

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія забезпечення безпеки інформаційних ресурсів організації на
основі рішень SASE»**

зі спеціальності

F5 Кібербезпека та захист інформації

(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*

Ілля ОПАЛЬКО

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62

ОПАЛЬКО Ілля

(прізвище, ім'я)

Керівник

к.т.н., доц. БОРСУКОВСЬКИЙ Юрій

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2026

ВСТУП

Актуальність дослідження. Сучасні організації функціонують у умовах розподілених інформаційних систем, віддаленого доступу співробітників, інтеграції локальної інфраструктури з хмарними сервісами та SaaS-рішеннями. Інформаційні ресурси при цьому розміщуються одночасно у власних дата-центрах, хмарних середовищах і на кінцевих пристроях користувачів, що ускладнює їхній захист традиційними засобами. Периметрові моделі безпеки, орієнтовані на статичний кордон мережі, виявляються недостатніми для середовищ, де користувачі, пристрої та сервіси постійно змінюють місце розташування, а значна частина трафіку рухається поза межами класичного периметра. Зростання кількості атак на корпоративні сервіси, витоків даних і випадків несанкціонованого використання хмарних ресурсів висуває на перший план завдання побудови цілісної технології захисту інформаційних ресурсів, яка враховує розподілений характер сучасних IT-інфраструктур.

У цьому контексті актуальності набувають рішення класу SASE (Secure Access Service Edge), що поєднують мережеві функції з хмарними сервісами безпеки та принципами Zero Trust. Такі платформи забезпечують інлайн-контроль трафіку, застосування єдиних політик доступу та захисту даних для внутрішніх і хмарних ресурсів, а також контекстно-орієнтоване керування доступом на основі атрибутів користувача, пристрою та застосунку. Використання SASE дає змогу перейти від фрагментованого набору локальних засобів захисту до єдиного керованого контуру, що охоплює основні інформаційні потоки організації. Тому дослідження технології забезпечення безпеки інформаційних ресурсів організації на основі рішень SASE є актуальним як з теоретичної, так і з практичної точки зору.

Об'єкт дослідження – процес забезпечення безпеки інформаційних ресурсів організації.

Предмет дослідження – технологія виявлення та забезпечення безпеки інформаційних ресурсів організації.

Мета роботи – розробити варіант застосування технологій забезпечення безпеки інформаційних ресурсів організації.

Наукові завдання:

проаналізувати основні загрози та вразливості інформаційних ресурсів в умовах використання локальних, хмарних і гібридних інфраструктур;

узагальнити підходи та засоби забезпечення безпеки інформаційних ресурсів, визначити їхні обмеження для розподілених середовищ доступу;

дослідити архітектуру та ключові компоненти рішень SASE (SWG, CASB, ZTNA, FWaaS, DLP) у контексті захисту інформаційних ресурсів;

проаналізувати можливості платформи SASE (на прикладі рішення Netskope SASE) для побудови єдиного контуру захисту інформаційних ресурсів організації;

сформувати технологію забезпечення безпеки інформаційних ресурсів організації на основі SASE та розробити практичні рекомендації щодо її впровадження.

Методи дослідження – опрацювання наукової та технічної літератури, аналіз сучасних рішень на ринку засобів захисту інформаційних ресурсів та хмарних сервісів, порівняння підходів до виявлення загроз і контролю доступу в розподілених та хмарних середовищах, узагальнення результатів аналізу для побудови цілісної технології захисту.

Практичне значення одержаних результатів: запропоновано варіант застосування технології забезпечення безпеки інформаційних ресурсів організації на основі платформи SASE, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

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 ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ

1.1. Визначення інформаційних ресурсів організації

Інформаційні ресурси організації в контексті кібербезпеки та захисту інформації доцільно визначати як сукупність структурованих і неструктурованих даних, документів, записів і знань, зафіксованих на матеріальних або електронних носіях, що створюються, обробляються, зберігаються, передаються чи знищуються в межах діяльності організації та мають цінність для досягнення її цілей. До цієї сукупності належать не лише власне дані, а й пов'язані з ними метадані, журнали подій, резервні копії, моделі й алгоритми, конфігурації систем, ділова переписка, договірна документація, а також знання персоналу, формалізовані у вигляді процедур, інструкцій і баз знань. Відмінність між «даними» та «інформаційними ресурсами» полягає в управлінському вимірі: ресурс передбачає власника, вартість, правила доступу, життєвий цикл і відповідальність.

У кібербезпеці інформаційні ресурси розглядаються як активи, що підлягають класифікації за чутливістю та критичністю, з подальшим призначенням власників і адміністраторів, визначенням прав доступу, вимог до зберігання, резервування, знищення або анонімізації. Таке трактування вбудовується у системи управління безпекою інформації та приватністю, де ресурси пов'язуються з процесами, технологіями та людьми. Основні властивості, що підлягають захисту, охоплюють конфіденційність, цілісність і доступність, а також автентичність, цілісність джерела, невідомість, підзвітність, приватність і мінімізацію даних. Для кожного ресурсу визначається прийнятний рівень ризику та механізми контролю: політики і процедури, технічні засоби (ідентифікація та автентифікація, керування доступом, шифрування, сегментація мережі, журналювання й моніторинг, DLP та аналітика), організаційні заходи (навчання, поділ обов'язків, перевірки постачальників) і фізичний захист.

