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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення безпечної роботи гібридних працівників організації на базі Fortinet Secure Access Service Edge»

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

_____ Андрій ЗАГОРУЙКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ЗАГОРУЙКО АНДРІЙ
(прізвище, ім'я)

Керівник д. ф. ПЕДЧЕНКО Євгвген
(науковий ступінь, вчене звання, прізвище,

Рецензент _____
(науковий ступінь, вчене звання, прізвище,

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BYOD — Bring Your Own Device

CASB — Cloud Access Security Broker

DLP — Data Loss Prevention

FWaaS — Firewall as a Service

MFA — Multi-Factor Authentication

NGFW — Next-Generation Firewall

PoP — Point of Presence

SASE — Secure Access Service Edge

SD-WAN — Software-Defined Wide Area Network

SIA — Secure Internet Access

SPA — Secure Private Access

SSE — Security Service Edge

SWG — Secure Web Gateway

TCO — Total Cost of Ownership

VPN — Virtual Private Network

WFA — Work From Anywhere

ZTNA — Zero Trust Network Access

ВСТУП

Актуальність дослідження. Традиційна парадигма кібербезпеки, яка спиралася на захист фізичного периметра офісу, остаточно втратила свою актуальність. В умовах сьогодення критично важливі дані більше не зберігаються виключно в локальних дата-центрах, а активно мігрують у хмарні середовища. Одночасно з цим стрімко зростає кількість віддалених працівників, а процеси цифрової трансформації вимагають від IT-підрозділів максимальної гнучкості для швидкої адаптації до нових бізнес-вимог.

Внаслідок такої децентралізації поняття класичного мережевого кордону зникає, що породжує необхідність у принципово нових підходах до захисту інформації та управління доступом. Організації стикаються з тим, що набір розрізнених інструментів попереднього покоління — таких як локальні міжмережеві екрани, шлюзи веб-безпеки, DLP-системи та CASB-рішення — стає неефективним і складним в управлінні в умовах хмарної архітектури.

Архітектура Secure Access Service Edge (SASE) пропонує вирішення цієї проблеми через конвергенцію мережевих технологій та функцій безпеки в єдину хмарну послугу. Ця модель дозволяє захищати активи компанії незалежно від їхньої локації. Оскільки користувачі та додатки вийшли за межі корпоративної мережі, засоби контролю більше не можуть залежати від апаратного забезпечення, прив'язаного до конкретного місця.

Замість застарілого підходу з маршрутизацією всього трафіку через центральний офіс для перевірки, SASE переносить інспекцію безпеки безпосередньо в хмару. Це дозволяє користувачам встановлювати пряме безпечне з'єднання з необхідними ресурсами. При коректному впровадженні така модель дозволяє відмовитися від громіздкого обладнання на периферії, забезпечуючи при цьому єдину та послідовну політику безпеки для всіх з'єднань.

Окрім технічної оптимізації, впровадження SASE дозволяє реалізувати концепцію "нульової довіри" (Zero Trust Network Access — ZTNA) на рівні

кожного окремого сеансу. На відміну від традиційних VPN, які часто надають надмірний доступ до мережі, SASE перевіряє ідентичність користувача та контекст запиту перед наданням доступу до конкретного додатка. Це мінімізує ризики горизонтального переміщення зловмисників усередині мережі у випадку компрометації облікового запису.

Також варто зазначити, що перехід на SASE суттєво покращує досвід користувачів (Digital Experience). Усунення необхідності "ганяти" трафік через перевантажені шлюзи центрального офісу зменшує затримки та підвищує швидкість роботи хмарних додатків. Це критично важливо для забезпечення продуктивності гібридних команд, які потребують стабільного доступу до відеоконференцій та інструментів спільної роботи.

Все вищезазначене підкреслює гостру актуальність теми даної кваліфікаційної роботи. Її основний зміст присвячено дослідженню технологій забезпечення безпечної діяльності гібридних працівників організації з використанням платформи FortiSASE, яка є одним з лідерів у цьому сегменті ринку.

Об'єкт дослідження –безпечна робота гібридних працівників організації.

Предмет дослідження – технологія забезпечення безпечної роботи гібридних працівників організації на прикладіі FortiSASE.

Мета роботи – розробити технологію забезпечення безпечної роботи гібридних працівників організації на основі розроблених топологій та загальні рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми забезпечення безпечної роботи гібридних працівників організації;

проаналізувати підходи до забезпечення безпечної роботи гібридних працівників організації;

проаналізувати існуючі рішення із забезпечення безпечної роботи гібридних працівників організації;

проаналізувати методи та засоби забезпечення безпечної роботи гібридних

працівників організації на базі FortiSASE;

розкрити технологію забезпечення безпечної роботи гібридних працівників організації на основі розроблених топологій.

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

Практичне значення одержаних результатів: запропоновано технологію забезпечення безпечної роботи гібридних працівників організації, а в основу якої розроблено рекомендації щодо її реалізації для фахівців з кібербезпеки.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ РОБОТИ ГІБРИДНИХ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми забезпечення безпечної роботи гібридних працівників організації

Гібридна робота стала домінуючою організаційною моделлю, і значна частина світової робочої сили використовує цей гнучкий підхід. Хоча він пропонує численні переваги, він також створює складні проблеми безпеки, які організації повинні вирішувати для захисту інформаційних ресурсів організації.

Перехід до гібридної роботи, яка поєднує роботу на місці та віддалену, прискорився завдяки розвитку технологій та зміні очікувань щодо робочої сили. Ця модель пропонує гнучкість, покращений баланс між роботою та особистим життям і доступ до ширшого пулу талантів. Однак вона також розширює поверхню атаки для кіберзагроз, що вимагає надійних заходів безпеки [1, 2].

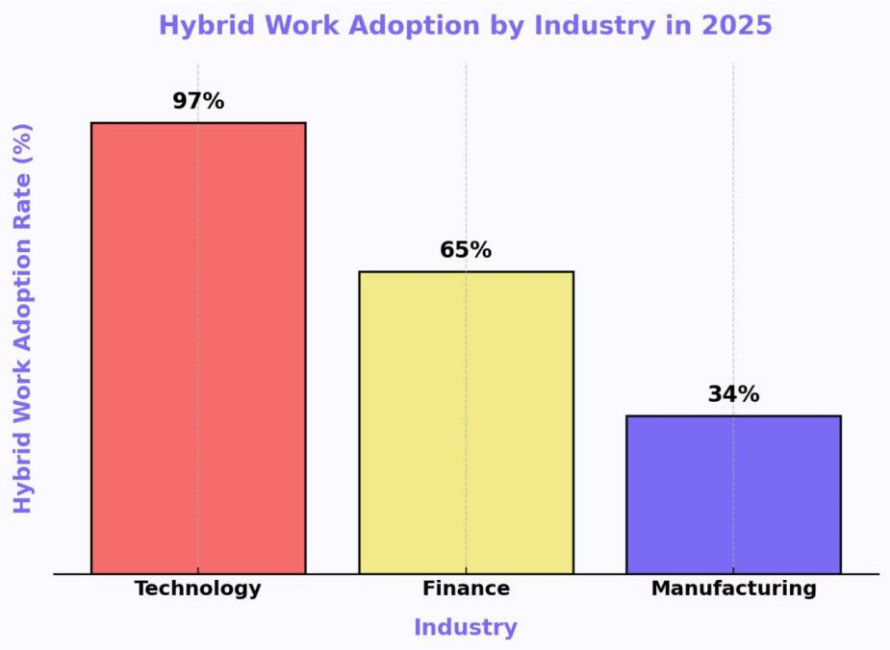


Рис.1.1. Гібридні працівники [2]

Глобальний ринок праці демонструє вражаючу регіональну асиметрію у впровадженні гібридних моделей. Так 53% працівників, які можуть працювати віддалено, надають перевагу гібридним схемам, тоді як інші залишаються офісно-

орієнтованою — ця нерівність корініться не стільки в технологічних розривах, скільки в культурних нормах, де фізична присутність часто свідчить про лояльність у колективістських суспільствах [2].

Економічний вплив стає дедалі відчутнішим. Accenture повідомляє, що 83% фахівців погодилися б на 5% зниження заробітної плати за гнучкий графік, тоді як компанії скорочують офісні витрати на 30–40% без втрати продуктивності. Дивно, але показники залученості показують, що гібридні працівники перевершують своїх колег з офісної роботи (51% проти 44%) та повністю віддалених колег (39%) [2].

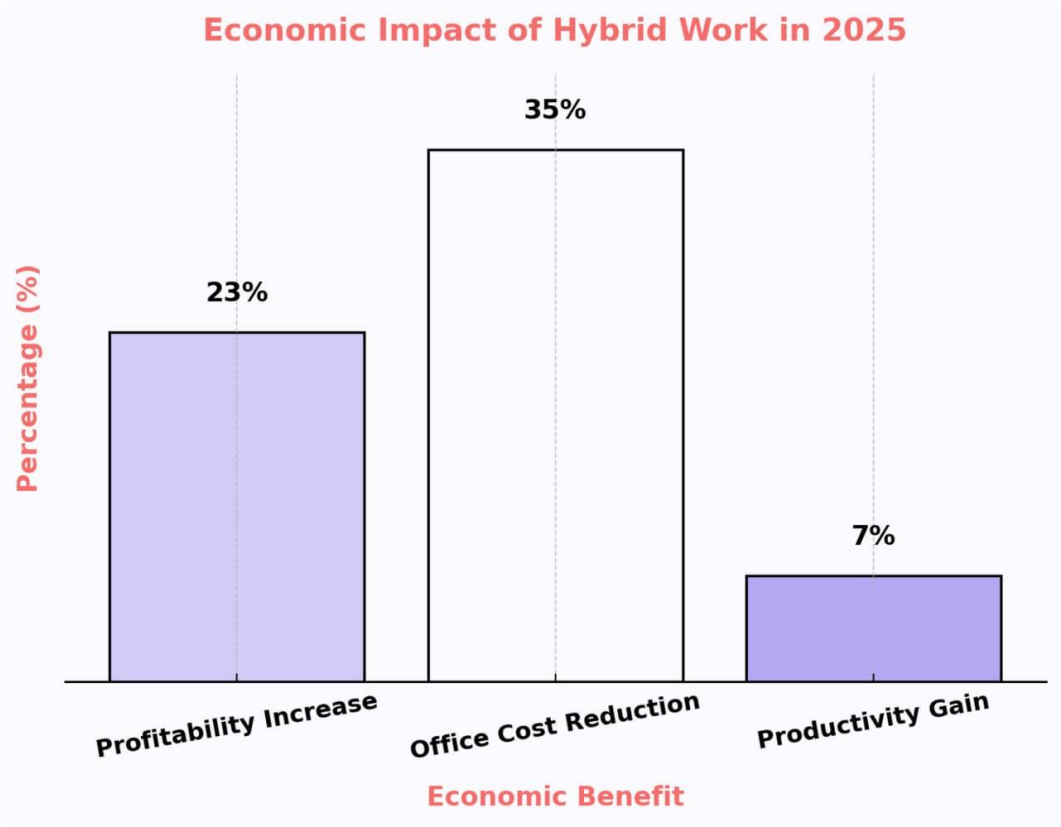


Рис. 1.2. Економічні впливи на гібридних працівників [2]

Оскільки компанії орієнтуються в гібридному середовищі, задоволеність працівників та якість життя стають вагомими чинниками, що впливають на вибір віддаленої роботи. Працівники цінують гнучкість, яка дозволяє їм поєднувати особисті та професійні зобов'язання, а віддалена робота забезпечує рівень свободи, який важко досягти в офісі. Фактично, багато працівників повідомляють, що можливість працювати з дому значно покращує баланс між роботою та особистим життям, що призводить до вищого рівня задоволеності та залученості.

Однак, цей компроміс не обходиться без труднощів. Хоча віддалена робота сприяє особистому благополуччю, вона також створює певний набір перешкод, головним чином щодо забезпечення безпеки. Згідно з дослідженням Metrigy, безпека залишається найважливішим викликом для компаній, які підтримують віддалену роботу. Забезпечення безпечного доступу до мереж і даних компанії, коли співробітники працюють з різних місць, вимагає надійних стратегій кібербезпеки, які є пріоритетними для IT-керівників.

Розробляючи стратегію гібридного робочого місця , вашим пріоритетом має бути створення структури, яка покращить зв'язок вашої команди та усуне будь-яку дистанцію, яку може створити фізична відсутність. Для успішного функціонування гібридної моделі важливо використовувати правильне програмне забезпечення для співпраці та питання безпеки, щоб переосмислити робоче місце вашої компанії.

Тому надалі розглянемо основні проблеми безпеки в гібридних робочих середовищах

*Розширена поверхня атаки***.** Віддалена робота збільшує вразливості, оскільки співробітники підключаються з різних місць, використовуючи різноманітні пристрої та мережі.

Ризики безпеки даних. Доступ до конфіденційних даних та їх передача можуть здійснюватися через незахищені мережі, що збільшує ризик витоку даних.

Загрози програм-вимагачів та шкідливих програм. Співробітники, які працюють віддалено, можуть бути більш вразливими до фішингових атак та атак шкідливих програм, що призводить до інцидентів із програмами-вимагачами.

Слабке управління паролями. Працівники можуть використовувати слабкі або повторно використані паролі, створюючи можливості для несанкціонованого доступу.

Незахищений обмін файлами. Працівники можуть використовувати незахищені методи обміну файлами, розкриваючи конфіденційні дані неавторизованим особам.

Використання загальнодоступного Wi-Fi. Підключення до загальнодоступних мереж Wi-Fi може призвести до розголошення конфіденційних даних.

Ризики безпеки BYOD. Працівники, які використовують особисті пристрої для роботи, можуть створювати вразливості безпеки, якщо пристрої не захищені належним чином.

Вразливості VPN. Традиційні VPN, хоча й призначені для безпечного доступу, можуть мати вразливості, які розкривають цілі мережі у разі порушення безпеки.

Атаки програм-вимагачів еволюціонують, стаючи швидшими та складнішими. У 2025 році загроза залишатиметься повсюдною, походячи як від великих угруповань, так і від «вовків-одинаків». Згідно з опитуванням 1300 організацій, кількість компаній, що постраждали принаймні від однієї атаки, трохи знизилася з 75% до 69% завдяки покращенню підготовки та співпраці [5].

У 2024 році влада розпочала кілька успішних операцій з ліквідації відомих груп кіберзагроз. Ліквідація цих більших груп, очевидно, є позитивним явищем для захисту від загроз. Однак кількість менших груп та «одиноких вовків», які поширюють атаки, зросла. Деякі групи також змістили свою ціль нижче за течією, уникаючи критичної інфраструктури, щоб зменшити контроль з боку правоохоронних органів, та орієнтуючись на малі та середні підприємства (МСП), які часто мають слабший кіберзахист.

Деякі з більших груп, які були закриті, зникли або припинили свою діяльність, включають:

LockBit, групу програм-вимагачів як послугу (RaaS), ліквідована правоохоронними органами під керівництвом Національного агентства з боротьби зі злочинністю Великої Британії спільно з ФБР та Європолом.

BlackCat, група RaaS, діяльність якої ФБР раніше зруйнувало у 2023 році, припинила свою діяльність у березні 2024 року після успішної атаки, спрямованої на Change Healthcare, та виплати викупу, як повідомляється, на суму понад 22 мільйони доларів США.

Black Basta, яка, схоже, припинила свою діяльність у 2025 році після того, як витік журналів чатів виявив занепокоєння щодо контролю з боку правоохоронних органів після атаки на Acension системи охорони здоров'я США, яка включала 140 лікарень у 19 штатах.

Зі зміною ландшафту загроз, зловмисники продовжують змінювати свою тактику. Примітно, що хоча тактика викрадання даних зазвичай використовується разом із шифруванням даних, кількість жертв, у яких викрадання здійснювалося лише за допомогою викупу, зросла протягом четвертого кварталу.

Викрадання даних відображає підхід «розгрому та захоплення», що є поширеним явищем у традиційних атаках програм-вимагачів, перед шифруванням. Це також трапляється з погано захищеними хмарними додатками та хмарною інфраструктурою.

Поряд із цим зрушенням до викрадання даних, а також до подвійного вимагання, яке поєднує як шифрування для обмеження доступу, так і публікацію конфіденційних викрадених даних, також спостерігається скорочення часу перебування, часу між компрометацією та запуском атаки, причому багато атаки відбуваються лише за лічені години [5].

У другому кварталі 2024 року Coveware by Veeam зазначила, що два з трьох головних зловмисників-вимагачів у цьому кварталі мали середній час перебування менше 24 годин.7 Це помітне зниження порівняно з попередніми кварталами, і ця тенденція продовжилася і в четвертому кварталі [5].

Коли зловмисники отримують доступ до мереж жертв, вони, як правило, використовують методи латерального переміщення. Вони шукають легкості вилучення або певної мети, наприклад, компрометації гіпервізорів VMware ESXi, щоб змусити жертв сплатити викуп. Ці ефективні та добре відпрацьовані стратегії часто призводять до швидших атак, які може бути важко виявити та стримати.

Занадто часто організації, які мають слабку систему кібербезпеки та складну мережеву архітектуру, є особливо вразливими до витоку даних та пов'язаних з цим кіберзагроз [5].

