ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту віддалених користувачів інформаційної системи організації»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Марк ЛУПАЧ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ЛУПАЧ Марк
(прізвище, ім'я)

Керівник ЧУМАК Надія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент д.е.н., проф.Легомінова Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

AV – antivirus

DMZs – Demilitarized Zones

DNS – Domain Name System

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

ETDR – Endpoint Threat Detection and Response

NGFW – Next-Generation Firewall

SSO – Single Sign-On

VPN – Virtual Private Network

ZT – Zero Trust

ZTA – Zero Trust Architecture

ZTNA – Zero Trust Network Acces

ВСТУП

Актуальність дослідження. Поширені кіберзагрози до інформаційних систем організацій, пов'язані з віддаленим доступом. Це включає фішингові атаки, слабкі паролі, незахищені домашні мережі та використання особистих пристроїв без належних заходів безпеки. Також існують ризики, пов'язані з невчасно оновленим програмним забезпеченням та недостатньою обізнаністю співробітників.

Системи захисту віддалених користувачів допомагають організаціям запобігти несанкціонованому доступу до важливих даних організації. Тому необхідно дослідити інформацію про відповідні методи та засоби, які використовуються для забезпечення безпеки віддалених підключень.

Методи та засоби способи, за допомогою яких системи захисту віддалених користувачів запобігають несанкціонованому доступу повинні включати використання багатофакторної аутентифікації для підтвердження особистості, шифрування даних під час передачі та зберігання, а також контроль доступу до мережевих ресурсів ораганізації.

До найбільш розповсюджених та рекомендованих систем захисту віддалених користувачів відносяться рішення VPN, яке створює зашифрований тунель для захищеної передачі даних, MFA, яке вимагає кілька способів підтвердження особистост, та ZTNA, що надає більш детальний контроль доступу, мінімізуючи ризики.

Існує декілька важливих законів та стандартів, які вимагають від організацій впровадження заходів безпеки для віддаленого доступу користувачів. До них належать HIPAA для захисту медичної інформації, GDPR для персональних даних в ЄС, PCI DSS для даних платіжних карток та міжнародний стандарт ISO/IEC 27001.

Ці нормативи часто визначають конкретні вимоги до систем захисту віддаленого доступу, такі як обов'язкове шифрування даних, використання

багатофакторної аутентифікації, контроль доступу, моніторинг сесій та ведення журналів подій, а також регулярне оновлення програмного забезпечення. Недотримання цих вимог може призвести до значних штрафів та завдати шкоди репутації.

Використання віртуальної приватної мережі (VPN) дозволяє створювати безпечне з'єднання віддаленого користувача з інформаційною системою організації. Це захищає конфіденційні дані від перехоплення в незахищених мережах.

Отже, організаціям необхідно впроваджувати заходи для забезпечення захисту віддалених користувачів до своєї інформаційної системи організації. Тому тема кваліфікаційної роботи є актуальною та затребуваною для вирішення потреб у забезпеченні кібербезпеки та захисту інформації.

Об'єкт дослідження – захист віддалених користувачів інформаційної системи організації.

Предмет дослідження – система захисту віддалених користувачів інформаційної системи організації на базі рішення FortiClient.

Мета роботи розробити варіант системи захисту віддалених користувачів на базі рішення FortiClient та рекомендації щодо застосування системи захисту віддалених користувачів організації.

Наукові завдання:

дослідити сутність проблеми захисту віддалених користувачів інформаційної системи організації;

проаналізувати основні підходи захисту віддалених користувачів інформаційної системи організації;

проаналізувати існуючі рішення захисту віддалених користувачів інформаційної системи організації;

проаналізувати методи та засоби захисту віддалених користувачів інформаційної системи організації на базі рішення FortiClient;

запропонувати варіант віддалених користувачів інформаційної системи організації на базі рішення FortiClient;

розробити рекомендацій щодо застосування методів та засобів захисту

віддалених користувачів інформаційної системи 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 віддалених користувачів організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми захисту віддалених користувачів організації

Сьогодні поширеним є віддалений доступ до інфраструктури корпоративної мережі. Однією з причин є збільшення віддаленої роботи під час пандемії та військових дій в Україні. Але навіть користувачі, які не є повністю віддаленими, часто потребують віддаленого доступу до відповідних систем: співробітники, які подорожують, сторонні постачальники послуг, постачальники ланцюгів поставок, ділові партнери, аудитори безпеки тощо [1].

Розвиток віддаленої роботи створює нові проблеми для організацій, які хочуть захистити свої ресурси та конфіденційну інформацію. Це пов’язано з тим, що все більше співробітників працюють за межами традиційного офісного середовища, компанії повинні шукати нові способи управління та моніторингу доступу до даних. Пристрої співробітників, домашні мережі Wi-Fi і невідомі програми сторонніх розробників становлять потенційну загрозу безпеці.

Пандемія Covid та війна в Україні змінила багато моделей віддаленої роботи. Технології та системи дозволяють працювати віддалено протягом тривалого часу. Однак деякі компанії не розуміють, як найкраще використовувати віддалену роботу.

Розглянемо загальну статистику щодо віддаленої роботи в організаціях .

– 16% організацій наймають виключно віддалених працівників.

– З 2005 року кількість тих, хто працює з дому, зросла на 140%.

– Зараз у США налічується 4,3 млн. працівників, які працюють з дому щонайменше 50% часу.

За останні десять років дистанційна робота зросла на 115%.

86% віддалених працівників вважають, що самостійна робота підвищує продуктивність.

Лише 4% віддалених працівників працюють у публічних приміщеннях, таких як кафе.

Три чверті віддалених працівників (75%) стверджують, що роботодавці не відшкодовують їм витрати на домашній інтернет.

Можна виділити переваги віддаленої роботи для організацій.

– Компанії, які дозволяють співробітникам працювати дистанційно, хоча б неповний робочий день, матимуть на 25% меншу плинність кадрів.

– Понад три чверті (76%) працівників залишаться працювати в організації, якщо матимуть більш гнучкий графік роботи.

– Працівники відділу продажів на 66% частіше працюють віддалено.

– 21% працівників відмовилися б від частини відпустки, щоб отримати гнучкий графік роботи.

– Більше чверті працівників (28%) погодилися б на зменшення заробітної плати на 10-20%, щоб отримати більш гнучкий графік та працювати віддалено.

– 20% працівників відмовилися б від пенсійних виплат заради віддаленої роботи.

– Менше половини (44%) віддалених працівників з необмеженою відпусткою братимуть лише два-три тижні відпустки на рік.

– Кожен десятий віддалений працівник з необмеженою відпусткою візьме лише один тиждень відпустки.

– Кожен двадцятий віддалений працівник з необмеженою відпусткою візьме менше одного тижня відпустки на рік.

– Дозвіл на віддалену роботу може заощадити роботодавцям 11 000 доларів на рік на витратах на працівників (офісні приміщення, електроенергія та інше).

Отже віддалена робота для користувачів інформаційної системи організацію відзначається особливою тенденцію, яка приводить до гнучкого й гібридного майбутнього сфери праці. Працюючи віддалено протягом досить довгого періоду часу, віддалені робітники тепер хочуть зберегти гнучкість свого графіку і можливість працювати віддалено з будь-якого місця, в будь-який час і на будь-

якому пристрої, навіть якщо вони повернуться в офіс.

Це посилює потребу організацій у перегляді своїх позиції щодо політик безпеки у секторі кібербезпеки, особливо коли необхідно створити стійкі організації. Безпека організації повинна стати шляхом до здатності бізнесу до швидкого відновлення, оскільки це дозволить організаціям працювати гнучко, надійно адаптуючись для захисту своїх інформаційних ресурсів та активів.

Отже, для організацій важливим питанням постає забезпечення гнучкісті, простоти використання, ефективна і безпечна мережева комунікація для впровадження рішень щодо спільної віддаленої роботи, незалежно від того, чи надаються ресурси через локальні центри обробки даних або в хмарі, а також на всіх призначених для користувача пристроях — робочих або особистих.

Отже, згідно статистики , як показано на рис 1.1, кількість віддалених користувачів у порівнянні з початком Covid-19 зменшилась, але тенденція віддаленої роботи зберігається.

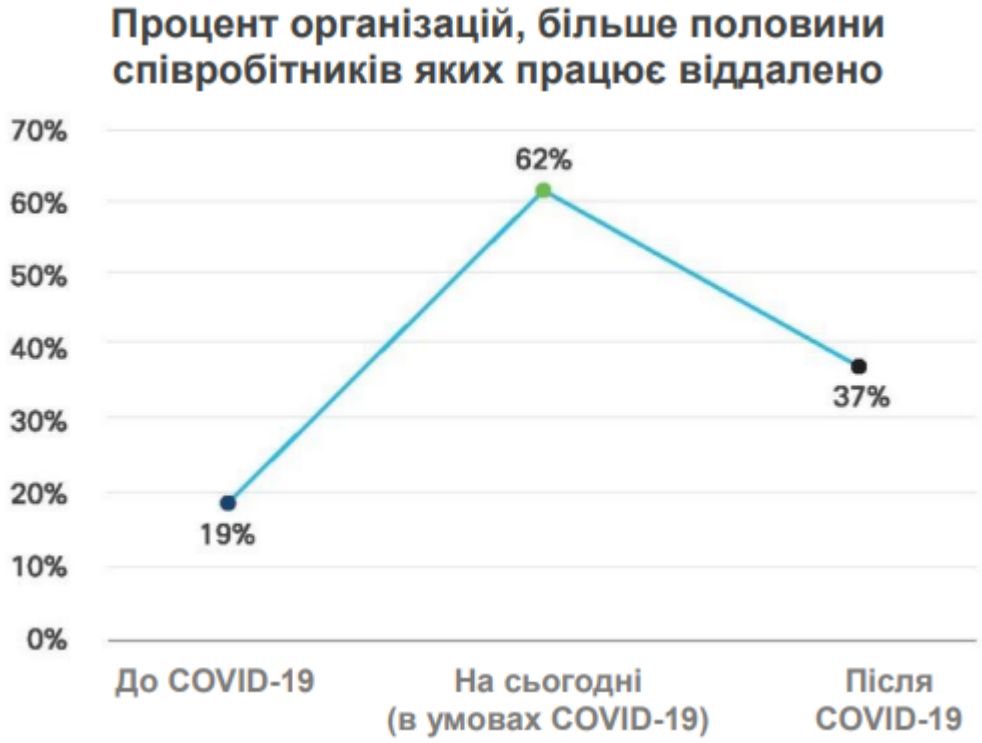


Рис.1.1. Відсоток організацій, який працює віддалено

Для малого, середнього та великого бізнесу також зберігається тенденція щодо віддаленої роботи користувачів їх організації.

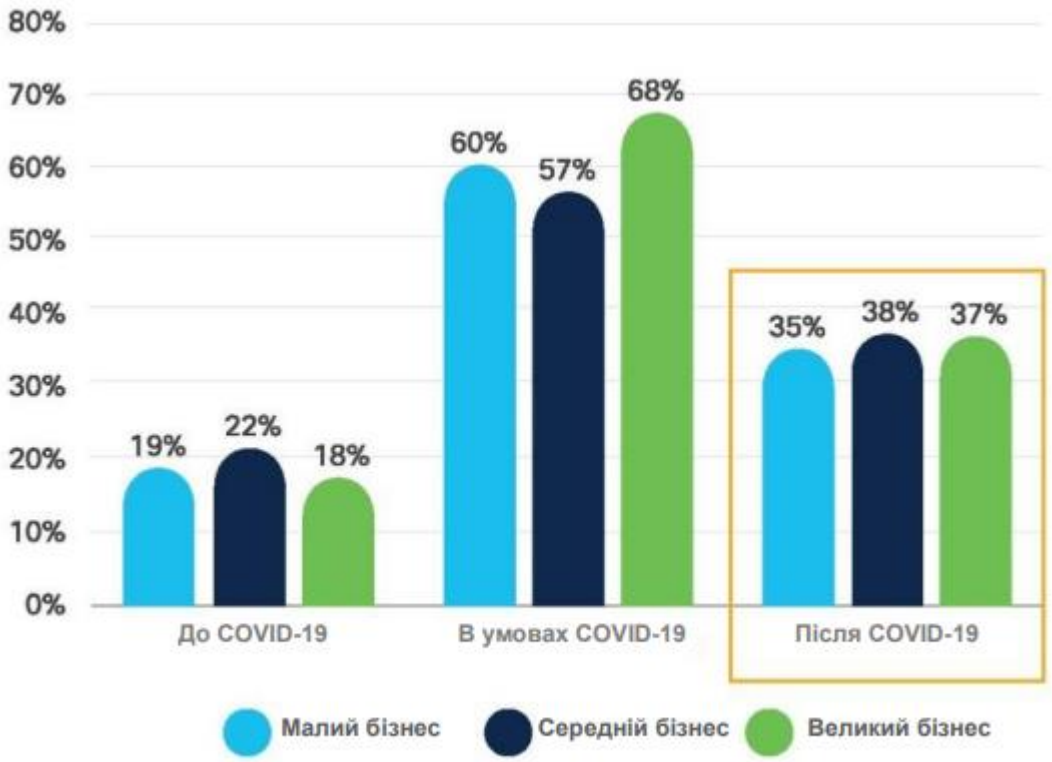


Рис. 1.2. Відсоток віддаленої роботи у малому, середньому та великому бізнесі

Щоб підтримувати безпеку, організації необхідно забезпечити всім віддаленим користувачам безперебійним доступом саме до тих програм і даних, які їм потрібні для роботи. Для цього потрібна надійна стратегія контролю доступу віддалених користувачів до інформаційної системи організації.

Забезпечення гнучкої і гібридної робочої тенденцію у майбутньому, потребує від компаній гарну і безпечну базова інфраструктуру[4]. Кібербезпека повинна очолювати корпоративні та стати головним пріоритетним напрямком для організацій. Про це говорить статистика [4]. Вісімдесят п'ять відсотків респондентів в усьому світі заявили, що кібербезпека є дуже важливою сьогодні.

Значна частина респондентів, а саме 44-50 % відмічають важливість кібербезпеки для їхнього бізнесу (Рис. 1.3).

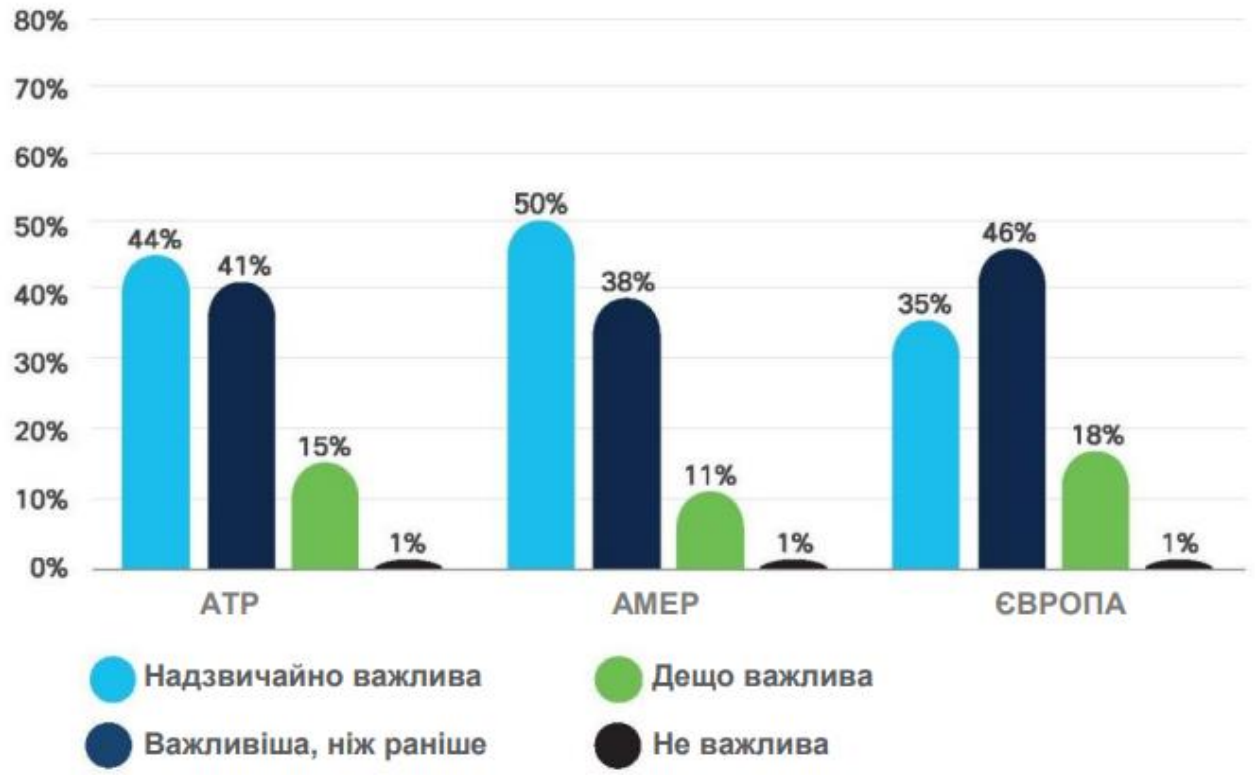


Рис. 1.3. Важливість кібербезпеки для бізнесу

Проведемо аналіз загроз, які можуть бути для віддалених користувачів інформаційної системи організації.

