії можуть створити надійний захист від ризиків кібербезпеки, пов’язаних із віддаленою роботою, і захистити цінні дані та операції.

Чому все таки потрібна політика безпеки віддаленої роботи? Вражаючі 47% компаній наразі пропонують своїм співробітникам віддалену роботу на повний робочий день, а вражаючі 82% пропонують своїм працівникам принаймні один день на тиждень працювати вдома. Дистанційна робота залишається, і організації повинні адаптуватися до мінливого ландшафту кібербезпеки.

Останні рецензовані дослідження показують, що віддалені працівники часто демонструють більш стійку поведінку щодо кібербезпеки, ніж їхні колеги, які працюють на місці. Проте рівень загрози залишається високим. Перехід на віддалену роботу збільшив середню вартість витоку даних на 137 000 доларів.

Усвідомлюючи ризики безпеці, пов’язані з віддаленою роботою, і застосовуючи найкращі практики, перелічені вище, стає можливим покращити кібербезпеку компанії та захистити віддалених працівників від загроз.

Щоб підтримувати цілісність і безпеку даних компанії та працівників в епоху цифрових технологій, стає життєво важливо розробити комплексну політику кібербезпеки для віддаленої та офісної роботи.

1.3. Аналіз існуючих рішень із захисту віддаленої роботи працівників організації

Існує багато різних рішень із захисту віддаленої роботи працівників на ринку, що надають різні можливості та функціональність. В залежності від вашої потреби можна обрати конкретну платформу, яка вам буде найзручніша у використанні та стане у нагоді саме з вашими унікальними сценаріями застосування.

Для початку розглянемо таке рішення як Cisco AnyConnect. Це одна з провідних платформ для захисту віддаленої роботи працівників, яке розробляється компанією Cisco Systems. Ця платформа надає широкий спектр можливостей для забезпечення безпеки та захисту корпоративних ресурсів під час роботи з віддаленими працівниками. Давайте розглянемо більш детально переваги та недоліки Cisco AnyConnect:

- шифрування трафіку – Cisco AnyConnect забезпечує шифрування всього трафіку, який пересилається між пристроями користувача та корпоративною мережею. Це забезпечує конфіденційність та захист від перехоплення чутливої інформації;
- гнучкі налаштування безпеки – програмне забезпечення має широкий набір налаштувань безпеки, які можуть бути налаштовані під конкретні потреби організації. Це включає в себе правила доступу, контроль вмісту, механізми автентифікації та інші;
- інтеграція з іншими системами безпеки – Cisco AnyConnect може інтегруватися з іншими системами безпеки, такими як системи моніторингу загроз, механізми ідентифікації та автентифікації, що дозволяє створювати комплексні заходи безпеки;
- ліцензування та підтримка – одним із недоліків Cisco AnyConnect є необхідність придбання ліцензій для його використання. Крім того, для ефективного використання програми може знадобитися підтримка з боку спеціалістів або IT-адміністраторів;
- складність налаштування та управління – для непрофесійних користувачів

або організацій може виникнути складність у налаштуванні та управлінні Cisco AnyConnect. Встановлення та налаштування програмного забезпечення може вимагати певних технічних знань.

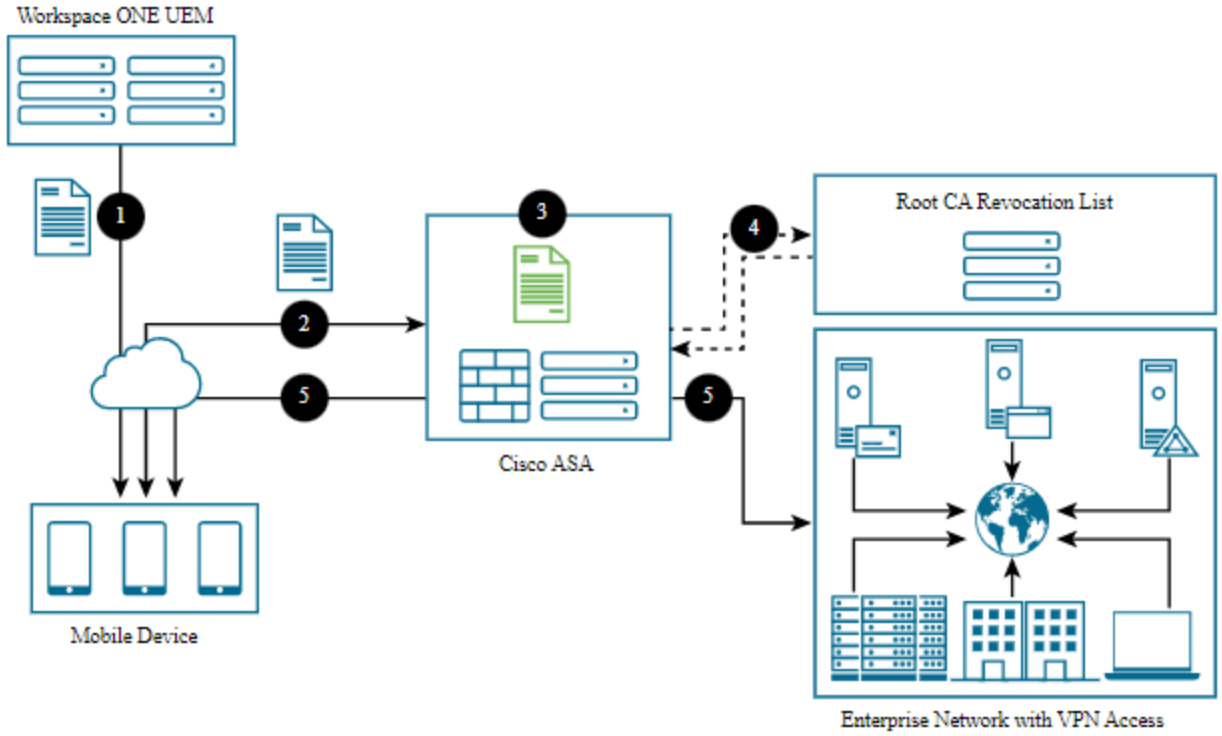

Рис. 1.5. Архітектура CiscoAnyConnect [8]

Архітектура CiscoAnyConnect працює наступним чином: автентифікація за допомогою сертифіката виконується з моменту реєстрації пристрою користувача в Workspace ONE Unified Endpoint Management (UEM), що є програмним забезпеченням, яке керує життєвим циклом пристрою та захищає корпоративні дані на пристроях, до моменту, коли користувач отримує VPN-доступ до захищеної корпоративної мережі. 1. Після реєстрації пристрою Workspace ONE UEM надсилає на пристрій профіль, який містить сертифікат ідентифікації користувача та налаштування конфігурації Cisco AnnyConnect. 2. Коли пристрій використовує VPN, пристрій надсилає сертифікат ідентифікації до кінцевої точки VPN ASA (Adaptive Security Appliance) для автентифікації. 3. ASA забезпечує створення та керування безпечними віртуальними приватними мережами для захисту комунікації та даних в корпоративних мережах та перевіряє, що сертифікат ідентифікації пристрою надійшов від того самого ЦС, що й його власний сертифікат ідентифікації, і обидва були підписані сертифікатом ЦС. 4. Додатково,

якщо перевірку CRL (Certificate Revocation List) увімкнено, яка перевіряє дійсності сертифіката шляхом перевірки його статусу у списку відкликаних сертифікатів, ASA регулярно отримує, аналізує та кешує CRL CA, щоб підтвердити, що сертифікат ідентифікації пристрою не було відкликано. 5. ASA надає пристрою доступ до VPN. Тепер пристрій може безпечно отримувати доступ до внутрішніх ресурсів підприємства.

Загалом, Cisco AnyConnect є потужним і надійним рішенням для захисту віддаленої роботи працівників, проте вимагає певних витрат на ліцензування та може бути складним у налаштуванні для деяких користувачів.

Далі буде розглянута не менш відома платформа як Microsoft Azure Active Directory (Azure AD). Вона є ідентифікаційним та керувальним сервісом, який надається Microsoft в хмарному середовищі Azure. Він використовується для керування ідентифікацією користувачів, контролю доступу та безпеки в хмарному середовищі. Ось детальніше про особливості цієї платформи в порівнянні з іншими рішеннями:

- автентифікація та контроль доступу – Azure AD надає можливості для автентифікації користувачів з використанням різних методів, включаючи паролі, MFA, сертифікати та інші. Це забезпечує контроль доступу до ресурсів на основі політик, ролей та умов, що дозволяє адміністраторам точно налаштувати права доступу користувачів;
- інтеграція з іншими сервісами Microsoft – однією з основних переваг Azure AD є його інтеграція з іншими сервісами та продуктами Microsoft, такими як Office 365, Microsoft 365, Azure, SharePoint, Teams тощо. Це дозволяє користувачам одночасно використовувати один обліковий запис для доступу до різних сервісів та додатків;
- моніторинг та аналіз активності користувачів – Azure AD забезпечує можливості моніторингу та аналізу активності користувачів, включаючи входи в систему, зміни прав доступу, намагання неуспішної автентифікації тощо. Це допомагає виявляти аномальну або підозрілу активність та реагувати на неї для запобігання потенційним кіберзагрозам;

- додаткові можливості безпеки – Azure AD пропонує додаткові можливості безпеки, такі як управління правами доступу, управління ідентифікацією та захист автентифікації. Включає в себе функції захисту від фішингу, виявлення несправжніх користувачів, контроль доступу на основі стану пристрою тощо.

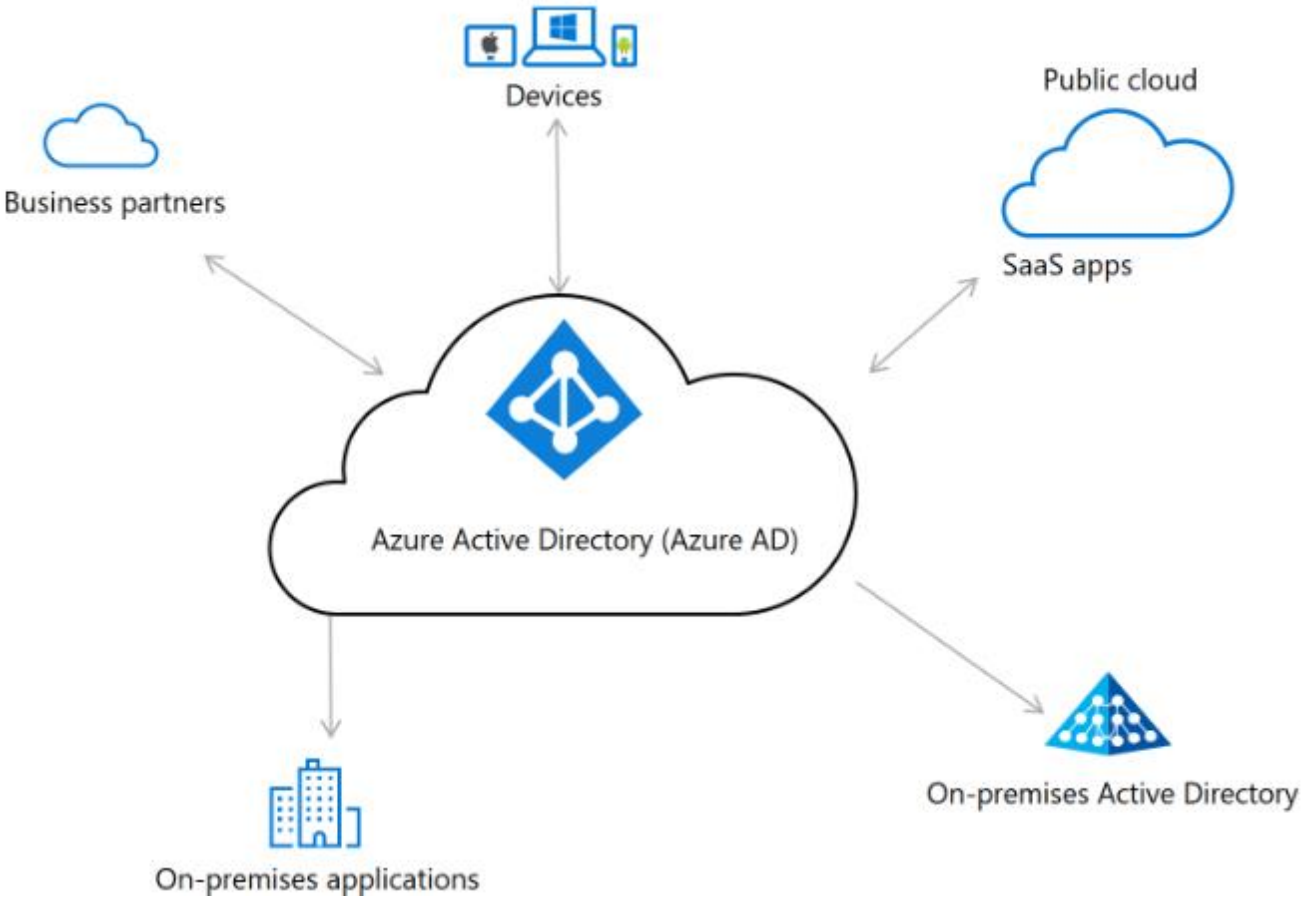

Рис. 1.6. Архітектура Microsoft Azure Active Directory [9]

Хоча Azure AD має свої переваги, варто враховувати, що він вимагає використання екосистеми Microsoft, а деякі функції можуть вимагати додаткової підписки. Однак для організацій, які вже використовують продукти Microsoft або планують мігрувати до хмарної інфраструктури Azure, Azure AD може бути відмінним вибором для захисту віддаленої роботи працівників організації.

Наступною буде представлена інноваційна платформа для захисту віддаленої роботи працівників, яка надає безпечний доступ до корпоративних даних без використання традиційних VPN. А саме це Zscaler Private Access (ZPA) і детальніше про її особливості та переваги порівняно з іншими платформами:

- безпечний доступ без VPN – Zscaler Private Access використовує архітектуру Zero Trust, що дозволяє забезпечити безпечний доступ до корпоративних ресурсів без використання VPN. Замість цього, вона забезпечує безпечне підключення до хмарних або локальних додатків без прямого підключення до мережі;
- гнучкість контролю доступу – ZPA надає гнучкі можливості для контролю доступу, що дозволяє адміністраторам точно налаштувати права доступу користувачів до різних ресурсів на основі різних параметрів, таких як ідентифікатори користувачів, стан пристроїв, мережеві умови тощо;
- захист від кіберзагроз – платформа забезпечує високий рівень захисту від різних кіберзагроз, включаючи атаки типу Man-in-the-Middle (MitM), фішинг, витоки даних тощо. Вона використовує передові технології шифрування та автентифікації для забезпечення безпеки даних та комунікацій;
- абонентська плата та підтримка – однією з переваг є можливість отримання технічної підтримки та регулярних оновлень за допомогою абонентської плати. Це дозволяє користувачам отримувати якісну підтримку та забезпечує постійне оновлення системи з метою забезпечення безпеки;
- інтеграція – чоча Zscaler Private Access може інтегруватися з різними системами, інтеграція може бути складною для деяких існуючих інфраструктур. Однак, якщо інтеграція належним чином налаштована, ZPA може бути потужним засобом захисту віддаленої роботи.

В цілому, Zscaler Private Access є перспективним інструментом для захисту віддаленої роботи працівників, який забезпечує безпечний доступ до корпоративних ресурсів, гнучкість контролю доступу та високий рівень захисту від кіберзагроз. Його варто розглядати серед інших платформ з цією метою, зокрема для компаній, що активно використовують хмарні сервіси та шукають альтернативні рішення до традиційних VPN.

Останнім розглянутим рішенням є FortiClient. Він являє собою програмне забезпечення для захисту віддаленої роботи працівників, розроблене компанією Fortinet. Ця платформа має ряд особливостей та функцій, що роблять її потужним

інструментом для забезпечення безпеки та захисту корпоративної мережі віддаленими працівниками. Ось детальніше про особливості FortiClient:

- VPN і захист трафіку – FortiClient надає можливість встановлення захищеного з'єднання з корпоративною мережею за допомогою VPN. Всі дані, що передаються через це з'єднання, шифруються, що забезпечує конфіденційність інформації;
- захист від загроз – FortiClient має вбудовані функції захисту від загроз, такі як антивірус, антиспам, антишпигунство та брандмауер. Це допомагає запобігти витокам даних та іншим кіберзагрозам;
- керування пристроями – платформа дозволяє адміністраторам керувати пристроями віддалених працівників, встановлювати політики безпеки, виконувати оновлення програмного забезпечення та виявляти потенційні загрози;
- інтеграція з Fortinet Security Fabric – FortiClient інтегрується з Fortinet Security Fabric, що дозволяє створювати комплексні заходи безпеки та автоматизувати процеси виявлення та реагування на загрози;
- підтримка різних платформ – FortiClient доступний для різних операційних систем, таких як Windows, macOS, Android та iOS, що робить його універсальним рішенням для захисту пристроїв віддалених працівників;
- централізоване управління – платформа надає централізовані засоби управління для адміністраторів, що дозволяє віддалено налаштовувати та керувати всіма пристроями, підключеними до мережі;
- багатофакторна автентифікація (MFA) – FortiClient підтримує багатофакторну автентифікацію та додаткові функції безпеки, що дозволяє забезпечити додатковий рівень захисту, вимагаючи від користувачів додаткових підтверджень для доступу до мережі.