На щастя, загальна вартість платежів, здійснених за програмами-вимагачами, зменшилася протягом 2024 року порівняно з 2023 роком. Більше третини організацій, постраждалих від атаки програм-вимагачів (36%), не сплатили викуп, а 25% не сплатили, але все одно змогли відновити свої дані.

Серед тих, хто сплатив, 82% сплатили менше, ніж початковий викуп, а 60% сплатили менше половини цієї суми.

Ці дані також узгоджуються з тим, що Coveware by Veeam бачила безпосередньо під час своєї роботи з постраждалими компаніями протягом 2024 року, коли середній платіж зменшився на 45% у четвертому кварталі приблизно до 110 тис. доларів США, що є найнижчим показником за весь час.

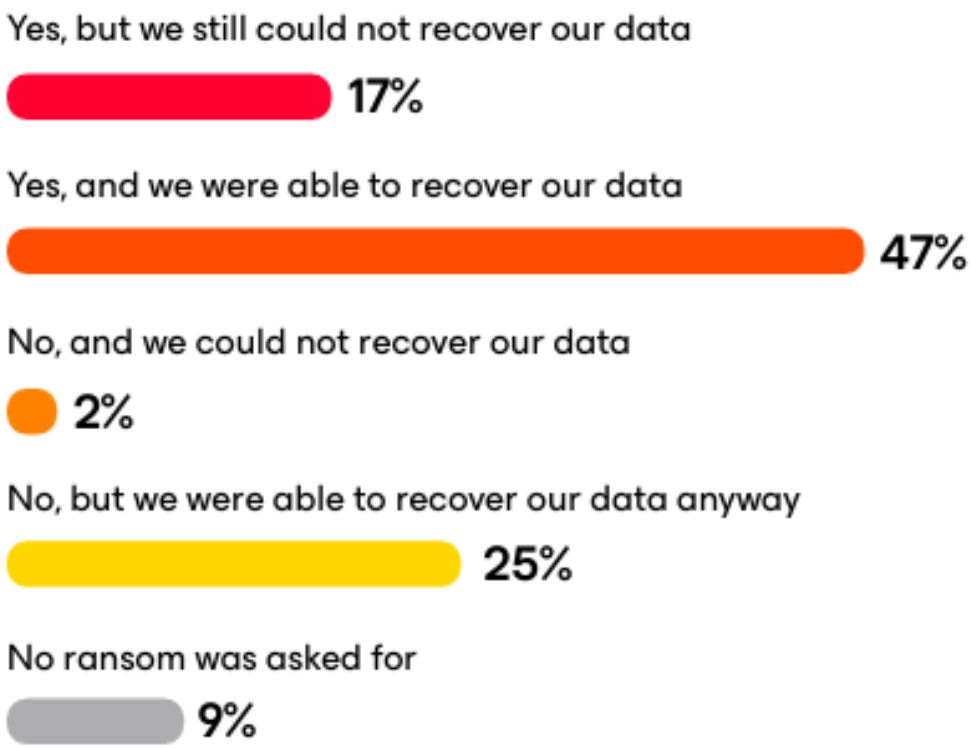


Рис.1.3. Кількість організацій, які сплатили викуп

Лише 25% компаній, які співпрацюють з експертами з реагування на інциденти від Coveware by Veeam, сплатили викуп, що стало «значною віхою в боротьбі з програмами-вимагачами».

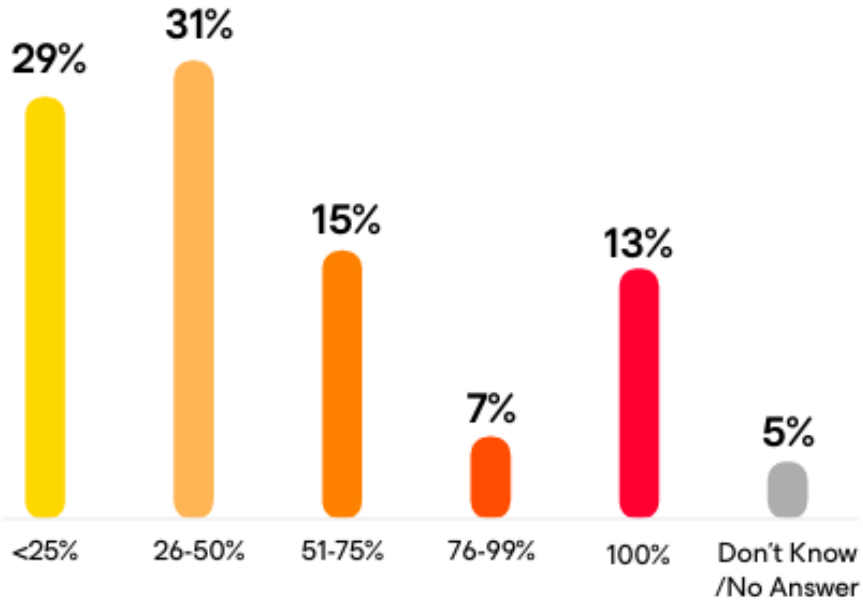


Рис.1.4. Відсоток сплаченого викупу

Порівняно з компаніями, які використовували послуги реагування на інциденти від Coveware by Veeam, інші організації на 156% частіше платили викуп. Це свідчить про те, що співпраця з досвідченими третіми сторонами для реагування на інциденти корелює з меншою кількістю виплат викупу, нижчими виплатами викупу та більш стійкими практиками загалом.

Жертви дедалі більше вагаються платити викуп, оскільки вони не можуть довіряти зловмисникам щодо розголошення їхніх даних. Організації також проактивно вдосконалили власні плани реагування на інциденти, зокрема шляхом використання незмінного резервного копіювання.

Співпраця посилює стійкість до програм-вимагачів та інших загроз. Покращення співпраці та комунікації між IT-відділами та командами безпеки також допомогає організаціям підвищити їхню кіберстійкість.

Однак більшість респондентів (52%) заявили, що потрібне значне покращення або повна перебудова для узгодження цих команд. І лише 11% сказали, що потрібне незначне покращення або взагалі жодне покращення.

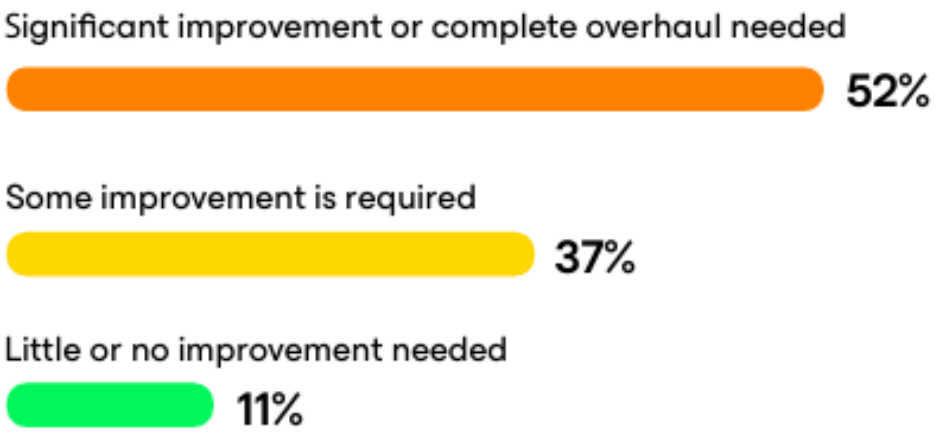


Рис. 1.5. Узгодження IT-операцій та команд безпеки

Водночас, гравці платформ та технологій співпрацюють для об'єднання даних про програми-вимагачі та інші загрози та надання послуг, які допомагають організаціям посилити їх захист. Повідомлення про програми-вимагачі та інші кібератак правоохоронним та регулюючим органам, а також тим партнерським мережам, що створюються, та галузевим біржам обміну інформацією, зміцнює колективний захист.

1.2. Аналіз підходів до забезпечення безпечної роботи гібридних працівників організації

Забезпечення безпечної роботи гібридних працівників необхідно враховувати основні ризики безпеки. Щоб зменшити ці ризики, організації повинні прийняти комплексну стратегію безпеки, яка включає наступні підходи:

Принципи нульової довіри (Zero Trust)

Впровадження моделі нульової довіри фундаментально змінює парадигму кібербезпеки, відмовляючись від застарілої концепції «довіряй, але перевіряй» на користь принципу «ніколи не довіряй, завжди перевіряй». У цій архітектурі мережа більше не поділяється на безпечну внутрішню зону та небезпечну зовнішню; натомість кожна спроба доступу розглядається як потенційно ворожа, незалежно від того, звідки вона походить. Це означає, що ідентифікація

користувача, стан його пристрою та контекст запиту повинні проходити сувору валидацію перед наданням доступу до будь-якого ресурсу.

Окрім перевірки на вході, модель нульової довіри передбачає безперервний моніторинг та оцінку ризиків протягом усього сеансу роботи. Системи автоматично обмежують права доступу до мінімально необхідного рівня (principle of least privilege), що дозволяє користувачеві виконувати лише свої безпосередні завдання. Такий підхід значно зменшує радіус ураження у випадку компрометації облікового запису, оскільки зловмисник не зможе вільно пересуватися мережею.

Багатофакторна автентифікація (MFA)

Застосування багатофакторної автентифікації (MFA) є критично важливим бар'єром, який значно ускладнює роботу зловмисників, навіть якщо їм вдалося викрасти пароль користувача. MFA вимагає від користувача надати два або більше доказів своєї особи з різних категорій: те, що він знає (пароль), те, що він має (смартфон, токен), або те, ким він є (біометрія). Такий багаторівневий захист робить викрадені облікові дані марними без доступу до фізичного пристрою або біометричних даних власника [3].

Крім того, сучасні рішення MFA стають адаптивними та інтелектуальними, аналізуючи контекст входу, такий як геолокація, час доби та тип пристрою. Якщо система помічає аномальну поведінку — наприклад, спробу входу з іншої країни через хвилину після входу з офісу — вона може вимагати додаткової перевірки. Це дозволяє ефективно протидіяти атакам типу «розпилення паролів» (password spraying) та фішинговим кампаніям [3].

Шифрування даних

Шифрування даних виступає останньою лінією оборони, яка гарантує конфіденційність інформації навіть у разі фізичного викрадення носіїв або перехоплення мережевого трафіку. Цей процес перетворює читабельні дані на незрозумілий набір символів, розкодувати який можна лише за наявності унікального ключа дешифрування. Важливо застосовувати шифрування як для даних у стані спокою (на жорстких дисках, серверах, у хмарі), так і для даних у русі (під час передачі через інтернет або внутрішні мережі) [3].

Надійне керування ключами шифрування є не менш важливим, ніж сам алгоритм захисту. Організації повинні впроваджувати суворі політики щодо створення, зберігання та ротації ключів, щоб запобігти їх компрометації. Завдяки цьому, навіть якщо хакери отримають доступ до бази даних клієнтів або інтелектуальної власності компанії, вони не зможуть використати цю інформацію або продати її, оскільки вона залишатиметься криптографічно захищеною [3].

Безпека кінцевих точок (Endpoint Security)

Впровадження надійних рішень для безпеки кінцевих точок є необхідністю в умовах, коли периметр мережі розмивається через віддалену роботу та використання мобільних пристроїв. Сучасні платформи захисту (такі як EDR та XDR) виходять далеко за межі можливостей традиційних антивірусів, які покладаються лише на сигнатури відомих загроз. Вони використовують поведінковий аналіз та штучний інтелект для виявлення підозрілої активності в реальному часі, блокуючи навіть нові та невідомі раніше атаки (zero-day attacks) [3].

Окрім виявлення загроз, ці рішення надають інструменти для швидкого реагування на інциденти та розслідування їх причин. Адміністратори безпеки можуть дистанційно ізолювати заражений пристрій від корпоративної мережі, запобігаючи поширенню шкідливого програмного забезпечення, та провести глибокий аналіз атаки. Це дозволяє не лише захистити конкретний ноутбук чи смартфон, а й посилити загальну стійкість організації до кіберзагроз [3].

Навчання з питань безпеки

Регулярне навчання з питань безпеки перетворює співробітників з «найслабшої ланки» на першу лінію оборони організації. Оскільки значна частина кібератак починається з соціальної інженерії, важливо, щоб кожен працівник умів розпізнавати ознаки фішингу, підозрілі посилання та спроби маніпуляції. Навчальні програми мають бути не одноразовими заходами, а постійним процесом, що включає симуляції реальних атак для перевірки пильності персоналу [3].

Крім того, формування культури кібербезпеки допомагає співробітникам зрозуміти їхню особисту роль у захисті корпоративних даних. Коли працівники усвідомлюють наслідки недбалого поводження з інформацією та знають чіткі алгоритми дій у разі виявлення загрози, вони стають активними учасниками системи безпеки. Це значно знижує ризик людської помилки, яка часто стає причиною серйозних витоків даних.

Запобігання втраті даних (DLP)

Рішення DLP (Data Loss Prevention) забезпечують глибоку видимість та контроль над переміщенням конфіденційної інформації всередині організації та за її межами. Системи DLP автоматично класифікують дані за ступенем важливості та застосовують політики безпеки, які запобігають їх несанкціонованій передачі через електронну пошту, месенджери, хмарні сховища або змінні носії. Це дозволяє захистити інтелектуальну власність, персональні дані клієнтів та фінансову звітність від випадкових або навмисних витоків [3].

Ефективна стратегія DLP також включає моніторинг використання даних у реальному часі, що дозволяє виявляти аномальну поведінку користувачів, яка може свідчити про внутрішню загрозу. Наприклад, якщо співробітник раптово намагається завантажити великий обсяг файлів на зовнішній сервер, система може автоматично заблокувати цю дію та сповістити службу безпеки. Таким чином, DLP допомагає дотримуватися нормативних вимог та зберігати репутацію компанії

Ізоляція віддаленого браузера (RBI) та контейнеризація

Технологія ізоляції віддаленого браузера (RBI) створює «повітряний зазор» між користувачем та інтернетом, виконуючи весь веб-код на віддаленому сервері в хмарі. Користувач отримує лише безпечний потік візуальної інформації (пікселі), що повністю виключає можливість завантаження шкідливих скриптів або експлойтів на кінцевий пристрій. Це дозволяє співробітникам вільно переглядати веб-ресурси, не наражаючи корпоративну мережу на небезпеку зараження через браузер [3].

Контейнеризація додатків, у свою чергу, дозволяє відокремити корпоративні програми та дані від особистого простору користувача на мобільному пристрої або ноутбуці. Розміщуючи робочі інструменти в захищених, зашифрованих контейнерах, компанія робить їх невидимими та недоступними для інших програм, які можуть бути скомпрометовані. Це не лише підвищує безпеку, але й спрощує керування даними в концепції BYOD (Bring Your Own Device), дозволяючи видаляти корпоративну інформацію без впливу на особисті файли працівника [3].

Відмова від VPN

Традиційні VPN-мережі стають архаїчним рішенням, яке не відповідає сучасним вимогам безпеки, оскільки вони часто надають користувачам надмірний доступ до всієї мережі. Якщо зловмисник отримує облікові дані VPN, він фактично отримує «ключі від королівства» і може вільно пересуватися внутрішньою інфраструктурою. Крім того, VPN часто створюють проблеми з продуктивністю, змушуючи весь трафік проходити через центральний шлюз, що сповільнює роботу хмарних додатків [3].

Натомість сучасні альтернативи, такі як ZTNA (Zero Trust Network Access), забезпечують доступ лише до конкретних програм, необхідних користувачеві для роботи, а не до мережі в цілому. Це робить інфраструктуру невидимою для зовнішнього світу та значно зменшує поверхню атаки. Відмова від VPN на користь таких технологій покращує користувацький досвід завдяки швидшому з'єднанню та забезпечує більш гранулярний контроль безпеки [3].

Безпечний доступ до сервісу на межі доступу (SASE)

Архітектура SASE (Secure Access Service Edge) об'єднує мережеві функції та функції безпеки в єдину хмарну платформу, забезпечуючи безпечний доступ до ресурсів незалежно від місцезнаходження користувачів. Це дозволяє організаціям відмовитися від складної та дорогої інфраструктури, що базується на централізованих дата-центрах, і надати співробітникам швидкий та захищений доступ до хмарних додатків та інтернету безпосередньо з їхніх пристроїв [3].

Впровадження SASE спрощує управління безпекою, оскільки політики застосовуються централізовано в хмарі, а не на кожному окремому пристрої чи шлюзі. Це забезпечує єдиний рівень захисту для всіх користувачів, незалежно від того, працюють вони в офісі, вдома чи в дорозі. Завдяки інтеграції таких технологій, як ZTNA, CASB та SWG, SASE створює гнучке та масштабоване середовище, що відповідає потребам сучасного гібридного робочого місця. Отже, для поставленого завдання основним підходом для вирішення задачі розглянемо детальніше Secure Access Service Edge [3].

Secure Access Service Edge (SASE) — це корпоративна стратегія, що об’єднує функції мережевої безпеки з можливостями глобальної мережі (WAN). Головною метою SASE є задоволення динамічних потреб сучасних організацій у безпечному доступі до ресурсів. Ця технологія відіграє критичну роль у захисті даних у будь-якій точці, охоплюючи межі мережі, хмарні середовища, центри обробки даних (ЦОД), ядро інфраструктури та кінцеві пристрої гібридних працівників [3, 6].