Динаміка віддаленої роботи значно змінилася з моменту початкового переходу до дистанційної роботи після пандемії. У міру того як компанії та співробітники адаптуються до нових ритмів, фокус змістився з адаптації на оптимізацію гнучкої організації роботи.

Думки користувачів різні: 52% співробітників віддають перевагу гібридній роботі, тоді як 27% віддають перевагу віддаленій роботі повний робочий день. Лише 21% віддають перевагу очній роботі повний робочий день [5].

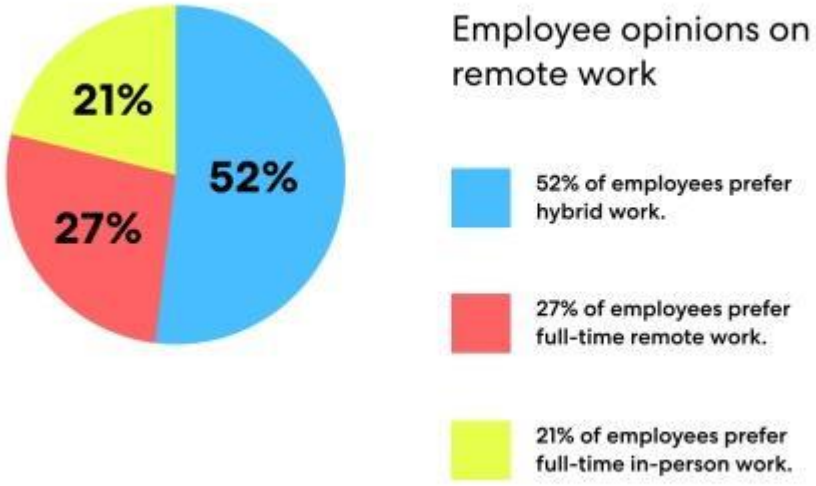


Рис. 1.4. Статистика щодо можливості віддаленої роботи

Можна виділити найбільші ризики безпеки, на які варто звернути увагу організаціям [6].

По-перше – це незахищені мережі Wi-Fi. Для роботи віддалені працівники часто покладаються на загальнодоступні чи домашні мережі Wi-Fi. Однак вони навряд чи такі безпечні, як ті, що знаходяться в офісному середовищі, піддаючи ризику дані, що передаються між їх пристроєм і корпоративними серверами.

По-друге – фішингові атаки. Згідно зі звітом Verizon про порушення даних за 2024 рік , 36% усіх порушень даних стосуються фішингу. Відсутність особистого спілкування та допомоги з боку IT-відділів робить віддалених користувачів більш сприйнятливими до таких атак.

По-третє - погане керування паролями. Жоден брандмауер чи VPN не є достатньо безпечними, щоб компенсувати ризик несанкціонованого доступу через слабкі паролі. Або ті що повторюються і, згідно з дослідженнями, складають 51% паролів, що використовуються в усьому світі.

Четверте - ризики зловмисного програмного забезпечення. Зменшення нагляду з боку IT-спеціалістів у поєднанні з поширеним використанням несхваленого обладнання та програмного забезпечення може створити ідеальну платформу для кіберзлочинців, які хочуть скористатися знаннями про віддалену

роботу організації.

По- п’яте – це недостатня підготовка співробітників. Коли справа доходить до зменшення ризиків віддаленої роботи, працівники можуть бути найслабшою ланкою або найсильнішим союзником. Незважаючи на цей факт, кожна третя компанія не може запропонувати віддаленим працівникам навчання з питань кібербезпеки.

З урахуванням того, що віддалені користувачі для організацій є критично важливим аспектом кібербезпеки з урахуванням сучасних гібридних моделей роботи, можна виділити основні загрози та поділити їх на кілька категорій:

1. Загрози на рівні пристрою.

Наведемо приклади такої загрози.

Викрадення або втрата пристрою — фізичний доступ до ноутбука, смартфона або планшета може призвести до компрометації даних.

Шкідливе ПЗ (Malware, Ransomware, Spyware) — зараження пристрою зловмисними програмами.

Rootkit'и та Backdoor'и — дозволяють прихований доступ до системи без відома користувача.

Ненадійне налаштування пристрою — відсутність пароля на екран блокування, використання старих версій ПЗ тощо.

2. Загрози на рівні мережі

Перехоплення трафіку (Man-in-the-Middle, MitM) — зловмисник перехоплює мережевий трафік у незахищених мережах (наприклад, публічний Wi-Fi).

DNS-спуфінг (DNS Spoofing) — підміна DNS-записів для перенаправлення на фальшиві сайти.

Атаки на VPN — експлуатація вразливостей у VPN-клієнтах чи протоколах.

DoS/DDoS-атаки — можуть порушити доступ до корпоративних сервісів.

3. Загрози на рівні автентифікації

Фішинг (Phishing) — спроби виманити облікові дані через підроблені веб-ресурси або електронні листи.

Brute Force / Password Spraying — автоматизовані атаки на слабкі паролі.

Credential Stuffing — використання викрадених облікових даних з інших сервісів.

Слабка або відсутня двофакторна автентифікація (2FA) або MFA.

4. Загрози на рівні програмного забезпечення

Уразливості в ПЗ (Exploits) — використання недоліків у додатках або ОС для отримання контролю над пристроєм.

Атаки через застаріле ПЗ — старі версії програм часто містять відомі вразливості.

Зловмисні розширення та плагіни — можуть викрадати дані або інфікувати систему.

5. Загрози на рівні даних

Витік конфіденційної інформації — може статися через фішинг, атаки на хмарні сервіси або недбалість користувачів.

Несанкціоноване копіювання даних — використання незахищених USB-носіїв або особистих хмарних сховищ.

Атаки на хмарні сховища (Cloud Threats) — доступ до корпоративних файлів через скомпрометовані облікові записи.

6. Загрози на рівні людського фактору

Соціальна інженерія (Social Engineering) — маніпуляції для отримання доступу до системи.

Недбалість співробітників — незахищене збереження паролів, використання особистих пристроїв для роботи.

Використання небезпечних програм — сторонні додатки, що можуть містити вразливості.

7. Загрози на рівні фізичного середовища

Компрометація пристрою під час подорожі — наприклад, підключення до шкідливих зарядних станцій (USB Juice Jacking).

Перехоплення екрану (Shoulder Surfing) — зловмисник підглядає за екраном пристрою в громадському місці.

Всі перераховані загрози є ризиками для організації, що можуть призвести до

небажаних наслідків в організації. Тому надалі розглянемо основні підходи для захисту віддалених користувачів інформаційної системи організації.

1.2. Аналіз підходів до захисту віддалених користувачів організації

Щоб допомогти організаціям забезпечити захист віддалених користувачів необхідно застосовувати кращі методи та засоби захисту віддаленого доступу.

До таких методів та засобів необхідно відносити створену комплексну систему захисту віддалених користувачів до інформаційної системи організації. Така система повинна включати наступні методи та засоби:

1. Застосовувати методи найменших привілеїв для віддаленого доступу

Робота повинна початись із проведення ретельної оцінки ризиків, щоб визначити та проаналізувати потенційні ризики та вразливі місця поточних методів віддаленого доступу. Необхідно провести ретельний аналіз усіх дозволів, причому перевірку проводять особи, які знають, яким користувачам до яких ресурсів потрібен доступ. Визначити осіб, які мають права віддаленого доступу, але насправді вони не потрібні для виконання своєї роботи. Усунути всі надмірні та невикористані права відповідно до принципу найменших привілеїв.

Визначити та вимкнути усі застарілі або неактивні облікові записи користувачів.

Підтримувати мінімальну кількість привілейованих облікових записів, оскільки вони є основними цілями для загроз.

Переконатися, що дозволи NTFS і дозволи для спільних ресурсів, як-от SharePoint, SharePoint Online, OneDrive для бізнесу та Teams, відповідають принципу найменших привілеїв.

Мінімізуйте зону атаки серверів та інших критичних систем, дезактивувавши або видаливши непотрібні мережеві служби чи функції.

Використовувати групи Active Directory і Azure AD для контролю доступу до інфраструктури організації. Регулярно перевіряти свої групи, їхні дозволи, щоб

переконатися, що ніхто не має надмірних дозволів.

2. Запровадити захист процесів автентифікації віддалених користувачів організації.

Використання лише паролів для автентифікації користувачів підвищує ризик витоку даних організації, оскільки паролі можуть бути надто легко скомпрометовані зловмисниками за допомогою атак грубої сили, фішингу та тактики соціальної інженерії. Щоб більш надійно підтверджувати особу віддалених користувачів необхідно налаштувати політику надійних паролів . Обов'язково визначити вимоги до довжини та складності роблять паролі складними для зловмисників.

Застосовувати політику блокування облікового запису, щоб заблокувати зловмисників, які намагаються проникнути у вашу мережу організації шляхом повторного вгадування пароля. Для цього необхідно встановити порогову кількість невдалих спроб на збалансованому рівні, щоб уникнути надмірного розчарування та втрати продуктивності для законних користувачів, які іноді можуть неправильно вводити свої паролі.

Застосувати або розгорнути менеджер паролів, щоб дозволити користувачам безпечно зберігати свої облікові дані та керувати ними.

Впровадити багатофакторну автентифікацію (MFA). Двофакторна автентифікація є найпростішою формою MFA; він вимагає від користувачів підтвердити свою особу двома способами, щоб отримати доступ. Параметри MFA включають те, що ви знаєте (наприклад, пароль), те, що у вас є (наприклад, код із маркера безпеки або сповіщення мобільного додатка), і те, що ви є (біометричні дані, як-от відбитки пальців або розпізнавання обличчя). MFA має бути реалізовано для всіх віддалених привілейованих доступу та всіх підключень віртуальної приватної мережі (VPN) [14-18].

3. Знати свої пристрої в організації

Зменшення поверхні атаки пристроїв, які використовуються для віддаленого доступу до ресурсів компанії, має вирішальне значення для уникнення інцидентів безпеки. Передові практики включають наступне:

Переконайтеся, що всі операційні системи та програми все ще отримують підтримку від постачальників. Замініть будь-яке програмне забезпечення, термін служби якого закінчився.

Підтримуйте всі операційні системи, мікропрограми та програмні додатки в актуальному стані та повністю виправляйте відомі вразливості.

Встановіть програмне забезпечення для виявлення та реагування інцендентів на кінцеві точки (EDR), антивірусне програмне забезпечення, програмне забезпечення для захисту від шкідливих програм та інше програмне забезпечення для захисту кінцевих точок.

Налаштуйте локальний брандмауер для всіх пристроїв відповідно до найкращих стандартів.

Використовуйте рішення для керування мобільними пристроями (MDM), щоб дозволити IT-адміністраторам дистанційно налаштовувати пристрої, блокувати та стирати дані з будь-якого втраченого чи вкраденого пристрою.

Перегляньте свою групову політику , щоб переконатися, що до машин, приєднаних до домену, застосовано правильні параметри безпеки та політики.

Вимкніть або видаліть мережеві служби, які не використовуються, і непотрібні програми.

4. Обмежити використання RDP

Зменшити або виключити використання протоколу віддаленого робочого столу (RDP), оскільки він є основною мішенню для зловмисників, які хочуть отримати доступ до корпоративних систем. Якщо організація все ж таки використовуєRDP, необхідно притримуватись таких правил:

Заборонити прямий доступ RDP із зовнішніх мереж. Замість цього встановіть підключення VPN як початковий крок, а потім підключіться до ресурсу всередині через RDP.

Обмежити RDP списком затверджених IP-адрес і облікових записів користувачів.

Увімкніть автентифікацію на рівні мережі (NLA), яка допомагає захистити підключення до віддаленого робочого столу, вимагаючи від клієнтів RDP

автентифікації перед встановленням сеансу. NLA також допомагає захистити від атак типу "людина посередині" .

5. Використовувати зашифровані дані в організації

Увімкніть локальне шифрування на всіх пристроях, щоб забезпечити конфіденційність і безпеку даних як у стані спокою, так і під час передачі під час віддаленого доступу. Опції включають BitLocker для Windows і FileVault для Mac OS.

6. Впровадити Zero Trust для доступу до мережі організації

Нульова довіра — це модель безпеки, заснована на принципі, згідно з яким жодна сутність не може бути довіреною за замовчуванням; натомість кожен запит на доступ до ресурсів потрібно оцінювати на наявність потенційних ризиків і може потребувати додаткової перевірки. Впровадження Zero Trust покращує безпеку віддаленого доступу, допомагаючи гарантувати блокування зловмисників, яким вдається прослизнути в середовище [18-24].

7. Проводити аудит

Для оперативного виявлення загроз та реагувати на них, організаціям необхідно уважно стежити за діяльністю всіх користувачів в інформаційній системі організації.

Аудит конфігурації — щоб переконатися, що конфігурація всіх критичних ресурсів відповідає вашому базовому рівню безпеки, вам потрібно перевірити всі зміни конфігурації на наявність помилок і зловмисної активності.

Аудит доступу — відстежуйте входи до хмарних і локальних ресурсів, а також входи до VPN. Підвищення кількості невдалих спроб входу та іншої незвичайної активності може свідчити про наявні загрози.

Аудит активності — відстежуйте дії користувачів щодо конфіденційної інформації , зокрема даних у хмарних рішеннях, які підтримують віддалених працівників, наприклад SharePoint Online, OneDrive для бізнесу та Teams. Наприклад, зміни членства в групі та дозволів можуть вказувати на підвищення привілеїв. Також слідкуйте за підозрілими сплесками активності навколо ваших мережевих портів і VPN-з’єднань, особливо сканування портів і невдалих спроб

входу, що може бути ознакою підбору пароля або інших атак грубої сили.

8. Постійні навчання безпеки для всіх користувачів

Інвестування в тренінги з усвідомлення загроз може значно підвищити рівень безпеки віддаленого доступу. Навчіть усіх користувачів, незалежно від того, чи вони віддалені, чи в офісі, вашій політиці кібербезпеки та тому, як вони ґрунтуються на найкращих практиках. Інформуйте їх про нові загрози, навчіть їх розпізнавати спроби фішингу та соціальної інженерії та повідомляти про них. Обов'язково продовжуйте тестування, наприклад імітацію фішингових атак, і усуньте будь-які слабкі місця, які ви виявите.

Отже сучасним організаціям потрібен віддалений доступ як для співробітників, так і для сторонніх користувачів. Однак вони повинні підтримувати безпеку свого середовища. Дотримуючись наведених тут передових методів, ви можете забезпечити надійну безпеку, не жертвуючи гнучкістю та гнучкістю, які пропонує віддалений доступ.

1.3. Аналіз існуючих рішень із захисту віддалених користувачів організації

Розглянемо рішення щодо захисту з'єднань, які забезпечують захищене з'днання віддалених користувачів. Для порівняння обрано наступні рішення:

– Cisco AnyConnect , яке є масштабованим рішенням для корпоративних мереж.

– Palo Alto GlobalProtect , яке дозволяє інтеграцію з NGFW для підвищеного рівня безпеки.

– Fortinet FortiClient, яке є зручним VPN-клієнтом із наданням додаткових функцій безпеки.

– Check Point Remote Access VPN, яке забезпечує безпечний доступ із глибоким рівнем контролю.

Проведемо порівняльний аналіз обраних VPN-рішень, які повинні забезпечити роботу віддалених користувачів для віддаленого доступу — Cisco

AnyConnect, Palo Alto GlobalProtect, Fortinet FortiClient та Check Point Remote Access VPN. В основу порівняння покладено наступні аспекти:

1. Інтеграція з екосистемою та сумісність

2. Безпека та функціональність

3. Продуктивність та масштабованість

4. Управління та адміністрування

Розглянемо кожний аспект в розрізі запропонованого рішення, щоб потім все об’єднати у загальну таблицю порівняння і вибору рішення для організації захищеного віддаленого доступу віддалених користувачів інформаційної системи організації (табл.1.1).

1. Інтеграція з екосистемою та сумісність

Cisco AnyConnect

Інтеграція: Найкраще працює в середовищі Cisco, тісно взаємодіє з іншими продуктами (наприклад, ASA, Firepower).

Платформи: Підтримує Windows, macOS, Linux, iOS та Android.

Palo Alto GlobalProtect

Інтеграція: Оптимальний вибір для організацій, що використовують Palo Alto Networks. Інтегрується з їхніми NGFW та іншими рішеннями безпеки, що дозволяє реалізувати комплексний підхід.