Життєвий цикл інформаційного ресурсу включає етапи створення або надходження, класифікації й маркування, зберігання та використання, передачі, архівування й знищення. На кожному етапі діють специфічні ризики: при створенні — помилки й надмірний збір; при зберіганні — несанкціонований доступ і корупція даних; під час передачі — перехоплення й модифікація; на етапі архівування — деградація носіїв і порушення режимів зберігання; при знищенні — залишкові сліди. Відповідно, проєктуються контрольні заходи: мінімізація, контроль версій, криптографічний захист у спокої та в транзиті, протидія втратам даних, журнали незаперечності, перевірювані процедури видалення з підтвердженням.

Особливе місце займають операційні та безпекові журнали, телеметрія і сповіщення, що самі є інформаційними ресурсами підвищеної чутливості: вони містять артефакти автентифікації, контент запитів, службові ключі та можуть розкривати структуру мережі чи бізнес-процесів. До складу ресурсів входять і дані, що обробляються зовнішніми провайдерами: хмарні сховища, SaaS-платформи, канали інтеграції з партнерами. У цих випадках захист забезпечується поєднанням договірних зобов'язань, технічних контролів провайдера, механізмів шифрування з управлінням ключами на боці організації, а також періодичними аудитами, тестуванням і безперервним моніторингом.

Важливо розрізняти власність, опіку та зобов'язання щодо ресурсів. Власник визначає цінність і правила доступу, опікун (кастодіан) забезпечує їх технічну реалізацію, а користувачі дотримуються встановлених обмежень. Для регульованих категорій даних (персональні, комерційна таємниця, критична інфраструктура) застосовуються додаткові вимоги щодо локалізації, строків зберігання, повідомлення про інциденти і прав суб'єктів даних. Усе це фіксується в реєстрі активів із прив'язкою до бізнес-процесів, класифікаційних рівнів і контрольних заходів, що дає можливість проводити оцінку ризиків, планувати безперервність діяльності та бюджетувати заходи безпеки [1].

Таким чином, «інформаційні ресурси організації» — це не просто масиви даних, а керована система знань і носіїв, на які поширюються політики, ролі, метрики, контрольні заходи та відповідальність. Їх коректне визначення й

інвентаризація є відправною точкою для побудови ефективної системи кіберзахисту: від архітектури доступу та шифрування до моніторингу подій і реагування на інциденти, забезпечуючи відтворюваність процесів, відповідність вимогам і стійкість організації до сучасних загроз.

1.2. Аналіз основних загроз та вразливостей інформаційних систем

Сучасні глобалізаційні процеси, що супроводжуються інформатизацією, неминуче зумовлюють розширення кола внутрішніх і зовнішніх загроз, пов'язаних з функціонуванням інформаційних систем організацій. Зростання масштабів використання цифрових технологій, у тому числі в критично важливих сферах, призводить до підвищення інтенсивності та складності деструктивних впливів на інформаційні активи. За таких умов виникає потреба у постійному перегляді, уточненні та систематизації підходів до управління ризиками. Попри значну кількість наукових праць, присвячених питанням інформаційної безпеки, сучасний аналіз загроз часто залишається фрагментованим і недостатньо інтегрованим з практичними механізмами захисту, що створює потребу в їх подальшому поглибленому дослідженні з орієнтацією на прикладні рішення для організацій різних секторів.

Методологічна основа спирається на таксономічні принципи, закріплені в міжнародних стандартах, зокрема серії ISO 27000, а також на аналіз емпіричних даних, представлених у профільних галузевих звітах, таких як ENISA Threat Landscape та Verizon Data Breach Investigations Report (DBIR) [2,3]. Поєднання нормативно-методичних підходів із результатами практичних спостережень дає змогу формувати узгоджену та актуальну систему класифікації загроз. У центрі уваги перебуває оцінювання їхнього впливу на ключові властивості інформації — конфіденційність, цілісність та доступність, які традиційно розглядаються як базові елементи архітектури кібербезпеки й слугують орієнтиром для побудови політик, процедур та технічних засобів захисту.

Для коректного управління ризиками принципово важливим є чітке розмежування понять «загроза» та «вразливість». Загроза розглядається як

потенційна причина інциденту, що може призвести до небажаних наслідків для інформаційної системи або інформаційних активів у вигляді порушення їх конфіденційності, цілісності чи доступності. Вразливість, своєю чергою, є слабким місцем у архітектурі, проєктуванні, реалізації або процесах управління системою, яке може бути використане однією або кількома загрозами для реалізації інциденту. Загрози можуть мати як навмисний характер, коли дії ініціюються з метою отримання неправомірної вигоди шляхом завдання шкоди інформації, так і випадковий, що пов'язаний з недостатністю організаційних або технічних заходів захисту, помилками персоналу чи дією масових деструктивних чинників. Забезпечення належного рівня конфіденційності, цілісності та доступності інформаційних активів як стратегічна мета архітектури безпеки досягається через цілеспрямовану розробку, впровадження та постійне вдосконалення системи засобів контролю, орієнтованих на проактивне виявлення потенційних вразливостей, попередження інцидентів і своєчасне реагування на них.

Систематична класифікація загроз за джерелом є базовим етапом аналізу ризиків і дає змогу відокремлювати заходи захисту, орієнтовані на периметр, від заходів, спрямованих на внутрішні сегменти інформаційної системи. Зовнішні загрози формуються за межами контрольованого периметра організації. До них належать високотехнологічні, цільові та масові вектори атак, зокрема шкідливе програмне забезпечення (віруси, трояни, мережеві «черв'яки»), несанкціоновані дії хакерських угруповань, масштабні DDoS-атаки, спрямовані на порушення доступності сервісів, а також таргетовані кампанії проти окремих організацій чи секторів. Окрему групу становлять соціально-інженерні вектори, такі як спам і фішинг, що використовуються для отримання облікових даних або ініціювання помилкових дій користувача. До засобів реалізації зовнішніх впливів також належать спеціалізовані промислові шкідливі програми (типу Stuxnet, Flame, Duqu), шпигунське програмне забезпечення (spyware, adware) та ботмережі, які застосовуються для скоординованих масованих атак [4].