Для забезпечення стабільного зв'язку та безпеки користувачів незалежно від їхнього розташування, мережеві та захисні рішення повинні конвергуватися на периферії та в хмарі. Технологія SASE консолідує мережеві можливості та функції безпеки в єдину хмарну платформу. Досягнення узгодженості підключення може стати складним викликом при спробі інтегрувати розрізнені продукти від багатьох різних постачальників. Натомість орієнтоване на платформу рішення SASE від єдиного вендора дозволяє об'єднати технології для підвищення операційної ефективності.

Організаціям важливо розгортати таке рішення SASE, яке легко інтегрується в ширшу архітектуру безпеки, гарантуючи надійне з'єднання та відмінний користувацький досвід. Як і у випадку з будь-якою новою можливістю, на ринку постійно з'являються постачальники, які прагнуть задовольнити нагальний попит і захопити частину нового ринку. Проте багато з цих пропозицій не відповідають обіцяним перевагам. Деякі з них базуються на незрілих технологіях або мають неадекватні функціональні можливості. Багато з них

працюють як ізольовані рішення, що не інтегруються з існуючими технологіями безпеки або гібридними мережами, що розширюються. Лише окремі рішення дозволяють побудувати цілісну систему, яка зменшує складність інфраструктури, а не поглиблює проблему розростання інструментів [3-6].

Для компаній, які намагаються керувати динамічною гібридною мережею, додавання ще одного окремого набору технологій може перевантажити обмежені ресурси IT-відділу. Ручне управління та обмежена аналітика загроз, яку пропонують багато постачальників SASE, часто не встигають за швидкою еволюцією сучасних кіберзагроз, залишаючи організації вразливими.

Компанія Cisco [7] наполягає на переході до конвергентної мережі та моделі безпеки на базі архітектури SASE. Ця технологія забезпечує операційне спрощення, а також стабільну безпеку та продуктивність, які необхідні для багатохмарного доступу та роботи гібридних команд. Такий результат досягається завдяки об’єднанню доменів мережі та безпеки, створюючи необхідну структуру для безперебійного підключення користувачів до додатків у складних розподілених середовищах.

Архітектура SASE швидко стає стандартом конвергенції для безпечного багатохмарного доступу. Протягом двох років близько 47% респондентів очікують підключити свої філії та віддалених клієнтів переважно за допомогою моделі SASE. Однак багато організацій намагаються реалізувати повний потенціал SASE, оскільки їхні рішення часто не мають певних можливостей або не забезпечують повної конвергенції мережі та безпеки [7].

Конвергенція SASE вимагає міцного фундаменту SD-WAN у поєднанні з розширеною хмарною безпекою або рішенням Security Service Edge (SSE) (рисунок 1.6). Лише тоді, коли ці архітектури будуть повністю об'єднані, IT-організації зможуть усвідомити всі переваги SASE. До цих переваг належать спрощена операційна модель, яка робить видимість, керування та контроль безпечного підключення користувачів максимально простими та послідовними незалежно від локації.

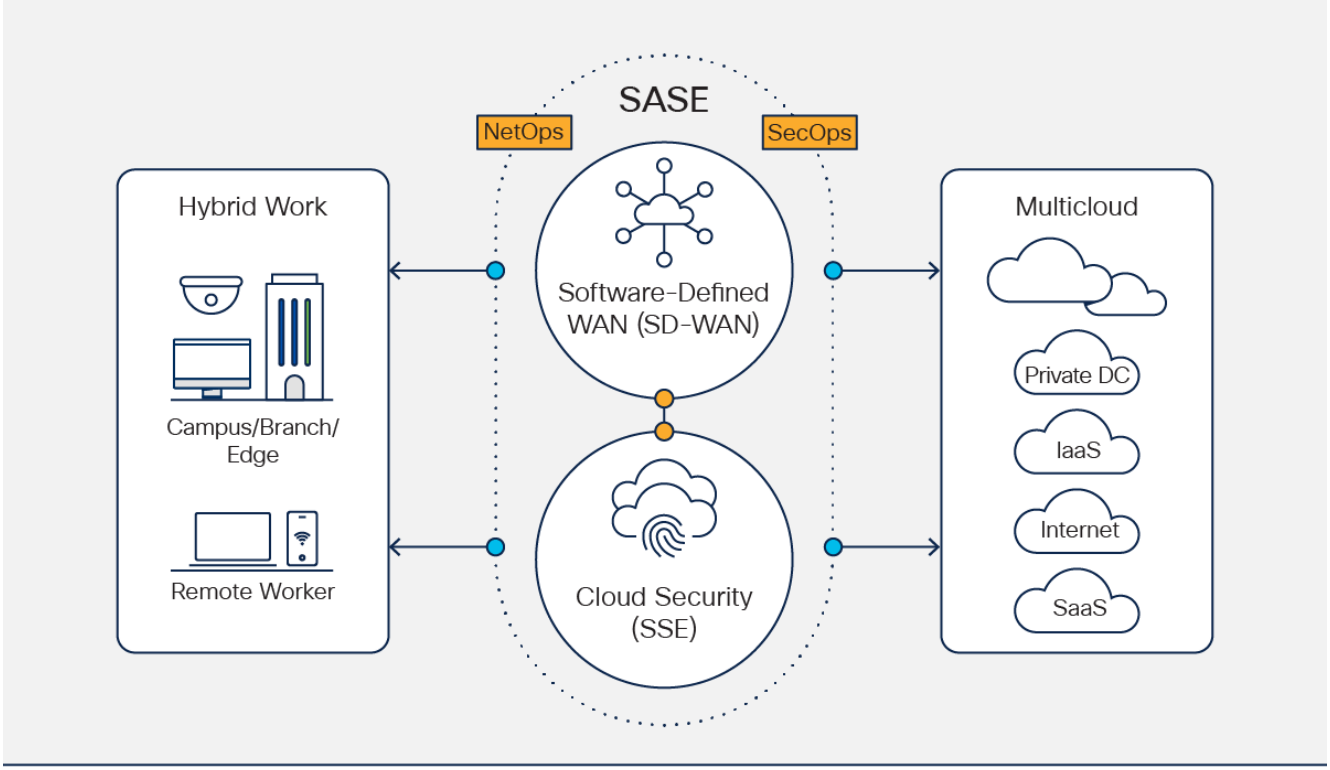


Рис. 1.6. Модель безпечного підключення – Secure Access Service Edge (SASE) [3]

Secure Access Service Edge (SASE) пропонує інтегровану модель мережі та безпеки у форматі послуги, яка об'єднує такі технології, як SD-WAN, SWG, CASB, NGFW та Zero Trust Network Access (ZTNA). Ця архітектура розроблена для підтримки різноманітних сценаріїв, від роботи філій до захисту віддалених співробітників та організації локального безпечного доступу. Надаючись переважно як хмарний сервіс, SASE гарантує доступ за принципом нульової довіри, опираючись на ідентифікацію пристроїв або об'єктів, а також враховуючи контекст у реальному часі та політики відповідності.

Використання уніфікованого рішення SASE дозволяє командам NetOps і SecOps значно підвищити ефективність IT-процесів, загальну продуктивність та рівень захисту завдяки стандартизації політик, обміну телеметрією та координації сповіщень між усіма компонентами. Створення більш узгодженої операційної моделі та оптимізація робочих процесів між цими підрозділами незмінно призводять до суттєвого покращення користувацького досвіду.

Повноцінне впровадження SASE здатне суттєво оптимізувати роботу, удосконалити взаємодію з користувачем та посилити кіберзахист. Наведемо кілька конкретних прикладів таких переваг [7]:

власний IT-підрозділ компанії Cisco зафіксував скорочення операційних витрат на 40% завдяки використанню SASE;

незалежне тестування продуктивності підтвердило, що Umbrella (ключовий елемент Cisco SASE) із налаштованими політиками безпеки працює так само ефективно, а часто навіть краще, ніж прямий доступ до SaaS-додатків через інтернет без захисту;

опитування клієнтів TechValidate демонструє, що 85% користувачів рішень Cisco зменшили кількість випадків зараження шкідливим ПЗ на 50% після переходу на архітектуру SASE.

Існує два ключові підходи до досягнення цих бажаних результатів. Перший передбачає використання окремих продуктів для мережі та безпеки/SSE, що зазвичай надаються одним або двома вендорами та інтегруються у комплексне рішення SASE; цей варіант підходить організаціям, які вже мають розгорнуті SSE або SD-WAN і потребують гнучкості налаштувань. Другий шлях — це уніфікований підхід, який пропонує всі мережеві та безпекові компоненти як єдиний готовий хмарний сервіс із централізованим керуванням. Якісно спроектоване уніфіковане рішення SASE забезпечує швидкість розгортання, простоту експлуатації та швидку окупність інвестицій.

Окрім питань безпеки, компанії повинні гарантувати, що гібридні робочі середовища сприяють високій продуктивності та ефективній співпраці. Для досягнення цієї мети необхідно забезпечити наступне:

Безпечні інструменти для співпраці. Надайте персоналу захищені платформи для спільної роботи.

Чітка комунікаційна політика. Розробіть зрозумілі правила та інструкції щодо комунікації, які будуть єдиними як для віддалених, так і для офісних працівників.

Продуктивність. Впроваджуйте технологічні рішення, що надають командам доступ до потужних робочих інструментів навіть у віддаленому режимі.

Майбутнє безпеки гібридної роботи. У міру подальшої еволюції гібридних моделей праці організації мусять зберігати пильність та адаптувати свої безпекові стратегії до появи нових загроз. Ставлячи безпеку на перше місце, компанії можуть сформувати захищене та продуктивне середовище для своїх працівників. Зосередження уваги на цих заходах дозволить організаціям ефективно мінімізувати ризики, пов'язані з гібридною роботою, та гарантувати збереження цінних даних і активів.

Отдже для подальшого дослідження існуючих рішень, які забезпечують безпечний доступ гібридних користувачів будемо розглядати рішення платформ SASE.

1.3. Аналіз існуючих рішень із забезпечення безпечного доступу гібридних працівників до корпоративних додатків

Ринок платформ SASE розвивається, оскільки на нього виходить все більше постачальників, а пропозиції стають зрілими. Тим не менш, існує диференціація у можливостях та стратегіях постачальників. Керівники I&O, відповідальні за мережі та кібербезпеку, повинні використовувати це дослідження, щоб визначити постачальника, який відповідає їхнім потребам.

На ринку рішень з’являється багато рішень з SASE. Саме квадрант Gartnera, Кожного року проводить дослідження різних рішень цього напряму [8]. Магічний квадрант надає уявлення про чотири типи постачальників технологій у будь-якій галузі:

Лідери добре виконують своє поточне бачення та мають гарні перспективи на завтрашній день.

Візіонери розуміють, куди рухається ринок, або мають бачення зміни ринкових правил, але ще не вміють його ефективно виконувати.

Нішеві гравці успішно зосереджуються на невеликому сегменті або ж не

зосереджені та не перевершують інших в інноваціях чи результатах.

Претенденти сьогодні добре справляються з поставленими завданнями або можуть домінувати у великому сегменті, але не демонструють розуміння напрямку розвитку ринку.

Рис. 1.7. Магічний квадрант для SASE одного постачальника [8]

Для проведення порівняльного аналізу візьмемо три варіант рішень від лідерів магічного квадранту SASE-рішень: Palo Alto Networks, Netskope та

Fortinet. Саме вони заходяться у квадраті Leaders (Лідери) на наданому рис.1.7. Це означає, що вони не лише мають чітке бачення розвитку технологій, але й здатні ефективно впроваджувати свої рішення у великих масштабах. Однак, кожен з них підходить до SASE з різною філософією.

Порівняння буде проводитись наступним чином, особливості, сильні та слабкі сторони. До критеріїв , які будуть включені до заключного порівняння буде включено ключова філософія, сильна сторона (Gartner), мережева частина (SD-WAN), захист даних (DLP/CASB), управління, складність впровадження, ціновий сегмент

1. Palo Alto Networks (Prisma SASE)

Розгорнутий опис: Palo Alto Networks пропонує платформу Prisma SASE, яка є однією з найбільш зрілих на ринку. Вона об’єднує хмарну безпеку (Prisma Access) та мережеві технології нового покоління (Prisma SD-WAN). Це рішення побудоване на базі багаторічного досвіду компанії у сфері фаєрволів, що дозволяє перенести потужність фізичного захисту в хмару без втрати функціональності. Вона забезпечує повний спектр перевірок трафіку (включно з розшифровкою SSL/TLS) на високій швидкості.

Сильні сторони

Еталонна безпека: Згідно з позицією на осі "Ability to Execute", компанія демонструє найвищу здатність до реалізації. Їхні механізми виявлення загроз (Threat Prevention) та пісочниця (WildFire) вважаються "золотим стандартом" у галузі.

Інтелектуальна автоматизація (AIOps): Платформа активно використовує штучний інтелект для автоматичного виявлення проблем у мережі та реагування на інциденти безпеки, що зменшує навантаження на адміністраторів.

Глобальне покриття: Має одну з найрозгалуженіших мереж точок присутності (PoP) з низькою затримкою, що критично для міжнародних корпорацій.

Слабкі сторони:

Цінова політика: Це рішення преміумкласу. Ліцензування може бути складним і дорогим, особливо коли мова йде про додавання нових модулів чи збільшення пропускної здатності.

Складність інтеграції компонентів: Оскільки платформа складається з кількох придбаних технологій (CloudGenix для SD-WAN), інколи керування потребує перемикання між різними інтерфейсами або глибшого навчання персоналу.

2. Netskope (Netskope One)

Розгорнутий опис: Netskope — це компанія, яка "народилася в хмарі" (cloud-native). Їхня платформа Netskope One спочатку розроблялася для захисту даних у хмарних додатках (CASB) та вебтрафіку (SWG). На відміну від традиційних мережевих вендорів, Netskope ставить у центр не "трубу" (мережу), а самі дані. Це робить їхнє рішення ідеальним для організацій, де співробітники працюють звідусіль, а критична інформація знаходиться в SaaS-додатках (Office 365, Salesforce тощо).

Сильні сторони

Візіонерський підхід: Найвища позиція за віссю "Completeness of Vision" вказує на те, що Netskope найкраще розуміє майбутні тренди, зокрема в контексті захисту даних.

Глибокий контекстний аналіз: Їхній рушій DLP (Data Loss Prevention) є надзвичайно потужним. Він розуміє не просто "хто" і "куди" йде, а "що" саме передається і в якому контексті (наприклад, розрізняє особистий та корпоративний акаунт Gmail).

Користувацький досвід (DEM): Рішення мінімально впливає на швидкість роботи користувача, забезпечуючи швидкий доступ до хмарних ресурсів без складних тунелів VPN.

Слабкі сторони:

SD-WAN як наздоганяючий елемент: Хоча Netskope активно розвиває свій мережевий стек (Borderless SD-WAN), він все ще має меншу історію впроваджень у складних фізичних мережах порівняно з Cisco чи Fortinet.

Залежність від хмари: Рішення найкраще працює в сценаріях "хмарного офісу". Для компаній із великою кількістю застарілих локальних дата-центрів (on-premise) архітектура може потребувати додаткових адаптерів.

3. Fortinet (FortiSASE / Unified SASE)

Розгорнутий опис: Fortinet пропонує унікальний підхід Unified SASE, де вся екосистема працює на одній операційній системі FortiOS. Це єдиний вендор, який зміг органічно об'єднати потужний апаратний захист (FortiGate) з хмарними сервісами (FortiSASE) без необхідності купувати сторонні компанії. Рішення дозволяє "розтягнути" політики безпеки з офісного фаєрвола на віддаленого працівника в кафе за кілька кліків.

Сильні сторони:

Справжня конвергенція: Це не набір інтегрованих продуктів, а єдина система. Агент на ноутбуці (FortiClient) спілкується з тією ж ОС, що і фаєрвол в офісі.

Вартість та ефективність (TCO): Fortinet традиційно пропонує найкраще співвідношення ціни та продуктивності. Ліцензійна модель проста і часто включає функції, за які інші вендори беруть додаткову плату.

Гнучкість розгортання: Як показує графік, Fortinet впевнено закріпився в лідерах. Рішення дозволяє легко будувати гібридні мережі, де частина трафіку йде через хмару, а частина обробляється локально на пристроях з ASIC-чіпами для максимальної швидкості.

Слабкі сторони:

Хмарна присутність: Хоча мережа Fortinet PoP швидко зростає, вона може бути менш щільною в деяких специфічних регіонах порівняно з величезною інфраструктурою Palo Alto або Netskope.

Сприйняття бренду: Деякі замовники все ще асоціюють Fortinet насамперед із "залізом", недооцінюючи їхні можливості в хмарній безпеці (SSE), хоча Gartner спростовує це їхнім положенням у квадранті.

Отже, після наданої стислої характеристики, за обраними критеріями проведемо порівняння обраних рішень.

Таблиця 1.1.