Платформи: Підтримує широкий спектр ОС, включаючи мобільні пристрої.

Fortinet FortiClient

Інтеграція: Найкраще інтегрується з пристроями FortiGate, доповнюючи інші засоби захисту, як антивірус та веб-фільтрація.

Платформи: Підтримує основні операційні системи та мобільні платформи.

Check Point Remote Access VPN

Інтеграція: Добре поєднується з іншими рішеннями Check Point, забезпечуючи централізоване управління політиками безпеки.

Платформи: Підтримка різноманітних ОС, що забезпечує гнучкість для користувачів.

2. Безпека та функціональність

Cisco AnyConnect

Безпека: Пропонує міцне шифрування, можливості перевірки стану кінцевих пристроїв (posture assessment) та інтеграцію з розширеними рішеннями безпеки Cisco.

Особливості: Висока надійність, багаторівнева автентифікація.

Palo Alto GlobalProtect

Безпека: Відзначається розширеною безпекою завдяки інтеграції з системою наступного покоління (NGFW), а також функціями оцінки стану пристроїв.

Особливості: Забезпечує детальний аналіз загроз і динамічне застосування політик безпеки.

Fortinet FortiClient

Безпека: Крім VPN, включає в себе компоненти антивірусу, антишкідливого ПЗ та веб-фільтрації, що забезпечує комплексний захист кінцевих пристроїв.

Особливості: Легкий агент з мінімальним впливом на продуктивність пристроїв.

Check Point Remote Access VPN

Безпека: Сфокусований на забезпеченні безпечного доступу через розгорнуту систему політик та інтегровану багаторівневу автентифікацію.

Особливості: Може бути налаштований з урахуванням специфічних вимог організації, забезпечуючи гнучкий контроль доступу.

3. Продуктивність та масштабованість

Cisco AnyConnect:

Забезпечує високу продуктивність та стабільність, що підтверджується численними великими розгортаннями в корпоративному середовищі.

Palo Alto GlobalProtect:

Призначений для великих організацій з розподіленою інфраструктурою; ефективно працює при інтеграції з сучасними мережевими компонентами.

Fortinet FortiClient:

Відомий своєю ефективністю та економічністю, особливо при використанні в поєднанні з пристроями FortiGate.

Check Point Remote Access VPN:

Пропонує надійну продуктивність із можливістю масштабування, що є важливим фактором для організацій з численними віддаленими користувачами.

4. Управління та адміністрування

Cisco AnyConnect:

Має зрілий інтерфейс управління та інтеграцію з централізованими системами управління мережами Cisco.

Palo Alto GlobalProtect:

Адміністрування через єдину консоль Palo Alto, що дозволяє централізовано керувати політиками безпеки по всій мережі.

Fortinet FortiClient:

Легко інтегрується в систему централізованого управління FortiGate, спрощуючи адміністрування та моніторинг.

Check Point Remote Access VPN:

Централізоване управління через Check Point SmartConsole, що дозволяє ефективно налаштовувати політики доступу та проводити аудит.

Таблиця 1.1.

Порівняння рішень віддаленого доступу до інформаційної системи користувачів

Рішення	Інтеграція з екосистемою та сумісність	Безпека та функціональність	Продуктивність та масштабованість	Управління та адміністрування
Cisco AnyConnect,	8	7	10	8
Palo Alto GlobalProtect,	9	8	9	10
Fortinet FortiClient	9	8	10	10
Check Point Remote	8	8	10	10

Розрахунок балів, отриманих за кожним параметром, виставлявся на основі експертної оцінки. Результат обраховувався як середнє значення по кожному рішенню.

Отже, зробимо короткий висновок по кожному рішенню для організації віддаленого доступу до інформаційної системи організації.

Cisco AnyConnect підійде для організацій, які вже використовують інфраструктуру Cisco і потребують високої надійності й широкої функціональності.

Palo Alto GlobalProtect є відмінним вибором для підприємств, що використовують NGFW від Palo Alto Networks та потребують глибокої інтеграції безпеки.

Fortinet FortiClient оптимальний варіант для тих, хто віддає перевагу комплексним рішенням Fortinet із інтегрованими антивірусом та іншими засобами захисту.

Check Point Remote Access VPN пропонує гнучке управління політиками безпеки та добре інтегрується в екосистему Check Point, що робить його ефективним вибором для організацій з високими вимогами до контролю доступу.

Кожен з цих продуктів має свої сильні сторони, тому вибір конкретного рішення залежатиме від існуючої інфраструктури, вимог до безпеки та бюджету організації. Тому в подальшому дослідженні будемо використовувати рішення Fortinet FortiClient, як рішення, яке відповідає найкраще вимогам згідно таблиці 1.1.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

https://docs.fortinet.com/document/forticlient/7.4.2/administration-guide/32775/fortigate-ssl-vpn-configuration

2.1. Архітектура та призначення Fortinet FortiClient

FortiClient — це Fabric Agent, який забезпечує захист, відповідність вимогам і безпечний доступ в єдиному модульному легкому клієнті. Агент Fabric — це програмне забезпечення кінцевої точки, яке працює на кінцевій точці, наприклад, ноутбуці або мобільному пристрої, і взаємодіє з Fortinet Security Fabric, щоб надати інформацію, видимість і контроль цьому пристрою. Основні аспекти, які надає Fortinet FortiClient це безпечний доступ та захист кінцевої точки віддаленого користуачі.

До складових архітектури FortiClient входить безпечний доступ, захист кінцевої точки, підтримка та конвергентний захист для запобігання розширеним загрозам.

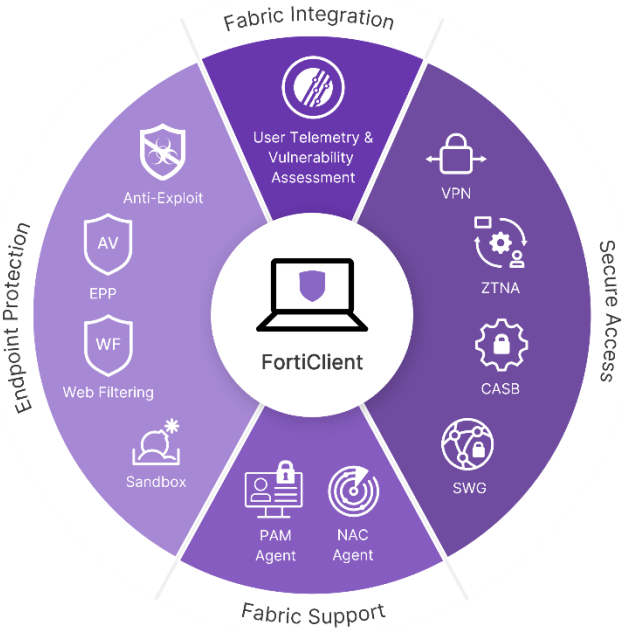


Рис.2.1. Архітектура FortiClient

В основі *безпечного доступу*, закладено, що агент Unified FortiClient дозволяє віддаленим працівникам безпечно підключатися до мережі за принципом нульової довіри. Ця версія підтримує тунелі, зашифровані як Universal ZTNA, так і VPN, а також фільтрацію URL-адрес і брокер безпеки доступу до хмари (CASB). FortiSASE надає розміщені в хмарі Universal ZTNA, CASB і SWG і включає агент Unified FortiClient. Включено централізоване керування через FortiClient EMS [14-17].

Захист кінцевої точки. Агент Unified FortiClient забезпечує розширені можливості безпеки, додаючи антивірус нового покоління (NGAV) на основі штучного інтелекту, карантин кінцевих точок і брандмауер програм, а також підтримку хмарної пісочниці, керування USB-пристроями та захисту від програм-вимагачів.

Конвергентний захист для запобігання розширеним загрозам. FortiEndpoint об’єднує безпечне підключення, захист кінцевих точок і розширені можливості, такі як виявлення кінцевих точок і відповідь (EDR) і розширене виявлення і відповідь (XDR), в одному агенті. Це спрощує керування та покращує видимість, одночасно зменшуючи витрати та складність. Рішення надає IT-командам необхідну видимість і контроль, а групам безпеки надають переваги автоматизованого виявлення загроз і реагування на них. Це мінімізує потребу в ручному втручанні та забезпечує швидше усунення загроз у всіх середовищах.

Керовані служби безпеки кінцевих точок. Щоб спростити початкове розгортання та розвантажити постійний моніторинг, Fortinet пропонує керовані послуги, орієнтовані на кінцеву точку, щоб забезпечити повну роботу рішення FortiClient, забезпечуючи налаштування, розгортання, налаштування, моніторинг уразливостей і загальний моніторинг безпеки кінцевої точки.

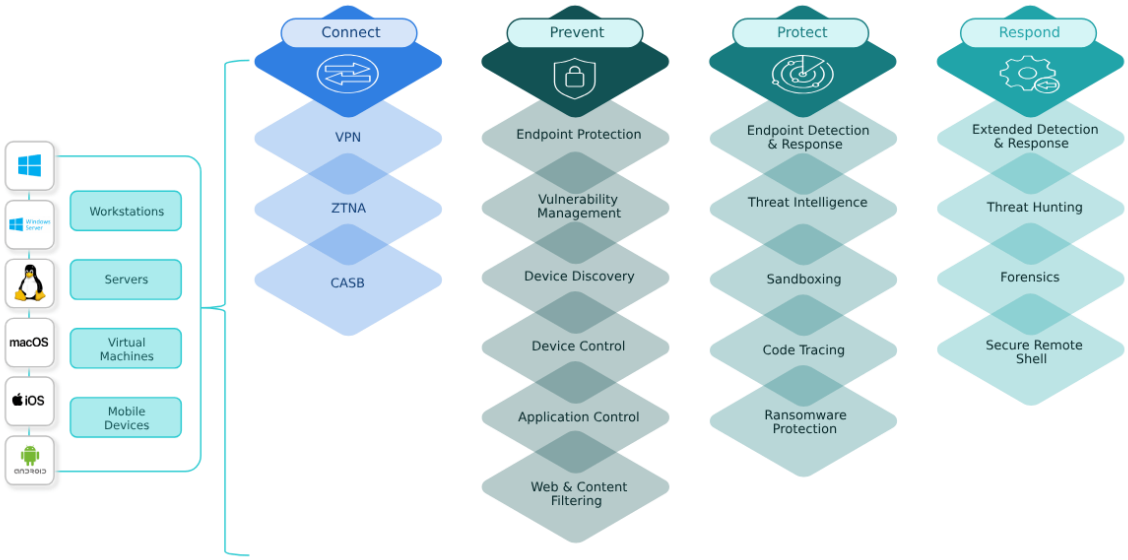


Рис. 2.2. Відповідність FortiClient до фреймворку NIST

Використання FortiClient для віддалених користувачів інформаційної системи організації відповідає фреймворку NIST з точки зору захисту, запобіганню загрозам, та наданню відповіді у разі виявлення загроз або проведення розслідувань інцидентів для віддалених користувачів. Розглянемо Функції FortiClient для організації віддаленого доступу.

FortiClient має кілька рівнів можливостей із підвищенням рівня захисту. Він інтегрується з багатьма ключовими компонентами Fortinet Security Fabric і централізовано керується сервером керування кінцевими точками (EMS) [7].

До основних функцій FortiClient відносяться модулі:

– ZTNA Edition;
– EPP/APT Edition;
– FortiClient EMS;
– FortiClient лише для VPN.

2.2. Функції модуля ZTNA Edition FortiClient для організації віддаленого доступу

Основні функці їмодуля ZTNA Edition надавати доступ до додатків із нульовою довірою, перевіряти місцезнаходження кінцевої точки в реальному часі, надавати покращений VPN із постійною оцінкою, застосовує агента уразливості та усунення загроз, проводить фільтрацію FortiGuard Web & Video Filtering, має вбудований CASB на основі API та централізоване управління через EMS і звітність доступності.

ZTNA забезпечує безпечний доступ до програм, розміщених де завгодно, незалежно від того, чи працюють користувачі віддалено чи в офісі [8].

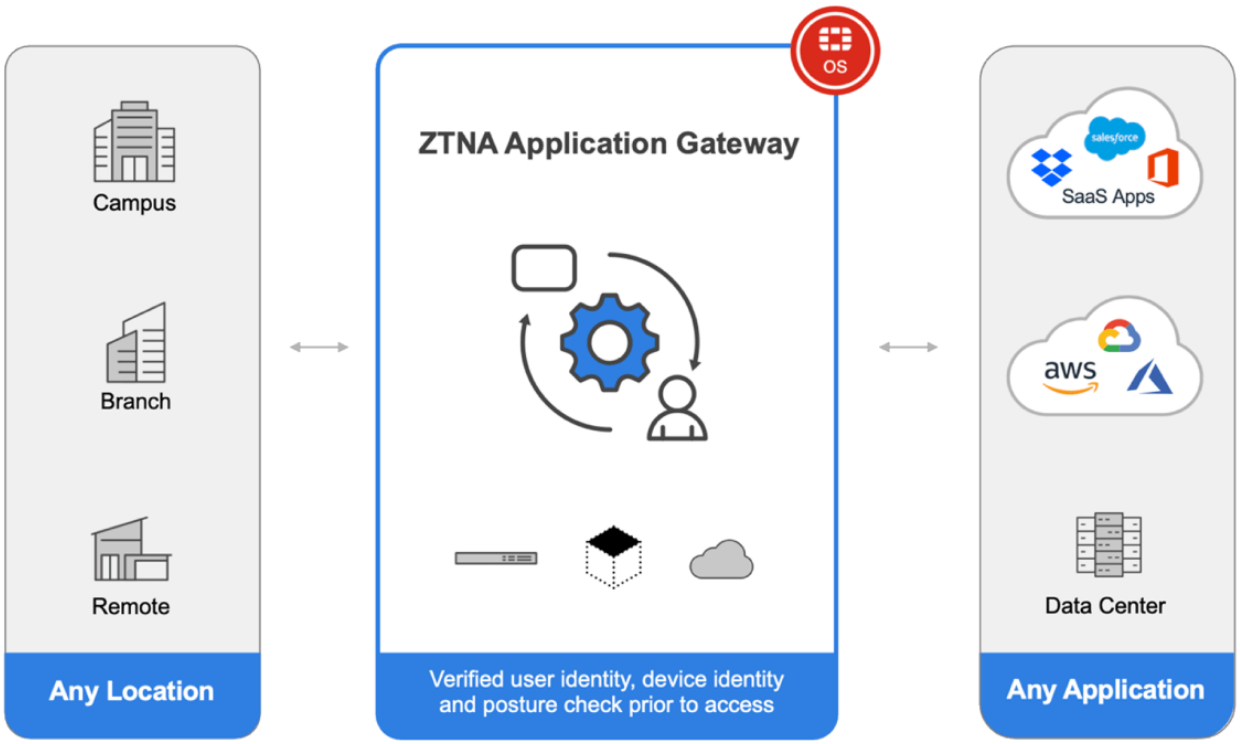


Рис.2.3 Доступ до програм згідно функції ZTNA Edition

Функція Zero Trust полягає в тому, щоб довіряти користувачам і пристроям лише після їх перевірки. Fortinet ZTNA захищає доступ до програми незалежно від того, де знаходяться користувачі. ZTNA, за галузевими стандартами, є продуктом або послугою, яка захищає програми, дозволяючи доступ до програми лише

довіреним суб'єктам. Довіра визначається брокером довіри, який постійно перевіряє особистість і контекст суб'єкта, що підключається, виконуючи при цьому контроль доступу на основі цих факторів [8,9].

В архітектурі інформаційної системи організації відповідно до ZTNA Edition архітектура організації буде виглядати як це показано на рис.2.4.