З урахуванням цих факторів можна зробити висновок, що FortiClient є одним із найкращих, відомих та надійних рішень для захисту віддаленої роботи працівників. Його широкий функціонал та можливості інтеграції з Fortinet Security Fabric роблять його популярним вибором для компаній, які шукають потужне,

комплексне та ефективне рішення для захисту корпоративних даних та мережі віддаленим працівникам.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІДДАЛЕНОЇ РОБОТИ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ FORTICLIENT

2.1. Архітектура та компоненти рішення FortiClient

FortiClient - це комплексне програмне забезпечення, розроблене компанією Fortinet та продовжує залишатися рушійною силою в розвитку кібербезпеки та конвергенції мережевих технологій і безпеки. Місія компанії - захищати людей, пристрої та дані скрізь і всюди. З цією метою їх портфель з понад 50 продуктів корпоративного класу є найбільшою інтегрованою пропозицією, що забезпечує перевірений кіберзахист скрізь, де він потрібен. Вони є одними з найбільш розгорнутих, запатентованих і перевірених у галузі. Також вони надають рішення для захисту віддаленої роботи працівників. Представлю детальніше їх архітектуру та компоненти цього рішення:

1) Клієнтська програма FortiClient:
    - центральною складовою FortiClient є сама клієнтська програма, яка встановлюється на пристроях користувачів (комп'ютерах, ноутбуках, смартфонах тощо) ;
    - клієнтська програма відповідає за встановлення та підтримку безпечного з'єднання з корпоративною мережею через VPN, а також за застосування політик безпеки та виявлення потенційних загроз на пристрої користувача.
2) Менеджер FortiGate:
    - FortiGate є центральною складовою в архітектурі FortiClient. Він відповідає за керування політиками безпеки, налаштуванням VPN-тунелів та моніторингом активності користувачів;
    - через FortiGate адміністратор може налаштовувати політики доступу, шифрування трафіку та виконувати інші операції з безпекою мережі.

3) FortiClient EMS (Enterprise Management Server):
    - FortiClient EMS є компонентом, що надає централізоване управління клієнтськими програмами FortiClient на різних пристроях;
    - він дозволяє адміністраторам віддалено керувати політиками безпеки, оновленнями програмного забезпечення та іншими аспектами безпеки на пристроях користувачів.
4) Інтеграція з FortiSandbox:
    - FortiClient може інтегруватися з FortiSandbox - продуктом компанії Fortinet для виявлення та аналізу потенційних загроз в ізольованому середовищі;
    - це дозволяє виявляти та блокувати навіть найсофістикованіші кіберзагрози, які можуть загрожувати безпеці користувачів та мережі.
5) Інтеграція з FortiAnalyzer:
    - FortiClient може також інтегруватися з FortiAnalyzer - продуктом для аналізу та моніторингу логів безпеки;
    - це дозволяє адміністраторам відстежувати та аналізувати події безпеки, спостерігати за активністю користувачів та виявляти можливі атаки.
6) Інтеграція з FortiAuthenticator:
    - FortiClient може інтегруватися з FortiAuthenticator - продуктом для багатофакторної автентифікації користувачів;
    - це дозволяє забезпечити додатковий рівень захисту, вимагаючи від користувачів додаткових підтверджень для доступу до мережі.
7) Інтеграція з FortiManager:
    - FortiClient може інтегруватися з FortiManager - центральним керувальним сервером для управління продуктами Fortinet;
    - це дозволяє адміністраторам керувати всіма продуктами Fortinet, включаючи FortiClient, з одного місця, спрощуючи процес управління та моніторингу.

8) Інтеграція з FortiGate Cloud:
   - FortiClient також може інтегруватися з FortiGate Cloud - хмарним рішенням для управління безпекою мережі;
   - це дозволяє адміністраторам отримувати доступ до управління безпекою мережі з будь-якого місця, використовуючи хмарні можливості, що сприяє більшій гнучкості та мобільності.
9) FortiClient Telemetry:
   - FortiClient Telemetry - це функціонал, який забезпечує збір та передачу статистичних даних про безпеку з клієнтських пристроїв до FortiGate для централізованого аналізу;
   - ця функція дозволяє адміністраторам отримати більше інформації про стан безпеки пристроїв користувачів та вчасно виявляти можливі загрози.
10) FortiMail:
   - FortiClient може також забезпечувати захист електронної пошти, виявляючи та блокуючи шкідливі листи, які можуть містити віруси, фішингові посилання або інші загрози.

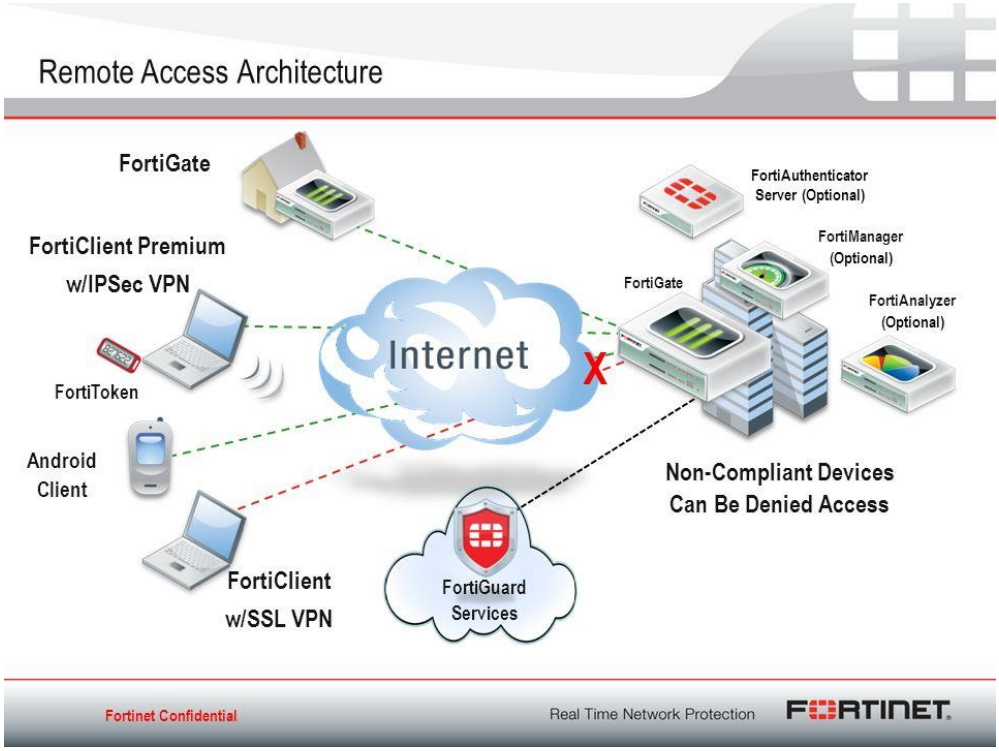

Рис. 2.1. Архітектура використання FortiClient [10]

Архітектура FortiClient побудована з урахуванням комплексності вимог потреб сучасного захищеного середовища щодо захисту віддаленої роботи працівників організації. Вона включає різноманітні компоненти та інтеграцію з іншими продуктами Fortinet, що дозволяє забезпечити цілісний, ефективний та комплексний захист від кіберзагроз. Інтергруючись один з одним, дані компоненти створюють цілісне захищене середовище, яке дозволяє адміністраторам ефективно керувати, захищати та моніторити безпеку корпоративної мережі та мережеві пристрої віддалених працівників організації.

2.2. Призначення та основні функції компонентів FortiClient

У цьому підпункті розглядається комплексний огляд основних компонентів рішення FortiClient, призначених для забезпечення безпеки віддаленої роботи працівників організації. Кожен з цих компонентів виконує важливі функції, спрямовані на захист мережі та даних, а також на управління безпековими політиками. В даному розділі буде надано докладний опис призначення та основних функцій кожного компонента FortiClient, що допоможе зрозуміти їхню роль у створенні ефективного та надійного захисту для корпоративної мережі. Опишу детально призначення та основні функції кожного компонента:

1) Менеджер FortiGate:
    - призначення: Менеджер FortiGate відповідає за керування політиками безпеки, налаштування VPN-тунелів та моніторинг активності користувачів;
    - основні функції: Налаштування та управління політиками безпеки для захисту мережі. Керування VPN-тунелями та забезпечення їх безпеки. Моніторинг активності користувачів та подій безпеки на мережі.
2) FortiClient EMS (Enterprise Management Server):
    - призначення: FortiClient EMS надає централізоване управління клієнтськими програмами FortiClient на різних пристроях;
    - основні функції: Централізоване управління політиками безпеки та налаштуваннями FortiClient. Моніторинг стану та активності пристроїв FortiClient. Віддалене надсилання оновлень та підтримка пристроїв користувачів.
3) FortiAnalyzer:
    - призначення: FortiAnalyzer відповідає за аналіз та моніторинг логів безпеки з різних пристроїв Fortinet;
    - основні функції: Збір, агрегація та аналіз логів безпеки з FortiGate, FortiClient та інших пристроїв Fortinet. Візуалізація даних та надання

звітів для аналізу подій безпеки.

4) FortiAuthenticator:
    - призначення: FortiAuthenticator забезпечує багатофакторну автентифікацію користувачів;
    - основні функції: Налаштування та управління процесом автентифікації користувачів за допомогою різних методів, таких як SMS, email, токени тощо. Підтримка SSO (Single Sign-On) та інших механізмів автентифікації.
5) FortiGate Cloud:
    - призначення: FortiGate Cloud надає хмарну платформу для управління безпекою мережі;
    - основні функції: Централізоване керування політиками безпеки, моніторинг активності та управління пристроями Fortinet у хмарному середовищі.
6) FortiClient Telemetry:
    - призначення: FortiClient Telemetry забезпечує збір та передачу статистичних даних про безпеку з клієнтських пристроїв до FortiGate для централізованого аналізу;
    - основні функції: Збір та передача статистичних даних про стан безпеки пристроїв користувачів. Централізований аналіз та моніторинг статусу
7) FortiMail:
    - призначення: Захист електронної пошти, забезпечуючи виявлення та блокування шкідливих листів, що можуть містити віруси, фішингові посилання або інші загрози;
    - основні функції: Аналіз вхідних та вихідних електронних листів на наявність шкідливого вмісту. Фільтрація спаму та блокування фішингових атак. Захист від витоку конфіденційної інформації через електронну пошту.

Кожен компонент FortiClient має своє призначення та набір основних

функцій, спрямованих на забезпечення безпеки та ефективного управління мережею. Ці компоненти можуть працювати як окремо, так і взаємодіяти між собою, створюючи цілісне та надійне середовище для захисту віддаленої роботи працівників організації.

1.3. Процеси функціонування рішення FortiClient

У цьому підрозділі буде розглянуто більш технічно як працюють основні методи захисту віддаленої роботи працівників організації з використанням FortiClient.

Для початку розглянемо таку технологію як IPsec VPN. IPsec VPN (Internet Protocol Security Virtual Private Network) - це технологія, яка забезпечує безпеку та конфіденційність комунікаційних каналів через інтернет або будь-яку іншу ненадійну мережу. Вона дозволяє створювати зашифровані тунелі між двома або більше мережами або пристроями, щоб захистити дані від несанкціонованого доступу та забезпечити конфіденційність, цілісність та автентифікацію. Основні характеристики IPsec VPN включають:

- шифрування даних: IPsec використовує різні шифрувальні алгоритми для захисту конфіденційності даних, що передаються через VPN-тунель;
- автентифікація: IPsec використовує методи автентифікації для перевірки ідентичності комунікаційних партнерів перед установкою VPN-з'єднання;
- цілісність: IPsec використовує хеш-функції для забезпечення цілісності даних, що передаються через VPN-тунель;
- керування ключами: IPsec використовує протоколи обміну ключами, у FortiClient це IKE, для забезпечення безпеки ключів шифрування і автентифікації, які використовуються для встановлення VPN-тунелю.

Архітектура IPSec (IP Security) використовує два протоколи для захисту трафіку або потоку даних. Це протоколи ESP (Encapsulation Security Payload) і AH (Authentication Header). Архітектура IPSec включає протоколи, алгоритми, DOI (Domain of Interpretation) та керування ключами. Усі ці компоненти дуже важливі для надання трьох основних послуг: конфіденційність, автентифікація, цілісність.

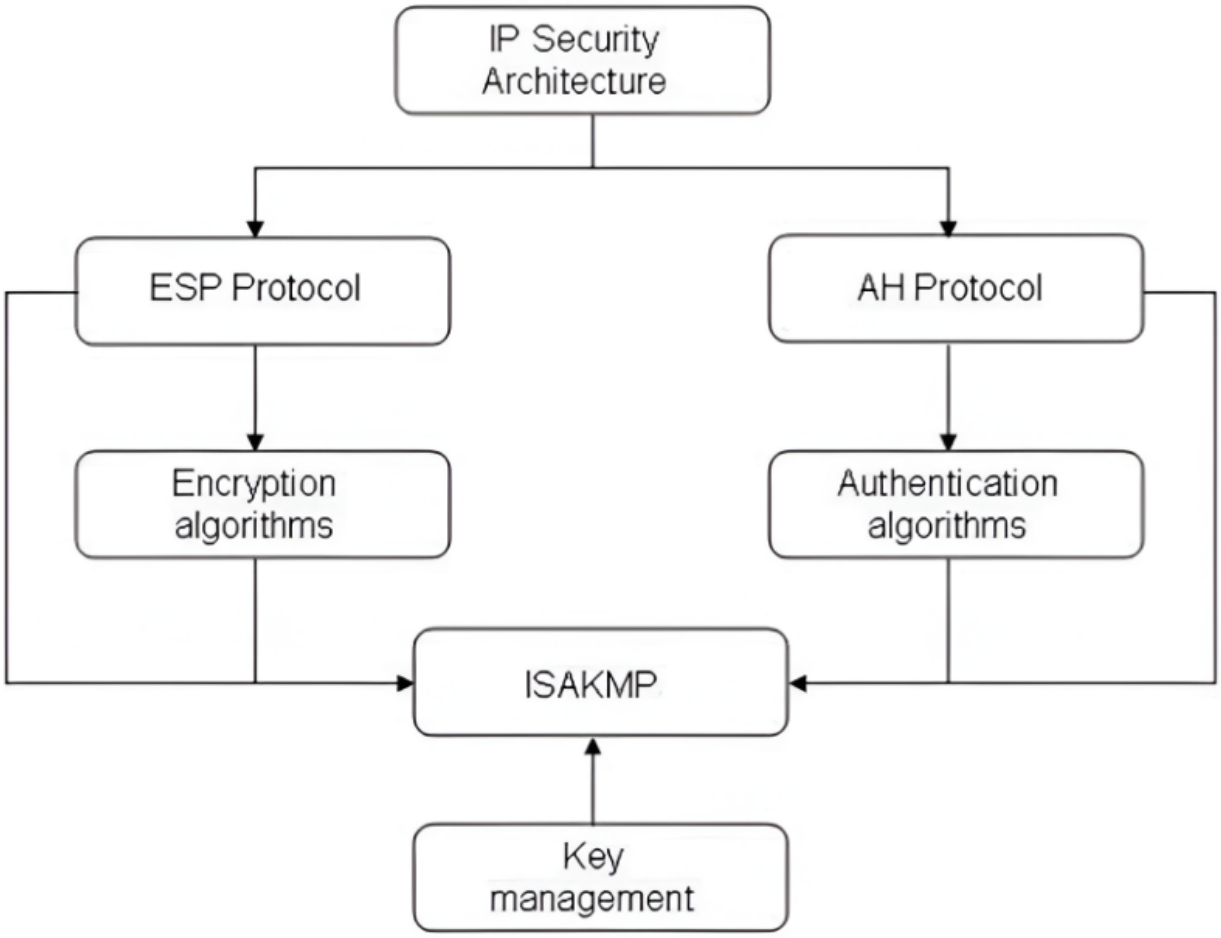

Рис. 2.2. Архітектура роботи IPsec [11]

Протокол ESP (Encapsulation Security Payload) є одним з двох основних протоколів, які використовуються в архітектурі IPsec для забезпечення конфіденційності даних, що передаються по мережі. Ось як він працює і яку роль він займає в архітектурі IPsec:

- захист даних: ESP відповідає за захист даних, які передаються між двома кінцями VPN-з'єднання;
- шифрування даних: при використанні ESP дані шифруються, щоб забезпечити їх конфіденційність під час передачі через неприватні мережі, такі як Інтернет;
- роль в архітектурі IPsec: ESP є одним з двох протоколів, які використовуються в архітектурі IPsec, разом з протоколом AH (Authentication Header). Він забезпечує захист даних на рівні пакетів, використовуючи шифрування та автентичність, щоб забезпечити безпеку передачі інформації в мережах VPN.