Порівняння лідерів SASE-рішень

Характеристика	Palo Alto Networks (Prisma)	Netskope (Netskope One)	Fortinet (FortiSASE)
Ключова філософія	Best-of-breed: Найкраща безпека за будь-яку ціну.	Data-centric: Безпека там, де ваші дані (в хмарі).	Convergence: Єдина ОС для мережі та безпеки.
Сильна сторона (Gartner)	Найвища здатність до виконання (Execution).	Найкраще стратегічне бачення (Vision).	Оптимальний баланс та швидке зростання.
Мережева частина (SD-WAN)	Потужна, але окрема (Prisma SD-WAN).	Інтегрована, але розвивається (Software-defined).	Вбудована в ядро системи (Secure SD-WAN).
Захист даних (DLP/CASB)	Дуже сильний, класичний підхід.	Лідер ринку, гранулярний контроль.	Ефективний, частина загальних політик.
Управління	Може вимагати кількох консолей.	Єдина хмарна консоль.	Єдина консоль (FortiManager/Cloud) для всього.
Складність впровадження	Висока, потребує сертифікованих інженерів.	Середня, легка для хмарних середовищ.	Низька для існуючих клієнтів Fortinet.
Ціновий сегмент	Високий (Premium).	Середній / Високий.	Найбільш конкурентний.

Аналіз "Магічного квадранта" та технічних можливостей дозволяє зробити чіткий вибір залежно від пріоритетів:

Якщо бюджет необмежений і головна мета — безкомпромісна безпека для глобальної корпорації, обирають Palo Alto Networks.

Якщо компанія повністю в хмарі (SaaS-first) і пріоритетом є захист даних та легкість для користувача — Netskope є фаворитом.

Fortinet (FortiSASE) є найбільш раціональним вибором ("золотою серединою") для більшості підприємств. Він забезпечує функціонал рівня Лідера Gartner, при цьому пропонує:

– Зниження витрат (найкращий TCO).
– Спрощення експлуатації (одна ОС).
– Безшовну інтеграцію для тих, хто вже має обладнання Fortinet.

Саме Fortinet виглядає як найкраще рішення для побудови уніфікованої, керованої та економічно.

.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ РОБОТИ ГІБРИДНИХ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ FORTISASE

2.1. Архітектура та основні функції рішення FortiSASE

Зі збільшенням кількості гібридних працівників організації повинні захищати своїх співробітників, тому що вони отримують доступ до мережі та додатків як з офісу, так і за його межами. Перехід на гібридну роботу, а саме з будь-якого місця (WFA-Work-From-Anywhere,) розширив поверхню атак, які включають домашні офіси і мобільних працівників. Це сприяло підвищення складності забезпечення ресурсів організацій [9].

Забезпечення безпеки в такому гібридному ландшафті стає серйозним випробуванням, оскільки трансформація інфраструктури часто відбувалася стихійно, без заздалегідь розробленої стратегії. Стрімке розширення меж мережі та інтеграція співробітників, що працюють у форматі WFA (Work From Anywhere), часто впроваджувалися як ізольовані ініціативи, що створило нові вразливості, якими активно користуються кіберзлочинці. Ця ситуація також призвела до суттєвого погіршення видимості дій користувачів, стану пристроїв та роботи додатків, що, у свою чергу, збільшує ризики та створює прогалини в системі захисту [9].

Архітектура служби безпечного доступу (SASE - Secure Access Service Edge) допомагає протистояти цим загрозам, забезпечуючи безпечний доступ і високопродуктивне з'єднання для користувачів у великих і малих філіях, а також у будь-якому віддаленому розташуванні. Однак багато рішень SASE вирішують лише частину проблеми [9].

SASE, скорочення від Secure Access Service Edge (Безпечний доступ до сервісу на межі) — це хмарна система безпеки, яка поєднує глобальні мережі (WAN) та служби мережевої безпеки в єдину, уніфіковану хмарну службу мережевої безпеки [10].

Рішення Fortinet Secure Access Service Edge (SASE) забезпечує безпечний доступ до Інтернету, хмари та додатків для гібридних працівників, одночасно спрощуючи операції. Воно поєднує SD-WAN з хмарним сервісом безпеки FortiSASE (SSE), що надається на периферії мережі, для розширення конвергенції мережевих та безпекових можливостей від межі мережі до віддалених користувачів [10].

Fortinet SASE надає комплексні рішення з кібербезпеки , пропонуючи всі основні функції SASE, включаючи найгнучкіші в галузі варіанти підключення, такі як точки доступу, комутатори, а також пристрої з агентами та без агентів, а також передові інтеграції зі штучним інтелектом. Ми включаємо уніфіковане управління, комплексний моніторинг цифрового досвіду (DEM) та послідовне забезпечення дотримання політик безпеки на основі принципів нульової довіри, як локально, так і в хмарі. Крім того, за допомогою Fortinet SASE ви можете адаптуватися до будь-якого середовища — локального, хмарного чи гібридного. Забезпечте безпечний веб-доступ для BYOD та підрядників, а також покращену видимість SD-WAN [10].

Глобальна мережа SASE від Fortinet охоплює понад 160 точок доступу (PoP), забезпечуючи низьку затримку та високу продуктивність з'єднання. Частина цієї мережі повністю належить Fortinet, що забезпечує кращий контроль, надійність та безпеку. Кожне хмарне розташування інтегрує безпеку FortiSASE локально, усуваючи необхідність зовнішньої маршрутизації трафіку для обробки безпеки. Fortinet також співпрацює з Google Cloud, щоб використовувати свою магістральну мережу PoP, використовуючи регіони Network Edge та Compute від Google для обходу перевантажень Інтернету та підвищення продуктивності. PoP постійно розширюються, щоб задовольнити зростаючий світовий попит на послуги SASE [10].

FortiSASE забезпечує вбудовану функціональність SD-WAN у кожній PoP, яка інтегрується з існуючими концентраторами FortiGate SD-WAN для безпечного приватного доступу (SPA). FortiSASE SPA забезпечує широкий та безперешкодний доступ до кожної приватної програми в середовищах приватних

центрів обробки даних, автоматично знаходячи найоптимальніший шлях до кожної критично важливої для бізнесу програми. Цю двонаправлену інтеграцію можна активувати менш ніж за п'ять хвилин, що забезпечує просте розгортання, постійний захист, оптимізацію продуктивності програм для віддалених користувачів та усунення несправностей IT [10].

Архітектура безпечного доступу до сервісів на межі мережі (SASE) стосується середовища кібербезпеки, яке забезпечує розширений захист аж до найвіддаленішого краю мережі: кінцевих точок користувачів. У цьому визначенні архітектури SASE користувачам надаються надійні функції безпеки безпосередньо на їхні пристрої з хмари, що дозволяє їм безпечно підключатися з будь-якого місця.

Діаграма архітектури SASE зовсім не схожа на традиційну структуру типу «hub and spoke» з центральним корпоративним центром обробки даних посередині. Ця структура вимагає зворотного зв'язку між даними від віддалених кінцевих точок та центром обробки даних, перш ніж вони потрапляють до потрібного місця призначення: хмари.

Архітектура мережі SASE, з іншого боку, забезпечує хмарну безпеку та дозволяє користувачам ноутбуків та інших мобільних пристроїв підключатися безпосередньо до хмари, насолоджуючись захистом, що працює безпосередньо на їхніх пристроях. Таким чином, архітектура безпеки SASE дозволяє користувачам користуватися перевагами безпечних з'єднань, не турбуючись про затримку, що виникає внаслідок зворотного зв'язку до брандмауера центру обробки даних.

Sovereign SASE – це фреймворк, який поєднує в собі розширену мережеву та хмарну безпеку з принципами суверенітету даних. Він дозволяє організаціям контролювати свої конфіденційні дані, дотримуючись регіональних правил щодо даних. Цей підхід особливо корисний для багатонаціональних компаній, які стикаються з постійно зростаючими загрозами кібербезпеці та складнощами у дотриманні вимог.

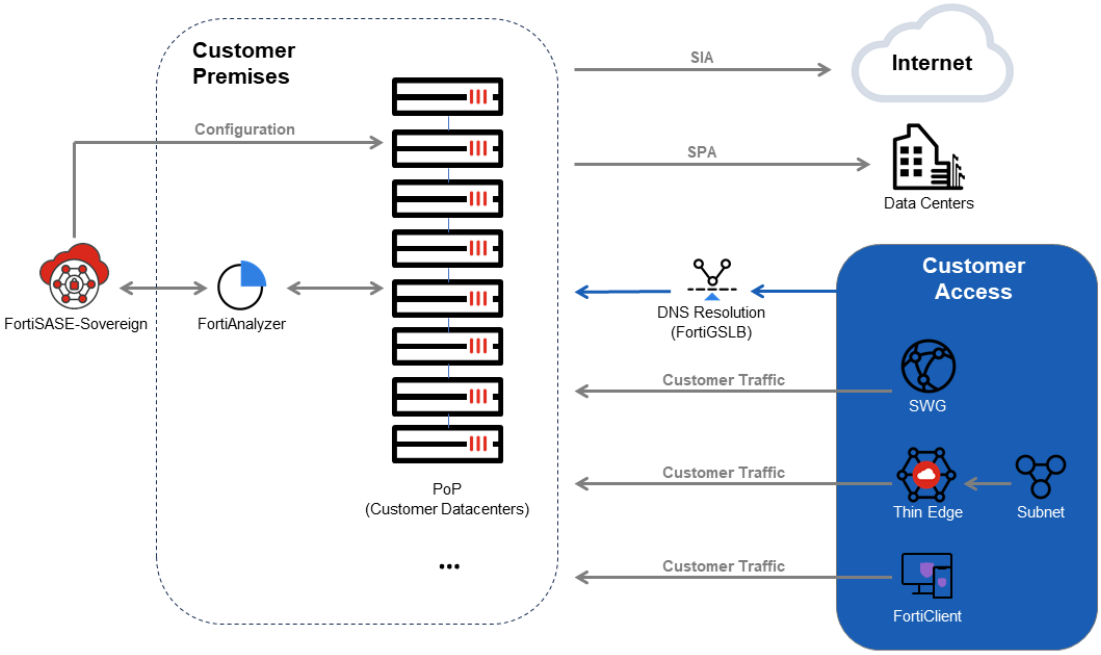


Рис.2.1. Архітектура FortiSASE

Як показано на рис 2.1, архітектура FortiSASE-Sovereign складається з таких компонентів:

– контролер;
– FortiAnalyzer;
– PoP FortiGate;
– доступ для клієнтів;
– контролер.

Серцем FortiSASE-Sovereign є контролер, який об'єднує FortiManager, FortiClient EMS та Zero Trust Network Access (ZTNA) для забезпечення централізованої безпеки, видимості та контролю над мережею. Контролер складається з таких компонентів:

1. Портал контролера — забезпечує зручний інтерфейс для керування конфігураціями, моніторингу стану безпеки та відображення ключової аналітики. Він забезпечує централізовану панель інструментів для легкого доступу до відповідної інформації.

2. FortiManager — служить головним центром керування, дозволяючи адміністраторам налаштовувати, контролювати та керувати пристроями Fortinet з єдиної платформи. Він спрощує застосування політик, налаштування пристроїв та оновлення прошивки, забезпечуючи безпечну та стабільну роботу мережі.

3. FortiClient EMS (сервер керування кінцевими точками) — розширює контроль над кінцевими точками, керуючи розгортанням, налаштуванням та моніторингом пристроїв FortiClient. Він забезпечує дотримання політик безпеки та забезпечує видимість стану пристроїв у режимі реального часу. Крім того, можливості ZTNA забезпечують суворий контроль доступу, гарантуючи, що до мережі можуть підключатися лише автентифіковані та відповідні пристрої.

4. FortiAnalyzer — це централізований інструмент для ведення журналу та аналітики, який аналізує дані безпеки, зібрані з пристроїв Fortinet.

5. PoP FortiGate. У конфігурації FortiSASE-Sovereign, FortiGate відіграє ключову роль у точці присутності безпеки (PoP). Ця конфігурація дозволяє підтримувати повний контроль над перевіркою безпеки та веденням журналу, забезпечуючи дотримання правил суверенітету даних, зберігаючи при цьому локалізований та надійний рівень безпеки.

Доступ для клієнтів

Доступ клієнтів означає безпечний та безперешкодний доступ кінцевих користувачів до внутрішніх та зовнішніх ресурсів. Він включає безпеку кінцевих точок, веб-фільтрацію та легкі периферійні рішення для забезпечення підвищеної безпеки та продуктивності.

– FortiClient — служить компонентом безпеки кінцевих точок, забезпечуючи безпечний доступ до корпоративних мереж через технології VPN, включаючи підключення SSL/IPsec VPN. Він гарантує віддаленим користувачам безпечний доступ до внутрішніх програм і ресурсів, незалежно від їхнього місцезнаходження.

– Безпечний веб-шлюз (SWG) — захищає кінцевих користувачів від веб-загроз, застосовуючи політики веб-фільтрації, блокуючи шкідливий контент і

блокуючи доступ до неавторизованих веб-сайтів. Він підвищує безпеку хмарних технологій, перевіряючи зашифрований трафік і пом'якшуючи фішингові атаки.

– Thin Edge — забезпечує легке рішення безпеки для віддалених офісів, невеликих філій та хмарних середовищ. Воно забезпечує базові функції безпеки, безпечне підключення та оптимізацію трафіку. Пропонує економічно ефективний спосіб розширення можливостей SASE на периферійні розташування.

FortiSASE-Sovereign пропонує комплексний набір функцій, розроблених для забезпечення безпечних, відповідних вимогам та ефективних послуг SASE.

На рис 2.1. наведено основні характеристики FortiSASE-Sovereign.

Рис.2.2. Характерстики FortiSASE

1. FortiSASE- пропонує повністю функціональне, готове до використання рішення з усіма необхідними компонентами для комплексного обслуговування SASE, яке включає Secure Web Gateway (SWG), Firewall as a Service (FWaaS) та Zero Trust Network Access (ZTNA) [11].

2. Повний операційний контроль над місцями розгортання, функціями SASE та інфраструктурою безпеки вашого FortiSASE . Це гарантує, що ви можете керувати власним середовищем та мати повний огляд його продуктивності [11].

3. FortiSASE забезпечує дотримання вами місцевих законів про місцезнаходження та конфіденційність даних, зберігаючи їх у визначених вами місцях. Ви маєте повний контроль над своїми даними та журналами, одночасно забезпечуючи конфіденційність та відповідність вимогам [11].

4. FortiSASE дозволяє налаштовувати політики безпеки та мережі відповідно до ваших місцевих норм та унікальних потреб бізнесу, що ще більше підвищує безпеку вашої мережі, відповідність нормативним вимогам та операційну ефективність [11].

5. FortiSAS пропонує простий та безперебійний процес розгортання завдяки найновішим пакетам обладнання та послуг захисту від загроз від Fortinet, що робить його економічно ефективним та швидким у впровадженні [11].

Ці функції роблять FortiSASE надійним SASE-рішенням для організацій, які прагнуть захистити свої дані, дотримуючись регіональних норм для гібриних працівників [11].

За допомогою FortiSASE віддалені користувачі (на основі агентів, без агентів та на основі сайтів) формують безпечні з'єднання з Інтернетом, центром обробки даних та хмарою, отримуючи доступ до глобальних точок присутності безпеки FortiSASE, які забезпечують дотримання політик безпеки організації незалежно від місцезнаходження віддалених користувачів. Нижче наведено приклади поширених випадків використання FortiSASE [11].

Таблиця 2.1.

Випадки використання FortiSASE

	Випадок використання	**Опис**
Безпечний доступ до Інтернету (SIA)	Агентний доступ віддаленого користувача до Інтернету	Безпечний доступ до Інтернету за допомогою агента FortiClient.
	Безагентний доступ віддаленого користувача до Інтернету	Безпечний доступ до Інтернету за допомогою безпечного веб-шлюзу FortiSASE-Sovereign .
	Віддалений доступ користувачів до Інтернету на базі сайту	Безпечний доступ до Інтернету за допомогою пристрою Thin Edge

		FortiExtender як розширення локальної мережі FortiSASE-Sovereign .
Безпечний приватний доступ	Приватний доступ до SD-WAN	Доступ до приватних корпоративних програм, розміщених за мережею FortiGate SD-WAN типу «hub-and-spoke», що розширює приватний доступ для програм на основі TCP та UDP та забезпечує резервування центру обробки даних.
	Приватний доступ до брандмауера наступного покоління (NGFW)	Доступ до приватних корпоративних програм, розміщених за FortiGate NGFW, що розширює приватний доступ для програм на основі UDP та віддалених користувачів без агентів.
SIA та SPA на базі сайту	Віддалені користувачі на базі сайту, що використовують FortiExtender/FortiGate/FortiAP як захищений граничний пункт	Безпечний доступ до Інтернету та приватних ресурсів за допомогою FortiExtender/FortiGate/FortiAP як розширення локальної мережі FortiSASE-Sovereign .

2.2. Основні компоненти загальної архітектури SASE

Архітектура Secure Access Service Edge (SASE) відноситься до середовища кібербезпеки, яке забезпечує розширений захист безпосередньо на найдальшій межі мережі: *кінцевих точках користувачів*. У цьому визначенні архітектури SASE користувачам надаються надійні функції безпеки безпосередньо на їхні пристрої з хмари, що дозволяє їм безпечно підключатися з будь-якого місця [8].

Архітектурна діаграма SASE не виглядає як традиційна мережа з центральним центром обробки даних посередині корпоративної мережі. Тому ця структура потребує зворотного зв’язку інформації від віддалених користуваччів або кінцевих точок до центру обробки даних, перш ніж надсилати їх до відповідного місця призначення, а саме у хмару.