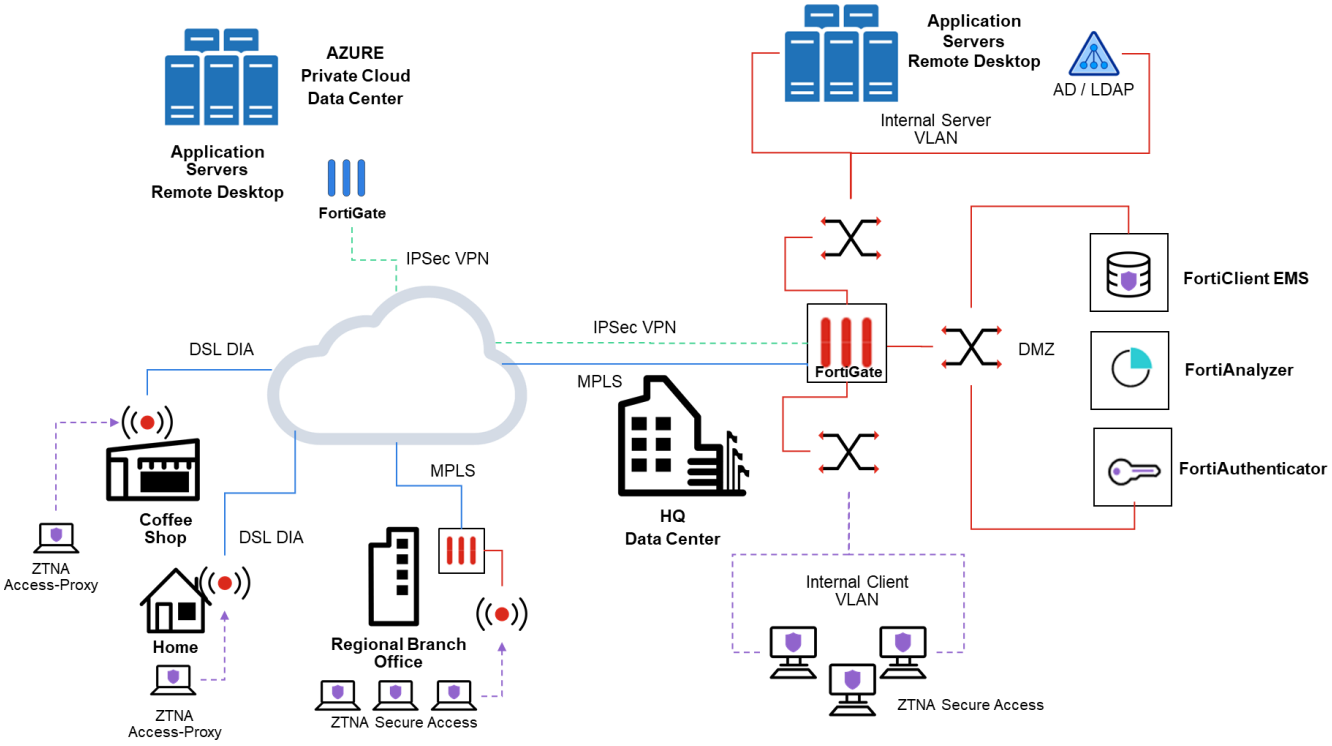


Рис.2.4. Архітектура організації відповідно до ZTNA Edition [9]

Показана архітектура на рис.2.4. показує, що довіреними особами є корпоративні користувачі та пристрої, які мають доступ із дому, кав'ярні, регіональних офісів і всередині корпоративної штаб-квартири (штаб-квартири). Їм потрібен доступ до серверів додатків у внутрішній серверній VLAN центрального офісу та до серверів додатків у хмарі. Вони можуть отримувати доступ до серверів програм за допомогою віддаленого робочого столу (RDP), SSH, HTTPS, SMB або іншими засобами.

Традиційно віддалені користувачі матимуть доступ через VPN до кожної із захищених мереж, для чого потрібно встановити різні віддалені тунелі. Внутрішні клієнти можуть випадково отримати більше доступу, ніж потрібно, наприклад, доступ до мережі DMZ.

ZTNA припускає, що жодні користувачі чи пристрої не є довіреними, доки довірчий брокер не підтвердить, що пристрій і користувач є ким вони є, а їхня безпека відповідає політиці організації. Це значно зменшує несанкціонований доступ із невідомого пристрою з викраденими обліковими даними та ймовірність того, що скомпрометований хост отримає доступ до захищених ресурсів. Контроль доступу на основі ролей зменшує бічні рухи та підтримує аналогічний контроль доступу на основі рівнів доступу незалежно від місця розташування.

2.3. Функції модуля EPP/APT FortiClient для організації віддаленого доступу

Функції модуля EPP/APT надає антивірус та захист від зловмисного програмного забезпечення на основі штучного інтелекту. Крім цієї функції для захисту віддалених користувачів можуть застосовувати додаткові функції захисту від програм-вимагачів і загроз, брандмауер програм (IPS), інтеграція з пісочницею, проводити інвентаризацію програмного забезпечення кінцевої точки та проведення аналітики кінцевої точку будь-якого користувача інформаційної системи організації.

Модуль «Захист від зловмисного програмного забезпечення» містить такі функції:

- Антивірус
- Хмарний захист від шкідливих програм
- AntiExploit
- Доступ до знімного носія
- Антивимагач
- Файли на карантині

FortiClient містить антивірусний (AV) компонент для сканування системних файлів, виконуваних файлів, знімних носіїв, файлів бібліотеки динамічного компонування (DLL) і драйверів. FortiClient також сканує та видаляє руткіти. У FortiClient частинами AV-компонента є файлове шкідливе програмне забезпечення,

шкідливі веб-сайти, захист від фішингу та спаму. AV-компонент FortiClient підтримує дванадцять рівнів вкладених стиснутих файлів для сканування. Для стиснених файлів FortiClient підтримує максимальний розмір файлу 1 Гб для антивірусного сканування. Для стисненого файлу розміром понад 1 ГБ FortiClient сканує його після розпакування.

FortiClient надає хмарний захист від шкідливих програм. Хмарна функція захисту від зловмисного програмного забезпечення допомагає захистити кінцеві точки від типів файлів із високим ризиком із зовнішніх джерел, таких як Інтернет або мережеві диски, надаючи запит FortiGuard, щоб визначити, чи є файли шкідливими. Нижче описано процес хмарного захисту від шкідливих програм.

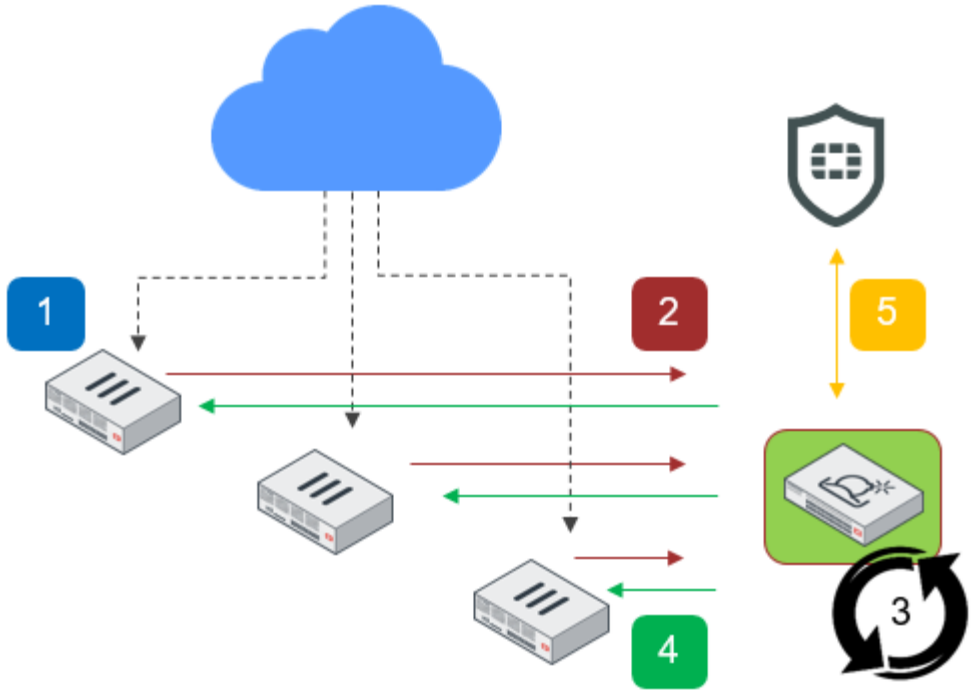
1. Файл високого ризику завантажується або виконується на кінцевій точці.
2. FortiClient генерує контрольну суму SHA1 для файлу.
3. FortiClient надсилає контрольну суму FortiGuard (FQDN з портом 8888), щоб визначити, чи є вона шкідливою для бібліотеки контрольних сум FortiGuard.
4. Якщо контрольну суму знайдено в бібліотеці, FortiGuard повідомляє FortiClient , що файл вважається шкідливим. За замовчуванням FortiClient поміщає файл у карантин.

Функція AntiExploit - функція виявлення експлойтів допомагає захистити вразливі кінцеві точки від атак невідомих експлойтів. FortiClient відстежує поведінку популярних програм, таких як веб-браузери (Internet Explorer, Chrome, Firefox) і програми Microsoft Office, проти експлойтів, які використовують уразливості нульового дня або невиправлені вразливості для зараження кінцевої точки. Після виявлення процес скомпрометованої програми припиняється. Функція виявлення експлойтів також допомагає захистити від атак на основі пам’яті та атак із завантаженням через накопичувач. Він також виявляє та блокує невідомі та відомі набори експлойтів. Це рішення без підписів. Функція виявлення експлойтів захищає програми від будь-яких дій, які можуть бути шкідливими, незалежно від того, спричиняють їх законні програми чи шкідливий код [9-10].

FortiClient підтримує інтеграцію з FortiSandbox (пісочниц), включаючи локальні пристрої FortiSandbox і FortiClient Cloud Sandbox (SaaS). Якщо налаштовано, FortiSandbox автоматично сканує файли, завантажені на кінцевій точці або зі знімних носіїв, підключених до кінцевої точки, або підключених мережевих дисків. FortiClient також автоматично сканує файли, завантажені за допомогою поштового клієнта на кінцевій точці або з Інтернету. У кожному разі, якщо файл не виявлено локально, а інтеграція FortiSandbox налаштована, FortiClient надсилає файл у FortiSandbox для подальшого аналізу. Користувачі кінцевих точок також можуть вручну надсилати файли у FortiSandbox для сканування [10].

Ви можете заблокувати доступ до файлів, доки FortiClient не поверне результат сканування FortiSandbox.

Після завершення сканування FortiClient може помістити в карантин/заборонити доступ до заражених файлів або попередити та сповістити кінцевого користувача про заражені файли, не поміщаючи файли на карантин. Якщо FortiSandbox надсилає FortiClient вердикт про те, що файл шкідливий, FortiClient також надсилає результати до EMS.



2.5. Процес сканування файлів FortiSandbox

Оскільки FortiSandbox отримує файли для сканування з різних джерел, він збирає та генерує AV-підписи для таких зразків. FortiClient періодично завантажує найновіші AV-підписи з FortiSandbox і застосовує їх локально до всіх AV-сканувань у реальному часі та на вимогу [10].

FortiClient може надсилати щодня максимум 300 файлів у FortiClient Cloud Sandbox (SaaS). Якщо кілька файлів надіслано приблизно в один і той же час, FortiClient надсилає один файл у FortiClient Cloud Sandbox (SaaS), чекає, доки не отримає вердикт щодо цього файлу, а потім надсилає наступний файл у FortiClient Cloud Sandbox (SaaS).

Максимальний розмір файлу для надсилання у FortiSandbox становить 200 МБ.

2.4. Функції модуля FortiClient EMS для організації віддаленого доступу

Функції модуля FortiClient EMS забезпечують інфраструктуру для встановлення та керування програмним забезпеченням FortiClient на кінцевих точках. FortiClient захищає кінцеві точки від вірусів, загроз і ризиків [11].

FortiClient EMS також надає інфраструктуру для встановлення та керування розширенням FortiClient Web Filter на кінцевих точках Google Chromebook. FortiClient захищає користувачів кінцевих точок, працюючи з FortiClient EMS для фільтрації веб-вмісту, який переглядають користувачі кінцевих точок на комп’ютерах Google Chromebook.

Основні компоненти FortiClient EMS та їх функції показано у таблиці 2.1.

Таблиця 2.1.

Компоненти FortiClient EMS

FortiClient EMS	Керує FortiClient на кінцевих точках, які підключаються до мережі організації. Керує розширенням FortiClient Web Filter, встановленим на кінцевих точках Google Chromebook, підключених до вашого домену Google. Включає таке програмне забезпечення:

	Консольне програмне забезпечення, яке керує профілями безпеки, FortiClient на кінцевих точках і кінцевих точках Chromebook Серверне програмне забезпечення, яке забезпечує безпечний зв'язок між кінцевими точками та консоллю, а також між кінцевими точками Chromebook і консоллю адміністратора Google.
База даних	Зберігає профілі та події безпеки. Також зберігає інформацію користувача, отриману з консолі адміністратора Google для Chromebook. База даних SQL інсталюється як частина інсталяції FortiClient EMS.
FortiClient	Допомагає забезпечити безпеку та захист кінцевих точок. Він працює на серверах, настільних комп'ютерах і портативних комп'ютерах, які ви хочете захистити. Додаткову інформацію див . у посібнику з адміністрування FortiClient .
Розширення FortiClient Web Filter	Зв'язується з FortiClient EMS і забезпечує веб-фільтрування кінцевих точок Google Chromebook.

На рис.2.6. непунктирними лініями показано, як підключаються різні компоненти для керування кінцевими точками Windows, macOS і Linux за допомогою FortiClient EMS. Пунктирні лінії показують, як компоненти використовуються для керування кінцевими точками Chromebook за допомогою FortiClient EMS.

FortiClient EMS дозволяє [11] :

Створювати і запровадьжувати профілі безпеки.

Керувати розгортанням, налаштуванням і оновленнями.

Керувати профілями безпеки з інтегрованої консолі керування.

Отримувати зведене уявлення про численні компоненти безпеки для всіх кінцевих точок у мережі та домені Google.

Виконувати комплексне встановлення компонентів безпеки та налаштовувати профілі.

Відстежувати веб-перегляд активності кінцевих точок.

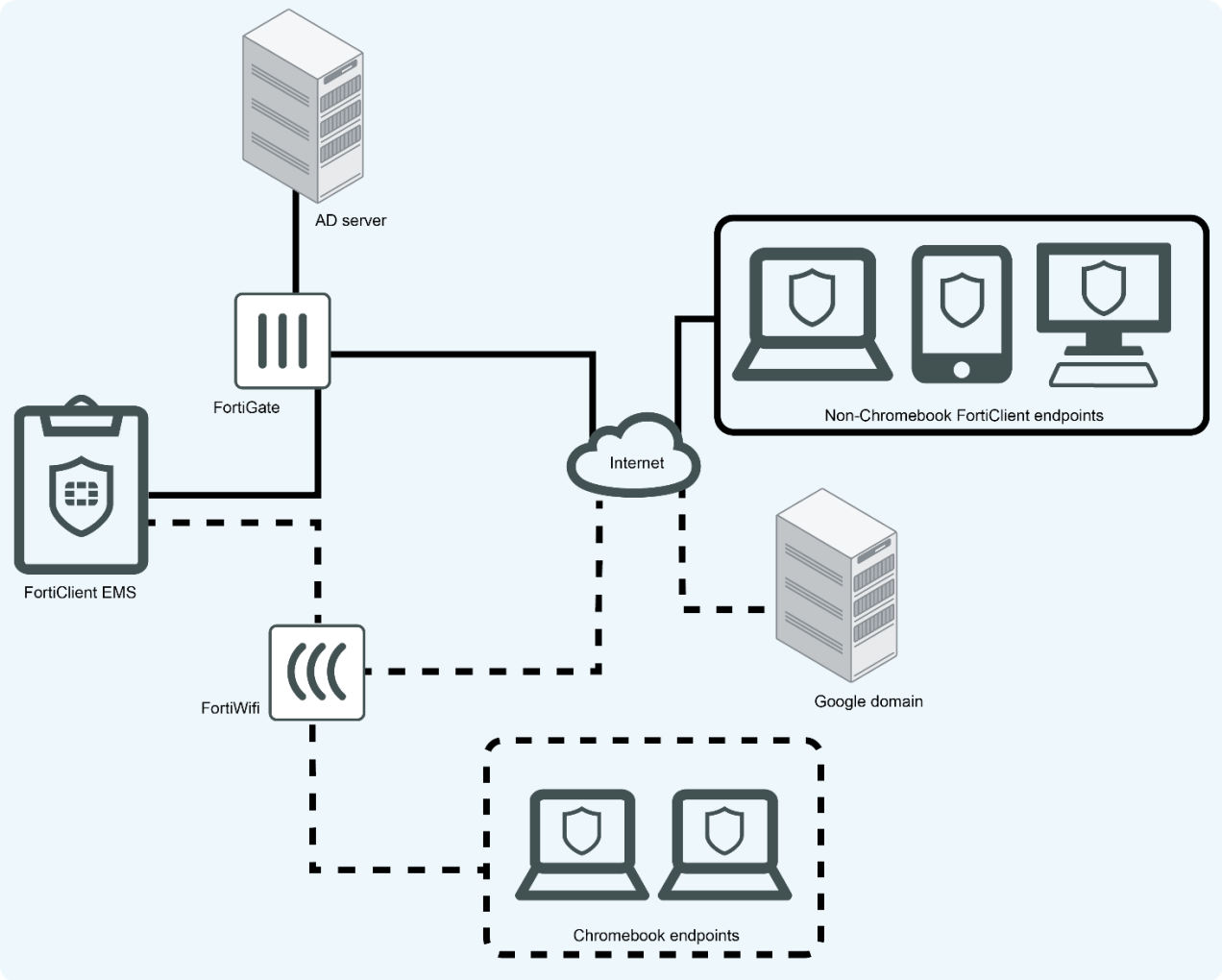


Рис.2.6. Підключення компонентів FortiClient EMS

2.5. Функції модуля FortiClient VPN-only для організації віддаленого доступу

Функції модуля FortiClient VPN-only дозволяють підключати віддалених користувачів до інформаційної системи організації. Для різних користувачів порпонуються відповідні завантаження FortiClient VPN-only, які залежать від типу операціної системи яку вони використовують.