Внутрішні загрози мають джерела всередині системи, хоча ініціація таких загроз може бути пов'язана із зовнішньою компрометацією. Реалізація ризику в цьому випадку відбувається через внутрішній доступ. До ключових внутрішніх

загроз належать витік інформації та несанкціонований доступ. Галузеві звіти, зокрема Verizon DBIR, фіксують значну частку інцидентів, пов'язаних із зловживанням привілеями (Privilege Misuse), що свідчить: навіть якщо зловмисник не є штатним інсайдером, компрометація облікового запису з надмірними правами доступу дає змогу реалізувати внутрішню загрозу в повному обсязі.

За характером впливу на інформаційну систему загрози поділяють на пасивні та активні. Пасивні загрози не призводять до зміни структури або змісту системи, їхній вплив переважно проявляється у порушенні конфіденційності чи доступності без модифікації самих даних. Прикладами є несанкціонований витік інформації або пасивне перехоплення мережевого трафіку. Активні загрози, навпаки, супроводжуються зміною структури чи вмісту системи: модифікацією даних, організацією відмови в обслуговуванні (DDoS), знищенням інформації або її шифруванням у межах атак типу ransomware. Додатково, за масштабом завданої шкоди розрізняють загальні загрози, що впливають на об'єкт безпеки в цілому, локальні, які зачіпають окремі його частини, та приватні, що стосуються конкретних властивостей окремих елементів.

Вразливості створюють умови для реалізації загроз і можуть класифікуватися за походженням. Об'єктивні вразливості зумовлені властивостями самої технології або складними умовами експлуатації й розташування інформації. До них належать, наприклад, недоліки в протоколах обміну даними чи інтерфейсах, а також проблеми, пов'язані з неповнотою або некоректністю окремих процесів функціонування системи. Суб'єктивні вразливості пов'язані з людським фактором — помилками адміністраторів, користувачів або розробників, недотриманням процедур, низьким рівнем обізнаності. Випадкові вразливості формуються внаслідок недостатності заходів захисту або впливу важкопрогнозованих масових факторів [5].

Аналіз взаємозв'язку між загрозами та вразливостями демонструє чіткий причинно-наслідковий зв'язок між типом вразливості й успішністю атаки. Суб'єктивні вразливості, зокрема помилки, недбалість або недостатня обізнаність персоналу, часто виступають каталізатором активних зовнішніх загроз. У галузевих звітах, таких як Verizon DBIR, серед поширених патернів інцидентів

виділяються категорії «Miscellaneous Errors» (різноманітні помилки) та «Social Engineering» (соціальна інженерія). Це означає, що такі загрози, як ransomware, нерідко використовують пасивні, суб'єктивні вразливості — наприклад, натискання на фішингове посилання або неправильну конфігурацію системи — для отримання початкового доступу. У такій ситуації суб'єктивна вразливість фактично перетворює потенційну зовнішню загрозу на реальну активну внутрішню атаку. Внутрішні загрози, навіть за відсутності умислу з боку працівників, часто є наслідком недоліків архітектури безпеки, насамперед недостатнього контролю доступу. Якщо не забезпечено принцип мінімальних привілеїв, компрометація навіть добросовісного облікового запису може призвести до несанкціонованого доступу та значного витоку даних, що кваліфікується як внутрішня загроза.

Сучасна ситуація у сфері кіберзагроз характеризується високопрофільними, фінансово мотивованими та стратегічно спланованими атаками. Аналіз звітів ENISA та Verizon DBIR дозволяє виокремити низку векторів, які мають пріоритетне значення для організаційних систем. Одним із ключових типів загроз залишається ransomware. Звіт ENISA Threat Landscape 2024 відзначає, що програми-вимагачі стабільно посідають провідне місце серед зареєстрованих інцидентів, поступаючись лише загрозам, спрямованим на порушення доступності. Еволюція ransomware пов'язана з поширенням моделі RaaS (Ransomware as a Service), що зменшує технічний поріг входу для зловмисників і сприяє комерціалізації відповідної діяльності. Сучасні кампанії часто передбачають подвійне або потрійне вимагання, коли потерпілу сторону змушують не лише відновлювати доступ до зашифрованих активів за оплати, а й додатково тиснуть загрозою оприлюднення викрадених конфіденційних даних. У звітному періоді серед найбільш активних угруповань фіксувалися LockBit, Cl0p та PLAY: LockBit продемонструвало значну стійкість та масштаб активності, а Cl0p раніше відзначалося експлуатацією низки вразливостей нульового дня. До секторів, які найчастіше фігурують серед постраждалих від атак ransomware, належать промисловість і виробництво, роздрібна торгівля та постачальники цифрових послуг [2,3].

Загрози, спрямовані на порушення доступності, посідають одне з провідних місць у класифікаціях ENISA. Вони охоплюють як класичні DDoS-атаки, що перевантажують мережеву інфраструктуру та обчислювальні ресурси, так і цілеспрямовані дії щодо критично важливих сервісів та елементів інфраструктури. DDoS-атаки продовжують залишатися однією з основних загроз для державних та приватних організацій у країнах ЄС. Додатковим чинником є зростання активності хактивістських угруповань, зумовлене регіональними конфліктами та значущими національними подіями. Такі кампанії часто мають ідеологічну або політичну мотивацію, що ускладнює їх прогнозування порівняно з переважно фінансово орієнтованими атаками [6].