Мережна архітектура SASE повинна забезпечити безпеку в хмарі та дозволити віддаленим користувачам, які мають ноутбуки та інші мобільні пристрої, підключатися безпосередньо до хмари, надаючи відповідну безпеку, яка буде працювати безпосередньо на їх кінцевих пристроях. Таким чином,

архітектура безпеки SASE дозволить віддаленим користувачам користуватися всіма перевагами захищених з’єднань, не вважаючи на затримку, яка є результатом зворотного зв’язку з брандмауером центру обробки даних [11].

Компоненти архітектури SASE

FortiSASE-Sovereign включає низку провідних у галузі, перевірених у дійсних умовах продуктів Fortinet, що забезпечують комплексне та безпечне рішення SASE. Нижче наведено його ключові компоненти:

Безпечний веб-шлюз (SWG) — захищає кінцевих користувачів від веб-загроз, фільтруючи та моніторячи веб-трафік [11].

Брандмауер як послуга (FWaaS) — надає можливості брандмауера як хмарний сервіс, забезпечуючи надійну безпеку мережі [11].

Zero Trust Network Access (ZTNA) — забезпечує суворий контроль доступу на основі ідентифікації користувача та стану пристрою, забезпечуючи безпечний доступ до програм [11].

Брокер безпеки доступу до хмари (CASB) — захищає хмарні програми та сервіси, забезпечуючи дотримання політик безпеки та прозорість використання хмари [11].

Ці компоненти працюють разом, щоб забезпечити надійне та гнучке рішення SASE, яке гарантує суверенітет даних та відповідність нормативним вимогам. Тому розглянемо їх біль детально.

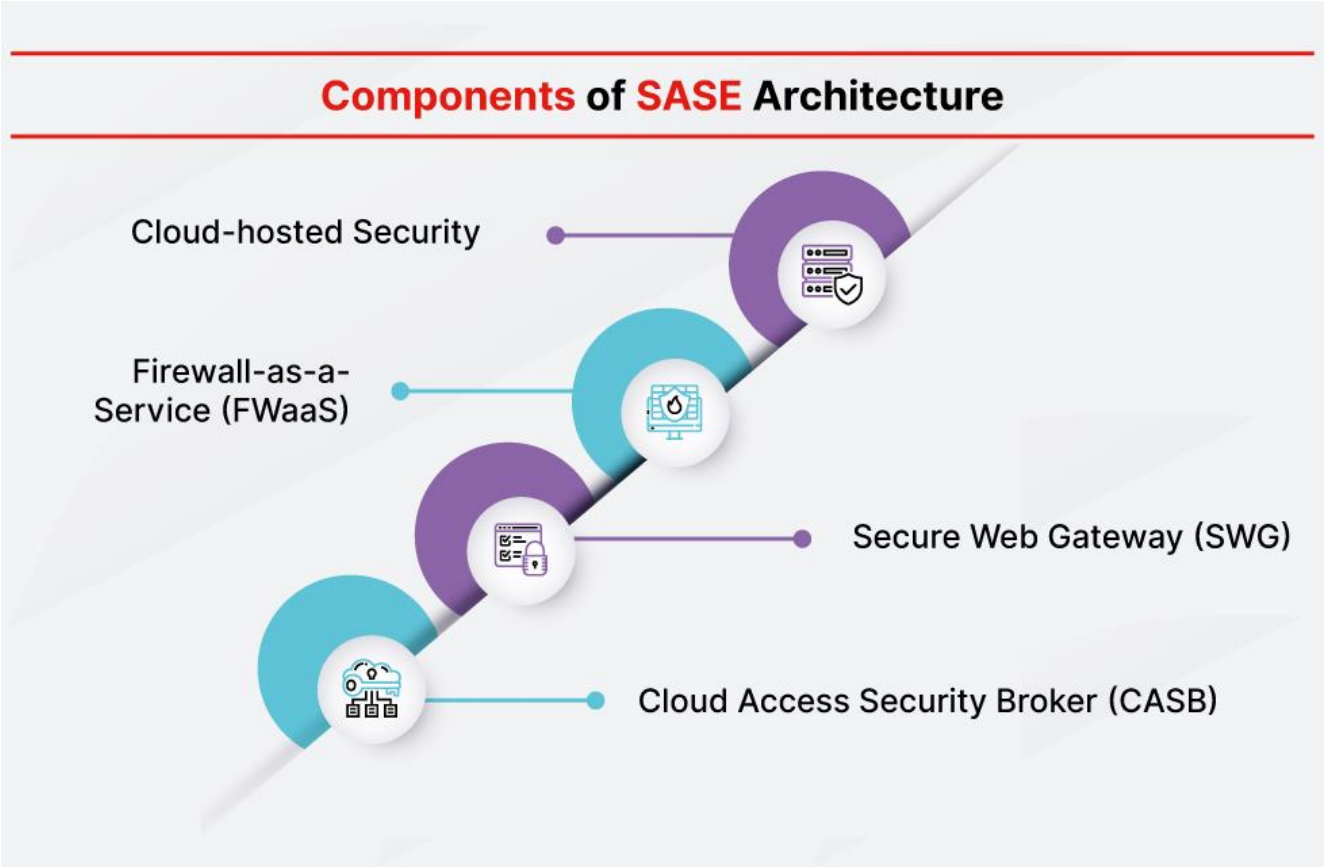


Рис. 2.3. Основні компоненти архітектури SASE [10]

Zero Trust Network Access (ZTNA)

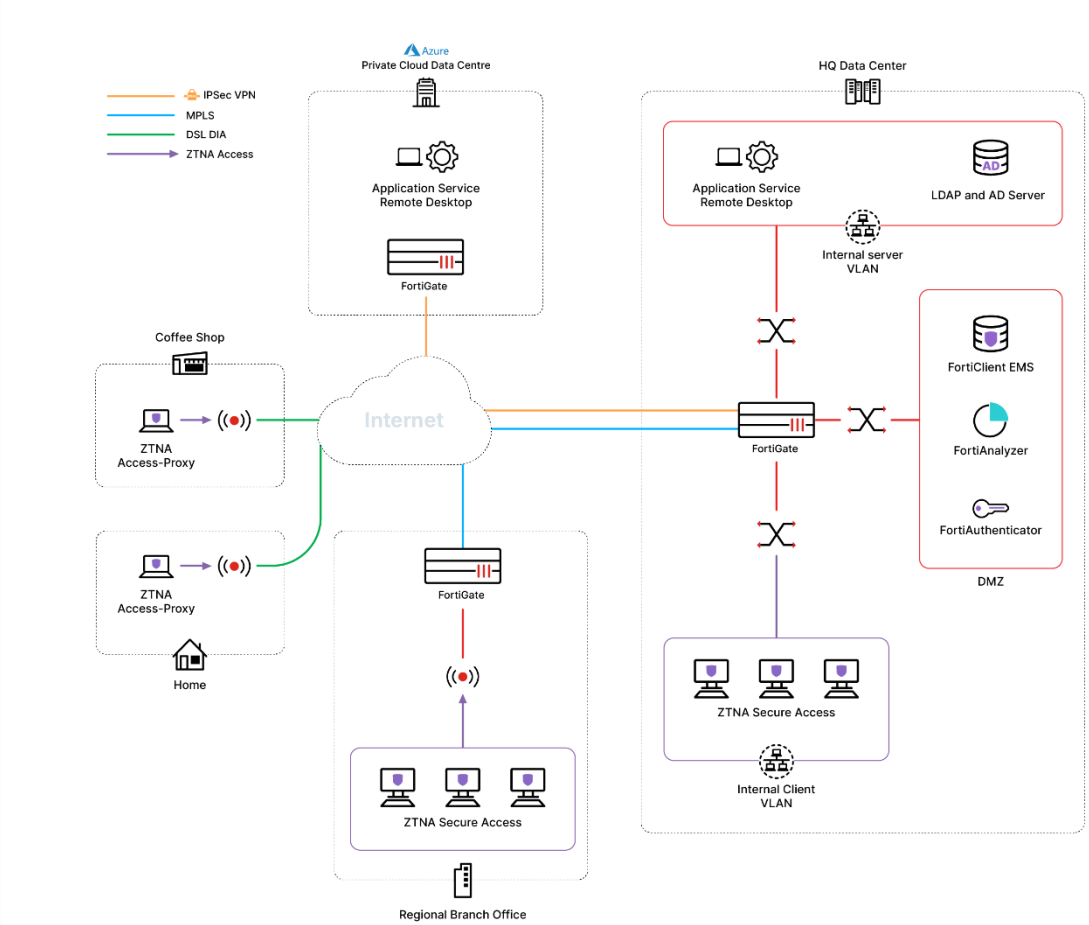
За допомогою проксі-сервера доступу ZTNA система формує безпечне з'єднання без використання dial-up VPN, і звужує поверхню доступу до певних програм, що зменшує поверхню атаки. У таблиці 2.2. наведено приклади поширених випадків використання ZTNA.

Таблиця 2.2.

Приклад використання ZTNA

Випадок використання	**Опис**
Проксі-сервер для доступу до веб-застосунків	Доступ до вебзастосунків через HTTPS за допомогою проксі-сервера доступу ZTNA
Проксі-сервер прямого доступу TCP (TFAP)	Доступ до інших програм за допомогою проксі-сервера прямого доступу ZTNA TCP
Ідентичність та позиція ZTNA	Використовуйте правила ZTNA для позначення кінцевих точок за допомогою телеметрії ідентифікації або положення
Інтеграція постачальників ідентифікаційних даних (IdP)	Інтеграція різних типів постачальників ідентифікаційних даних для використання з багатофакторною автентифікацією (MFA)

На рис.2.4 наведено приклад архітектури ZTNA



Згідно архітектури, незалежно від того, де знаходяться віддалені користувачі, вони можуть завжди безпечно отримувати доступ до внутрішніх ресурсів інформаційної системи організації за допомогою ZTNA без додаткових VPN-підключень. Проксі-сервер доступу FortiGate обав'язково перевірить ідентифікацію пристрів, ідентифікацію користувачів, стан пристрів, геолокацію, час і дозволи відповідних програм, перед тим як надати дозволи доступу, щоб забезпечити політики організації всередині та за межами корпоративної мережі [12].

Брандмауер як послуга (FWaaS). FWaaS забезпечує ті самі функції безпеки, що й стандартний апаратний брандмауер, але використовує програмне забезпечення в хмарі. Це особливо корисно при спробі забезпечити гнучкі, постійно змінювані програмно-визначені мережеві рішення (SD-WAN). Користувачам не потрібно підключатися до фізичного брандмауера. Натомість їхні передачі захищені програмним забезпеченням, розміщеним у хмарі, що

забезпечує їм безпеку незалежно від того, де вони знаходяться [10-12].

Безпечний веб-шлюз (SWG). Безпечний веб-шлюз (SWG), також відомий як безпечний Інтернет-шлюз (SIG), блокує неавторизований трафік від потрапляння в мережу вашої організації. Багато в чому SWG робить для корпоративної мережі запобігає - проникненню небажаних людей і даних [10-12].

В архітектурі Secure Access Service Edge SWG реалізовано для кожного окремого пристрою, підключеного до корпоративної мережі. Серед інших технологій SWG використовує інформацію системи доменних імен (DNS) для виявлення джерел небажаного трафіку [10-12].

Брокер безпеки доступу до хмари (CASB). CASB знаходиться між користувачем, який отримує доступ до хмари, і хмарною програмою, до якої він намагається отримати доступ. Він використовується для моніторингу діяльності та забезпечення дотримання політики безпеки організації [10-12].

Оптимізований вибір шляху включає забезпечення того, що шляхи різних типів трафіку спрямовуються до потрібних ресурсів у відповідний час. Рішення SD-WAN може вирішувати, куди йде мережевий трафік і як ним керувати, щоб забезпечити високу якість роботи для всіх користувачів[10-12].

SD-WAN- hub

У топології SASE «SD-WAN- hub» є центральною точкою підключення для пристроїв у корпоративному регіоні рис.2.4. У рішенні Fortinet Secure SD-WAN хаб виконує дві основні функції:

Міжсайтове з’єднання (IPsec-сервер) - зовнішні з’єднання від пристроїв до приватних ресурсів

Маршрутизація (селектори BGP та/або P2): Централізація маршрутизації та сприяння ADVPN-з'єднанням для трафіку між точками доступу

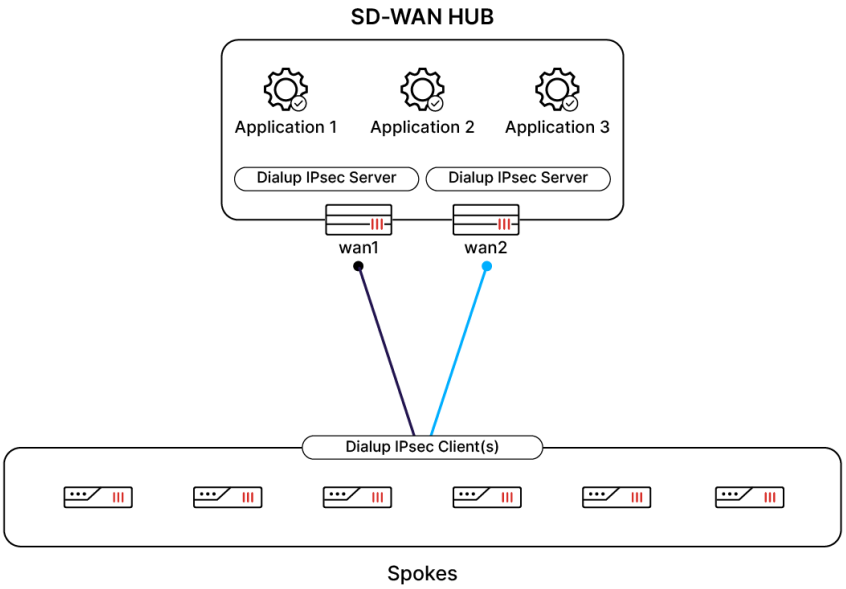


Рис.2.4. SD-WAN- hub

Концентратор SD-WAN традиційно розміщується поблизу приватних ресурсів або служб, до яких потрібен доступ з інших місць розташування. Приклади включають:

– Розташування основного центрального вузла (HQ);
– Центри обробки даних;
– Великі кампуси;
– Постачальники публічних хмарних послуг.

Отже, завдяки FortiSASE гібридні працівники отримують розширений захист доступу, який вони могли б отримувати з пристроєм який був підключений з середини організації.

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ ГІБРИДНИХ ПРАЦІВНИКІВ ДО КОРПОРАТИВНИХ ДОДАТКІВ

3.1. Варіанти архітектури FortiSASE для організацій

Розглянемо варіанти архітектури для організації, якій необхідно розширити периметр безпеки для віддалених користувачів для SIA, має кілька внутрішньо розміщених програм та використовує кілька SaaS-програм від різних постачальників.

У таблиці 3.1 проедставлено які цілі безпеки матиме організації та відповідне рішення SASE для кожної з цих цілей.

Таблиця 3.1.

Рішення SASE для цілей безпеки

Ціль безпеки	Рішення SASE
Забезпення безпечного доступ до Інтернету для віддалених користувачів з кінцевими точками, такими як робочі станції та мобільні пристрої.	Безпечний доступ до Інтернету для віддалених користувачів на основі агентів, що використовують FortiClient та FortiSASE-Sovereign FWaaS.
Забезпечення безпечний доступ до Інтернету для віддалених користувачів лише для веб-трафіку або для кінцевих точок на основі веббраузерів, таких як Chromebook.	Безпечний доступ до Інтернету для віддалених користувачів без агентів, що використовують явний веб-проксі у веббраузерах та службу FortiSASE-Sovereign SWG.
Забезпечити безпечний доступ до Інтернету для сайтів, що використовують пристрої з тонким клієнтом.	Безпечний доступ до Інтернету для віддалених користувачів на базі сайту, які використовують FortiExtender як розширення локальної мережі для FortiSASE-Sovereign .
Забезпечити безпечний доступ до Інтернету для сайтів, що використовують пристрій FortiGate, одночасно забезпечуючи безпечний приватний доступ до приватних ресурсів за FortiGate.	Безпечний доступ до Інтернету для віддалених користувачів на базі сайту, які використовують FortiGate як розширення локальної мережі для FortiSASE-Sovereign .
Контролюватипрямий доступ до внутрішніх мереж для програм на основі TCP, таких як веб-програми або віддалені робочі столи.	Безпечний приватний доступ за допомогою проксі-серверів доступу FortiGate ZTNA, FortiClient та служби керування кінцевими точками FortiSASE-Sovereign .
Забезпечте безперешкодний доступ до внутрішніх мереж за існуючими мережами FortiGate SD-WAN для програм на основі TCP та UDP.	Безпечний приватний доступ за допомогою SD-WAN.

Забезпечити безперешкодний доступ до внутрішніх мереж за нещодавно розгорнутим FortiGate NGFW для програм на основі TCP та UDP.	Безпечний приватний доступ за допомогою NGFW.

В кожному окремому випадку пропонується використання FortiSASE-Sovereign з відповідним проєктои і топологіям для цих цілей безпеки. Крім цього розуміти, що запропоновані окремі топології можна комбінувати, якщо варіанти використання FortiSASE-Sovereign комбінуються на основі цілей і вимог безпеки[10, 11] .