Рис. 2.7. Типи завантажень FortiClient VPN-only

FortiClient VPN-only посилює безпеку VPN з використанням ZTNA. І нтеграція тегів ZTNA FortiGate в інфраструктуру VPN пропонує потужне рішення для підвищення безпеки VPN. Теги ZTNA — це функція, яка пропонується виключно з ліцензованими версіями FortiClient (FortiClient EMS). Теги ZTNA — це об’єкти, які призначаються кінцевим точкам FortiClient у режимі реального часу. Теги ZTNA використовуються в політиках брандмауера на FortiGate, щоб дозволити або заборонити доступ до VPN і мережевих ресурсів відповідно до правил безпеки організації. Ці правила відповідності застосовуються в режимі реального часу, тим самим захищаючи організацію від загроз безпеці, що постійно змінюються.

У наведеній таблиці 2.2 порівнюються функції безкоштовного окремого FortiClient лише для VPN та ліцензованого FortiClient, яким керує EMS, на відповідність вимогам безпеки.

Таблиця 2.2.

Порівняння функцій безкоштовного FortiClient VPN-only

Особливість	Безкоштовний автономний FortiClient лише для VPN	Ліцензований FortiClient
Базове підключення VPN	так	так
Керовані профілі віддаленого доступу	немає	так
Відповідність за допомогою тегів ZTNA: Дозволяти або блокувати з'єднання VPN на основі стану безпеки ZTNA Перевірки стану безпеки політики брандмауера за допомогою тегів ZTNA	немає	так

Для налаштування підключення FortiClient VPN-only необхідно налаштувати VPN з'єднання на Forti Gate як SSL VPN.

Конфігурація SSL VPN складається з таких частин:

– Портал SSL VPN

– Область SSL VPN

– Налаштування SSL VPN

– Політика брандмауера

Щоб налаштувати портал SSL VPN необхідно використовувати стандартний профіль повного доступу або доступу до тунелю. Необхідно переконатися, що в режимі тунелю розділене тунелювання налаштовано та ввімкнено на основі призначення політики. За потреби можна налаштувати додаткові параметри.

Щоб налаштувати область SSL VPN необхідно зробити наступні кроки:

1. Перейдіть до Система > Видимість функцій.
2. Увімкнути області SSL-VPN .
3. Натисніть Застосувати .
4. У розділі VPN > Сфери SSL-VPN натисніть Створити новий .
5. Введіть URL-шлях pki-ldap-machine.
6. Натисніть OK , щоб зберегти.

Щоб налаштувати параметри SSL VPN:

1. Перейдіть до Система > Налаштування SSL-VPN.
2. Введіть такі значення, як показано в таблиці 2.3.
3. У розділі «Автентифікація/Зіставлення порталу» натисніть «Створити новий» , щоб створити нове зіставлення.
4. Встановіть для користувачів/груп значення PKI-Machine-Group.
5. Встановіть для Realm значення Specify .
6. Виберіть область /pki-ldap-machine.
7. Налаштуйте повний доступ до порталу.
8. Натисніть OK , щоб зберегти.
9. Відредагуйте запис Усі інші користувачі/групи :
    a. Встановіть для порталу заборонений доступ.
    b. Натисніть OK , щоб зберегти.

Таблиця 2.3.

Значення для налаштування параметрів SSL VPN

Поле	Значення
Увімкніть SSL-VPN	Увімкнути
Слухати через інтерфейс(и)	порт3
Слухайте на Порті	10443
Сертифікат сервера	ztna-підстановка. Центр сертифікації Windows видає цей сертифікат сервера з підстановкою.
DNS-сервер	Вкажіть
DNS-сервер №1	10.88.0.1

Щоб налаштувати політику брандмауера:

У розділі «Політика та об’єкти» > «Політика брандмауера» натисніть «Створити нову» , щоб створити нову політику.

Введіть значення з таблиці 2.3.

Таблиця 2.4.

Значення налаштування політик брандмауера

Поле	**Значення**
Ім'я	VPN-машина
Вхідний інтерфейс	Інтерфейс тунелю SSL-VPN (ssl.root)
Вихідний інтерфейс	порт2
Джерело	все, PKI-Machine-Group
Пункт призначення	Створіть об’єкт адреси для веб-сервера 10.88.0.3/32 і будь-яких інших серверів, до яких необхідно отримати доступ.
розклад	завжди
Сервіс	ВСЕ
Дія	ПРИЙНЯТИ
Журнал дозволу трафіку	Увімкнено, усі сеанси

За потреби можна налаштувати будь-які інші параметри профілів безпеки.

Після налаштування VPN на брендмауері, віддалений клієнт має бути зареєстрований і керований EMS, щоб отримати профіль віддаленого доступу VPN для підключення до VPN. Тому політика брандмауера повинна дозволяти доступ до сервера EMS.

Тому налаштувати профіль віддаленого доступу в EMS, щоб дозволити попередній вхід у VPN.

Можна застосуати два варіанта такого підключення.

У першому прикладі створюється тунель із конфігураціями для ввімкнення попереднього входу у VPN із сертифікатом машини. Користувачі можуть вибрати FortiClient VPN на сторінці входу в Windows.

У другому приклад робить ще один крок вперед і дозволяє Windows автоматично підключатися до тунелю під час запуску.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО СТВОРЕННЯ ЗАХИЩЕННОГО З'ЄДНАННЯ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1. Варіант налаштування SSL-VPN з використанням програмного забезпечення FortiClient і автентифікації Active Directory

FortiGate Remote Access (SSL – VPN) – це рішення, яке набагато легше налаштувати, ніж на інших конкурентах міжмережевих екранів. Розглянемо як налаштувати віддалений доступ до брандмауера FortiGate за допомогою програмного забезпечення FortiClient і автентифікації Active Directory. На рис.3.1. показано топологію мережі до якої буде робитись підключення.

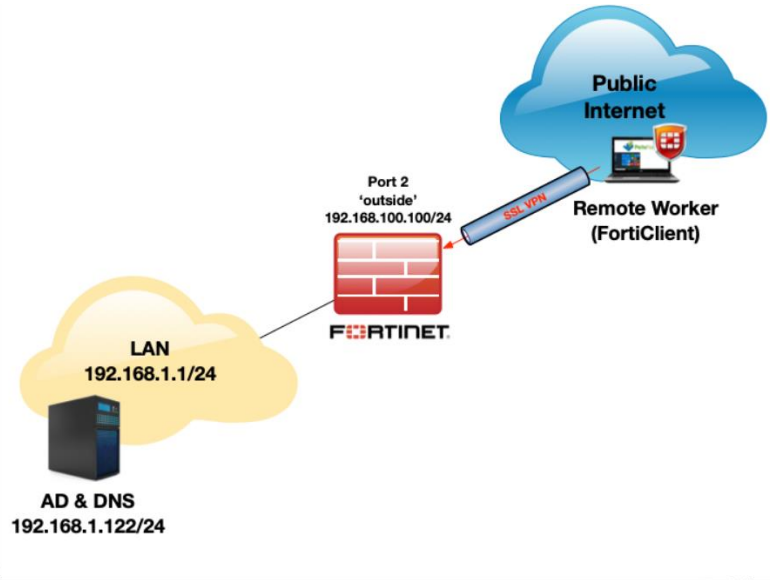


Рис.3.1. Топологія підключення

Для підключення використано самопідписаний сертифікат на FortiGate, у робочому середовищі можна придбати публічно підписаний.

Основні кроки створення з'днання на FortiGate наступні.

Крок 1: Передумови FortiGate LDAPS

Перш ніж почати, нам потрібно переконатися, що нш брандмауер може розпізнавати внутрішній DNS. (Оскільки ім'я сертифіката Kerberos на контролері домену перевіряється під час виконання запитів LDAPS, якщо ви не хочете цього робити, вимкніть перевірку ідентифікації сервера під час налаштування сервера

LDAP нижче). Або ви можете додати IP- адресу до сертифіката Kerberos серверів як « Альтернативне ім’я суб’єкта ».

Мережа > DNS > Вказати > Додати у ваші внутрішні DNS-сервери > Застосувати.

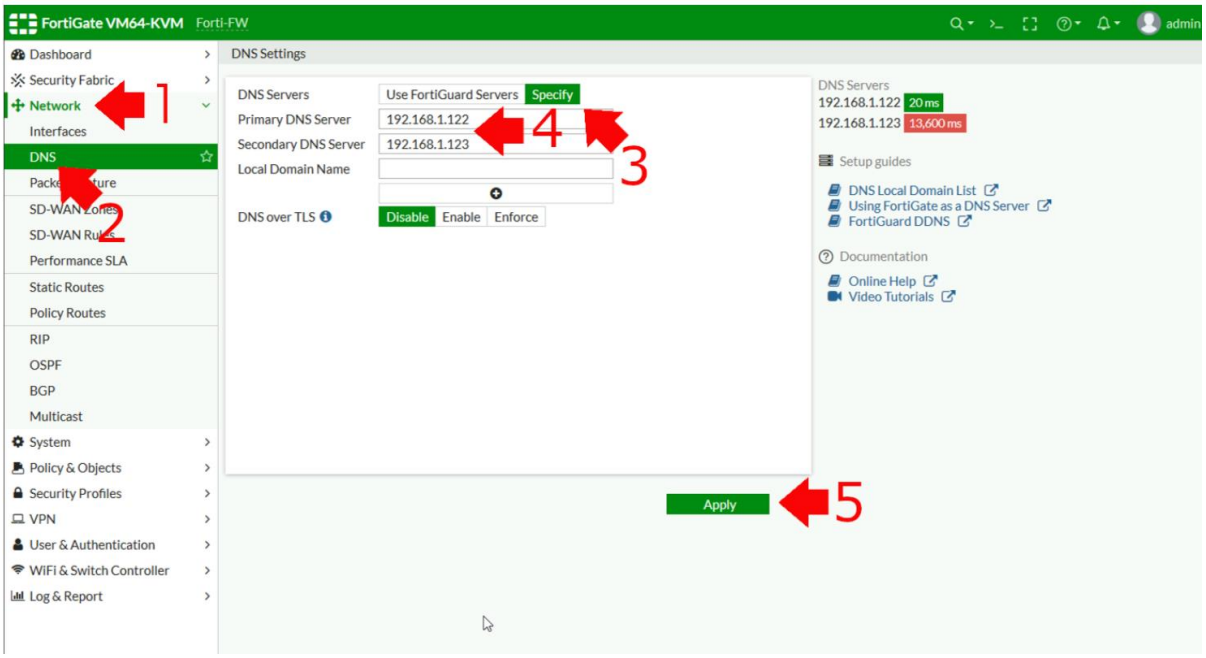


Рис.3.2. Передумови FortiGate LDAPS

Для виконання LDAPS FortiGate має довіряти сертифікатам, які використовує наш контролер домену. Щоб увімкнути це, потрібна копія сертифіката ЦС для ЦС, який їх видав.

Підготуйтеся до прив’язки каналу LDAPS

Щоб «Імпортувати» сертифікат у Fortigate > Система > Сертифікати > Імпорт > Сертифікат ЦС (рис.3.3).

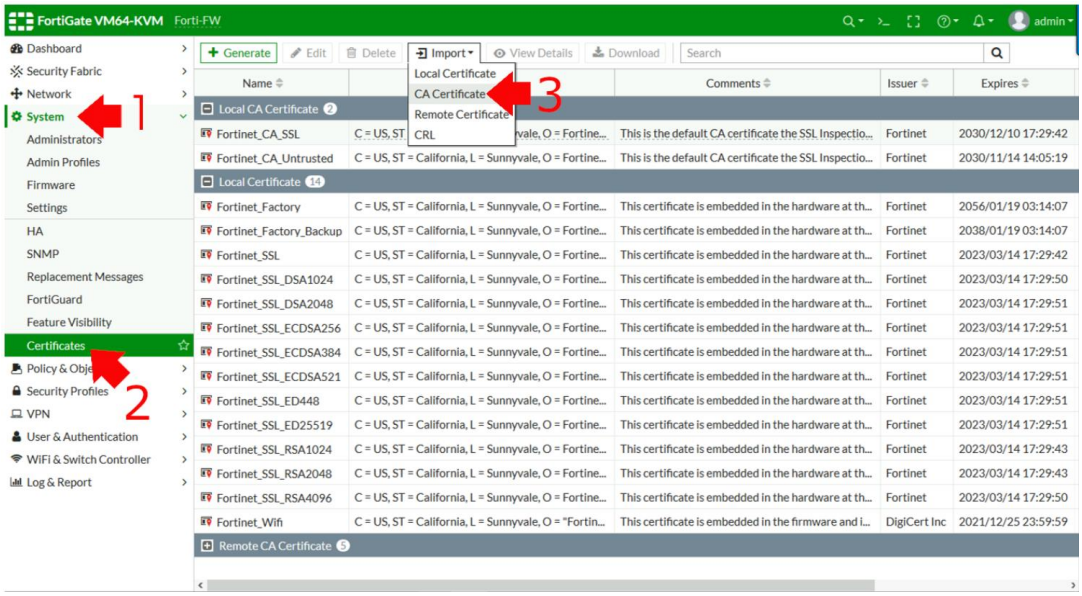


Рис.3.3. Імпорт сертифіката

Файл > Завантажити > Перейдіть до свого сертифіката ЦС > Відкрити > ОК(Рисю3.4).

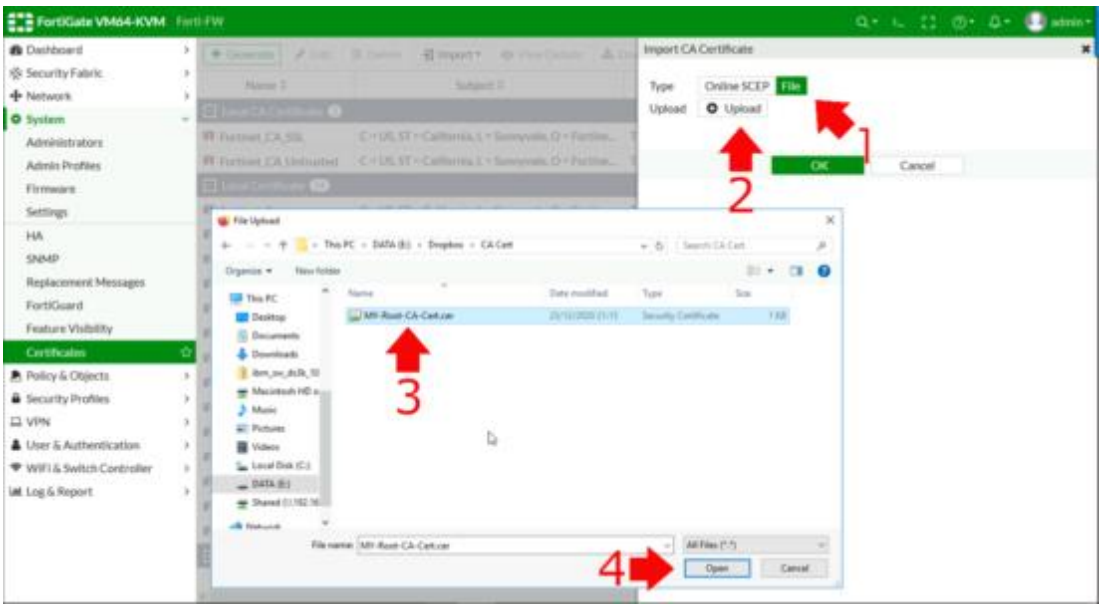


Рис.3.4. Завантаження сертифікату

Крок 2: Дозволити автентифікацію FortiGate LDAPS (Active Directory)

Користувач і автентифікація > Сервери LDAP > Додати (рис.3.5)

Ім'я: My-DC

IP-адреса/ім'я сервера: використовуйте FQDN сервера (або потрібно вказати IP-адресу в сертифікаті Kerberos як SAN !)

ServerPort: 636 (Ми не використовуємо 389 LDAP НЕ безпечний!)

Загальний ідентифікатор імені: sAMAccountName

Доменне ім'я: введіть DN верхнього рівня вашого домену або організаційного підрозділу , до якого входять усі ваші користувачі/групи.

Тип перев'язки: звичайний.

Ім'я користувача: у форматі ДОМЕН\ім'я користувача. Примітка. Досить мати звичайний обліковий запис користувача домену, для цього НЕ ОБОВ'ЯЗКОВО бути адміністратором домену.

Пароль: для вказаного вище користувача.

Безпечне підключення: LDAPS.