Соціальна інженерія виступає не стільки самостійним видом загрози, скільки одним із основних векторів початкового доступу. У звіті Verizon DBIR вона розглядається як один із найпоширеніших патернів інцидентів поряд із системним вторгненням і помилками конфігурації. Механізм її експлуатації полягає у впливі на поведінку користувача з метою спонукати його до дій, що суперечать політикам безпеки, або до розкриття конфіденційної інформації. Це може бути реалізовано у формі фішингу, цільового spear-phishing, pretexting (створення вигаданого приводу) та інших комунікаційних практик. Результативність соціальної інженерії ґрунтується на використанні суб'єктивних вразливостей, зокрема помилок користувачів і несвідомого зловживання привілеями. Таким чином, успіх зовнішньої атаки у багатьох випадках прямо залежить від внутрішніх людських слабких місць.

Атаки на ланцюги поставок розглядаються ENISA як «горизонтальна загроза», оскільки вони здатні одночасно впливати на кілька інших категорій загроз. Високий рівень залежності сучасних організацій від зовнішніх постачальників послуг і програмного забезпечення формує системну вразливість: компрометація одного критично важливого контрагента може призвести до масштабного проникнення в інфраструктуру багатьох клієнтів. Це створює додаткові завдання для фахівців з інформаційної безпеки в частині управління зовнішніми ризиками. Показовими є інциденти із 3CX та з відкритим проєктом XZ Utils. У випадку XZ Utils зловмисник, використовуючи тривалу кампанію

соціальної інженерії, отримав статус мейнтейнера проєкту й інтегрував шкідливий код, який забезпечував можливість віддаленого виконання коду (RCE) через SSH. Ця подія продемонструвала, що навіть базові компоненти програмної інфраструктури — бібліотеки та утиліти з відкритим вихідним кодом — можуть стати каналом для масштабних атак внаслідок зловживання довірою до спільноти розробників.

Вразливості нульового дня (Zero-Day) становлять окремий, особливо критичний клас загроз. Вони експлуатуються зловмисниками до того, як розробник програмного забезпечення випустить виправлення, що істотно ускладнює їх виявлення традиційними засобами захисту. Такі вразливості часто використовуються у високоцільових атаках або як канал початкового доступу в межах широкомасштабних кампаній, у тому числі атак на ланцюги поставок.

Аналіз поєднання зазначених загроз дає змогу простежити внутрішню логіку сучасної злочинної кіберекосистеми. Комерціалізована модель RaaS виступає для зловмисників основною метою монетизації. Для її реалізації потрібен результативний вектор початкового доступу, який забезпечується або експлуатацією вразливостей нульового дня, або успішними операціями соціальної інженерії. Атаки на ланцюги поставок виконують роль механізму масштабування: компрометація одного стратегічно важливого елемента інфраструктури дає змогу отримати доступ до великої кількості кінцевих організацій. У такій конфігурації вразливість нульового дня чи соціально-інженерна атака виступають вектором початкового проникнення, ланцюг поставок — каналом поширення, а RaaS — інструментом системної фінансової вигоди для зловмисників.

Архітектурні вразливості та пов'язані з ними вектори ризику в гібридних та хмарних середовищах стають одним із ключових чинників формування загального рівня кібербезпеки організацій. Масова міграція інфраструктури й даних до хмарних сервісів зміщує акцент від класичного периметрового захисту до управління ідентичністю, доступом та коректністю конфігурацій. У цих умовах помилки проєктування, налаштувань і розподілу привілеїв безпосередньо трансформуються у вразливості, які можуть бути використані як внутрішніми, так і зовнішніми суб'єктами загроз.

Однією з найбільш поширених і критичних вразливостей хмарних інфраструктур є неправильна конфігурація (cloud misconfiguration). Вона виникає у випадках, коли адміністратори чи користувачі некоректно застосовують параметри безпеки: не обмежують доступ до ресурсів, не активують шифрування даних, залишають облікові записи з паролями за замовчуванням або допускають помилки в управлінні дозволами. Прямим наслідком таких помилок є проблема надмірних привілеїв (excessive permissions), коли ідентичності в хмарних середовищах (AWS, Google Cloud Platform, Microsoft Azure) отримують більший обсяг прав, ніж це є необхідним для виконання їхніх функцій. За результатами досліджень, значна частка людських ідентифікаторів у великих хмарних середовищах належить до категорій високого або критичного ризику за рівнем наданих дозволів; для окремих сервісів цей показник сягає близько 87 % для ідентичностей з високим ризиком. Такі надмірні привілеї суттєво розширюють можливості зловмисника після компрометації облікового запису. Оскільки організації все частіше розміщують у хмарі критичні дані, вони фактично виводять їх за межі традиційного захисту корпоративного брандмауера, роблячи залежними від надійності постачальника послуг і якості власних внутрішніх конфігурацій. Публічні хмарні сховища, які використовує переважна більшість організацій, стають особливо привабливими цілями за наявності надмірних прав доступу.