SIA для віддалених користувачів на основі агентів

Безпечний доступ до Інтернету (SIA) для віддалених користувачів на основі агентів є найтиповішим випадком використання, який включає встановлення та налаштування FortiClient на підтримуваних кінцевих точках, включаючи кінцеві точки Windows, macOS та Linux. У цьому випадку використання брандмауер як послуга FortiSASE-Sovereign (FWaaS) розміщується між кінцевою точкою та Інтернетом. Оскільки FortiClient по суті налаштовує повнотунельний SSL/IPSec VPN з FWaaS, SIA на основі агентів захищає весь інтернет-трафік та протоколи за допомогою політик VPN. Кожна кінцева точка підключається до точки присутності безпеки.

У цьому випадку можна досягти автентифікації користувачів, налаштувавши джерело автентифікації як Active Directory/LDAP або RADIUS, або як постачальника ідентифікації SAML.

Автоматизувати початкове налаштування кінцевих точок можна за допомогою інструмента керування мобільними пристроями (MDM). Розгортання кінцевим користувачем передбачає введення коду запрошення у FortiClient, а потім використання імені користувача та пароля для входу в тунель Secure Internet Access SSL/IPSec VPN до FortiSASE-Sovereign .

Типова топологія для розгортання цього прикладу показано на рис.3.1.

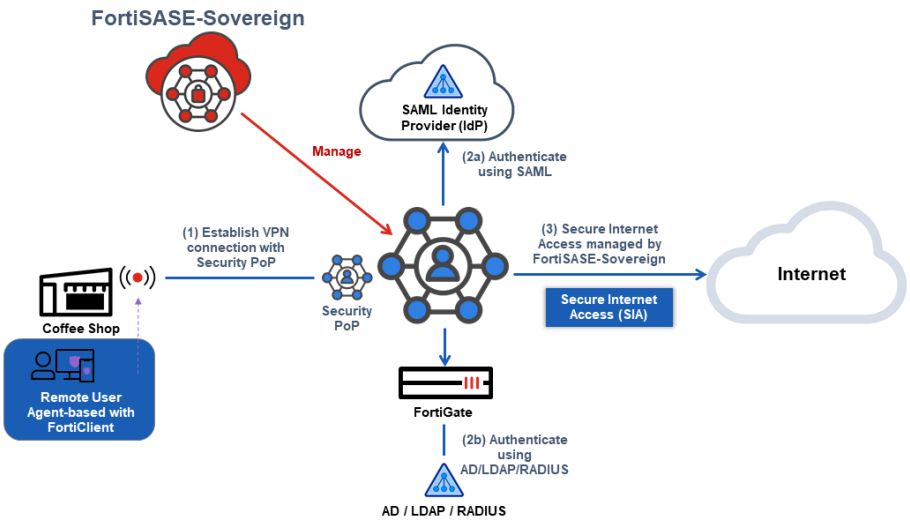


Рис.3.1. *SIA для віддалених користувачів на основі агентів*

SIA для віддалених користувачів без агентів

SIA для віддалених користувачів без агентів передбачає налаштування веб-браузера або пристрою на базі браузера з використанням файлу автоматичної конфігурації проксі-сервера (PAC) для використання служби FortiSASE-Sovereign SWG як явного веб-проксі. Веб-браузер перенаправлятиме HTTP- та HTTPS-трафік до SWG, що захищає веб-трафік користувача шляхом впровадження політик безпеки SWG. Весь інший невеб-трафік обійде FortiSASE-Sovereign і буде перенаправлено безпосередньо в Інтернет. У цьому випадку автентифікацію користувачів можна здійснити, налаштувавши джерело автентифікації як Active Directory/LDAP або RADIUS, або як постачальника ідентифікації SAML.

Початкове налаштування параметрів проксі-сервера для веббраузерів можна автоматизувати за допомогою об'єктів групової політики Windows (GPO) або Microsoft System Center Configuration Manager (SCCM).

На рис.3.2. показано топологію для розгортання цього прикладу.

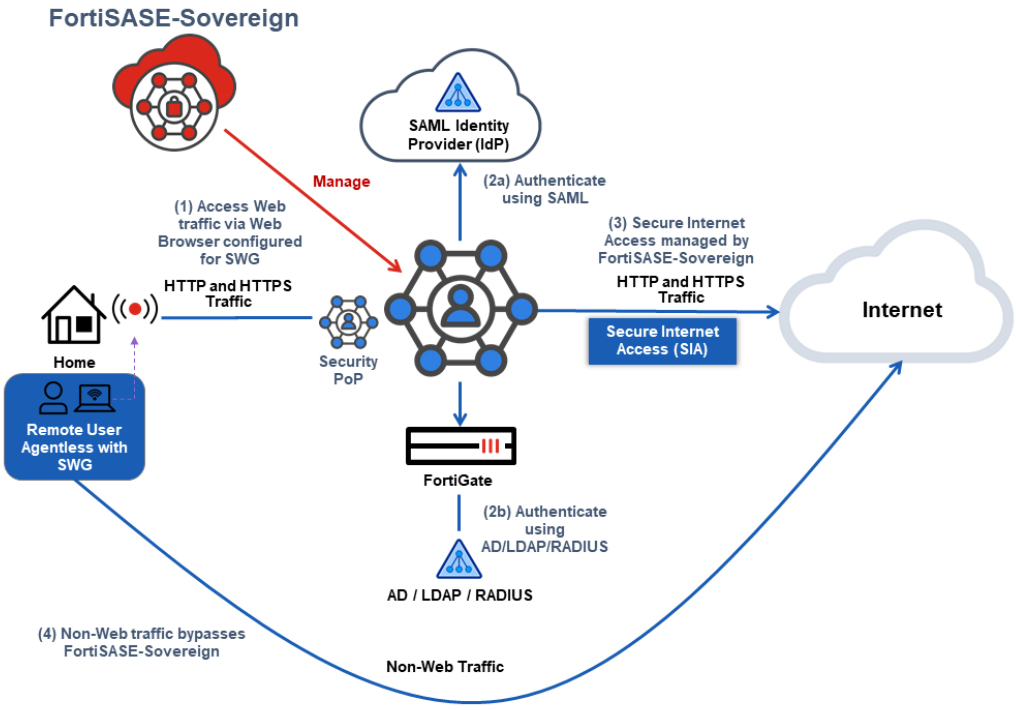


Рис.3.2. SIA для віддалених користувачів без агентів

SIA для віддалених користувачів на базі сайту, що використовують FortiExtender

SIA для віддалених користувачів на базі сайту передбачає налаштування FortiExtender як розширення локальної мережі шляхом створення тунелю VXLAN-over-IPsec між FortiExtender та FortiSASE-Sovereign . Це створює мережу другого рівня між FortiSASE-Sovereign та мережею за віддаленим FortiExtender.

У цьому випадку використання SIA, оскільки FortiExtender відповідає за централізацію підключення сайту до FortiSASE-Sovereign FWaaS, кінцеві точки потрібно налаштувати лише в їхніх IP-параметрах для переадресації трафіку на FortiExtender як шлюз за замовчуванням. Як результат, налаштування окремих робочих станцій або пристроїв мінімізується, оскільки FortiClient не потрібно встановлювати на кінцеві точки, а кінцеві точки на основі веб-браузера не потребують явного налаштування параметрів веб-проксі.

На рис.3.3. показано топологію для розгортання цього прикладу.

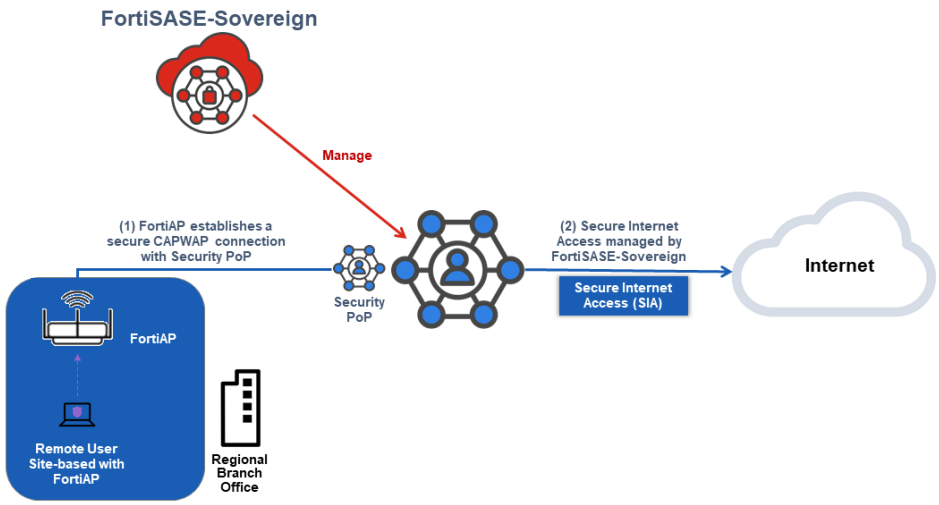


Рис.3.3. SIA для віддалених користувачів на базі сайту

Безпечний приватний доступ (SPA) за допомогою ZTNA

Віддалені користувачі на базі агентів FortiSASE-Sovereign можуть безпечно отримувати доступ до приватних ресурсів, а саме до програм на основі TCP, використовуючи ZTNA. Цей варіант використання пропонує прямий (найкоротший) шлях до приватних ресурсів та автентифікацію користувачів для кожного сеансу, що забезпечує вищу продуктивність та безпеку. ZTNA має такі вимоги:

FortiGate має бути розташований у центрі обробки даних центрального офісу організації (локально, у приватній хмарі або публічній хмарі) та налаштований як проксі-сервер доступу ZTNA, який контролює доступ до ресурсів за FortiGate.

Віддалені користувачі повинні бути агентами з встановленим FortiClient.

ZTNA вимагає, щоб FortiClient керувався службою керування кінцевими точками FortiSASE-Sovereign для виявлення інформації про пристрій кінцевої точки, реєстрації інформації про користувачів та стану безпеки, а також для запиту та отримання сертифіката клієнта від служби керування кінцевими точками FortiSASE-Sovereign . Служба керування кінцевими точками FortiSASE-Sovereign застосовує правила тегування ZTNA для позначення клієнтів. Потім FortiSASE-Sovereign надає доступ до тегів та даних сертифіката клієнта FortiGate.

Проксі-сервер доступу FortiGate ZTNA використовує сертифікат клієнта для перевірки особи клієнта та надає або забороняє доступ на основі тегів ZTNA клієнта.

У цьому випадку автентифікація користувачів досягається за рахунок налаштування джерела автентифікації як Active Directory/LDAP або RADIUS, або як постачальника ідентифікації SAML.

На рис.3.4. показано топологію для розгортання цього прикладу.

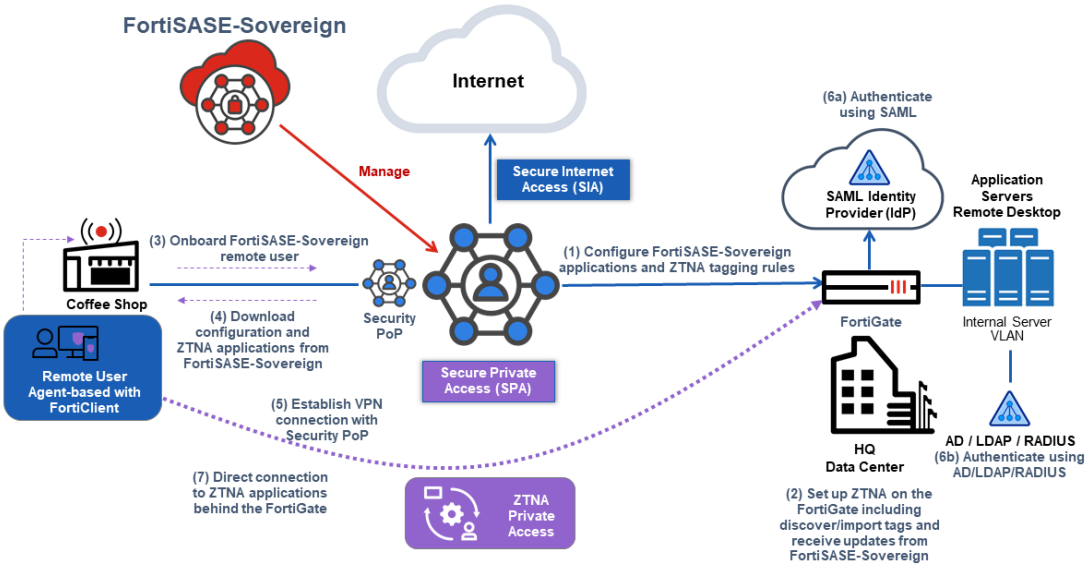


Рис.3.4. *Безпечний приватний доступ (SPA) за допомогою ZTNA*

SPA з використанням SD-WAN

Організації з існуючими розгортаннями FortiGate SD-WAN можуть надати своїм віддаленим користувачам доступ до приватних ресурсів за допомогою FortiSASE-Sovereign. Цей варіант використання пропонує ширший та безперешкодний доступ до приватно розміщених програм, як на основі TCP, так і UDP.

У випадку використання SD-WAN SPA, точки доступу до мережі Security PoP виконують роль ліній у мережі SD-WAN організації, спираючись на накладки IPsec VPN та BGP для захисту та маршрутизації трафіку між точками доступу та мережами, що знаходяться за концентраторами та спицями SD-WAN організації.

Існуючі розгортання мереж FortiGate SD-WAN відповідають найкращим практикам Fortinet щодо архітектури та розгортання SD-WAN для таких топологій:

SD-WAN з єдиним центром обробки даних/хабом

SD-WAN з двома центрами обробки даних/хабами

SD-WAN з підтримкою до чотирьох центрів обробки даних/хабів

Типова топологія для розгортання цього прикладу показано на рис.3.5.

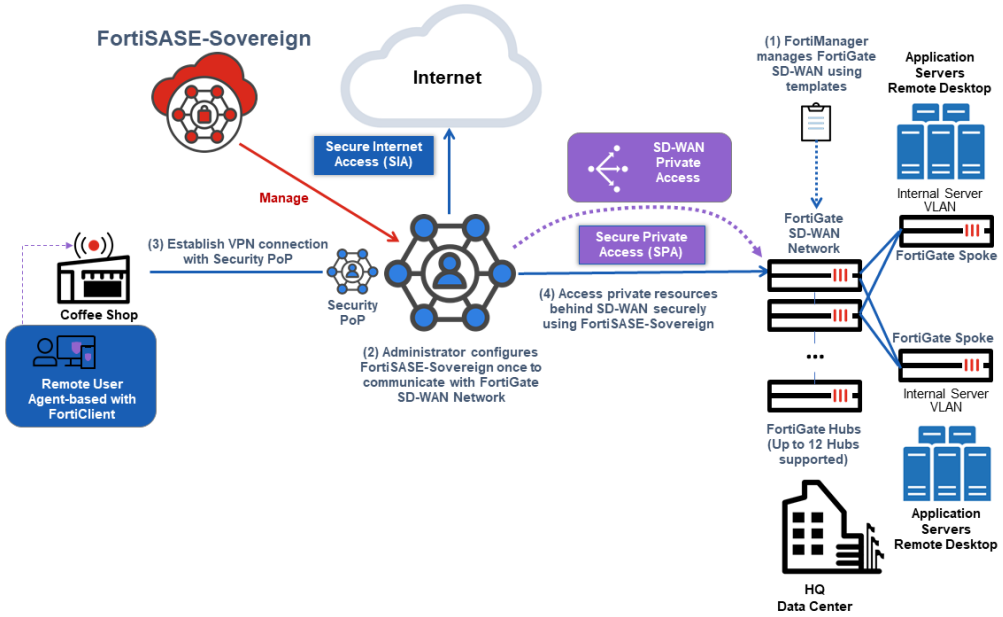


Рис.3.5. SPA з використанням SD-WAN

Точки доступу (PoP) безпеки FortiSASE-Sovereign та хаби FortiGate організації утворюють традиційну топологію типу «hub-and-spoke», яка підтримує конфігурацію автоматичного виявлення VPN Fortinet (ADVPN). ADVPN – це технологія IPsec, яка дозволяє лініям традиційної VPN типу «hub-and-spoke» встановлювати динамічні прямі тунелі на вимогу, відомі як скорочені тунелі, між собою, щоб уникнути маршрутизації через пристрій-хаб топології.

Віддалені користувачі FortiSASE-Sovereign можуть отримувати доступ до приватних ресурсів за концентратором(ами) FortiGate безпосередньо через тунелі IPsec FortiSASE-Sovereign. Якщо приватний ресурс знаходиться за пристроєм-

спонсором філії організації, вони можуть підключатися безпосередньо до цього ресурсу філії через прямий, динамічний тунель ADVPN на вимогу до спонсора філії. Таким чином, варіанти використання SPA з концентраторами FortiGate дозволяють ініціювати трафік лише від спонсорів PoP FortiSASE-Sovereign до спонсорів FortiGate філії організації.

Безпечний приватний доступ за допомогою NGFW

Організації, які вже розгорнули брандмауери наступного покоління FortiGate (NGFW), можуть надати своїм віддаленим користувачам, що використовують FortiSASE-Sovereign, доступ до приватних ресурсів. Цей варіант використання пропонує ширший та безперешкодний доступ до приватно розміщених програм, як на основі TCP, так і UDP.

У випадку використання NGFW SPA спочатку необхідно перетворити NGFW на окремий VPN-хаб IPsec, а точки присутності безпеки (PoP) виступатимуть як посередники для цього хаба, спираючись на оверлеї IPsec VPN та BGP для захисту та маршрутизації трафіку між PoP та мережами, що стоять за NGFW організації. Цей приклад проектування підтримує до чотирьох хабів.