Протокол IPsec, а саме ESP(Інкапсуляція Безпечного Корисного навантаження), може бути реалізована у двох режимах корисного навантаження безпеки: режимі тунелювання (Tunnel Mode) та режимі транспорту (Transport Mode). У режимі тунелювання весь пакет даних шифрується і додається до нового IP-пакету з заголовком IPsec, що забезпечує захист всього трафіку між двома кінцевими точками мережі, зазвичай цей режим використовується для створення безпечних VPN-тунелей між мережами. У режимі транспорту лише самі дані, а не весь IP-пакет, зашифровуються, що дозволяє захистити тільки зміст пакетів, зазвичай цей режим використовується для забезпечення безпеки комунікації між двома кінцями. Кожне застосування IPsec може використовувати різні параметри застосування безпеки, визначені DOI(Область Інтерпретації).

AH (Authentication Header) є одним з двох основних протоколів, які використовуються в архітектурі IPsec (Internet Protocol Security) для забезпечення безпеки передачі даних. Ось як AH(Заголовок Автентифікації) працює та яку роль він виконує в архітектурі IPsec:

- захист цілісності даних: AH використовується для захисту цілісності даних, які передаються між двома кінцями VPN-з'єднання. Він додає до кожного IP-пакету автентичний заголовок, який містить контрольну суму (хеш) даних. Ця контрольна сума обчислюється на основі всього пакета, включаючи заголовок IP, під час передачі пакету через мережу;
- автентифікація даних: AH також використовується для автентифікації даних. Крім контрольної суми, цей протокол також може містити інформацію про автентифікацію, таку як ідентифікатори безпеки та інші параметри, які допомагають перевірити автентичність даних і впевнитися, що вони були відправлені відповідним відправником і не були змінені під час передачі;
- роль в архітектурі IPsec: AH є одним з двох основних протоколів, які використовуються в архітектурі IPsec, разом з ESP (Encapsulating Security Payload). Він забезпечує захист цілісності та автентифікацію даних на рівні пакетів IP, допомагаючи забезпечити безпеку та

конфіденційність інформації в мережах VPN.

У контексті архітектури IPsec ESP та AH можуть взаємодоповнювати один одного для забезпечення комплексного захисту комунікації:

- ESP забезпечує конфіденційність даних шляхом їх шифрування, тоді як AH забезпечує аутентифікацію цих даних та гарантує їхню цілісність;
- ESP може бути використаний для шифрування даних та забезпечення конфіденційності, а потім AH може додати аутентичний тег для перевірки їх цілісності;
- у деяких випадках ESP може використовуватись самостійно для захисту даних, без AH, особливо якщо конфіденційність даних є більш важливою, ніж їх аутентифікація.

Отже, ESP і AH разом доповнюють один одного, забезпечуючи комплексний захист даних в архітектурі IPsec, включаючи конфіденційність, цілісність та автентифікацію даних.

Domain of Interpretation (DOI) є одним з ключових концептів у структурі IPsec (Internet Protocol Security). Він визначає контекст та параметри застосування безпеки, які використовуються в IPsec. DOI встановлює зміст та значення параметрів безпеки, таких як алгоритми шифрування, методи аутентифікації, обмін ключами та інші параметри, що визначаються для конкретних застосувань або середовищ. У контексті IPsec, DOI взаємодіє з протоколами AH та ESP наступним чином:

1) AH (Authentication Header):
    - AH використовується для забезпечення автентифікації та цілісності даних. Саме DOI визначає параметри, які використовуються в AH, такі як алгоритми автентифікації, ключі, алгоритми гешування тощо;
    - DOI визначає, які конкретні методи автентифікації та алгоритми хешування використовуються в AH для підпису та перевірки цілісності пакетів.
2) ESP (Encapsulating Security Payload):

- ESP використовується для шифрування та захисту конфіденційності даних. DOI визначає параметри, які використовуються в ESP, такі як алгоритми шифрування, ключі, методи автентифікації, вектори ініціалізації тощо;
- DOI встановлює, які конкретні методи шифрування та автентифікації використовуються в ESP для захисту даних.

Роль DOI в архітектурі IPsec полягає в тому, що він визначає набір параметрів безпеки, які можуть бути використані в конкретному контексті або середовищі. Він гарантує, що протоколи AH та ESP використовують одні й ті ж параметри застосування безпеки на обох кінцях з'єднання, що дозволяє їм ефективно взаємодіяти та забезпечувати безпеку передачі даних в рамках IPsec.

Як згадувалося вище, у FortiClient використовується IKE. IKE (Internet Key Exchange) є протоколом, який використовується в IPsec VPN для встановлення безпеки і обміну ключами між двома кінцями VPN-з'єднання. Він грає критичну роль у забезпеченні безпеки та конфіденційності даних, які передаються через віртуальну приватну мережу.

Ось конкретні ситуації, де і як використовується протокол IKE:

- встановлення VPN-з'єднання: під час встановлення IPsec VPN-з'єднання протокол IKE використовується для обміну ключами та параметрами безпеки між двома пристроями, які спілкуються між собою;
- автентифікація: IKE дозволяє пристроям перевірити свою взаємну ідентичність і переконатися, що вони взаємодіють з вірними партнерами VPN. Це може бути здійснено за допомогою різних методів автентифікації, таких як предварні обміни ключів (Pre-Shared Keys), сертифікати або інші методи;
- обмін ключами: після встановлення безпечного каналу зв'язку за допомогою IKE, він використовується для обміну симетричними ключами шифрування та іншими параметрами безпеки, які будуть використовуватися для шифрування трафіку IPsec;

- підтримка безпеки зв'язку: протокол IKE забезпечує механізми для переговорів між пристроями щодо параметрів безпеки, таких як типи шифрування, алгоритми хешування, методи автентифікації тощо, для забезпечення оптимальної безпеки зв'язку;
- обмін ключами IKE Phase 1 та IKE Phase 2: протокол IKE складається з двох основних фаз, відомих як IKE Phase 1 та IKE Phase 2. У Phase 1 відбувається встановлення безпечного каналу та обмін ключами для подальших обмінів у Phase 2, де вже відбувається обмін ключами IPsec.

В цілому, IKE використовується для забезпечення безпеки та автентифікації між двома кінцями VPN-з'єднання і грає ключову роль у забезпеченні безпеки віддалених з'єднань.

Розглянемо як працюють обидві фази обміну ключами. Конфігурація фази 1 в першу чергу визначає параметри, що використовуються в переговорах IKE (Internet Key Exchange) між кінцями тунелю IPsec. Локальний кінець - це інтерфейс FortiGate, який ініціює переговори IKE. Віддалений кінець - це віддалений шлюз, який відповідає і обмінюється повідомленнями з ініціатором. Тому їх іноді називають ініціатором і відповідачем. Мета фази 1 - забезпечити безпеку тунелю з одним двонаправленим IKE SA (асоціацією безпеки) для узгодження параметрів фази 2 IKE. Далі буде наведена таблиця складових першої фази:

Таблиця 1.1.

Фаза 1

Мережа	
IP версія	Протокол, IPv4 або IPv6.
Віддалений шлюз	Категорія віддаленого з'єднання: • статична IP-адреса: віддалений партнер має статичну IP-адресу; • користувач комутованого доступу: один або декілька клієнтів FortiClient або FortiGate з динамічною IP-адресою підключаються до FortiGate; • динамічний DNS: до FortiGate підключається віддалений партнер, який має доменне ім'я і підписаний на послугу динамічного DNS.
IP-адреса	IP-адреса віддаленого однорангового пристрою. Цей параметр доступний лише тоді, коли віддалений шлюз має статичну IP-адресу.
Динамічний DNS	Доменне ім'я віддаленого однорангового вузла. Цей параметр доступний лише тоді, коли віддалений шлюз має динамічний DNS.
Інтерфейс	Інтерфейс, через який віддалені однорангові або комутовані клієнти підключаються до FortiGate. Ця опція доступна тільки в режимі NAT.

	За замовчуванням, IP-адресою локального VPN-шлюзу є IP-адреса інтерфейсу, який було обрано (Первинний IP у полі Локальний шлюз).
Локальний шлюз	IP-адреса для локального кінця VPN-тунелю (за замовчуванням використовується Primary IP): • вторинний IP: вторинна адреса інтерфейсу, вибраного у полі Інтерфейс; • вказати: введіть адресу вручну.
Конфігурація режиму	Цей параметр доступний, лише якщо віддаленим шлюзом є користувач комутованого доступу. Налаштування діапазону клієнтських IP-адрес, маски/довжини префікса підмережі, DNS-серверу і можливість роздільного тунелю для автоматизації адресації віддалених клієнтів.
Обхід NAT	Ця опція доступна лише тоді, коли віддалений шлюз має статичну IP-адресу або динамічну DNS. ESP (encapsulating security payload), протокол для шифрування даних у сеансі VPN, за замовчуванням використовує IP-протокол 50. Однак він не використовує жодних номерів портів, тому при проходженні через пристрій NAT пакети не можуть бути демультиплексовані. Увімкнення обходу NAT інкапсулює ESP-пакет в UDP-пакет, таким чином додаючи до нього унікальний порт джерела. Це дозволяє пристрою NAT зіставляти пакети з правильним сеансом. • увімкнено: пристрій NAT існує між локальним FortiGate і одноранговим пристроєм або клієнтом VPN. Вихідні зашифровані пакети загорнуті в IP-заголовок UDP, який містить номер порту. Для надійного з'єднання локальний FortiGate і одноранговий або клієнт VPN повинні мати однакові налаштування обходу NAT (обидва вибрані або обидва зняті). Якщо є сумніви, увімкніть обхід NAT; • вимкнути: вимкнути налаштування обходу NAT; • примусово: FortiGate буде використовувати нульове значення порту при побудові хешу виявлення NAT для однорангового пристрою. Це змушує одноранговий пристрій думати, що він знаходиться за пристроєм NAT, і він буде використовувати UDP інкапсуляцію для IPsec, навіть якщо NAT відсутній. Цей підхід забезпечує сумісність з будь-якою реалізацією IPsec, яка підтримує NAT-T RFC.
Keepalive Частота	Налаштування частоти Keepalive. Цей параметр доступний лише тоді, коли для параметра *Обхід NAT* встановлено значення Увімкнути або Примусово. Пристрій NAT між одноранговими VPN може видалити сеанс, якщо VPN-з'єднання залишається бездіяльним занадто довго. Значення являє собою інтервал у секундах, протягом якого з'єднання буде підтримуватися періодичними пакетами з підтриманням зв'язку. Інтервал підтримання має бути меншим за значення тривалості сеансу, що використовується пристроєм NAT.
Виявлення мертвих однорангових пристроїв	Відновлює VPN-тунелі на неактивних з'єднаннях і очищає неактивні IKE-пари, якщо потрібно. Ця функція мінімізує трафік, необхідний для перевірки доступності або недоступності (мертвого) VPN-пула. Доступні наступні варіанти:

	• вимкнути: вимкнути виявлення неактивних однорангових підключень (DPD); • на холостому ходу: вмикати DPD, коли IPsec не працює; • на вимогу: Пасивно надсилає DPD, щоб зменшити навантаження на брандмауер. Вмикає DPD лише тоді, коли вихідні пакети IPsec надсилаються, але відповідь від однорангового пристрою не надходить. Коли трафік відсутній і отримано останній DPD-ACK, IKE не буде періодично надсилати DPD. Сповіщення надходять щоразу, коли тунель піднімається або опускається, або щоб тримати тунельне з'єднання відкритим, коли всередині тунелю не генерується трафік. Наприклад, у сценаріях, коли клієнт комутованого доступу або динамічний одноранговий DNS підключається з IP-адреси, яка періодично змінюється, трафік може бути призупинено на час зміни IP-адреси.
Пряме виправлення помилок	Увімкніть на обох кінцях тунелю, щоб виправити помилки при передачі даних, надсилаючи надлишкові дані через VPN.
Створення пристрою	Додатковий параметр. Якщо увімкнено, для кожного тунелю буде створено динамічний інтерфейс (мережевий пристрій).
Автентифікація	
Метод	Попередньо наданий ключ, або підпис.
Попередньо наданий ключ	Попередньо наданий ключ, який FortiGate буде використовувати для автентифікації на віддаленому вузлі або клієнті під час переговорів фази 1. Той самий ключ повинен бути визначений на віддаленому одноранговому пристрої або клієнті.
Назва сертифікату	Сертифікат сервера, який FortiGate буде використовувати для автентифікації перед віддаленим одноранговим або комутованим клієнтом під час фази 1 переговорів.
Версія IKE	v1 або v2
Режим	Ця опція доступна лише тоді, коли вибрано IKEv1. Доступні два варіанти: • агресивний: обмін параметрами фази 1 відбувається в одному повідомленні з незашифрованою автентифікаційною інформацією; • основний (захист ідентифікатора): обмін параметрами фази 1 відбувається в кілька раундів із зашифрованою автентифікаційною інформацією.
Налаштування вузла	Параметри автентифікації VPN-вузлів або клієнтів залежно від налаштувань віддаленого шлюзу та методу автентифікації.
Будь-який ідентифікатор вузла	Приймає локальний ідентифікатор будь-якого віддаленого вузла або клієнтського VPN. FortiGate не перевіряє ідентифікатори (локальні ідентифікатори). Режим може бути встановлений на Агресивний або Основний. Цей параметр можна використовувати з автентифікацією за допомогою цифрового сертифіката, але для більшої безпеки використовуйте одноранговий сертифікат.
Конкретний ідентифікатор вузла	Цей параметр доступний, лише якщо увімкнено Агресивний режим. Введіть ідентифікатор, який використовується для автентифікації віддаленого однорангового пристрою. Ідентифікатор повинен збігатися з локальним ідентифікатором, налаштованим адміністратором віддаленого однорангового пристрою.
Сертифікат вузла	Визначте сертифікат ЦС, який використовується для автентифікації

	віддаленого однорангового пристрою, коли режим автентифікації - Підпис.
Ідентифікатор вузла з діалогової групи	Автентифікація декількох клієнтів FortiGate або FortiClient, які використовують унікальні ідентифікатори та унікальні попередньо надані ключі (або тільки унікальні попередньо надані ключі), через один і той самий VPN-тунель. Ви повинні створити групу діалогових-користувачів для цілей автентифікації. Виберіть групу зі списку поруч з опцією Ідентифікатор однорангового користувача з діалап-групи.
Шифрування	Існують наступні алгоритми шифрування з симетричним ключем: • DES: цифровий стандарт шифрування, 64-розрядний блоковий алгоритм, який використовує 56-розрядний ключ; • 3DES: потрійний DES; звичайний текст шифрується тричі трьома ключами; • AES128: Advanced Encryption Standard, 128-бітний блоковий алгоритм, який використовує 128-бітний ключ; • AES128GCM: AES в режимі Галуа/лічильника, 128-бітний блоковий алгоритм, який використовує 128-бітний ключ. Доступний тільки для IKEv2; • AES192: 128-бітний блоковий алгоритм, який використовує 192-бітний ключ; • AES256: 128-бітний блоковий алгоритм, який використовує 256-бітний ключ; • AES256GCM: AES в режимі Галуа/лічильника, 128-бітний блоковий алгоритм, який використовує 256-бітний ключ. Доступний лише для IKEv2; • CHACHA20POLY1305: 128-бітний блоковий алгоритм, який використовує 128-бітний ключ і симетричний шифр. Доступний лише для IKEv2.
Автентифікація	Доступні наступні дайджести повідомлень, які перевіряють автентичність повідомлення під час зашифрованого сеансу зв'язку: • MD5: дайджест повідомлення 5; • SHA1: безпечний алгоритм хешування 1; 160-бітний дайджест повідомлення; • SHA256: 256-бітний дайджест повідомлення; • SHA384: 384-бітний дайджест повідомлення; • SHA512: 512-бітний дайджест повідомлення.
Diffie-Hellman групи	Алгоритми з асиметричним ключем, що використовуються для криптографії з відкритим ключем. Виберіть один або декілька з груп 1, 2, 5 і 14-32. Принаймні одне з налаштувань груп Діффі-Хеллмана (DH) на віддаленому одноранговому пристрої або клієнті повинно відповідати одному з налаштувань на FortiGate. Невідповідність однієї або декількох груп DH призведе до невдалих переговорів.
Термін служби ключа	Час (у секундах), який має пройти до закінчення терміну дії ключа шифрування IKE. Коли термін дії ключа закінчується, новий ключ генерується без переривання роботи сервісу. Час життя ключа може становити від 120 до 172 800 секунд.
Ім'я користувача	Ім'я користувача, яке використовується для автентифікації.