Фундаментальні архітектурні слабкі місця нерідко пов'язані з відсутністю комплексного, системно спроектованого підходу до безпеки. Якщо в архітектурі не реалізовано принцип багаторівневого захисту (defense in depth), а засоби контролю зосереджені лише на одному рівні — наприклад, на мережевому периметрі чи окремих прикладних сервісах, — порушення цілісності цього єдиного рубежу може призвести до масштабної компрометації всієї системи. Додатковими чинниками ризику є недостатній контроль доступу (слабкі механізми автентифікації й авторизації, відсутність або формальність політик паролів, невпроваджена чи вибіркова багатофакторна автентифікація, обмежене використання розподілу доступу на основі ролей) та технічні прогалини, пов'язані з відсутністю шифрування даних у стані спокою, під час передавання або обробки, а також з

невикористанням чи неправильним налаштуванням систем виявлення та запобігання вторгненням [6].

1.3. Аналіз підходів до забезпечення безпеки інформаційних ресурсів організації

Сучасна архітектура корпоративних інформаційних ресурсів перебуває в стані суттєвої трансформації. Перехід до гібридних і віддалених форм роботи, широке впровадження хмарних сервісів на рівні SaaS, PaaS та IaaS, а також зростання кількості підключених пристроїв, зокрема IoT, призвели до фактичного розмивання традиційного мережевого периметра. За таких умов забезпечення безпеки не може ґрунтуватися лише на контролі межі мережі й потребує переорієнтації на захист самих інформаційних ресурсів і механізмів доступу до них.

Базові принципи інформаційної безпеки, відомі як триада CIA (конфіденційність, цілісність, доступність), залишаються концептуальним фундаментом будь-якої програми захисту. Конфіденційність передбачає недопущення несанкціонованого доступу до даних, цілісність — збереження їх точності та незмінності під час зберігання й передавання, а доступність — гарантоване надання доступу до систем і інформації уповноваженим користувачам у потрібний час. Водночас, коли інформаційні активи одночасно розміщені в локальних дата-центрах, публічних хмарах і на пристроях віддалених користувачів, стратегія безпеки має змістити акцент із захисту окремих мережевих сегментів на цілісний захист даних, сервісів та ідентичностей. Це, у свою чергу, потребує впровадження зрілих систем управління безпекою, що спираються на міжнародно визнані стандарти та фреймворки.

Для стандартизації та контролю заходів безпеки організації широко застосовують міжнародні фреймворки, серед яких одними з найпоширеніших є ISO/IEC 27001 та NIST Cybersecurity Framework. ISO/IEC 27001 визначає вимоги до створення, впровадження та підтримки системи управління інформаційною безпекою (ISMS). Він пропонує структурований набір контролів, які добираються

відповідно до результатів оцінки ризиків, та дає змогу вибудувати повторювані процеси управління безпекою. Важливою перевагою цього стандарту є можливість отримання сертифікації, яка слугує незалежним підтвердженням рівня захисту конфіденційної інформації й підвищує довіру з боку клієнтів і партнерів на міжнародному рівні. Стандарт особливо релевантний для організацій з достатнім рівнем операційної зрілості, які готові формалізувати процеси ризик-орієнтованого менеджменту.

NIST Cybersecurity Framework є добровільним фреймворком, орієнтованим на управління та зменшення кіберризиків. Він був розроблений насамперед для об'єктів критичної інфраструктури, але завдяки гнучкості широко застосовується й у некритичних, у тому числі неамериканських, організаціях. На відміну від ISO/IEC 27001, цей фреймворк має більш технічний характер і часто використовується як основа для побудови базової позиції кібербезпеки в організаціях, що лише формують свою програму захисту. Він допомагає оцінити поточний стан, виявити прогалини та задати напрямок поступового підвищення зрілості.

Практика показує, що ISO/IEC 27001 та NIST CSF доцільно застосовувати у взаємодоповнювальний спосіб. NIST CSF часто використовується як інструмент первинної оцінки технічної зрілості й ризиків, тоді як ISO/IEC 27001 — для формалізації процесів управління на рівні ISMS та подальшої сертифікації. Такий підхід дає змогу забезпечити, щоб архітектурні зміни, зокрема перехід до моделей Zero Trust або SASE, реалізовувалися не як реакція на окремі інциденти, а як елемент структурованого, ризик-орієнтованого процесу управління безпекою.

Домінуючою моделлю була концепція захисту в глибину, яка передбачала багаторівневий захист, сфокусований навколо мережевого периметра. Вважалося, що все, що знаходиться в межах захищеної брандмауером мережі, є умовно довіреним, тоді як трафік ззовні потребує посиленого контролю. У розподілених і динамічних середовищах така модель демонструє низку обмежень. Вона створює ризик хибного відчуття захищеності, ускладнює координацію великої кількості незалежних шарів захисту та не забезпечує належного контролю всередині мережі. Найбільш критичною проблемою є те, що після порушення периметра, наприклад у результаті фішингової атаки або компрометації пристрою IoT, зловмисник

отримує можливість здійснювати латеральне переміщення в межах інфраструктури, оскільки внутрішній трафік часто розглядається як довірений.

У відповідь на ці обмеження сформувалася парадигма Zero Trust, яка пропонує відмову від припущення про довіру на підставі мережевого або фізичного розташування. Фундаментальним принципом є відсутність довіри за замовчуванням і обов'язкова перевірка кожного запиту доступу. Фокус захисту переноситься з меж мережі на конкретні ресурси, ідентичності та контекст доступу. У рамках такої архітектури сувора автентифікація та авторизація здійснюються щодо кожного користувача й пристрою до встановлення сесії з корпоративними ресурсами; багатофакторна автентифікація стає базовою вимогою. Додатково реалізується принцип найменших привілеїв із використанням гранульованого, адаптивного контролю доступу, коли суб'єкти отримують рівно стільки прав і на такий період, які є необхідними для виконання конкретних задач, а умови доступу визначаються політиками умовного доступу. Мікросегментація мережі дозволяє поділити інфраструктуру на ізольовані зони з власними правилами доступу, що істотно знижує ризик поширення атаки у разі компрометації окремого сегмента.