Топологія для розгортання цього прикладу показано на рис.3.6.

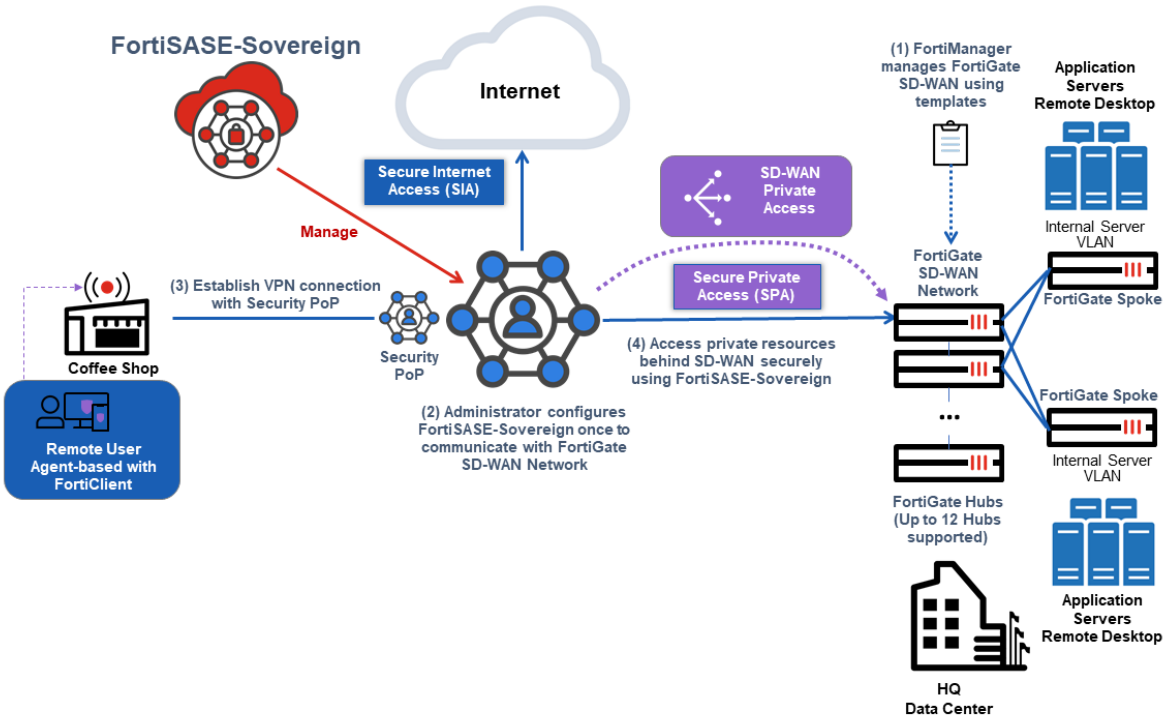


Рис.3.6. Безпечний приватний доступ за допомогою NGFW

Безпечний доступ до SaaS за допомогою FortiSASE-Sovereign Inline-CASB

FortiSASE-Sovereign пропонує функціональність брокера безпеки доступу Inline-cloud (Inline-CASB) для своїх компонентів контролю програм та безпеки веб-фільтрів, що вимагає використання глибокої перевірки SSL для забезпечення безпечного доступу до програмного забезпечення як послуги (SaaS) (SSA) для віддалених користувачів FortiSASE-Sovereign на основі агентів та без агентів.

Для випадку використання SSA, FortiSASE-Sovereign пропонує функціональність Inline-CASB для своїх компонентів контролю програм та безпеки веб-фільтрів, що вимагає глибокої перевірки SSL, щоб забезпечити безпечний доступ віддалених користувачів FortiSASE-Sovereign на основі агентів та без агентів до SaaS-застосунків.

FortiSASE-Sovereign використовує контроль додатків та глибоку перевірку SSL, щоб діяти як вбудований CASB, забезпечуючи контроль доступу до трафіку хмарних додатків SaaS. CASB розташовується між користувачами та їхнім хмарним сервісом для забезпечення дотримання політик безпеки під час доступу до хмарних ресурсів.

Крім того, FortiSASE-Sovereign використовує веб-фільтр та глибоку перевірку SSL з компонентом безпеки Inline-CASB для налаштування заголовків, коли віддалені користувачі без агентів (SWG) або на основі агентів (FortiClient) отримують доступ до SaaS-додатків. Після налаштування FortiSASE-Sovereign перехоплює HTTP-заголовки та може змінювати їх для вихідного трафіку, і цей процес також широко відомий як вставка HTTP-заголовків. Налаштовуючи HTTP-заголовки для вихідного трафіку FortiSASE-Sovereign , призначеного для SaaS-додатків, веб-фільтр з Inline-CASB може контролювати поведінку SaaS-додатків, обмежуючи доступ орендарів.

Компоненти контролю програм та веб-фільтрації вимагають глибокої перевірки SSL для виконання вбудованого сканування та виявлення вмісту в зашифрованих корисних навантаженнях.

Веб-фільтр FortiSASE-Sovereign з Inline-CASB та керування програмами FortiSASE-Sovereign з Inline-CASB не потребують жодних спеціальних ліцензій,

окрім ліцензування FortiSASE-Sovereign на користувача та кінцеву точку .

Топологія для розгортання цього прикладу показано на рис.3.7.

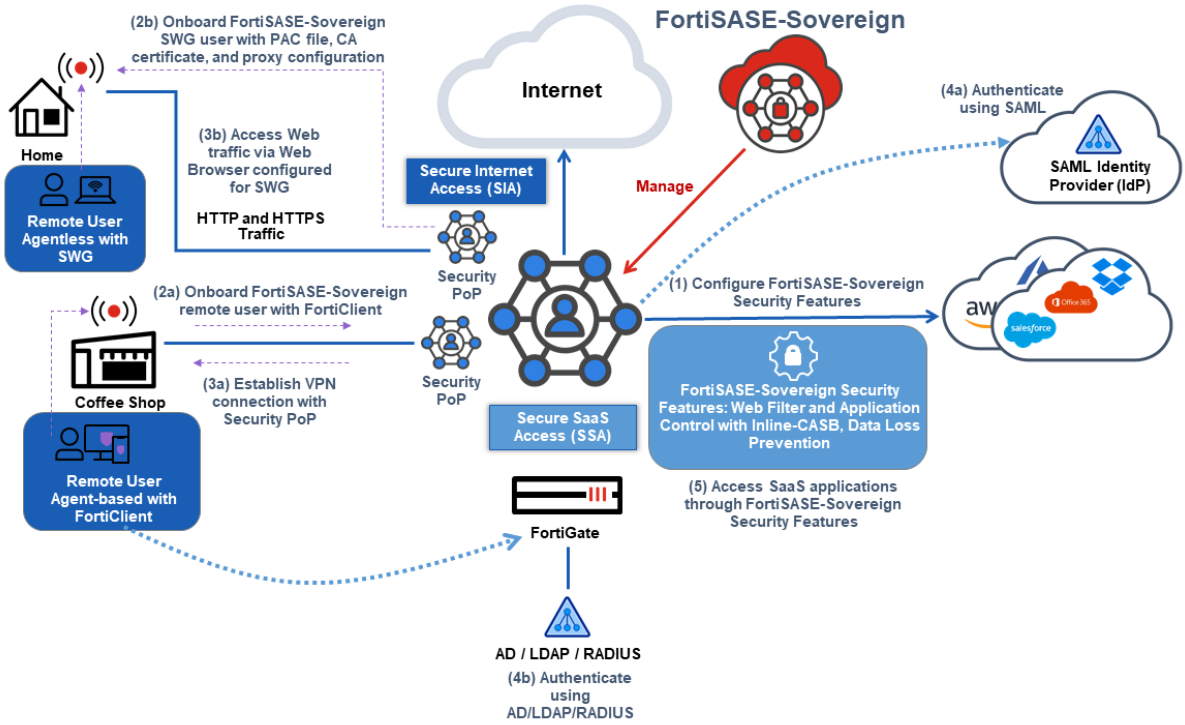


Рис.3.7. *Безпечний доступ до SaaS за допомогою FortiSASE-Sovereign Inline-CASB*

3.2. Технологія застосування FortiSASE для захисту гбридних користувачів організації

Технологія Fortinet Unified SASE забезпечує безперебійний та безпечний доступ з будь-якого місця завдяки захисту від загроз на основі штучного інтелекту, принципу нульової довіри та уніфікованим політикам безпеки. Він поєднує в собі розширений моніторинг SD-WAN та цифрового досвіду для спрощення управління, покращення взаємодії з користувачем та захисту даних.

Інтегроване рішення з наскрізною нульовою довірою та прозорістю об'єднує мережеві та безпекові функції в рамках однієї ОС, об'єднуючи агентів, всі дані, управління та політики для безперебійного захисту на всіх локаціях та пристроях гібридних користувачів.

Fortinet забезпечує гнучке підключення з безперешкодним доступом до

програм і даних з будь-якого місця, одночасно оптимізуючи продуктивність для віддалених та локальних користувачів. Гнучкі варіанти розгортання підтримують хмарні та локальні середовища, тонку периферію, будь-яку іншу периферію та будь-який пристрій.

Згідно розглянутих топологій, які залежать ві цілей безпеки розглянемо декілька технологій, які забезпечать захищений доступ до ресурсів організації гібридним працівникам, які є найбільш розповсюдженими і затребуваними.

Технологія безпечного доступу до Інтернету та SaaS

Fortinet Unified SASE захищає користувачів, які мають доступ до Інтернету та SaaS-додатків, за допомогою хмарних засобів безпеки, включаючи FWaaS, SWG, CASB та розширений DLP. Він забезпечує дотримання узгоджених політик та блокує загрози без перенаправлення трафіку до центрів обробки даних. Отже, технологія включає декілька засобів необхідних для організація для виконання безечного доступу до Інтернету та SAAS (рис. 3.8).

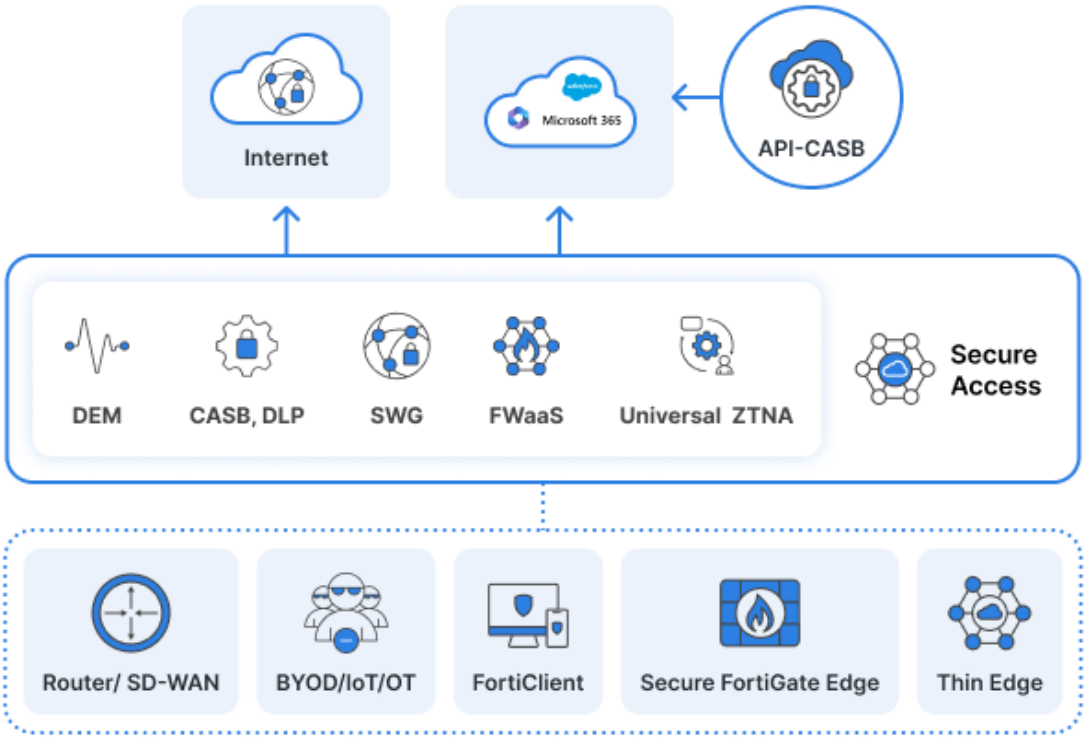


Рис.3.8. Технологія безпечного доступу до Інтернету та SaaS

Технологія приватного доступу до додатків без VPN

Така технологія усуває складність застарілих VPN за допомогою агентної або безагентної ZTNA. Уніфікована SASE забезпечує безпечний доступ до внутрішніх програм, застосовуючи політики на основі ідентифікації та контекстні елементи керування для підрядників, BYOD та віддалених співробітників (рис.3.9).

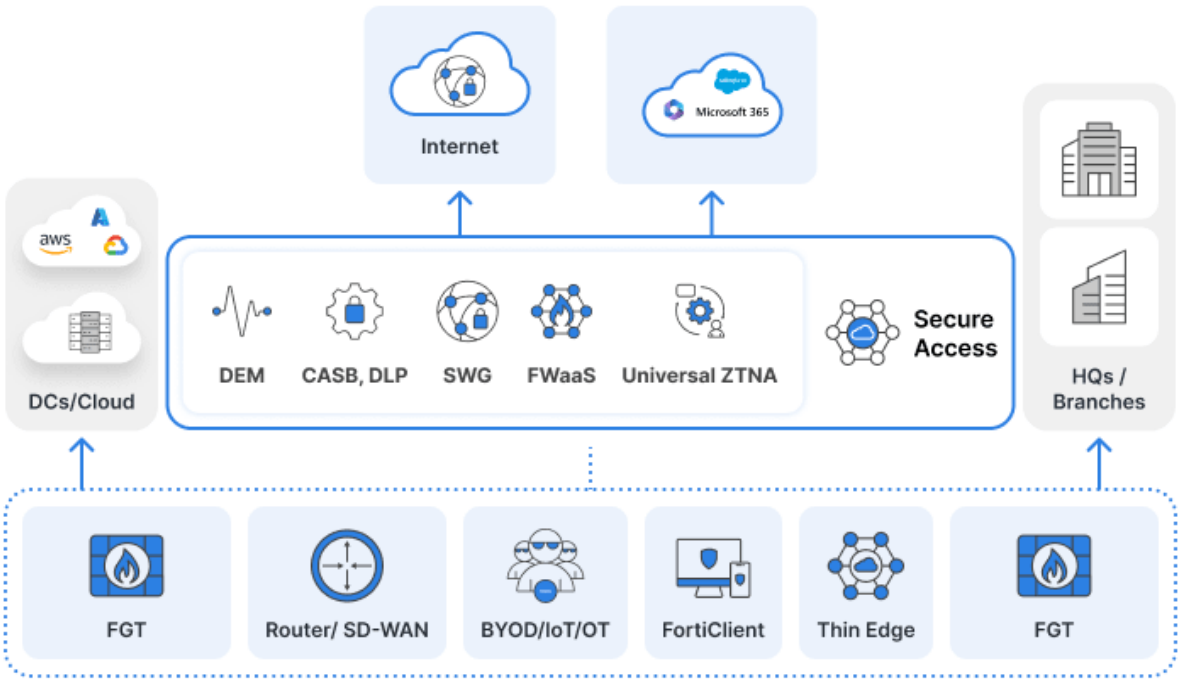


Рис.3.9. Технологія приватного доступу до додатків без VPN

Технологія адаптації та підключення філій організації

Технологія дозволяє швидко підключайте нові або віддалені філії за допомогою інтегрованих SD-WAN та SSE, а також можливостей тонких клієнтів периферії. Уніфікована SASE спрощує розгортання, забезпечує стабільну безпеку та оптимізовану продуктивність завдяки своїй глобальній магістралі та хмарній архітектурі.

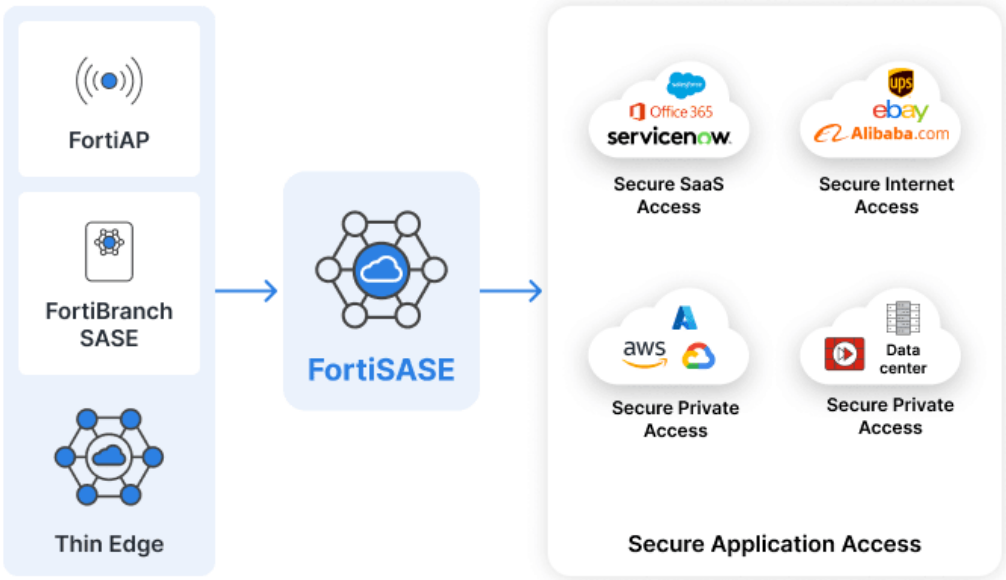


Рис.3.10. Технологія адаптації та підключення філій організації

Отже, Fortinet Unified SASE забезпечує безпечний доступ до Інтернету, хмари та додатків для гібридних працівників, одночасно спрощуючи операції. Воно поєднує безпечну SD-WAN (рис.3.11) з хмарним сервісом безпеки FortiSASE (SSE), що надається на периферії мережі, для розширення конвергенції мережевих та безпекових можливостей від периферії мережі до віддалених користувачів.