Пароль	Пароль, який використовується для автентифікації.

Після успішного завершення фази 1 починається фаза 2. У фазі 2 вузол або клієнт VPN та FortiGate знову обмінюються ключами для встановлення захищеного каналу зв'язку. Параметри пропозиції фази 2 вибирають алгоритми шифрування та автентифікації, необхідні для генерації ключів для захисту деталей реалізації асоціацій безпеки. Ключі генеруються автоматично за допомогою алгоритму Діффі-Хеллмана.

Основні налаштування фази 2 пов'язують параметри фази 2 IPsec з конфігурацією фази 1, яка визначає віддалену кінцеву точку VPN-тунелю. У більшості випадків потрібно налаштувати лише базові параметри фази 2.

Деякі параметри можна налаштувати в інтерфейсі командного рядка. Далі буде представлено які є доступні опції налаштування VPN після створення тунелю:

Таблиця 1.2.

Фаза 2

Локальна адреса	Значення 0.0.0.0.0/0 означає всі IP-адреси за локальним одноранговим VPN. Додайте певну адресу або діапазон, щоб дозволити трафік тільки з і на цю локальну адресу.
Віддалена адреса	Введіть IP-адресу призначення, яка відповідає одержувачам або мережі за віддаленим VPN-вузлом. Значення 0.0.0.0/0 означає всі IP-адреси за віддаленим одноранговим VPN-сервером.
Розширений	Виберіть алгоритми шифрування та автентифікації, які будуть запропоновані віддаленому VPN-вузлу. Щоб встановити VPN-з'єднання, принаймні одна із зазначених пропозицій повинна відповідати конфігурації на віддаленому одноранговому комп'ютері.
Шифрування	Доступні наступні алгоритми шифрування з симетричним ключем: • NULL: не використовувати алгоритм шифрування; • DES: Цифровий стандарт шифрування, 64-бітний блоковий алгоритм, який використовує 56-бітний ключ; 3DES: потрійний DES; звичайний текст шифрується тричі трьома ключами. • AES128: Advanced Encryption Standard, 128-бітний блоковий алгоритм, який використовує 128-бітний ключ; • AES128GCM: AES в режимі Галуа/лічильника, 128-бітний блоковий алгоритм, який використовує 128-бітний ключ. Доступний тільки для IKEv2; • AES192: 128-бітний блоковий алгоритм, який використовує 192-бітний ключ; • AES256: 128-бітний блоковий алгоритм, який використовує 256-бітний ключ; • AES256GCM: AES в режимі Галуа/лічильника, 128-бітний блоковий алгоритм, який використовує 256-бітний ключ.

	Доступний лише для IKEv2; • CHACHA20POLY1305: 128-бітний блоковий алгоритм, який використовує 128-бітний ключ і симетричний шифр. Доступний лише для IKEv2.
Автентифікація	Доступні наступні дайджести повідомлень, які перевіряють автентичність повідомлень під час зашифрованого сеансу: • NULL: не використовувати дайджест повідомлень; • MD5: дайджест повідомлення 5; • SHA1: безпечний алгоритм хешування 1; 160-бітний дайджест повідомлення; • SHA256: 256-бітний дайджест повідомлення; • SHA384: 384-бітний дайджест повідомлення; • SHA512: 512-бітний дайджест повідомлення.
Увімкнути виявлення повторів	Атаки повтору відбуваються, коли несанкціонована сторона перехоплює серію IPsec-пакетів і відтворює їх назад в тунель. Виявлення повторів дозволяє FortiGate перевіряти всі IPsec-пакети на предмет того, чи були вони отримані раніше. Якщо будь-які зашифровані пакети надходять не в порядку, FortiGate відкидає їх.
Увімкнути Perfect Forward Secrecy (PFS)	Ідеальна пряма секретність (PFS) покращує безпеку, примушуючи до нового обміну Diffie-Hellman щоразу, коли закінчується термін дії ключа.
Група Diffie-Hellman	Алгоритми з асиметричним ключем, що використовуються для криптографії з відкритим ключем. Виберіть один або декілька з груп 1, 2, 5 і 14-32. Принаймні одне з налаштувань груп Діффі-Хеллмана (DH) на віддаленому вузлі або клієнті повинно відповідати одному з налаштувань на FortiGate. Невідповідність однієї або декількох груп DH призведе до невдалих переговорів.
Локальний порт	Введіть номер порту, який локальний VPN-провайдер використовує для транспортування трафіку, пов'язаного із зазначеним сервісом (номер протоколу). Діапазон від 0 до 65535. Щоб вказати всі порти, виберіть Усі або введіть 0.
Віддалений порт	Введіть номер порту, який віддалений партнер VPN використовує для передачі трафіку, пов'язаного із зазначеним сервісом (номер протоколу). Щоб вказати всі порти, виберіть Усі або введіть 0.
Протокол	Введіть номер IP-протоколу служби. Щоб вказати всі сервіси, виберіть Усі або введіть 0.
Автоматичні переговори	Виберіть цю опцію, щоб тунель автоматично переукладався після закінчення терміну його дії.
Autokey Keep Alive	Виберіть цю опцію, щоб тунель залишався активним, коли дані не обробляються.
Термін служби ключа	Виберіть метод визначення терміну дії ключа фази 2: • секунди; • кілобайти; • обидва. Введіть відповідне значення для параметрів Секунди та/або Кілобайти у текстових полях. Якщо вибрано "Обидва", термін дії ключа закінчується після закінчення часу або після обробки певної кількості кілобайт.

Загалом, IKE дозволяє створювати безпечні VPN-з'єднання, забезпечуючи автентифікацію, конфіденційність та цілісність даних, що передаються через мережу.

Необхідно пам’ятати, що існує деякі тонкощі роботи методу призначення першої доступної адреси. Коли користувач відключається від VPN-тунелю, не завжди бажано, щоб звільнена IP-адреса використовувалася негайно. У IPsec VPN IP-адреси можуть утримуватися протягом певного інтервалу затримки, перш ніж повертатися назад у пул для призначення. Як і раніше, використовується метод призначення першої доступної адреси. Далі буде показаний приклад роботи IPsec VPN з утриманням IP-адреси:

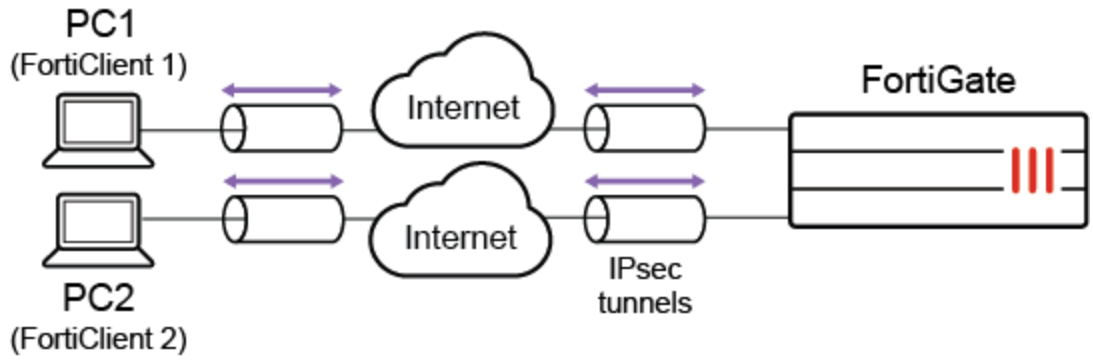

Рис. 2.3. Приклад роботи IPsec VPN з утриманням IP-адреси [12]

У цьому сценарії два комп'ютери встановлюють з'єднання з VPN. Інтервал затримки повторного використання IP-адреси застосовується для того, щоб гарантувати, що звільнена адреса залишається недоступною для повторного використання протягом щонайменше чотирьох хвилин. Після закінчення цього інтервалу IP-адреса знову стає доступною для клієнтів. Крім того, використовується двостекове призначення адрес, що підтримує як IPv4, так і IPv6.

IPsec VPN широко використовується для забезпечення безпеки віртуальних приватних мереж в корпоративних мережах та для забезпечення безпеки підключення віддалених користувачів до корпоративних ресурсів через Інтернет.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІДДАЛЕНОЇ РОБОТИ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ

3.1. Варіант розгортання системи захисту віддаленої роботи працівників організації на базі FortiClient

Для початку розгортання нашого VPN з'єдання потрібно зайти на сайт FortiGate та створити користувача, під обліковим записом якого ми будемо під'єднуватися до VPN з'єдання. Зазвичай його створенням займається саме організація. Спершу обираємо тип користувача.

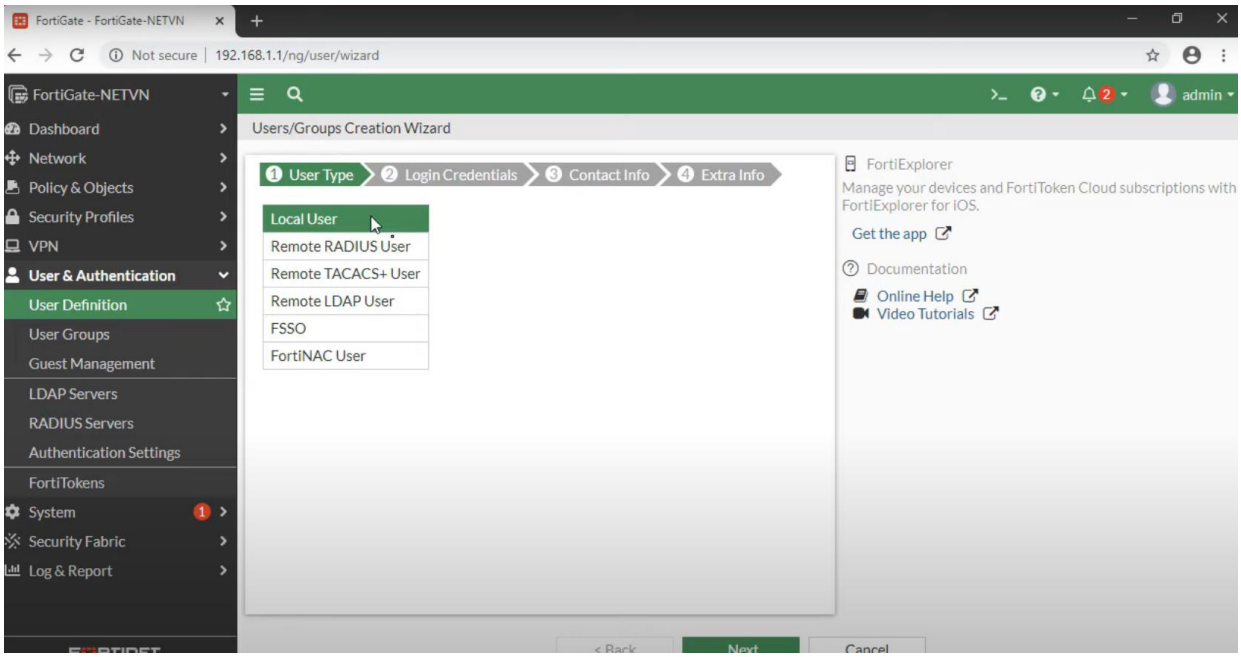

Рис. 3.1. Вибір типу користувача для створення облікового запису

Далі вигадуємо ім'я та пароль користувача облікового запису.

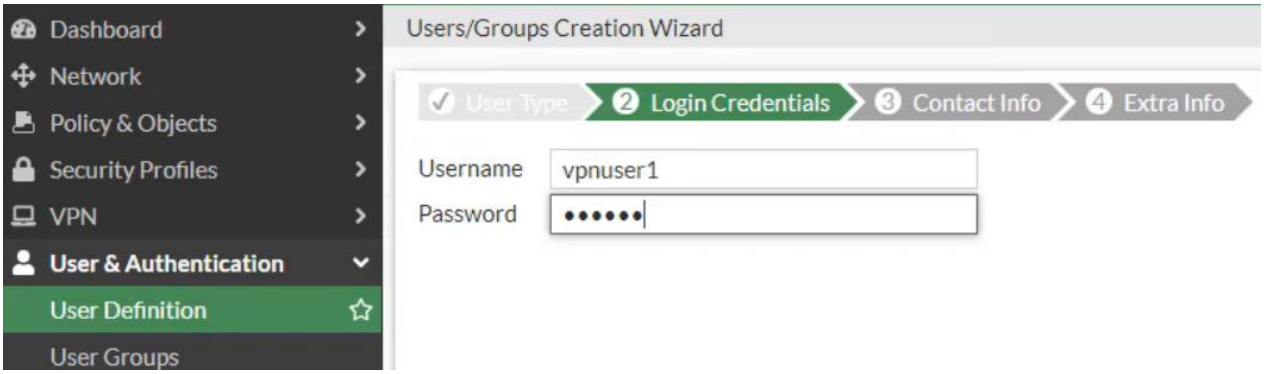

Рис. 3.2. Створення імені та паролю облікового запису

Тут можна одразу натискати кнопку “submit” або одразу додати користувача до Групи користувачів, якщо вона вже створена.

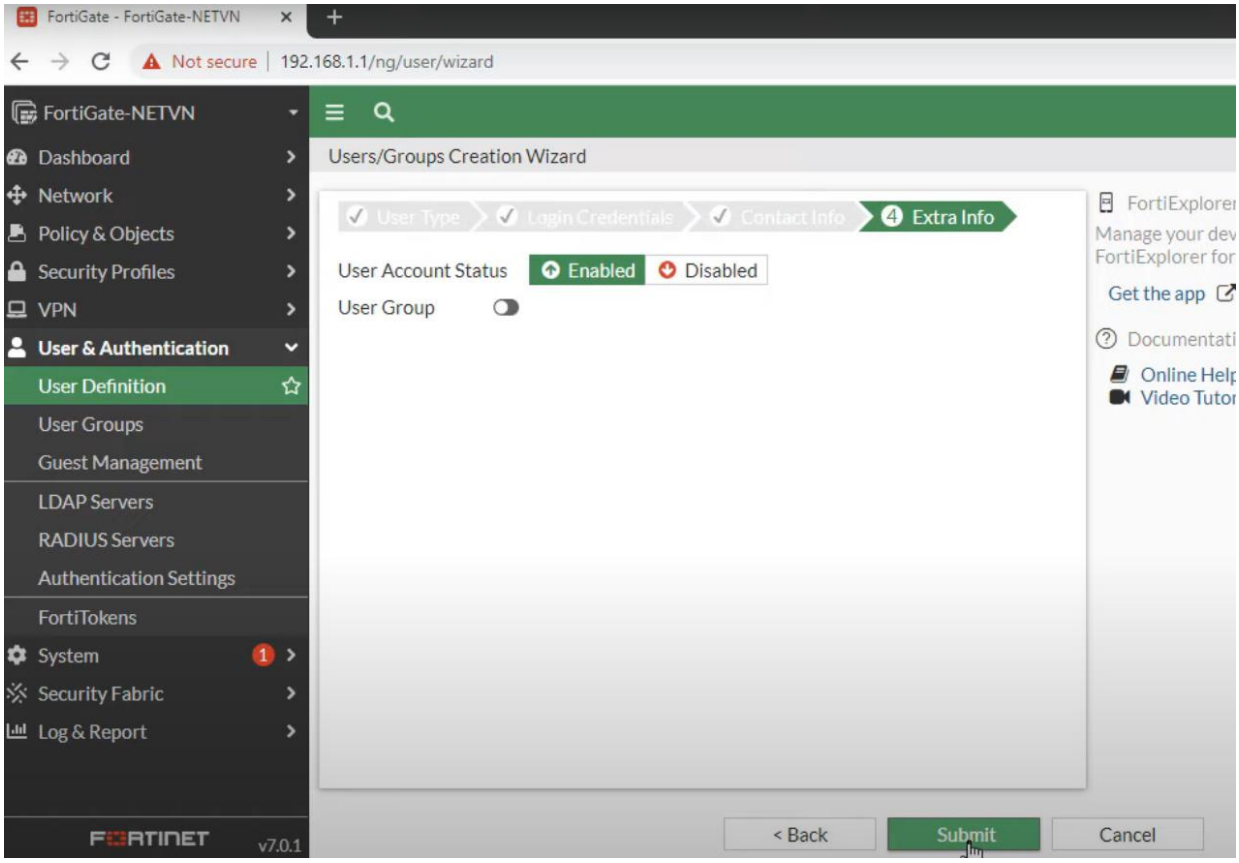

Рис. 3.3. Останній етап створення облікового запису

Тепер ми побачимо створений обліковий запис, ім’я та пароль якого співпадають з тими які ми вказували раніше.