Практична імплементація Zero Trust вимагає послідовного, поетапного підходу. Насамперед необхідно провести інвентаризацію активів і визначити поверхню захисту, тобто сукупність критичних даних, сервісів і систем, які потребують пріоритетного захисту в локальному та хмарному середовищах. Далі здійснюється постійна верифікація ідентичностей і пристроїв, у тому числі оцінка їхнього стану безпеки за допомогою відповідних платформ моніторингу та захисту кінцевих точок. Наступним кроком є детальне мапування робочих процесів із визначенням того, які ідентичності отримують доступ до яких ресурсів, за яких умов і через які канали. На цій основі формуються й автоматизуються адаптивні політики доступу, що враховують контекстні параметри: місцезнаходження, тип пристрою, оцінку ризику тощо.

У такій конфігурації Zero Trust виступає каталізатором архітектурної конвергенції. Оскільки підхід передбачає побудову ідентифікаційно орієнтованих з'єднань замість широких мережеских тунелів, виникає потреба у використанні хмароорієнтованих платформ, здатних забезпечити єдину політику доступу

незалежно від місця розташування користувача або ресурсу. Це створює передумови для впровадження моделей на кшталт SASE, які поєднують мережеві функції та функції безпеки в єдиній хмарній архітектурі й забезпечують узгоджене застосування політик у динамічних гібридних середовищах [7].

Secure Access Service Edge (SASE) розглядається як архітектурний підхід, запропонований аналітичною компанією Gartner, який надає механізми реалізації принципів Zero Trust у розподілених, гібридних інфраструктурах. SASE являє собою хмароорієнтовану архітектуру, що поєднує мережеві функції (зокрема, SD-WAN) із сервісами безпеки, які надаються у форматі «безпека як послуга». Її поява зумовлена необхідністю перенесення функцій мережевого й безпекового контролю з локальних апаратних рішень у центрах обробки даних до віртуалізованих сервісів у хмарі. Це дає змогу організаціям спрощувати управління, гнучко масштабуватися та забезпечувати єдиний підхід до захисту незалежно від того, чи користувач працює у філії, головному офісі або віддалено. В основі SASE лежить доступ, організований за принципами Zero Trust, де рішення щодо надання доступу приймаються на основі ідентичності сутності та контексту в реальному часі.

Ключові компоненти архітектури SASE

SASE консолідує в межах єдиної глобально розподіленої хмарної платформи основні функції мережевої безпеки і доступу, формуючи наскрізний контур захисту. До таких компонентів належать:

- Zero Trust Network Access (ZTNA), який забезпечує безпечний, ідентифікаційно орієнтований доступ до приватних застосунків і фактично замінює традиційні VPN-рішення, що надавали доступ до широких мережевих сегментів.
- Secure Web Gateway (SWG), який здійснює контроль і фільтрацію веб-трафіку користувачів, застосовуючи політики безпеки, категоризацію ресурсів та захист від веб-загроз.
- Cloud Access Security Broker (CASB), що розширює корпоративні політики безпеки на хмарні застосунки та платформи, забезпечуючи контроль доступу, моніторинг використання сервісів та захист даних у середовищах SaaS і PaaS.

– Firewall as a Service (FWaaS) або міжмережевий екран нового покоління, реалізований як хмарний сервіс, який послідовно застосовує політики фільтрації та інспекції трафіку на всіх точках доступу.

– Software-Defined Wide Area Network (SD-WAN), що відповідає за оптимізацію маршрутизації трафіку й продуктивність підключень до вузлів SASE, забезпечуючи стабільний та керований доступ до ресурсів.

У сукупності ці компоненти створюють цілісну модель, у якій мережевий трафік і запити доступу проходять через єдиний контрольний контур, орієнтований на ідентичність і контекст.

Zero Trust Network Access є центральним елементом логіки контролю доступу в архітектурі SASE. На відміну від традиційних VPN, які зазвичай відкривали доступ до цілих сегментів мережі, ZTNA забезпечує доступ лише до конкретних, явно дозволених застосунків. Рішення про доступ приймається на основі ідентичності користувача та пристрою, а також додаткових контекстних параметрів (місцезнаходження, тип і стан пристрою, оцінка ризику).

У межах SASE рішення ZTNA інтегруються з постачальниками ідентичностей, такими як служби корпоративного каталогу або хмарні сервіси керування ідентичностями, що забезпечує єдиний вхід та застосування політик умовного доступу на краю мережі. Такий підхід суттєво зменшує площу потенційної атаки: користувачі та пристрої бачать лише ті ресурси, до яких їм надано право доступу, а у разі компрометації облікових даних масштаби можливих наслідків обмежуються набором чітко визначених дозволів. Крім того, централізоване управління політиками й автоматизоване їх застосування забезпечують масштабованість і гнучкість, необхідні для підтримки сучасних розподілених бізнес-процесів, у тому числі внутрішніх сервісів і мікросервісної архітектури.

Основною перевагою SASE є можливість застосування єдиного, ідентифікаційно орієнтованого підходу до безпеки через хмарну Edge-інфраструктуру, незалежно від місця розміщення користувачів, даних або застосунків. Це забезпечує узгоджену перевірку, автентифікацію й авторизацію трафіку, пристроїв та запитів доступу, а також уніфіковане застосування політик.