Сертифікат: виберіть ВАШ сертифікат ЦС .

Перевірка ідентифікації сервера: увімкнено..

Клацніть «*Перевірити підключення*». Має бути написано успішно, тоді ви можете перевірити облікові дані іншого користувача домену як тест > OK.

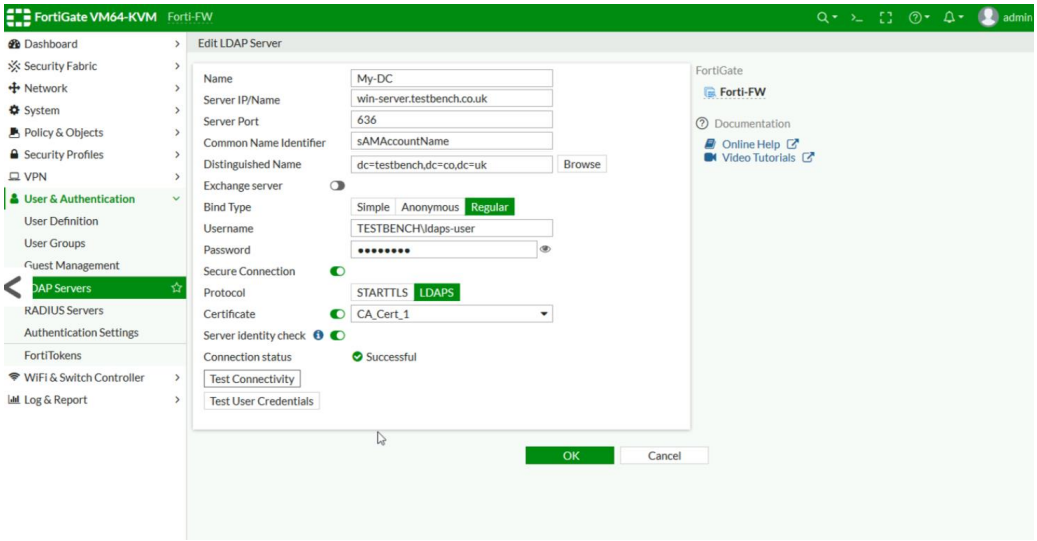


Рис. 3.5 Налаштування LDAP

Далі необхідно перейти до налаштуваннядомену / Active Directory. У своєму Active Directory створити групу безпеки під назвою GS-VPN-Users і помістити туди свій об'єкт користувача.

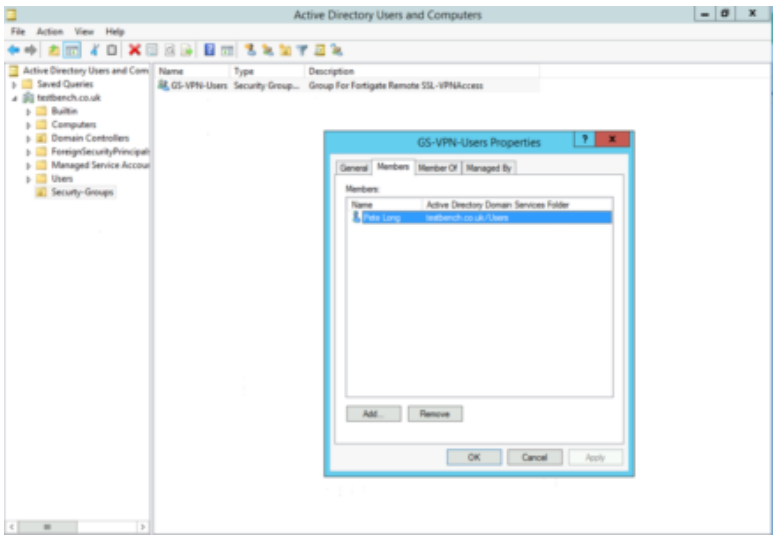


Рис.3.6. Створення користувача в домені AD

Тепер потрібно створити ГРУПУ БРАНДМАУЕРА та додати до неї свою ГРУПУ ACTIVE DIRECTORY (Рис.3.7). Користувач і автентифікація > Групи користувачів > Створити нову. Потім треба їй дати назву та тип брендмауера. (рисю3.7).

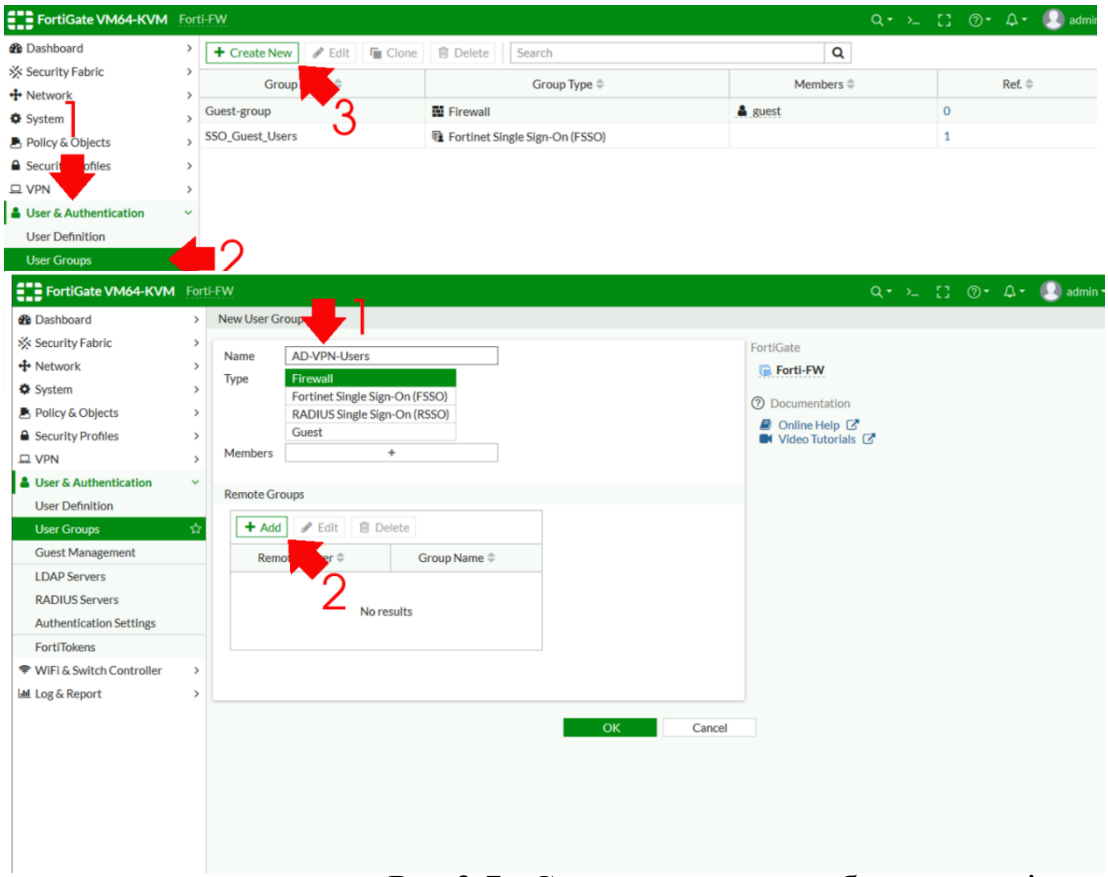


Рис.3.7. Створення групи у брендмауері

Змініть розкривний список «Віддалений сервер» на ваш сервер LDAPS > перейдіть до групи ACTIVE DIRECTORY GROUP , клацніть правою кнопкою миші та виберіть «Додати вибране» (На здоров'я, мені знадобилося три рази, щоб знайти FortiNet!) > OK.

Якщо все добре, ви маєте побачити свій сервер LDAPS ТА розпізнавальну назву вашої групи *AD* (перевірте, чи не пропущено!) > OK (3.8).

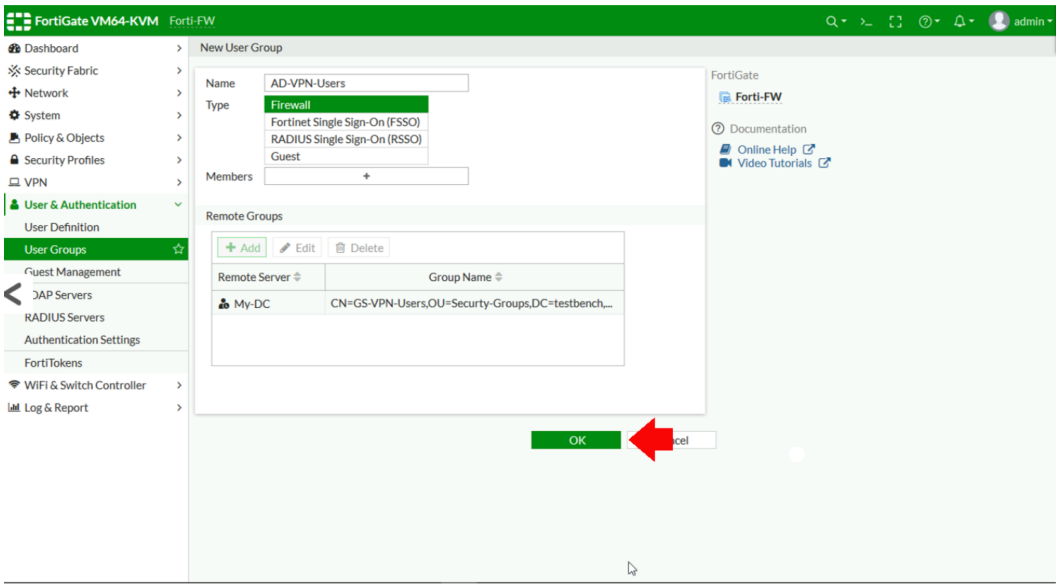


Рис.3.8. Завершення налаштування групи

Крок 3: Налаштувння FortiGate SSL-VPN

Спочатку нам потрібен портал SSL > VPN > Портали SSL-VPN > Створити новий (рис.3.9).

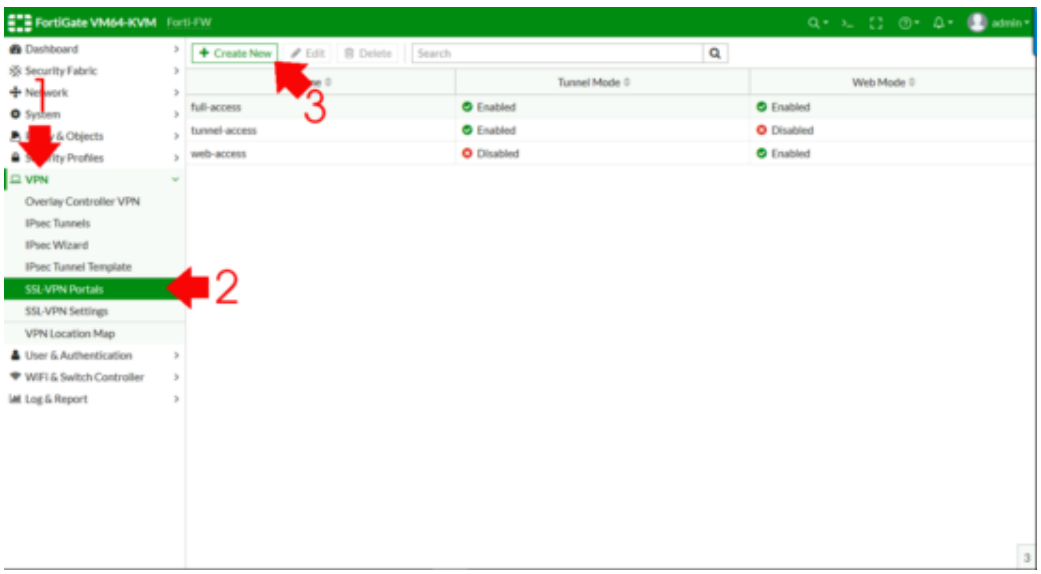


Рис. 3.9. Налаштування портал SSL -VPN

Назва : SSL-VPN_REMOT-ACCESS

Увімкнути розділене тунелювання: увімкнено. (Якщо цього не зробити, віддалені клієнти повинні зайти через FortiGate для веб-доступу), як це показано на рис.3.10.

Пули вихідних IP-адрес: додайте, потім створіть.

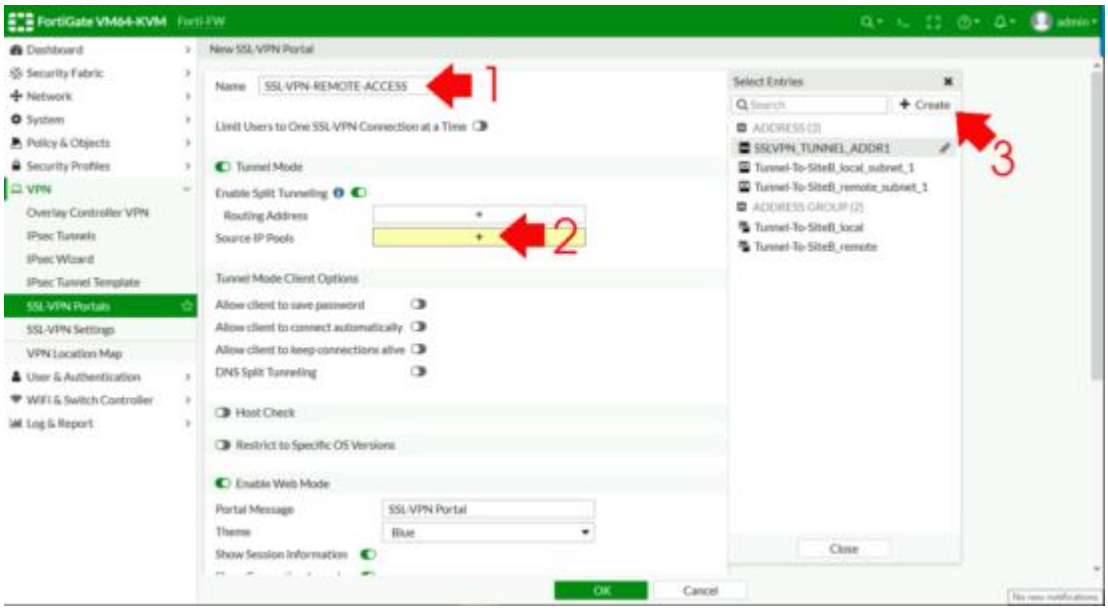


Рис.3.10 Налаштування SSL-VPN Portal

Для створення пулу адрес необхідно додати наступну інформацію:

Назва : REMOTE-VPN_POOL

Тип: Діапазон IP

Діапазон IP: підмережа, яку ви бажаєте використовувати. (Примітка : якщо ви використовуєте маршрутизацію у своїй локальній мережі , переконайтеся, що є маршрут назад до FortiGate для цієї підмережі, інакше трапляться погані речі!)

Інтерфейс: тунельний інтерфейс SSL-VPN

Переходимо до налаштування FortiGate SSL-VPN (Рис.3.11)

Це робиться наступним чином:

1. VPN > Налаштування SSL-VPN > Прослуховування на інтерфейсах.

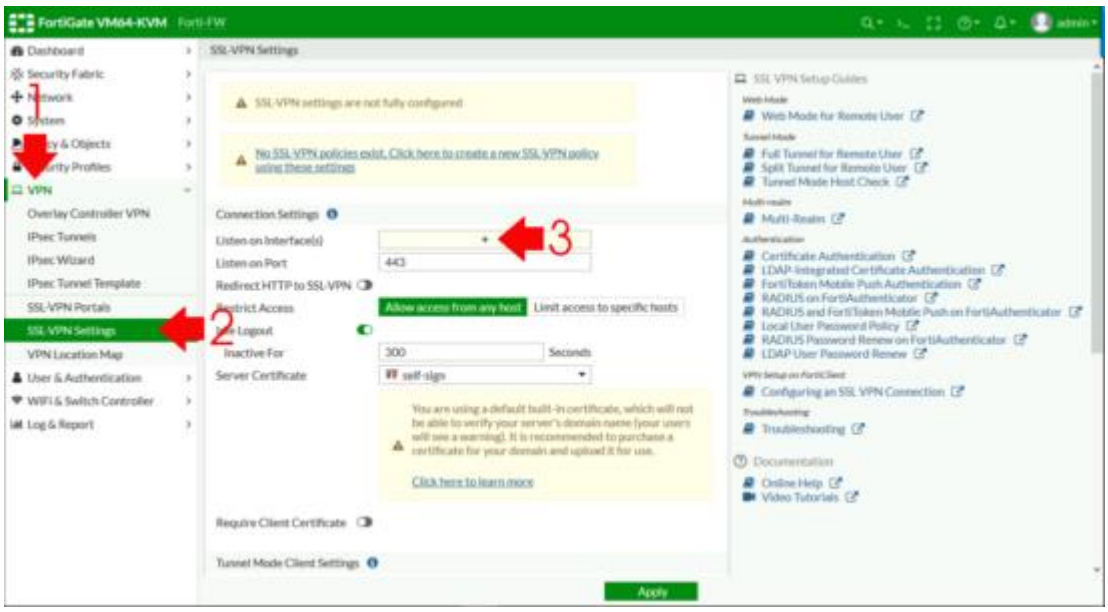


Рис. 3.11 Налаштування FortiGate SSL-VPN

2. Встановіть зовнішній (WAN) інтерфейс > Діапазон адрес > Укажіть користувацькі діапазони IP > Діапазони IP > Додайте в створений вище пул.