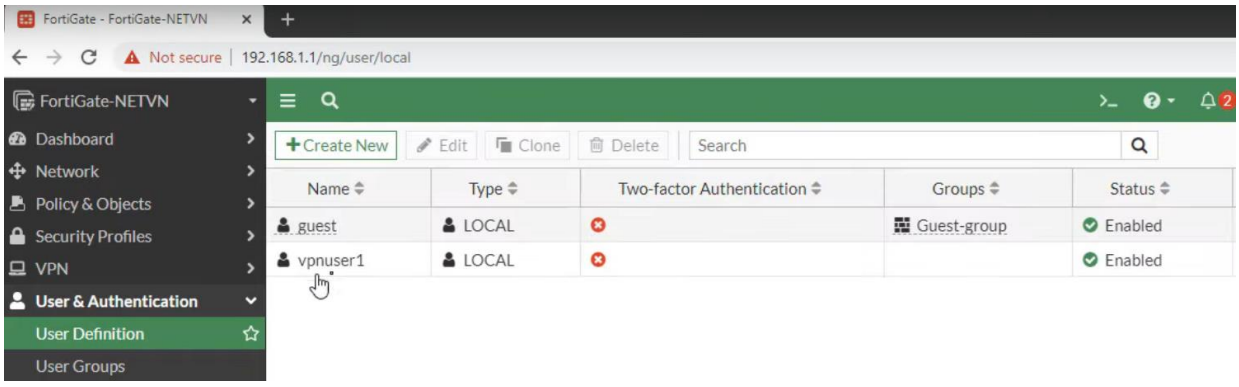

Рис 3.4. Створений обліковий запис користувача

Далі додаємо обліковий запис користувача до Групи користувачів. Для цього переходимо до пункту меню “User Groups” та натискаємо “Create New”.

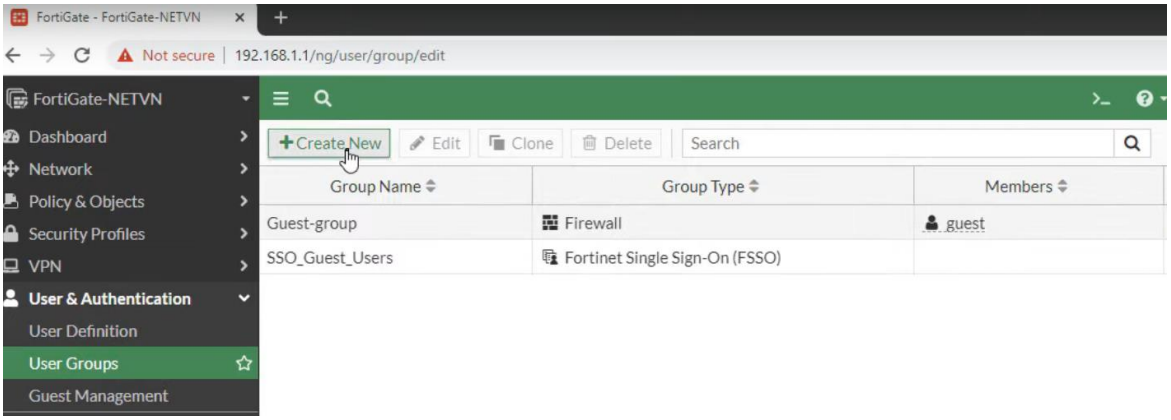

Рис. 3.5. Створення нової Групи Користувачів

Тут створюємо Групу користувачів з довільною назвою, у моєму випадку це буде "vpn-group" то додаємо учасників, а саме той обліковий запис, створений нами раніше. Далі просто натискаємо "OK" для підтвердження створення Групи.

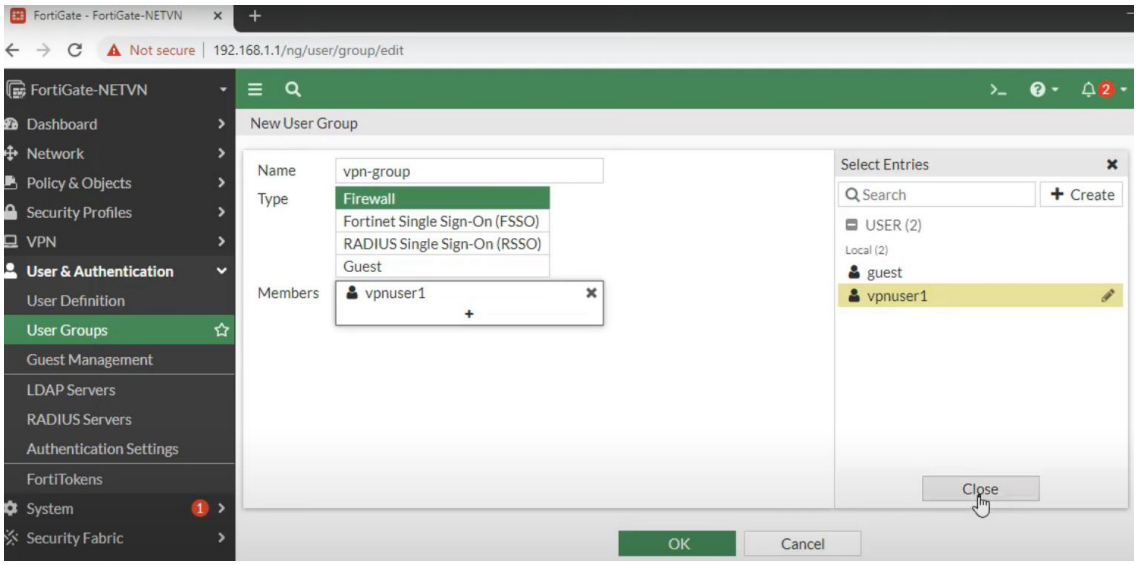

Рис. 3.6. Додавання користувача до створеної групи

Тепер ми бачимо створену нами Групу користувачів з тим обліковим записом, який ми створювали раніше.

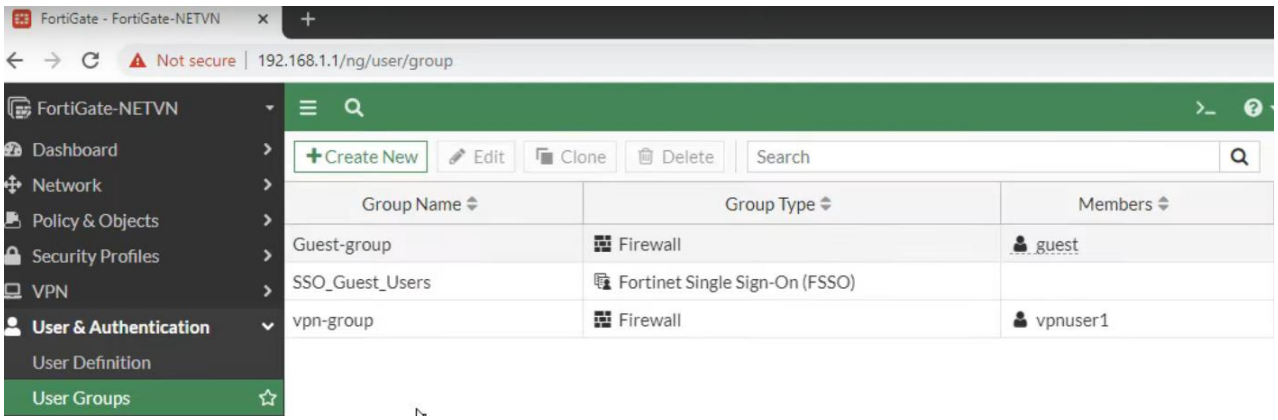

Рис. 3.7. Вдало створена Група користувачів та доданий до неї обліковий запис

Далі потрібно задати діапазон адрес для внутрішніх мереж VPN. Для цього в списку зліва переходимо до пункт “Policy & Objects”, потім в її підпункт “Addresses” та натискаємо “Create New”.

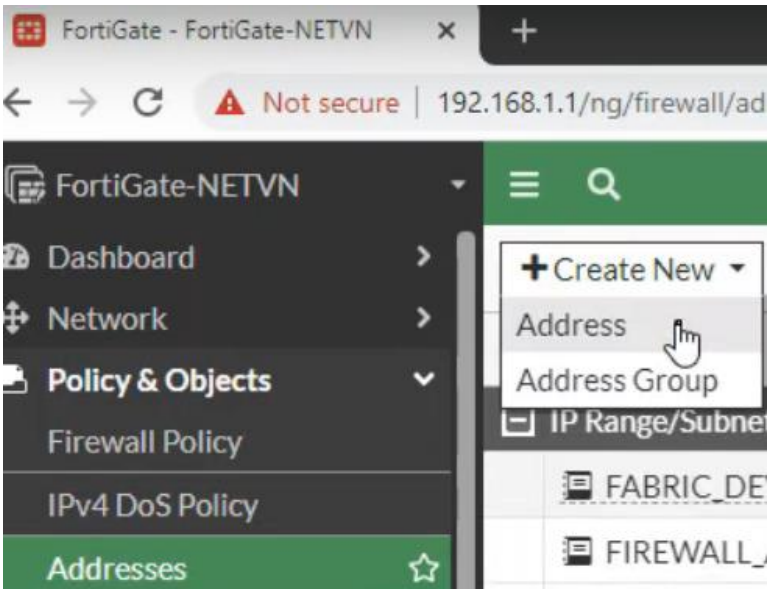

Рис. 3.8. Створюємо діапазон адрес для внутрішніх мереж VPN

Далі задаємо діапазон адрес для внутрішніх мереж VPN, обираємо Інтерфейс “LAN (LAN)” та натискаємо кнопку “OK”.

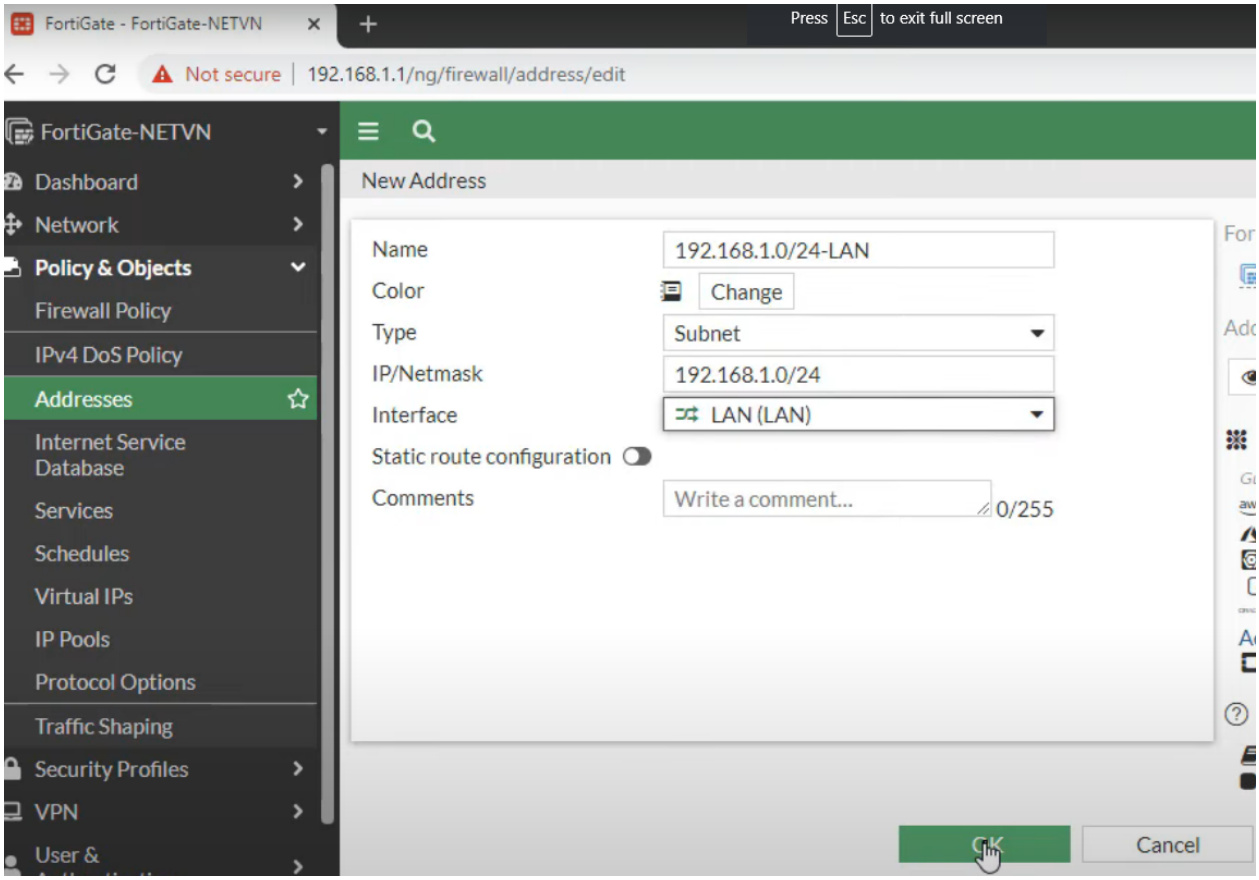

Рис. 3.9. Задання діапазону адрес для внутрішніх мереж VPN

Тепер в нас є вдало заданий діапазон адрес для внутрішніх мереж VPN.

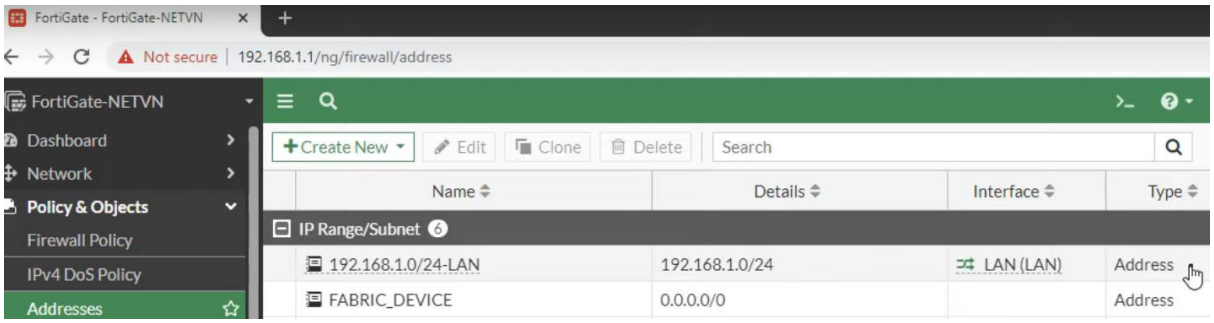

Рис. 3.10. Вдало заданий діапазон адрес для внутрішніх мереж VPN

Зараз будемо проводити налаштування самого VPN з'єднання. У лівому списку вибираємо пункт "VPN", далі в підпункт "IPsec Wizard". Даємо довільну назву, у моєму випадку "client-to-client", обираємо тип шаблону "Remote Access", а віддалений тип пристрою залишаємо без змін та натискаємо далі.