До ключових переваг SASE належать: послідовність політик безпеки на всіх точках доступу; підвищення операційної ефективності завдяки переходу від розрізнених апаратних рішень до хмарних сервісів; конвергенція таких функцій, як CASB, ZTNA та SWG, у межах єдиної платформи, що покращує оглядовість та керованість захисту.

Водночас перехід до архітектури SASE супроводжується низкою викликів. Для великих організацій із значним обсягом застарілої інфраструктури трансформація може вимагати суттєвих ресурсів, як технічних, так і організаційних. Додатковою складністю є вибір моделі впровадження: комплексне рішення від одного постачальника або інтеграція окремих, спеціалізованих рішень різних вендорів. У другому випадку постає завдання узгодження політик і сумісності, що ускладнює проектування й підтримку цілісної архітектури.

У контексті використання хмарних сервісів безпека реалізується в межах моделі розподіленої відповідальності. Постачальник хмарних послуг відповідає за захист базової інфраструктури, фізичну й частково віртуальну безпеку платформ, тоді як клієнт несе відповідальність за захист власних даних, конфігурацій, прикладної логіки, кінцевих точок і, насамперед, за управління ідентичністю та доступом. На практиці значна частина інцидентів пов'язана саме з помилками конфігурації з боку клієнта та недостатнім контролем привілеїв.

У середовищі, де периметр у класичному розумінні зникає, ідентичність фактично стає новим периметром безпеки. Ефективне управління ідентичностями та доступом є критичною умовою для реалізації Zero Trust. Сучасні підходи до управління доступом включають використання політик умовного доступу, які враховують роль користувача, тип і стан пристрою, рівень ризику; обов'язкове застосування багатофакторної автентифікації для доступу до критичних ресурсів; чітке визначення ролей і областей дії дозволів. Додатково важливе місце посідає криптографічний захист, що забезпечується через інфраструктуру керування ключами й протоколи захищеного обміну даними.

Технології управління безпекою у хмарі (CSPM, CASB, CIEM)

Зростання складності конфігурацій і кількості ідентичностей у хмарних середовищах зумовило появу спеціалізованих інструментів, які доповнюють традиційні засоби безпеки та підтримують реалізацію принципів Zero Trust.

Рішення класу Cloud Security Posture Management (CSPM) призначені для постійного аналізу стану хмарних середовищ (IaaS, PaaS, SaaS) на предмет ризиків, зокрема неправильно налаштованих сервісів, відсутності шифрування, надмірних дозволів або відкритих до мережі ресурсів. Такі інструменти забезпечують безперервний моніторинг, звітність щодо відповідності політикам і часто містять механізми автоматичного виправлення виявлених проблем, що дає змогу зменшити ймовірність інцидентів, пов'язаних з помилками конфігурацій.

Cloud Access Security Broker, у свою чергу, виступає посередником між користувачами та хмарними сервісами, застосовуючи корпоративні політики безпеки до доступу й обробки даних у хмарних застосунках. CASB надає оглядовість щодо використання хмарних сервісів, підтримує реалізацію таких заходів, як застосування MFA, контроль типів пристроїв, шифрування даних у стані спокою та при передаванні, а також інтегрується з архітектурою SASE для узгодженого застосування політик.

Cloud Infrastructure Entitlement Management (CIEM) зосереджений на управлінні правами доступу в мультихмарних інфраструктурах. Унаслідок великої кількості людських і машинних ідентичностей, а також динамічного характеру призначення прав, у хмарі швидко накопичуються надмірні, невикористовувані або некоректні дозволи. CIEM-платформи аналізують конфігурації доступу, виявляють ризиковані привілеї, пропонують їх оптимізацію й допомагають реалізувати принцип найменших привілеїв. Це дозволяє зменшити ймовірність зловживання компрометованими обліковими записами та обмежити масштаби можливих наслідків інцидентів. У комплексі з іншими компонентами хмарних платформ захисту застосунків CIEM посилює реалізацію Zero Trust у хмарних середовищах.

Інтеграція безпеки в життєві цикли розробки та операційної діяльності

Організації, які активно розвивають цифрові сервіси, не можуть розглядати безпеку виключно як завершальний етап контролю після розробки. Такий підхід призводить до накопичення технічного боргу й підвищення ризиків. Концепція

DevSecOps передбачає інтеграцію безпеки на всіх етапах життєвого циклу розробки програмного забезпечення, тобто «зсув безпеки вліво» — до етапів проєктування й розробки.

У межах безпечного життєвого циклу розробки (SSDLC) вразливості виявляються і усуваються якомога раніше, коли вартість їх виправлення є найнижчою. Безпека стає спільною відповідальністю всіх учасників процесу розробки, а не окремої команди аудиту. Це досягається, зокрема, шляхом інтеграції механізмів SAST, DAST та IAST у конвеєри безперервної інтеграції та доставки (CI/CD), що дає змогу автоматизувати перевірки коду і застосунків на відповідність вимогам безпеки. У підсумку застосунки, до яких забезпечується доступ через SASE, проєктуються та розгортаються з урахуванням вимог безпеки з самого початку.

Зі зростанням кількості сигналів від різних систем безпеки (SIEM, EDR, SASE-платформи) особливого значення набуває автоматизація операційних процесів. Платформи класу SOAR (Security Orchestration, Automation and Response) дозволяють централізувати обробку оповіщень, оркеструвати взаємодію між інструментами та автоматизувати типові сценарії реагування через так звані плейбуки. Це зменшує час реакції на інциденти, знижує навантаження на аналітиків і дає змогу фокусувати увагу на найбільш критичних загрозах.