3. DNS-сервер > Указати > Додати внутрішні DNS-сервери > Відображення порталу автентифікації > Створити новий.

4. Користувачі/групи: Ваша ГРУПА ОГОЛОШЕНЬ.

5. Портал : Ваш портал

6. Застосувати (рис.3.12)

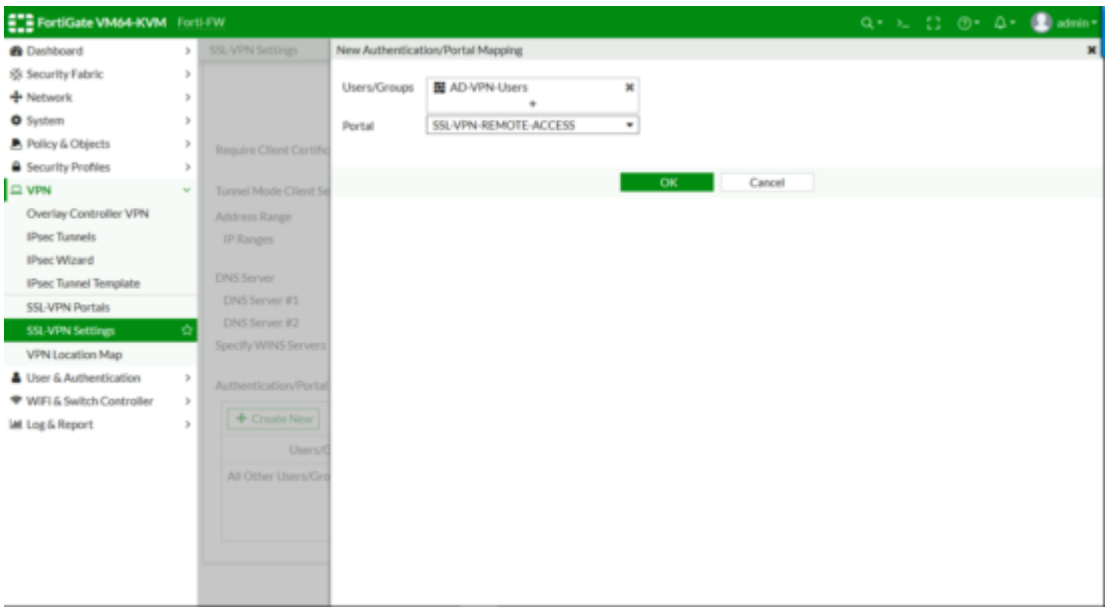
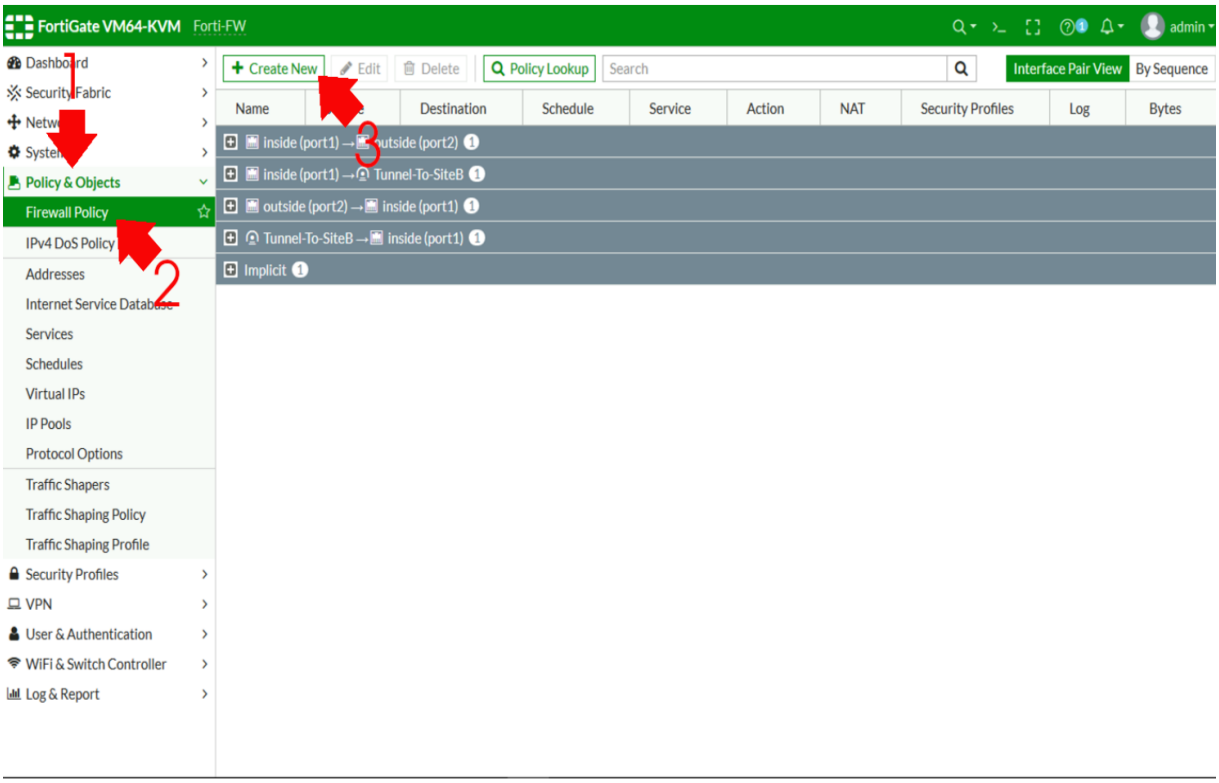


Рис. 3.12. Кінцевий етап налаштування FortiGate SSL-VPN

Терер необхідно налаштувати політику брандмауера FortiGate SSL-VPN., яка складається з наступних етапів:

Політика та об’єкти > Політика брандмауера (або політика IPV4 у старих версіях) > Створити новий (Рис.3.13).



3.123. Налаштування політик брендмауера

При створенні політики небхідно заповнити поля (Рис. 3.14):

Ім'я: REMOVE-VPN-FIREWALL-POLICE

Вхідний інтерфейс: тунельний інтерфейс SSL-VPN.

Вихідний інтерфейс: внутрішній (LAN).

Джерело: ваш віддалений IP-пул ТА ваша група FIREWALL.

Призначення: локальна локальна мережа (пам’ятайте, якщо ви хочете отримати доступ до DMZ, додайте його також)

Розклад: завжди

Дія: Прийняти

NAT: вимкнено

Генерувати журнали під час початку сеансу: увімкнено

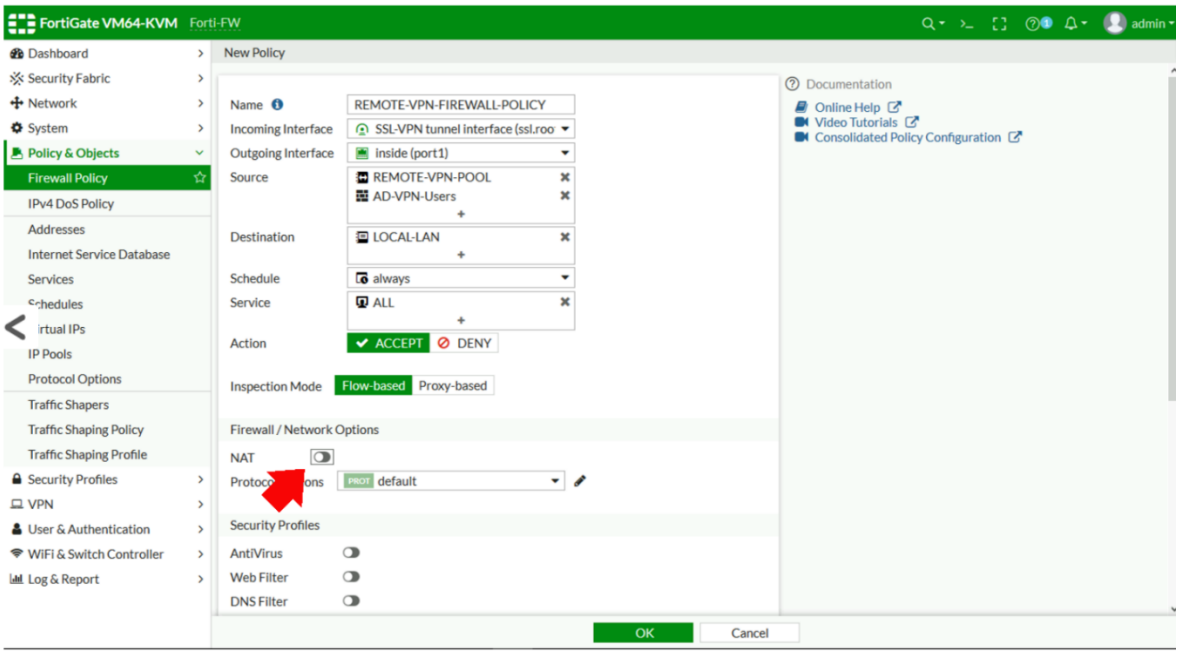


Рис.3.14. Створення нової політики

Крок 4: Перевірка FortiGate SSL-VPN

У віддаленому клієнті перейдіть до загальнодоступного IP/FQDN брандмауера та увійдіть у систему. Ви повинні побачити портал SSL-VPN, який ви створили, і мати можливість завантажити програмне забезпечення FortiClient (VPN) для вашої версії ОС.

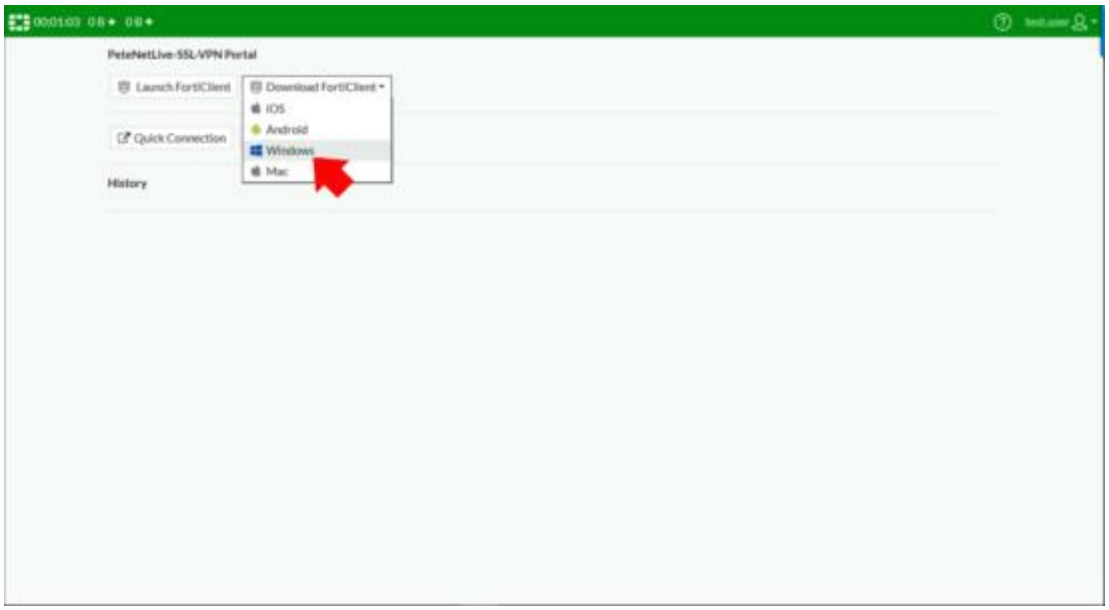


Рис.3.15. Портал SSL-VPN для завантаження FortiClient

Тепер необхідно Встановіть FortiClient (Примітка: це лише компонент VPN, а не повний FortiClient).

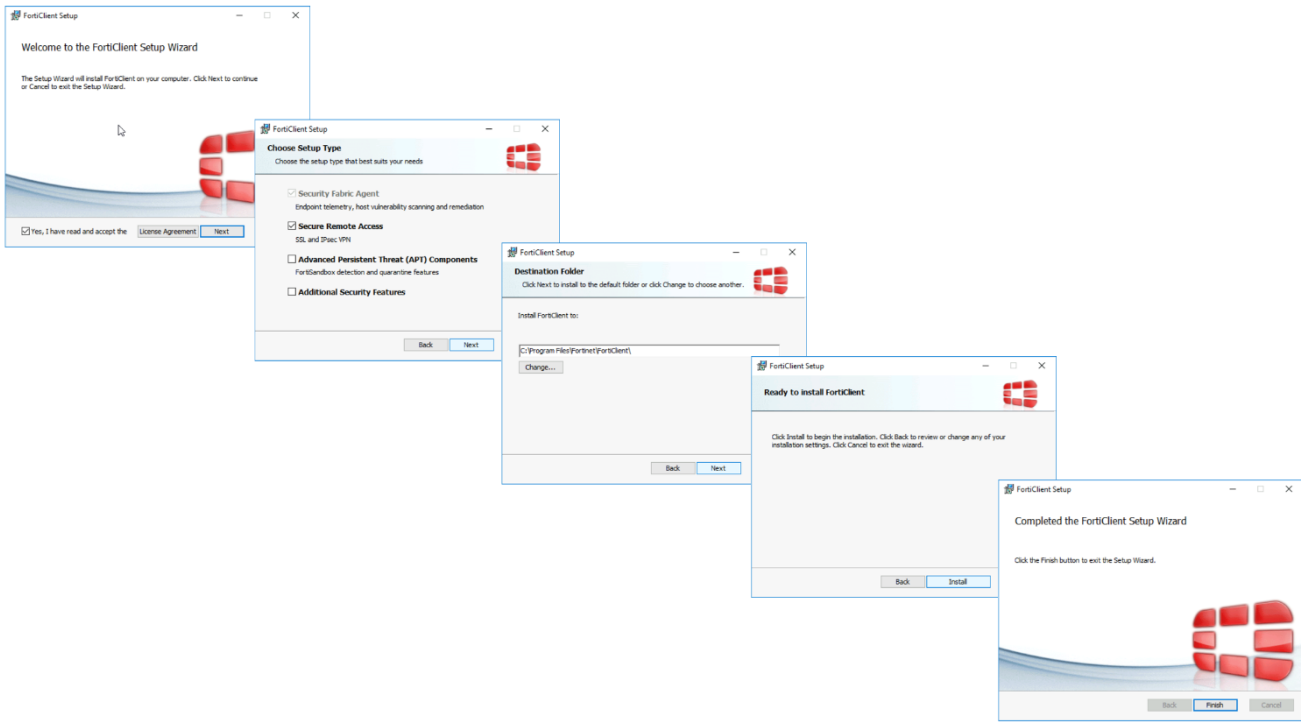


Рис.3.16. Встановлення FortiClient

Тепер необхідно перейти до налаштування FortiClient з боку користувача за такими етапами (Рис.3.17):

Віддалений доступ > Налаштувати VPN.