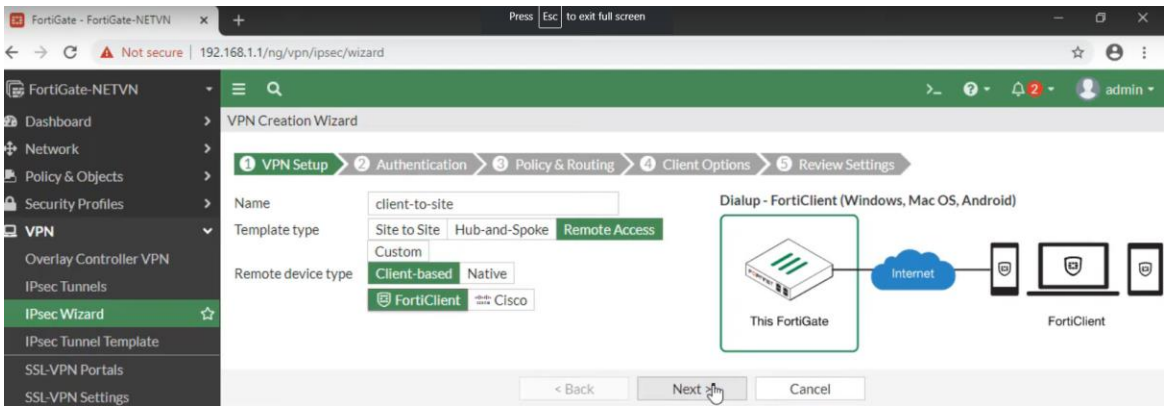

Рис. 3.11. Налаштування VPN

Для вхідного інтерфейсу обираємо порт WAN пристрою. В полі "Pre-shared Key" вводимо довільний зразок ключа, у мене це буде "sample". В полі "User Group" обираємо ту групу VPN, яку створювали раніше та натискаємо далі.

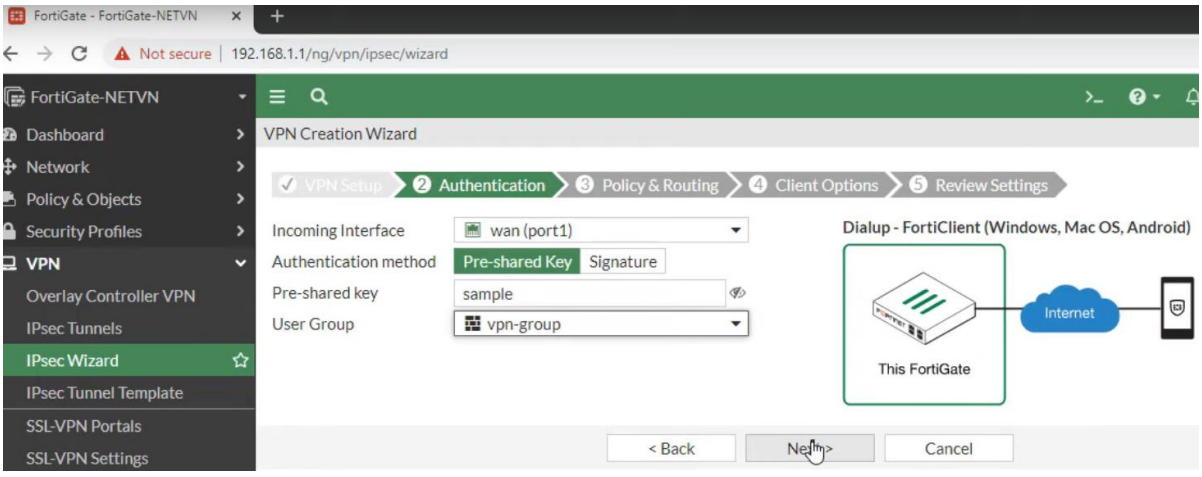

Рис. 3.12. Налаштування автентифікації

У локальному інтерфейсі обираємо порт LAN, у локальній адресі вказуємо діапазон адрес для IPsec LAN який був створений раніше. У діапазон адрес клієнта вводимо IP-адресу для VPN-клієнта та натискаємо далі.

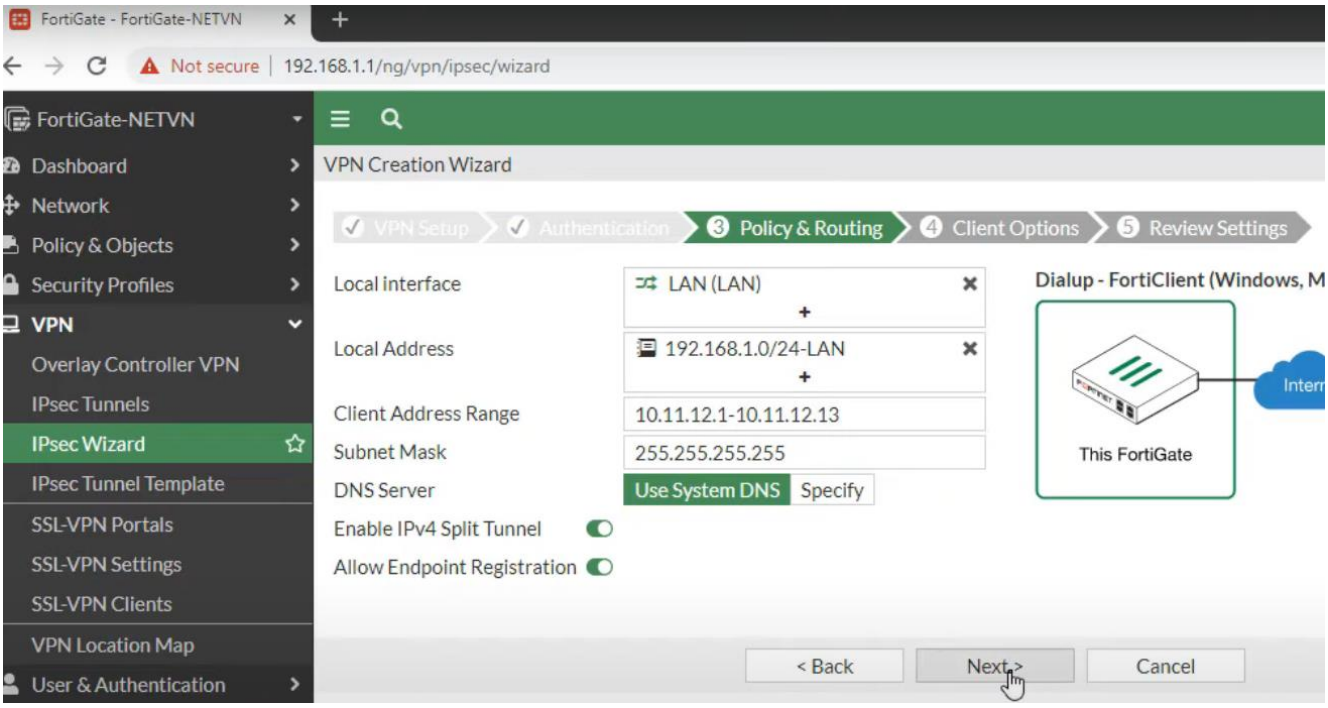

Рис. 3.13. Налаштування політик та маршрутизації

Тут обираємо потрібні функції та натискаємо далі.

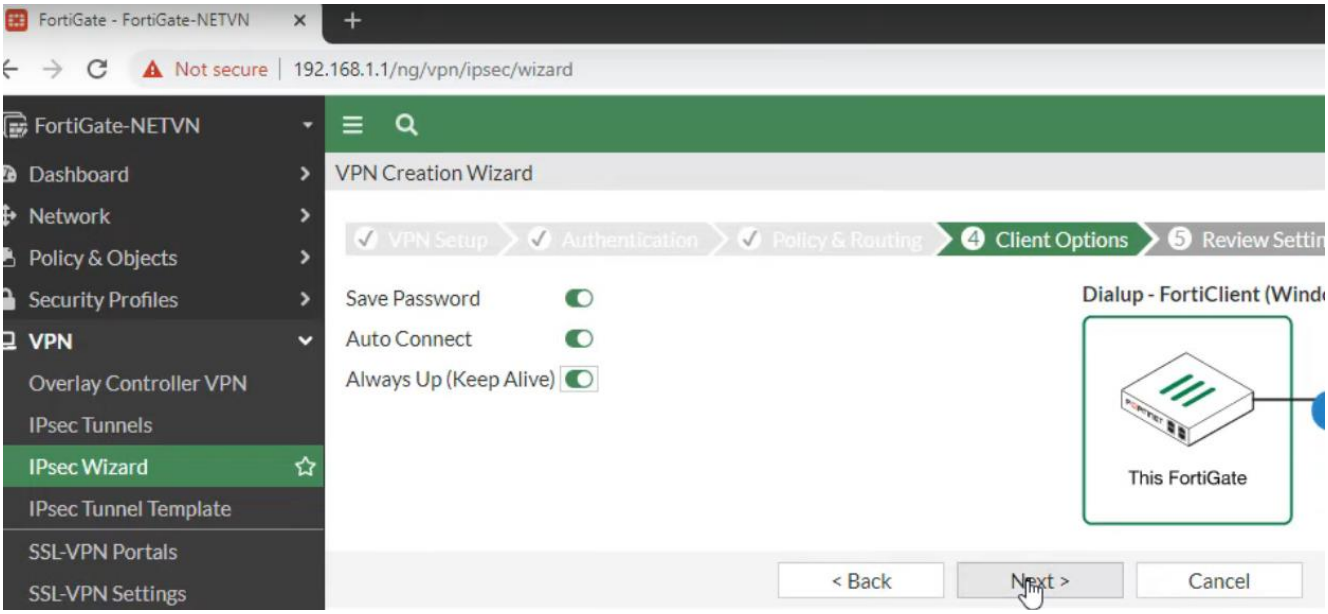

Рис. 3.14. Вибір додаткових функції

Перевіряємо налаштування і якщо все правильно, то натискаємо створити.

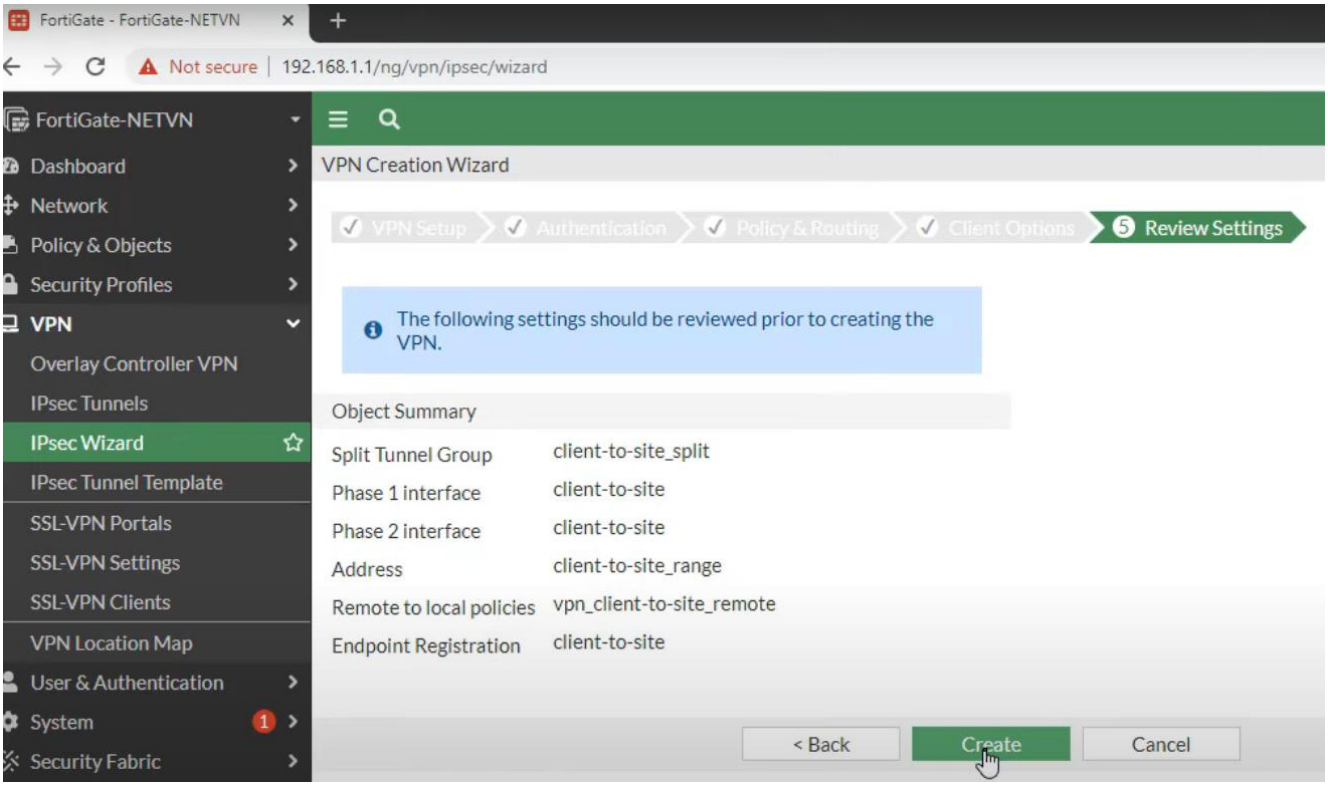

Рис. 3.15. Перевірка заданих налаштувань

Тепер маємо налаштований VPN на стороні сервера.

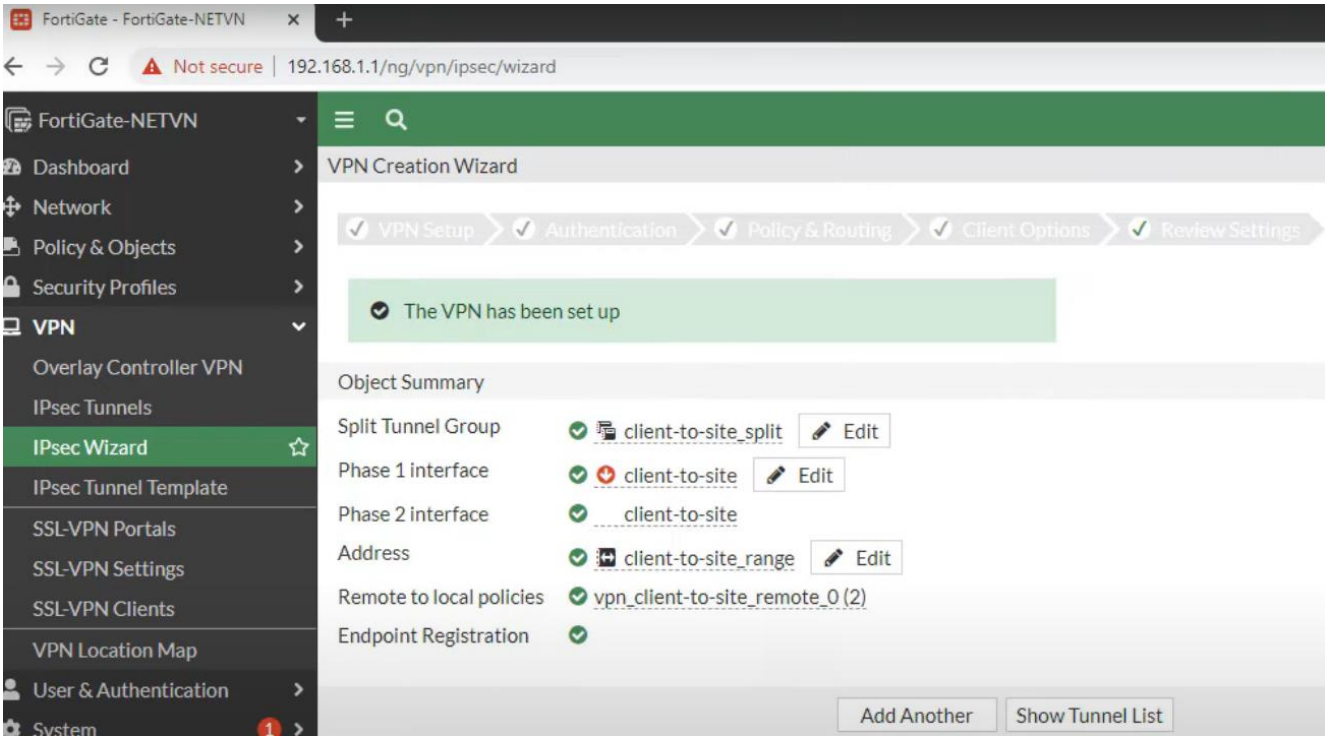

Рис. 3.16. Налаштований VPN на стороні сервера

Далі ми маємо переглянути інформацію о VPN-сервері для проведення налаштувань на стороні клієнта, тобто робітника організації. В лівому списку йдемо до підпункту “IPsec Tunnels” та натискаємо кнопку редагування створенного

нами тунелю.