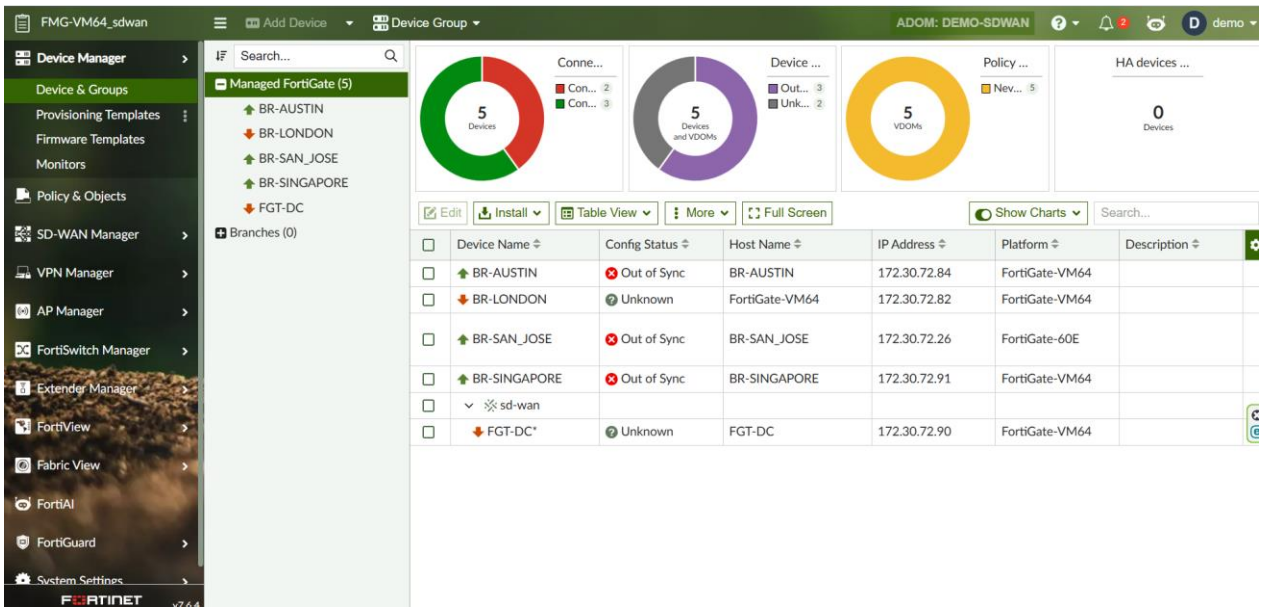


Рис.3.11. FortiSASE SD-WAN

FortiGate є основою Fortinet Security Fabric, яка дозволяє консолідувати інструменти безпеки в єдину систему управління SASE (3.12).

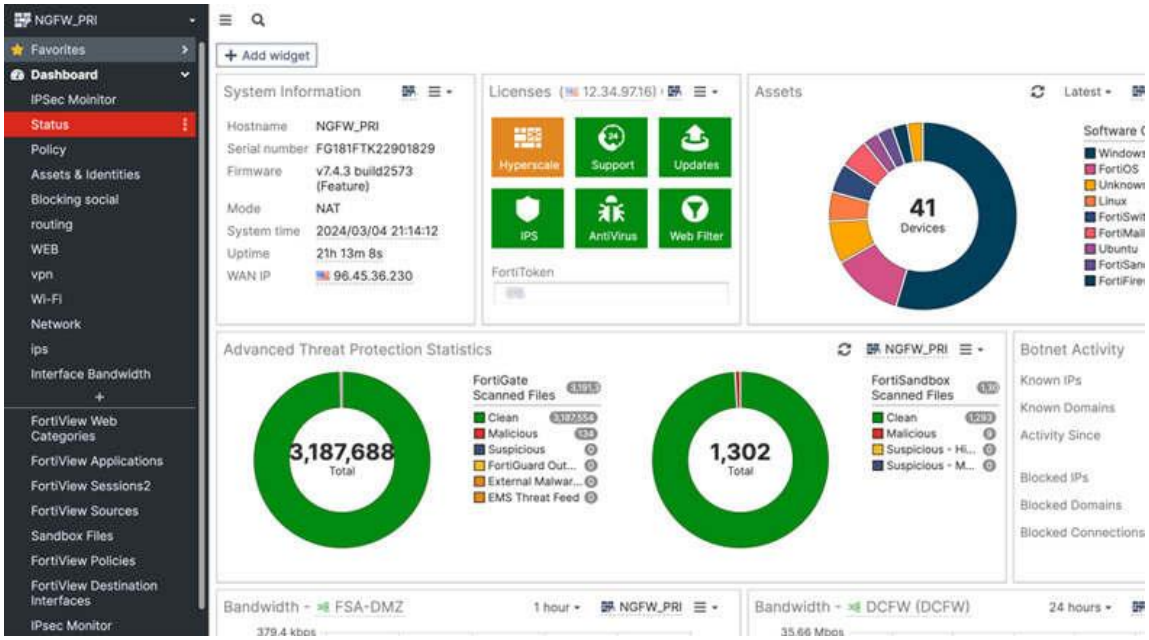


Рис.3.12. FortiGate

FortiGate забезпечує безпеку розгортань у філіях, кампусах, центрах обробки даних та хмарних системах будь-якого розміру.

FortiGate NGFW для забезпечення мережевої безпеки, впроваджуючи архітектуру нульової довіри та розгортаючи глобальну, безпечну SD-WAN.

Всі рішення легко інтегруються у платформу FortiSASE і дозволяють в залежності від вимог до гибридних працівників, надавати безпечний доступ до необхідних ресерсів.

3.3. Рекомендації щодо застосування технології безпечної роботи гібридних працівників організації

SASE є критично важливою для гібридної безпеки робочої сили. Тому рекомендації щодо захисту гібридних користувачі повинні включати наступне.

Безпечний доступ за принципом нульової довіри з будь-якого місця

Можливості ZTNA від SASE формують основу її підходу до безпеки на основі ідентифікації, дозволяючи користувачам безпечно та надійно підключатися до хмарних програм або отримувати доступ до внутрішніх ресурсів. ZTNA усуває

неявну довіру, тобто кожен користувач повинен підтвердити свою особу перед підключенням до корпоративних служб. Нульова довіра SASE забезпечує детальний та контекстуальний доступ на основі ідентифікації, стану пристрою, місцезнаходження та інших критичних факторів.

Користувачі повинні постійно автентифікувати себе, в ідеалі використовуючи більш надійні методи, такі як багатофакторна автентифікація, що обмежує ризик крадіжки облікових даних. Крім того, засоби контролю нульової довіри SASE мінімізують вплив горизонтального переміщення через сегментацію мережі та забезпечення автентифікації, коли користувачі намагаються отримати доступ до різних систем.

ZTNA сприяє переходу від мережевих периметрів до безпеки на основі ідентифікації, автентифікація користувачів і пристроїв, а також постійний моніторинг підозрілих запитів на доступ. Таке зміщення фокусу на те, як і де застосовуються ваші засоби контролю безпеки, є критично важливим для забезпечення гібридної робочої сили SASE та захисту від складних векторів атак.

Захист від нових загроз та вразливостей

Гібридні робочі сили збільшують поверхню для атак, створюючи набагато більше точок входу, які зловмисники можуть використати для отримання несанкціонованого доступу до корпоративних ресурсів. Вони також створюють операційні труднощі, ускладнюючи для команд безпеки захист усього вашого цифрового сліду та забезпечення правильного налаштування кожного пристрою, програми та хмарного сервісу.

Рішення SASE надаються в хмарі та оновлюються автоматично, що дозволяє організаціям швидше реагувати на нові загрози. Крім того, SASE спрощує управління мережею, полегшуючи виявлення потенційних вразливостей та неправильних конфігурацій. Розширена ідентифікація загроз, що забезпечується гібридними рішеннями SASE для робочої сили, базується на комплексній прозорості, яку вони забезпечують.

Комплексне управління видимістю SASE

Розподілені робочі сили значно ускладнюють моніторинг та управління

кінцевими точками та трафіком. Об'єднуючи засоби контролю та інструменти безпеки в єдине рішення, SASE централізує управління та аналітику, забезпечуючи глибокий огляд активності користувачів, мережевого трафіку, використання програм та інцидентів безпеки.

Ключовим прикладом управління видимістю SASE є ідентифікація тіньових IT. Інтегровані інструменти CASB забезпечують забезпечення безпечних політик використання SaaS та захищають ваші дані, коли вони залишають контрольовані мережі та пристрої.

Зібравши всі ці дані разом, ви можете отримати цілісне розуміння вашої мережі та краще виявляти потенційні загрози в режимі реального часу. Це включає гібридні рішення SASE для робочої сили, які поєднують найновішу аналітику загроз та сигнатури атак з аналітикою штучного інтелекту та машинного навчання для точного виявлення підозрілої поведінки.

Узгоджені політики безпеки в різних середовищах

SASE дозволяє застосовувати єдині політики в локальних, віддалених та хмарних середовищах, зменшуючи ймовірність прогалин у безпеці, мінімізуючи неправильні конфігурації та забезпечуючи дотримання співробітниками найкращих практик. Хмарне рішення, яке охоплює кожен периметр, політики SASE застосовуються на точках підключення, забезпечуючи захист користувача, а не чекаючи, поки трафік пройде певний периметр мережі.

Узгоджені політики дозволяють розширити внутрішні засоби контролю безпеки на хмару та віддалених користувачів, отримуючи доступ до масштабованості та гнучкості хмари, одночасно сприяючи гібридній робочій силі. Наприклад, оскільки конфіденційні бізнес-дані переміщуються між пристроями, мережами та хмарними сервісами, SASE дозволяє вам застосовувати узгоджені політики запобігання втраті даних (DLP), які визначають засоби контролю доступу та стандарти шифрування.

Запобігання загрозам у великих масштабах

Кількість кібератак, спрямованих на організації, продовжує зростати. Дані за другий квартал 2025 року показали, що кількість атак зросла на 21% порівняно

з 2024 роком і на 58% порівняно з аналогічним періодом 2023 року. Гібридні працівники наражають вас на низку загроз поза традиційним периметром безпеки. Однак, за допомогою хмарного рішення SASE ви можете впровадити масштабоване, багаторівневе виявлення та запобігання загрозам, побудоване на низці передових технологій безпеки.

Причини, чому SASE є критично важливим для гібридної безпеки робочої сили, демонструють його можливості у захисті віддалених користувачів та ресурсів, до яких вони отримують доступ.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було проведено комплексне дослідження проблеми та методів забезпечення безпечної роботи гібридних працівників організації. На основі аналізу отримано наступні висновки:

Встановлено, що перехід до гібридної моделі роботи (WFA) став домінуючим трендом, проте він значно розширив поверхню кібератак. Основними загрозами для організацій у 2024–2025 роках залишаються програми-вимагачі, фішинг та незахищені канали передачі даних. Статистика свідчить про необхідність переходу від традиційного захисту периметра до концепції, орієнтованої на ідентичність.

Проаналізовано сучасні методи захисту, серед яких ключовими є принципи нульової довіри (Zero Trust), багатофакторна автентифікація (MFA) та шифрування даних. Визначено, що найбільш ефективною стратегією для комплексного вирішення проблем гібридної роботи є архітектура SASE (Secure Access Service Edge), яка об'єднує мережеві функції (SD-WAN) та функції безпеки (SSE) у єдину хмарну платформу.

Проведено порівняльний аналіз провідних рішень на ринку SASE (Palo Alto Networks, Netskope, Fortinet). Обґрунтовано вибір платформи Fortinet (FortiSASE) як найбільш раціонального рішення для більшості підприємств. Основними аргументами стали: єдина операційна система (FortiOS) для всіх компонентів, конвергенція мережі та безпеки, найкращий показник сукупної вартості володіння (TCO) та простота масштабування для існуючих клієнтів.

Детально розглянуто архітектуру FortiSASE, яка включає компоненти Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS) та Zero Trust Network Access (ZTNA). Ця архітектура дозволяє забезпечити захист користувачів незалежно від їхнього місцезнаходження без необхідності маршрутизації трафіку через центральний дата-центр, що покращує продуктивність роботи.

Розроблено та описано типові топології, які лежать в основі технології

безпечного доступу гібридних користувачів для забезпечення безпечного доступу в різних сценаріях:

Secure Internet Access (SIA): для захисту доступу до Інтернету (агентний та безагентний методи).

Secure Private Access (SPA): для доступу до корпоративних ресурсів через ZTNA або SD-WAN.

SaaS Access: з використанням Inline-CASB для контролю хмарних додатків.

Сформульовано практичні рекомендації щодо впровадження технології, які включають перехід на модель нульової довіри (ZTNA) замість традиційних VPN, забезпечення повної видимості трафіку та застосування узгоджених політик безпеки для всіх типів підключень. Впровадження запропонованої технології для досягнення різних цілей безпеки дозволить організаціям мінімізувати ризики витоку даних, знизити операційні витрати та підвищити ефективність роботи гібридних команд.

ПЕРЕЛІК ПОСИЛАНЬ

1. Hybrid Work: Navigating Security Challenges in the Modern Enterprise [Electronic resource] // Cloud Security Alliance. – 2025. – Режим доступу: https://cloudsecurityalliance.org/blog/2025/03/24/hybrid-work-navigating-security-challenges-in-the-modern-enterprise (дата звернення: 30.11.2025).

2. Hybrid Work in 2025: The Symbiosis of Technology and Human Capital in the Digital Transformation Era [Electronic resource] // Albi Marketing. – Режим доступу: https://albimarketing.com/blog/hybrid-work-in-2025-the-symbiosis-of-technology-and-human-capital-in-the-digital-transformation-era/ (дата звернення: 01.12.2025).

3. Hybrid Work Strategies: Navigating the Future of Employee Engagement in 2025 [Electronic resource] // Metrigy. – Режим доступу: https://metrigy.com/hybrid-work-strategies-navigating-the-future-of-employee-engagement-in-2025/ (дата звернення: 01.12.2025).

4. Hybrid Work Statistics [Electronic resource] // Zoom Blog. – Режим доступу: https://www.zoom.com/en/blog/hybrid-work-statistics/ (дата звернення: 30.11.2025).

5. 2025 Ransomware Trends and Proactive Strategies [Electronic resource] : Report / Veeam Software. – 2025. – 18 p. – (Veeam Insights).

6. Miller L. Single-Vendor SASE For Dummies. Fortinet Special Edition [Electronic resource] / Lawrence Miller. – Hoboken : John Wiley & Sons, Inc., 2023. – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/ebook/single-vendor-sase-for-dummies.pdf (дата звернення: 05.12.2025).

7. 2025 Global Networking Trends Report [Electronic resource] // Cisco. – 2023. – Режим доступу: https://www.cisco.com/c/en_uk/solutions/enterprise-networks/xa-09-2023-networking-report.html (дата звернення: 26.11.2025).

8. Gartner Magic Quadrant for SASE Platforms [Electronic resource] // Gartner. – Режим доступу: https://www.gartner.com/en/documents/6701734 (дата звернення: 10.12.2025).

9. Secure Your Hybrid Workforce with Fortinet Unified SASE [Electronic resource] : Solution Guide // Fortinet. – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortisase-cloud-delivered-securtiy-to-every-user.pdf (дата звернення: 11.12.2025).

10. Architecture [Electronic resource] // FortiSASE Sovereign Documentation. – Режим доступу: https://docs.fortinet.com/document/fortisase-sovereign/latest/architecture-guide/861420/architecture (дата звернення: 06.12.2025).

11. FortiSASE Sovereign Architecture Guide [Electronic resource] // Fortinet Documentation Library. – Режим доступу: https://docs.fortinet.com/document/fortisase-sovereign/latest/architecture-guide/861420/architecture (дата звернення: 12.12.2025).

12. What is ZTNA architecture? [Electronic resource] // FortiGate / FortiOS 7.0.0 Documentation. – Режим доступу: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-architecture/800134/what-is-ztna-architecture (дата звернення: 12.12.2025).

13. SD-WAN & SD-Branch Concept Guide: Introduction [Electronic resource] // FortiGate / FortiOS 7.0.0 Documentation. – Режим доступу: https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-sd-branch-concept-guide/336354/introduction (дата звернення: 12.12.2025).

14. A comprehensive SASE solution to secure the hybrid workforce [Electronic resource] // Fortinet Solutions. – Режим доступу: https://www.fortinet.com/solutions/unified-sase (дата звернення: 12.12.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)