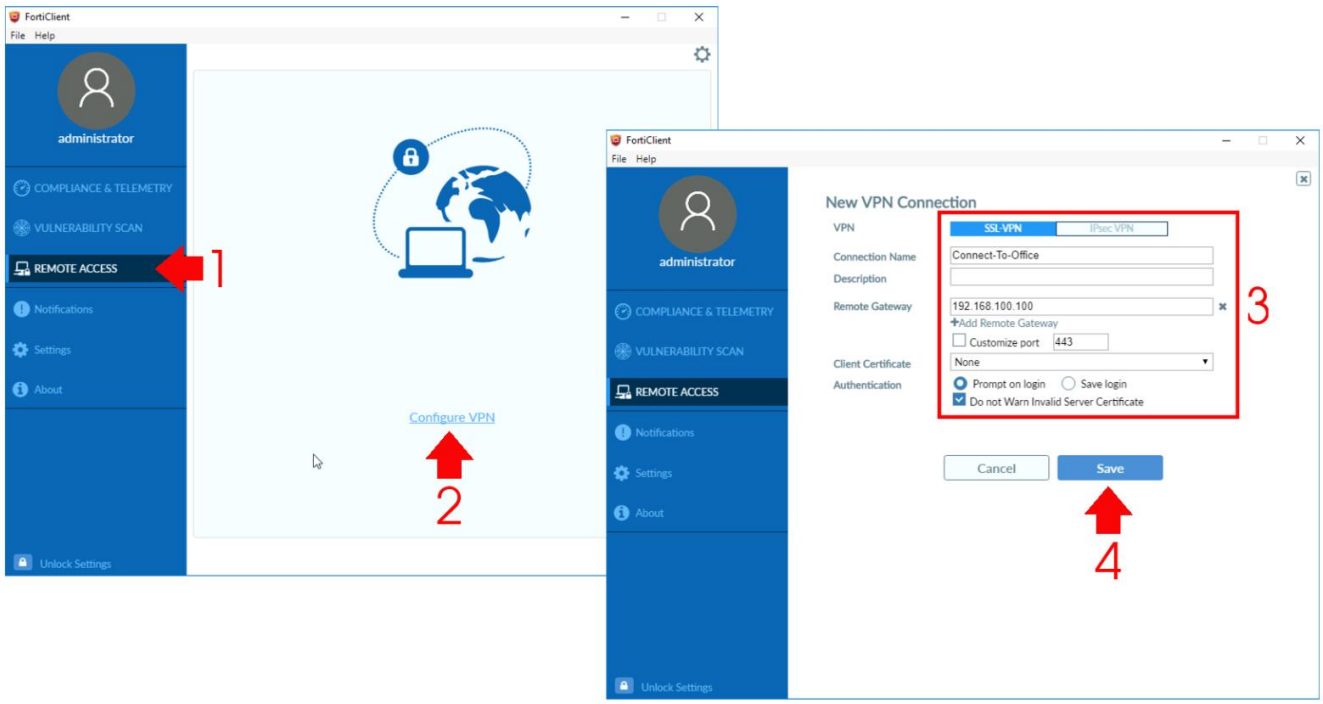


Рис.3.1.7 Налаштування FortiClient з боку користувача

Назва підключення: Connect to Office.

Віддалений шлюз: IP або FQDN FortiGate.

Автентифікація: підказка під час входу (якщо ви не хочете, щоб це запам’яталося).

Не попереджати про недійсний сертифікат сервера: увімкнено (якщо ви не використовуєте загальнодоступний сертифікат на FortiGate).

Зберегти.

Тепер необхідно перевірте з’єднання і переконатися, що можна перевірити внутрішні IP-адреси та імена DNS (Рис.318).

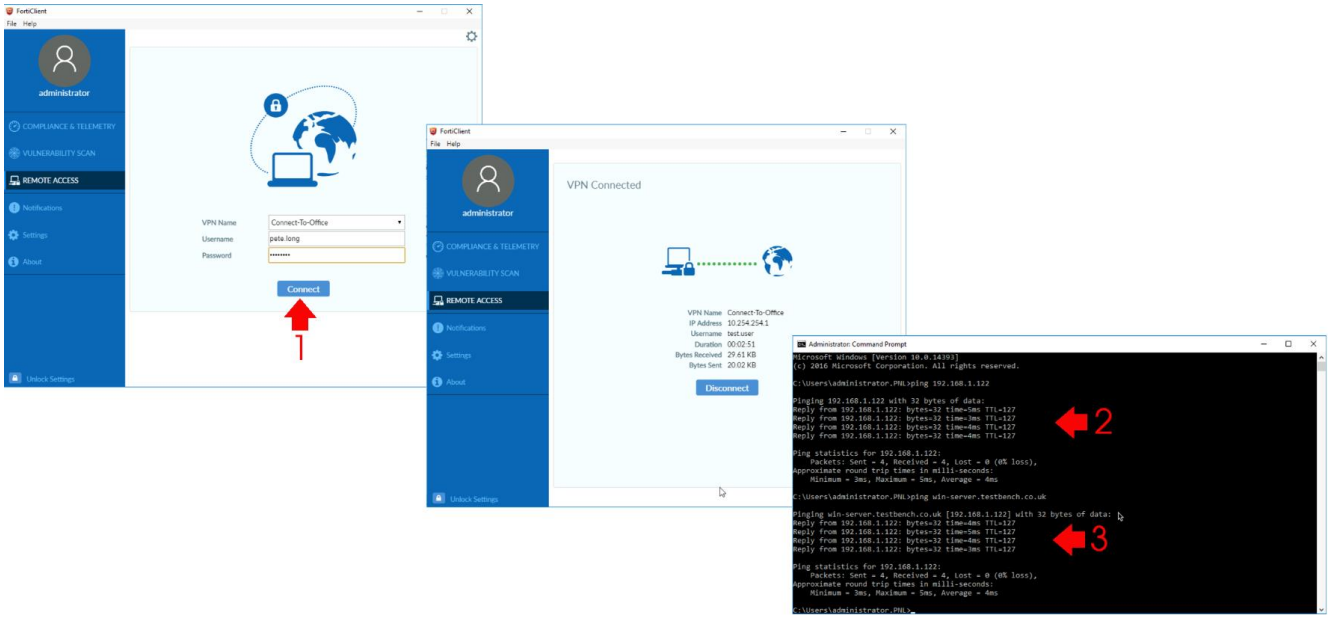


Рис. 3.18. Перевірка створеного SSL-VPN на FortiClient

Отже, в даному розділі було показано варіант налаштування SSL-VPN FortiClient для організації віддаленої роботи користувачам інформаційної системи організації. Хотілось би зауважити, що в роботі показано мінімальний набір кроків по налаштуванню SSL-VPN FortiClient.

3.2. Розробка рекомендацій щодо захисту віддалених користувачів до інформаційної системи організації

Сучасним організаціям важливо впроваджувати захисту віддалених користувачів своєї інформаційної системи. Це пов’язано з тим, що збільшується

кількість загроз, які можуть вплинути на всі бізнес-процеси організацій.

Це зумовлено кількома ключовими факторами:

1. Зростання кількості та складності кіберзагроз:

– Кіберзлочинці постійно вдосконалюють свої методи, використовуючи соціальну інженерію, шкідливе програмне забезпечення та інші техніки для проникнення в корпоративні мережі.

– Віддалені працівники, використовуючи домашні мережі та особисті пристрої, можуть стати слабкою ланкою в системі безпеки організації.

2. Розширення практики віддаленої роботи:

– Глобалізація та розвиток технологій сприяють збільшенню числа віддалених працівників.

– Це створює нові виклики для забезпечення безпеки даних, оскільки контроль над віддаленими пристроями та мережами обмежений.

3. Захист бізнес-процесів:

– Успішна кібератака може призвести до зупинки бізнес-процесів, втрати конфіденційної інформації та фінансових збитків.

– Захист віддалених користувачів є ключовим елементом забезпечення безперервності бізнесу.

Використання сучасних технологій і рішень захисту віддалених користувачів дозволить організаціям контролювати своїх віддалених користувачів та надавати їм сервіси, які забезпечать захищений доступ до інформаційної системи організації.

Це можна досягти завдяки комплексному підходу до захисту віддалених користувачів організації, який включає використання та впровадження різних заходів безпеки.

Впровадження Zero Trust архітектури. Така модель безпеки передбачає, що жоден користувач чи пристрій не може вважатися довіреним за замовчуванням, незалежно від його розташування. Кожен запит на доступ до ресурсів перевіряється та аутентифікується, що значно знижує ризик несанкціонованого доступу.

Використання хмарних рішень безпеки. Хмарні платформи надають масштабовані та гнучкі рішення для захисту віддалених користувачів, такі як CASB

(Cloud Access Security Broker), SWG (Secure Web Gateway) та ZTNA (Zero Trust Network Access). Ці інструменти забезпечують моніторинг трафіку, фільтрацію шкідливого контенту та контроль доступу до хмарних додатків.

Застосування технологій Endpoint Detection and Response (EDR). EDR системи дозволяють виявляти та реагувати на кіберзагрози на кінцевих пристроях, таких як ноутбуки та смартфони. Це забезпечує постійний моніторинг активності користувачів та виявлення аномальної поведінки.

Використання інструментів Mobile Device Management (MDM). MDM системи дозволяють організаціям керувати та захищати мобільні пристрої, які використовуються для віддаленої роботи. Це включає в себе встановлення політик безпеки, шифрування даних та віддалене видалення інформації в разі втрати або крадіжки пристрою.

Постійне навчання та підвищення обізнаності користувачів. Регулярні тренінги та інформаційні кампанії допомагають користувачам розуміти ризики кібербезпеки та дотримуватися правил безпечної роботи. Це включає в себе навчання розпізнаванню фішингових атак, використанню надійних паролів та безпечній роботі в інтернеті.

Загальні рекомендацій для організації VPN для віддалених користувачів інформаційної системи організації включають наступні кроки.

1. При налаштуванні FortiGate необхідно включити SSL-VPN. Для цього необхідно переконатися, що SSL-VPN активовано на FortiGate. Налаштувати параметри SSL-VPN, такі як порт, діапазон IP-адрес і методи автентифікації.

Для втентифікації необхідно використовувати надійні методи автентифікації, такі як багатофакторна автентифікація (MFA), для підвищення безпеки.

Обв’язково необхідно інтегрувати FortiGate з сервером Active Directory або іншим сервером аутентифікації.

Розробити політики доступу, які повинні включати політики доступу, щоб обмежити доступ віддалених користувачів до внутрішніх ресурсів відповідно до їхніх потреб.

За необхідністю можна розмежувати доступ до внутрішніх ресурсів,

наприклад, розділити доступ до тих чи інших ресурсів, для різних відділів організації.

Використовувати SSL-сертифікати, видані довіреним центром сертифікації, для захисту з'єднання SSL-VPN.

Для доступу до системи необхідно налаштувати FortiClient для встановлення та налаштування віддалених користувачів. Для цього необхідно надати користувачам інструкції щодо встановлення та налаштування FortiClient.

За необхідністю налаштувати FortiClient для автоматичного підключення до FortiGate при запуску.

Створити профілі VPN для різних груп користувачів з різними налаштуваннями та надати користувачам відповідні профілі VPN.

Для забезпечення безпеки активізувати функції безпеки FortiClient, такі як антивірусний захист і веб-фільтрація.

Регулярно оновлювати FortiClient для забезпечення безпеки та сумісності.

Рекомендації щодо використання користувачами включають в себе навчання користувачів правилам безпечного використання SSL-VPN.

Проводити вчасно моніторинг та аудит веденню журналів SSL-VPN-з'єднань.

Використовуйте додаткові модулі, такі як FortiAnalyzer для аналізу журналів та виявлення аномальної поведінки.

Дотримання запропонованих рекомендацій дозволить ефективно використовувати FortiClient для роботи SSL-VPN та забезпечити безпечний доступ віддалених користувачів до інформаційної системи організації.

ВИСНОВКИ

В кваліфікаційній роботі проведено дослідження проблеми захисту віддалених користувачів інформаційної системи організації, визначено його мету та завдання. Розвиток інформаційних технологій дозволив організаціям використовувати віддалену роботу своїх працівників, які є користувачами інформаційної системи. Це спричинило низку проблем з забезпечення кібербезпеки в організаціях у зв'язку з загрозами, які є дуже різними. Тому для захисту віддалених користувачів інформаційної системи необхідно впроваджувати систему кіберзахисту, яка дозволить захищати віддалені з'єднання від сучасних загроз безпеці.

В роботі проведено аналіз рівень, в основу яких покладено методи та засоби які використовуються системою захисту віддалених користувачів. На основі порівняння цих рішень було обрано систему FortiClient, яка на відміну від інших є найбільш простою у використанні для вирішення проблеми захисту віддалених користувачів інформаційної системи організації.

В роботі для обраної системи проведено аналіз методів та засобів системи FortiClient, яка складається з декількох модулів, які дозволяють на основі сучасних рішень впровадити захищене з'єднання для віддалених користувачів. Таке рішення дозволить легко моніторити і виявляти інциденти фахівцям з кібербезпеки.

На основі проведеного дослідження запропоновано варіант налаштування SSL-VPN з'єднання FortiClient з боку адміністратора безпеки, яке дозволяє обраним групам віддалених користувачів інформаційної системи організації безпечний доступ до ресурсів організації.

В результаті виконаної роботи, а саме створення системи захисту віддалених користувачів, розроблено загальні рекомендації для фахівців з кібербезпеки для вирішення проблеми захисту віддалених користувачів організації, які дозволять створювати комплексну систему захисту.

Таким чином реалізація такої системи захисту віддалених користувачів

інформаційної системи організації повинна сприяти розвитку та ефективному захисту інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. *Netwrix*. Remote Access Security Best Practices. URL: https://www.netwrix.com/remote-access-security-best-practices.html

2. Mandadi, S. Cybersecurity Risks in Remote Work and Learning Environments and Methods of Combating Them / S. Mandadi, S. P. Gochhayat, V. Torremocha, J. Kethar // Journal of Student Research. – 2024. – Vol. 13, № 2. URL: https://doi.org/10.47611/jsrhs.v13i2.6808

3. The 58 Number of Remote Work Statistics. URL: https://www.ranktracker.com/uk/blog/the-58-number-of-remote-work-statistics/

4. Cisco. Future of Secure Remote Work Report. URL: https://www.cisco.com/c/dam/global/uk_ua/products/future-of-secure-remote-work-report.pdf

5. Статистика загроз віддаленої роботи // Velocity Global. URL: https://velocityglobal.com/resources/blog/remote-work-statistics/

6. Загрози безпеки віддалених користувачів // Tresorit. URL: https://tresorit.com/blog/remote-access-security-key-risks-to-watch-out-for-and-how-to-mitigate-them/

7. Складові FortiClient // Fortinet. URL: https://www.fortinet.com/support/product-downloads

8. ZTNA Edition // Fortinet. URL: https://www.fortinet.com/solutions/enterprise-midsize-business/network-access/application-access

9. Призначення ZTNA Edition // Fortinet. URL: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-concept-guide/126213/what-is-ztna#:~:text=ZTNA%2C%20by%20industry%20standards%2C%20is,control%20based%20on%20these%20factors.

10. Робота FortiSandbox // Fortinet. URL: https://docs.fortinet.com/document/fortisandbox/5.0.0/best-practices/621838/overview

11. Модуль FortiClient EMS // Fortinet. URL: https://docs.fortinet.com/document/forticlient/6.0.2/ems-administration-guide/75181/forticlient-ems-components.

12. Comparative Quality of Service Analysis of VPN Protocols on IPv6 / S. T. Oktavia et al. Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI). 2024. Vol. 12, no. 3. P. 461–471. URL: https://doi.org/10.23887/janapati.v12i3.69264 (date of access: 17.03.2025).

13. Budiyanto S., Gunawan D. Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice over Internet Protocol. IEEE Access. 2023. P. 1. URL: https://doi.org/10.1109/access.2023.3286032 (date of access: 17.03.2025).

14. ZTNA vs VPN: What's the Difference? // Sangfor Glossary. URL: https://www.sangfor.com/glossary/cybersecurity/zero-trust-network-access-ztna-vs-virtual-private-network-vpn (дата звернення: 18.03.2025).

15. ZTNA vs VPN: Which One to Choose? // NordLayer. URL: https://nordlayer.com/blog/ztna-vs-vpn-whats-the-difference/ (дата звернення: 18.03.2025).

16. ZTNA vs VPN: Secure Remote Work and Access // Trend Micro (US). URL: https://www.trendmicro.com/en_us/research/22/h/ztna-vs-vpn-secure-remote-work.html (дата звернення: 18.03.2025).

17. ZTNA vs VPN: The ultimate showdown // GoodAccess. URL: https://www.goodaccess.com/blog/ztna-vs-vpn (дата звернення: 18.03.2025).

18. Zero Trust Network Access (ZTNA) vs VPNs // Kong Inc. URL: https://konghq.com/blog/engineering/ztna-vs-vpns (дата звернення: 18.03.2025).

19. Switch to Zero Trust Network Access // Zscaler. URL: https://www.zscaler.com/resources/infographics/switch-to-zero-trust-network-access.pdf (дата звернення: 18.03.2025).

20. What Is Zero Trust Network Access (ZTNA) // Palo Alto Networks. URL: https://www.paloaltonetworks.ca/cyberpedia/what-is-zero-trust-network-access-ztna (дата звернення: 18.03.2025).

21. ZTNA vs VPN: the main advantages of ZTNA over VPN // cyberelements.

URL: https://cyberelements.io/ztna-vs-vpn/ (дата звернення: 18.03.2025).

22. What Is Zero Trust Network Access (ZTNA)? // Zscaler. URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access (дата звернення: 18.03.2025).

23. Top Six Advantages of ZTNA // ProActive Information Management. URL: https://www.proactive-info.com/blog/top-six-advantages-of-ztna (дата звернення: 18.03.2025).

24. Understanding the Pros and Cons of Zero Trust Network Architecture // Sentia Solutions. URL: https://www.sentia.ca/Blog/ArtMID/1133/ArticleID/207/Understanding-the-Pros-and-Cons-of-Zero-Trust-Network-Architecture (дата звернення: 18.03.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

https://www.zscaler.com/products-and-solutions/zscaler-private-access