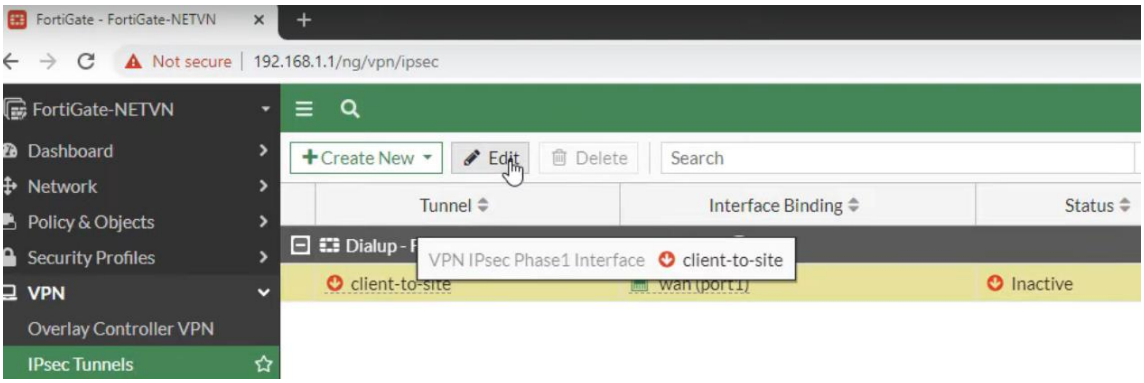

Рис. 3.17. Редагування тунелю VPN

Натискаємо конвертувати у налаштовуваний тунель.

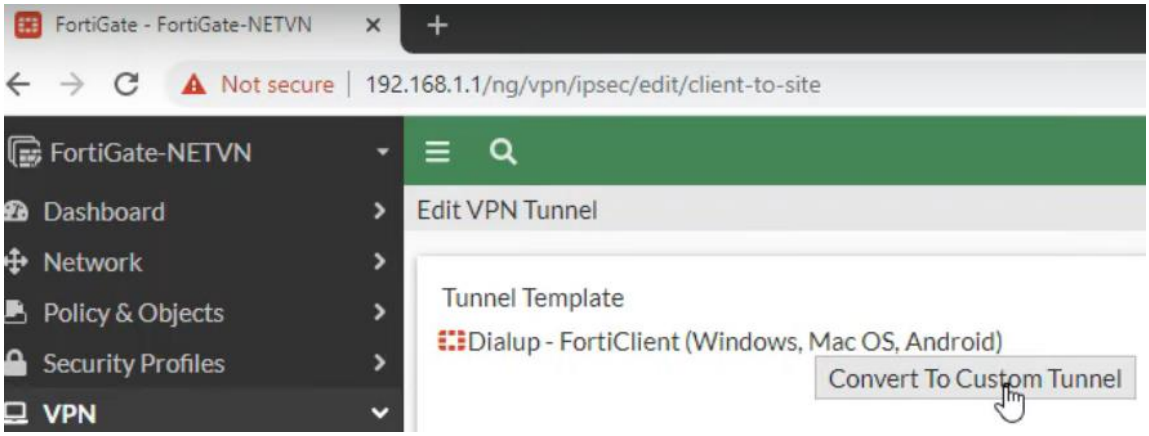

Рис. 3.18. Робимо тунель VPN налаштовуваним

Зберігаємо інформацію з “Phase 1 Proporsal” для подальшого налаштування VPN на стороні працівника організації.

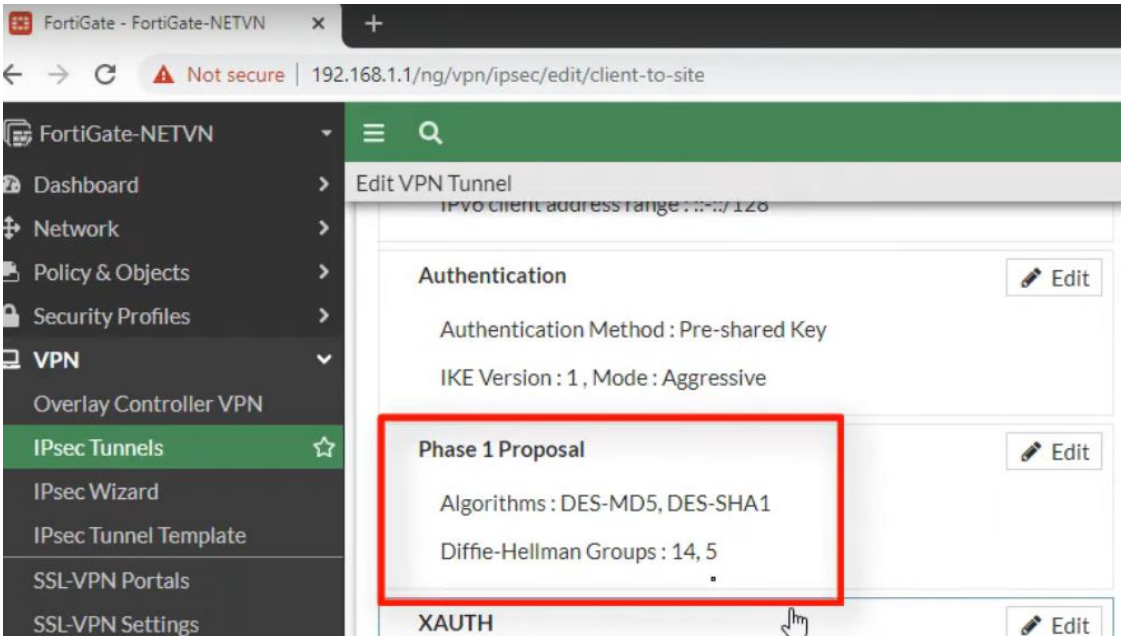

Рис. 3.19. Запам’ятовуємо налаштування з “Phase 1 Proporsal”

Спускаємось трохи нижче та натискаємо редагувати “Phase 2 Proporsal”, обираємо просунутий режим, запам’ятовуємо налаштування з нього та натискаємо “OK”.

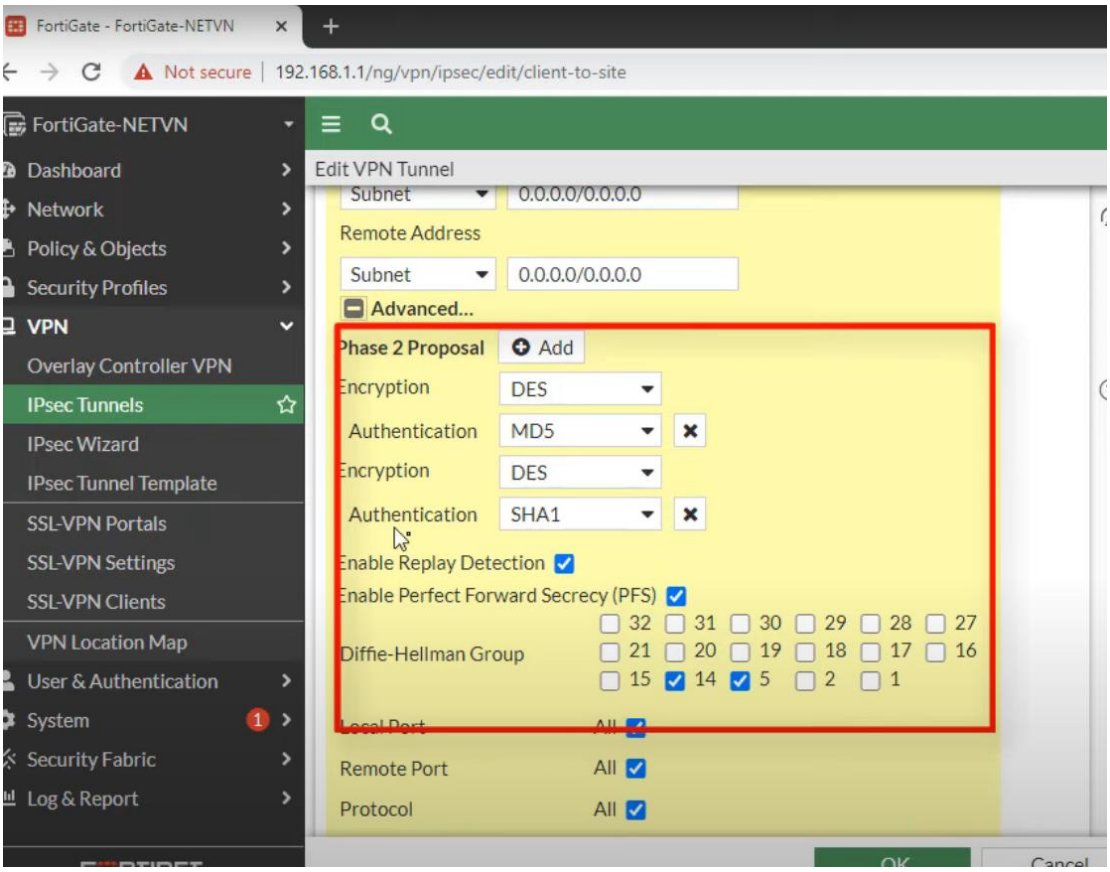

Рис. 3.20. Запам’ятовуємо налаштування з “Phase 2 Proporsal”

Зі сторони робітника організації тепер ми можемо завантажити та встановити FortiClient. Натискаємо конфігурація VPN. Обираємо IPsec VPN, даємо довільну назву, у моєму випадку це буде “connect-to-FortiGate”, вписуємо віддалений шлюз, у методі автентифікації обриємо “Pre-shared key”, вводимо наш ключ та вписуємо ім’я користувача створені раніше.

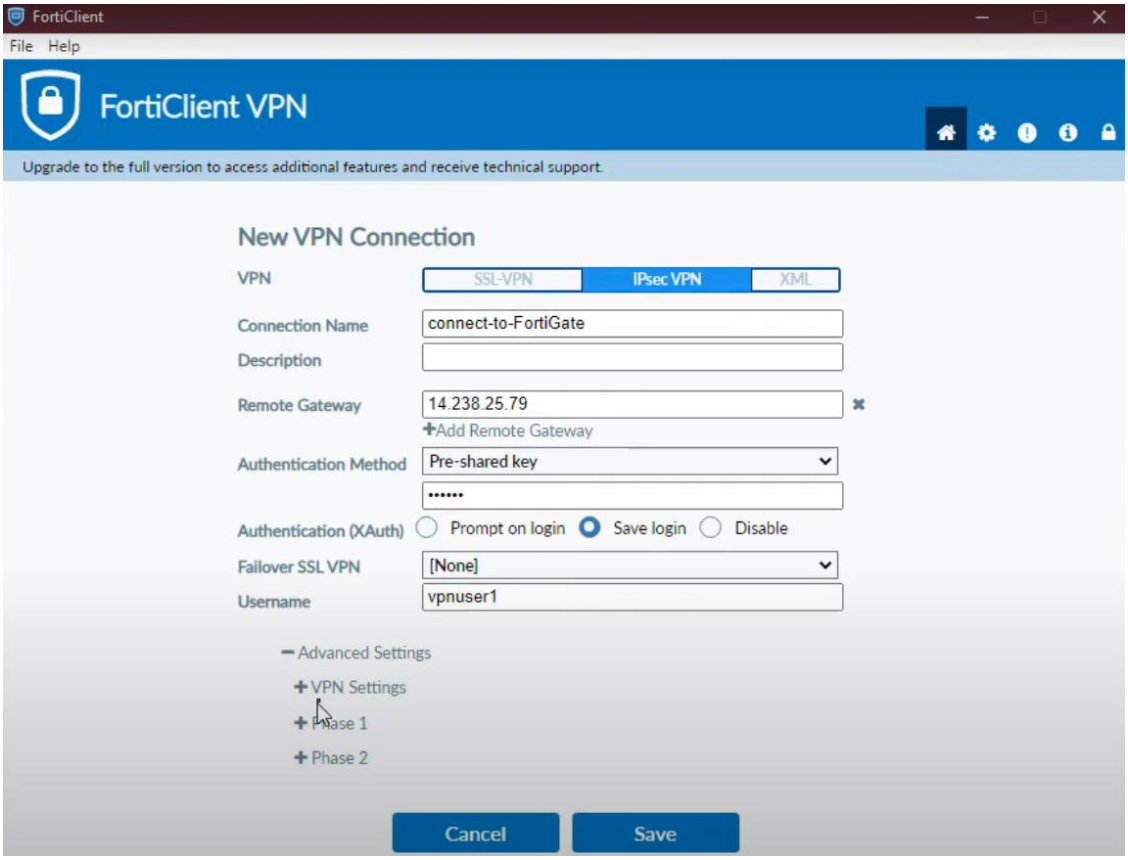

Рис. 3.21. Заповнення VPN з'єдання відомими нами даними

У просунутих налашутваннях обраємо підпункт "Phase 1" та налаштовуємо тут так само конфігурацію, як і в нашому VPN-сервері, яку ми мали запам'ятати

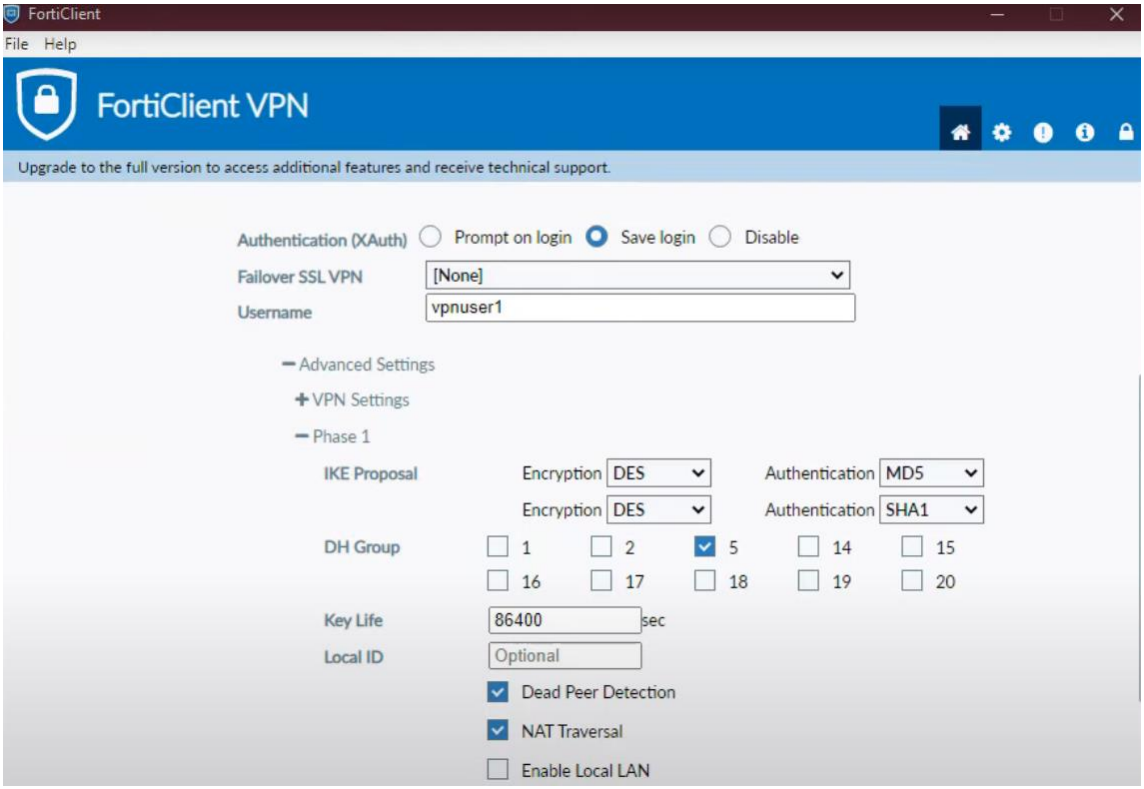

Рис. 3.22. Налашутвання "Phase 1" на стороні робітника організації

Таким самим способом налаштовуємо конфігурацію підпункту “Phase 2” та натискаємо зберегти

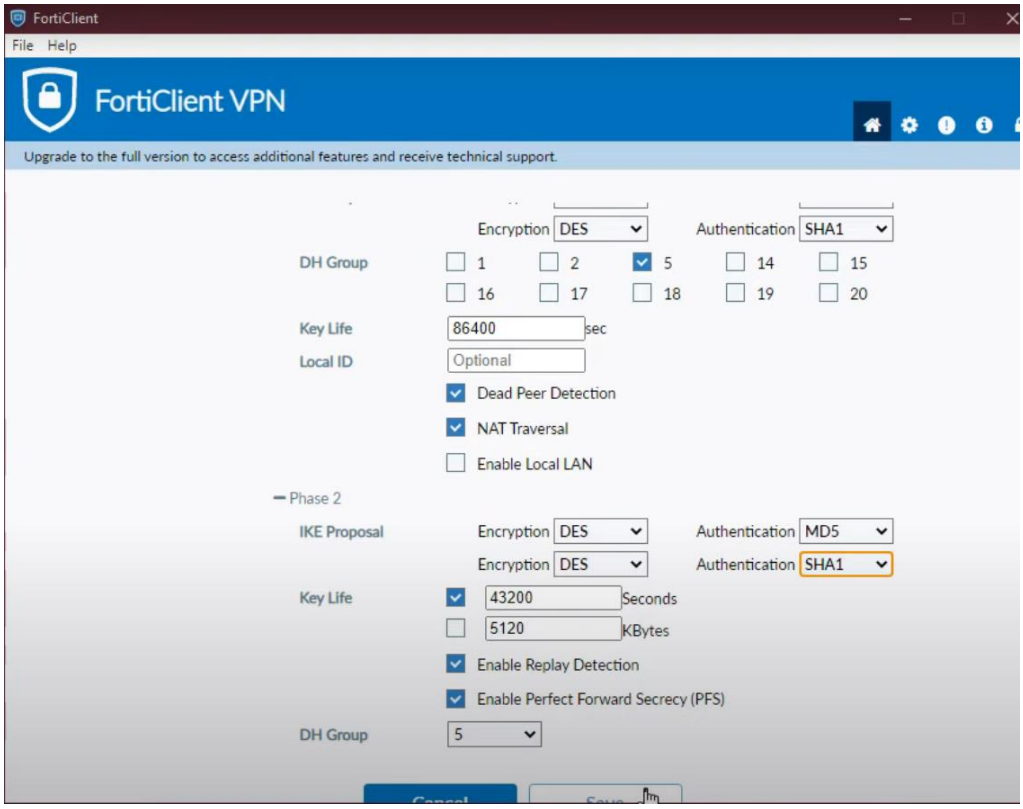

Рис. 3.23. Налашутвання “Phase 2” на стороні робітника організації

Вводимо ім’я користувача та пароль які ми створювали раніше, натискаємо під’єднатися

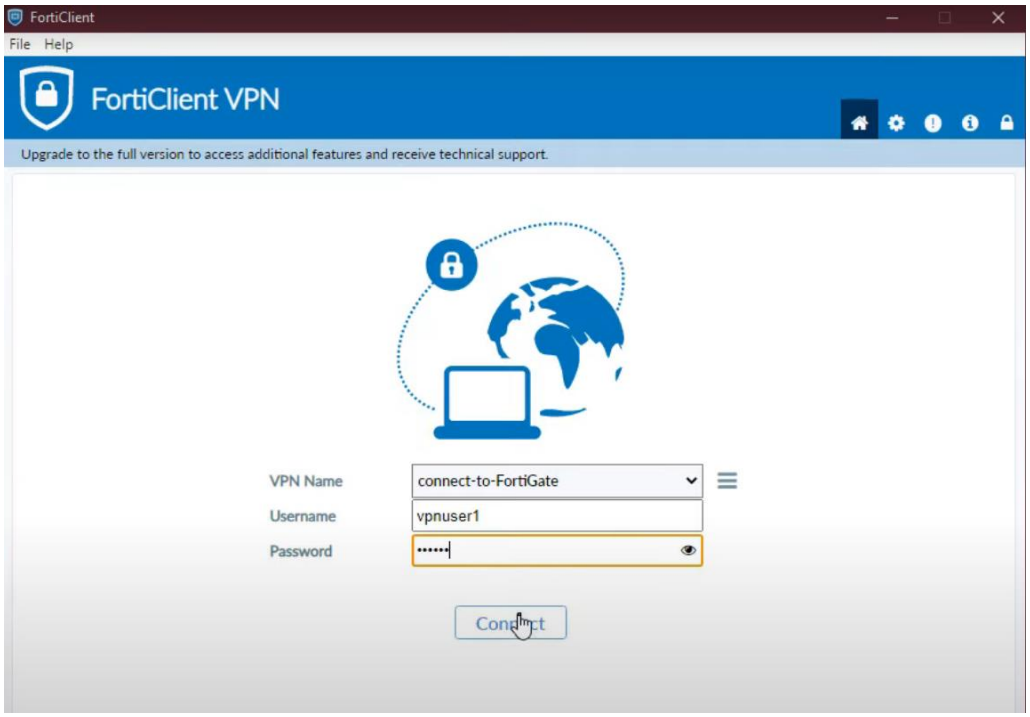

Рис. 3.24. Вводимо дані користувача створеного раніше

Успіх! VPN з'єднання встановлене вдало і тепер робітник може безпечно працювати віддалено

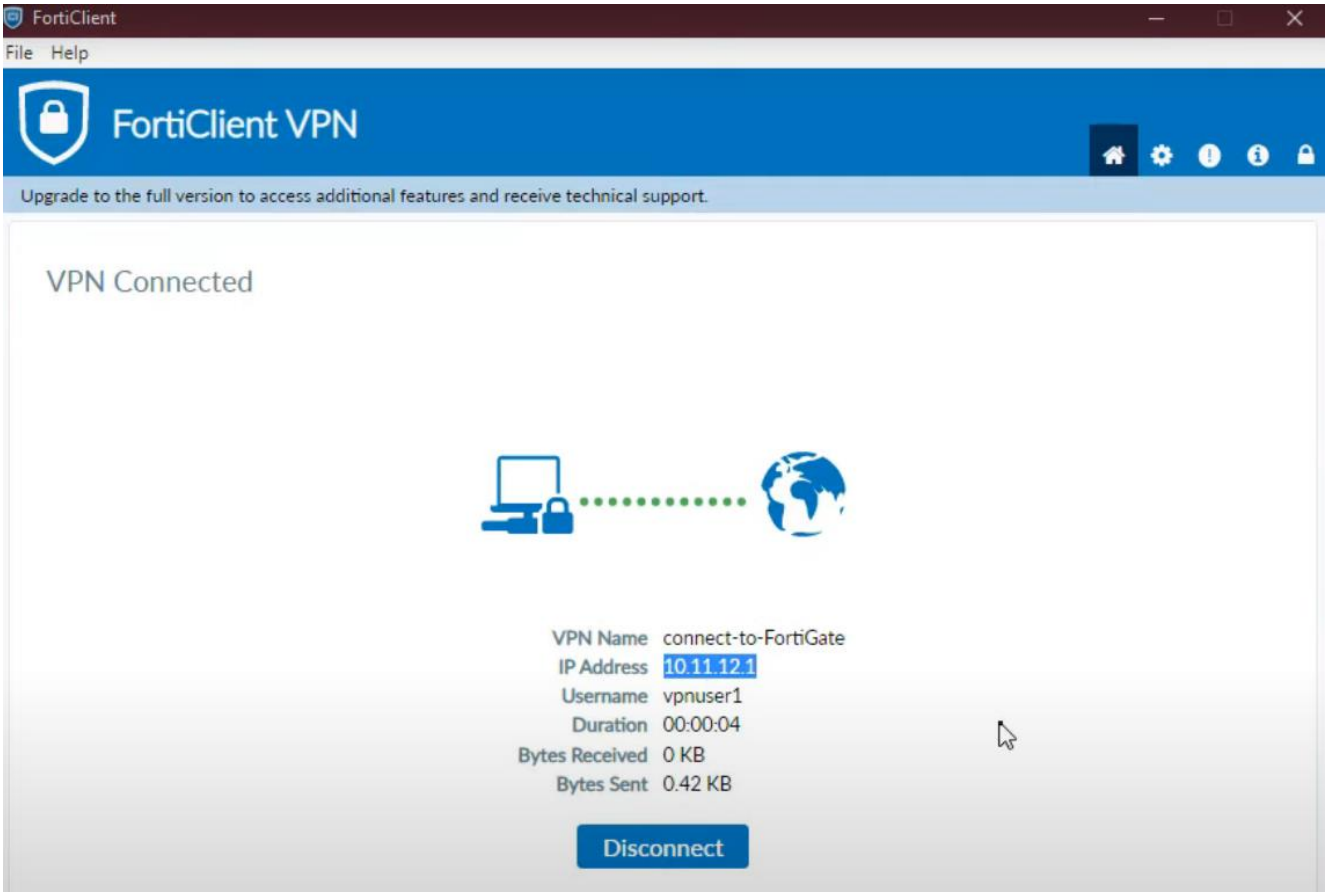

Рис. 3.25. Успішне VPN з'єднання зі сторони віддаленого працівника

Зі сторони серверу все також чудово працює

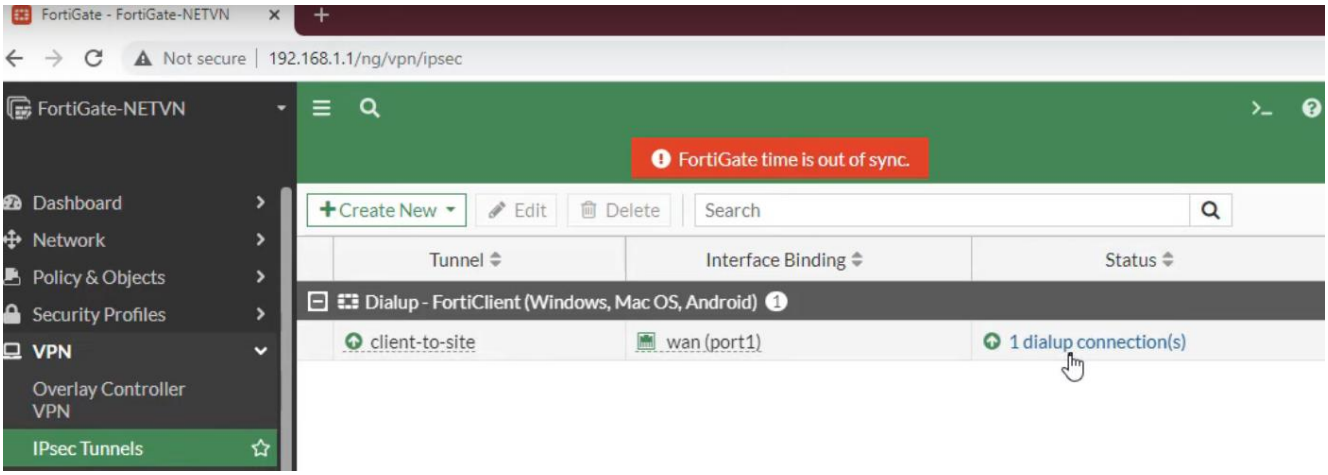

Рис. 3.26. Успішне VPN з'єднання зі сторони серверу

За допомогою FortiClient було успішно налаштовано та встановлено VPN-з'єдання, що забезпечить безпеку та автентифікованість віддаленого працівника, дозволяючи продовжити роботу віддалено.

3.2. Рекомендації щодо застосування методів та засобів захисту віддаленої роботи працівників організації

Захист віддаленої роботи працівників є критично важливим аспектом для будь-якої організації, особливо у сучасному світі, де зростає кількість віддалених працівників та постійно знаходяться нові методи та вектори атак. Нижче подано детальний огляд рекомендацій щодо застосування методів та засобів захисту віддаленої роботи працівників організації:

- використання VPN для захисту віддаленої роботи працівників є критично важливим з точки зору забезпечення конфіденційності, цілісності та доступності даних;
- використання та оновлення антивірусного програмного забезпечення для захисту віддаленої роботи працівників є критично важливим для забезпечення безпеки і надійності інформаційних систем;
- використання методів автентифікації та доступу таких як MFA є критично важливим для захисту віддаленої роботи працівників з огляду на збільшення загроз кібербезпеки та ризику доступу до конфіденційної інформації
- шифрування даних для захисту віддаленої роботи працівників є критично важливим, оскільки забезпечує конфіденційність, цілісність та доступність інформації, що передається через мережу;
- використання політик безпеки, зі сторони організації це їх створення та впровадження, а зі сторони віддаленого працівника – їх дотримання, та навчання працівників також є важливими аспектами для захисту віддаленої роботи працівників;
- моніторинг та аналіз безпеки зі сторони організації є невід'ємними складовими захисту віддаленої роботи працівників, оскільки дозволяють вчасно виявляти, аналізувати та реагувати на потенційні загрози та аномалії в мережі.
- регулярне проведення навчання робітників щодо кращих практик безпеки. Це допоможе уникнути людських помилок.

Загальною метою цих рекомендацій є створення безпечного та надійного робочого середовища для віддалених працівників, забезпечення конфіденційності, цілісності та доступності інформації, а також мінімізація ризиків кіберзагроз. Це важливо не лише для захисту інформації компанії, але і для збереження довіри та репутації бізнесу

ВИСНОВКИ

В роботі проведено дослідження проблеми захисту віддаленої роботи працівників організації, визначено його мету та завдання. Сьогодні існують серйозні проблеми захисту віддаленої роботи працівників організацій від нових і все більш витончених загроз. Спостерігається зростання ризиків для безпеки віддаленої роботи працівників організацій, які посилюються недостатньою підготовленістю їх до протидії новим загрозам за допомогою існуючих платформ із захисту віддаленої роботи працівників.

Проведено аналіз існуючих методів та засобів захисту віддаленої роботи працівників організації. Рішення FortiClient забезпечує захист та контроль кінцевих робочих станцій та серверів з технологією нульової довіри та безпечним клієнтом віддаленого доступу VPN, що дозволяє захищати віддалену роботу працівників організації. Тому FortiClient відіграє визначальну роль у загальній системі забезпечення захисту віддаленої роботи працівників організації.

Отже, захисту віддаленої роботи працівників організації є ключовим аспектом сучасної кібербезпеки, оскільки організації стикаються з дедалі складнішими кібератаками. FortiClient – це комплексне рішення для забезпечення захисту та контролю кінцевих робочих станцій та серверів з технологією нульової довіри та безпечним клієнтом віддаленого доступу VPN, що дозволяє захищати віддалену роботу працівників організації.

FortiClient може допомогти організаціям скористатися останніми рекомендаціями, забезпечуючи комплексний захист віддаленої роботи працівників організації, інтегруючись з іншими продуктами Fortinet, що створює цілісний захист мережі, виявляючи та усуваючи загрози безпеці в реальному часі завдяки використанню штучного інтелекту, підтримуючи мобільність, гнучкість, високу масштабованість та ефективність, централізованість управління, спрощуючи впровадження найкращих практик захисту віддаленої роботи працівників організації.

Таким чином, правильна реалізація рекомендацій захисту віддаленої роботи працівників організації сприятиме ефективному захисту як корпоративних інформаційних ресурсів, так і конфіденційності робітників у цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2022 Remote work becoming more popular URL: https://www.gartner.com/en/human-resources/trends/remote-work-revolution (дата звернення: 02.23.2024).

2. 2022 - 2023 Characteristics of homeworkers URL: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/characteristicsofhomeworkersgreatbritain/september2022tojanuary2023#:~:text=Overall%2C%2044%25%20of%20workers%20reported,reporting%20working%20from%20home%20only. (дата звернення: 02.23.2024).

3. Common Security Risks of Remote Working 2023 https://www.statista.com/statistics/1384003/cybersecurity-concern-level-in-remote-work/ (дата звернення: 02.23.2024).

4. Threat Intelligence Index 2022. URL: https://www.ibm.com/downloads/cas/ADLMYLAZ (дата звернення: 02.23.2024).

5. Endpoint Detection and Response (EDR). Solutions Reviews and Ratings. GARTNER. URL: https://heimdalsecurity.com/blog/remote-work-security/ (дата звернення: 02.23.2024).

6. Essential Remote Work Cybersecurity Statistics In 2024 URL: https://zipdo.co/statistics/remote-work-cybersecurity/ (дата звернення: 02.25.2024).

7. Statistics Of Cyber Security Risks When Working from Home URL: https://www.dbxuk.com/statistics/cyber-security-risks-wfh (дата звернення: 02.25.2024).

8. VMware Workspace ONE UEM Product Documentation: CiscoAnyConnect URL: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Certificate_Authority_Integrations/GUID-CiscoAnyConnect.html (дата звернення: 03.31.2024).

9. Identity architecture design: Microsoft Azure Active Directory URL: https://learn.microsoft.com/en-us/azure/architecture/identity/identity-start-here (дата

звернення: 03.31.2024).

10. Remote Access Architecture. Datasheet. URL: https://www.exclusive-networks.com/wp-content/uploads/2021/08/fortinet-datasheet-forticlient.pdf (дата звернення: 03.31.2024).

11. Security Issues in IPv6 Networks URL: https://www.researchgate.net/publication/52011701_Security_Issues_in_IPv6_Networks (дата звернення: 03.31.2024).

12. IPsec VPN IP address assignments. Datasheet. URL: https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/4729/ipsec-vpn-ip-address-assignments (дата звернення: 03.31.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)