Роль штучного інтелекту та машинного навчання в сучасних програмах захисту полягає у переході від суто реактивних до проактивних та прогностичних моделей. Алгоритми машинного навчання застосовуються для виявлення аномалій у поведінці користувачів, пристроїв та сервісів, побудови поведінкових профілів (UEBA) і прогнозування можливих сценаріїв атак на основі історичних даних. Це розширює можливості загрозорозвідки й проактивного полювання на загрози, коли потенційно небезпечна активність виявляється до того, як призводить до повноцінного інциденту.

Ефективний захист інформаційних ресурсів в умовах гібридної та мультимарної інфраструктури потребує відмови від орієнтації на традиційний мережевий периметр і поступового впровадження підходів, заснованих на Zero Trust. Концепція SASE у цьому контексті є однією з ключових архітектурних

моделей, яка об'єднує мережеві функції й функції безпеки в єдину хмароорієнтовану платформу, забезпечуючи ідентифікаційно керований, гранульований доступ до ресурсів.

Успішна реалізація архітектур Zero Trust і SASE залежить від якості управління ідентичностями та привілеями, а також від рівня інтеграції безпеки в процеси розробки й операційної діяльності. Інструменти на кшталт CIEM, CSPM та CASB підсилюють контроль над хмарними конфігураціями й правами доступу, тоді як DevSecOps, SOAR та аналітика на основі ШІ забезпечують безперервність, автоматизованість і проактивний характер заходів безпеки [8].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗЦІЇ

2.1. Методи та засоби забезпечення безпеки інформаційної системи організації

У проведеному дослідженні Gartner постачальників рішень класу Secure Access Service Edge (SASE) виконано ідентифікацію, аналіз та оцінювання ключових учасників ринку. У звіті показано, якою мірою кожен постачальник відповідає визначеним вимогам, а також окреслено підходи, що можуть бути використані організаціями під час вибору платформи SASE з урахуванням власних пріоритетів та потреб.

Розвиток рішень SASE інтерпретується як еволюція від поєднання окремих сервісів до платформного підходу. Хоча значна кількість постачальників виводить на ринок комплексні пропозиції, які поєднують сервіси периферійної безпеки (Security Service Edge, SSE), доступ з нульовою довірою (Zero Trust Network Access, ZTNA) та програмно-визначені глобальні мережі (SD-WAN), сформувалася окрема група з восьми постачальників, які демонструють підвищений рівень інновацій у сфері SASE. Для цих рішень характерне не лише об'єднання функцій у рамках єдиної платформи та консолі керування, а й розширення меж функціональності, зокрема посилення контролю над некерованими пристроями (наприклад, за рахунок використання корпоративних браузерів) та забезпечення узгодженості сервісів у глобальних розгортаннях. Політики безпеки та користувацький досвід у таких платформах залишаються послідовними незалежно від географічного розташування користувача, що визначає їх як референтну модель для інтелектуальних та уніфікованих рішень SASE [19].

Під час інтерпретації результатів оцінювання рішень SASE на основі цього дослідження доцільно враховувати три ключові аспекти. Перший аспект стосується платформи як інтегрованого середовища. Розвинені платформи виходять за межі простого паритету функцій і забезпечують адаптивні інтерфейси та робочі процеси, які підлаштовуються під потреби операційних команд. У межах спільної зони

перетину мережевих та безпекових функцій такі платформи створюють єдине середовище співпраці для команд мережевої інфраструктури й інформаційної безпеки, поєднуючи управління політиками, аналітику та видимість. Функції, подання та елементи керування динамічно відображаються залежно від ролі користувача, що дозволяє виявляти, класифікувати та інтерпретувати аналітичні дані, спираючись на єдине джерело достовірної інформації без необхідності перемикання між різними консолями.

Другий аспект стосується запобігання витоку даних (Data Loss Prevention, DLP), яке вважається одним з основних чинників диференціації платформ SASE. Сучасні засоби DLP виходять за межі базової контентної фільтрації і реалізують контекстно-залежний захист на основі ідентичності в хмарних, веб- та приватних застосунках. Уніфіковані платформи, що інтегрують розвинуті механізми DLP у власну архітектуру, здатні застосовувати детальні політики, виявляти витoki конфіденційної інформації в режимі, наближеному до реального часу, та адаптувати засоби контролю залежно від поведінки користувачів і рівня ризику. Постачальники, які глибоко вбудовують DLP у структуру SASE, вирізняються послідовним застосуванням політик, спрощеним управлінням та підвищеною прозорістю руху даних.

Третій аспект пов'язаний зі застосуванням штучного інтелекту, особливо генеративних моделей (genAI). З поширенням таких технологій платформи SASE переходять до нового рівня операційного інтелекту. Генеративні та інші моделі ШІ використовуються для автоматизації створення політик, виявлення загроз, аналізу трафіку та підтримки систем управління ідентичністю. Інтерфейси природної мови дають змогу ІТ-командам інтуїтивно взаємодіяти з платформами SASE, формувати аналітичні звіти, налаштовувати політики доступу та створювати звітність щодо відповідності без необхідності глибокої експертизи в галузі мережевих технологій. Найбільш перспективними вважаються рішення, у яких можливості природної мови інтегруються з механізмами автоматизованого виявлення аномалій, кореляції загроз на основі векторних уявлень та агентного ШІ, орієнтованого на оптимізацію безпечного доступу та ефективності роботи периферійних мереж.

У рамках методології Forrester Wave™ постачальників SASE класифіковано на три групи: «Лідери», «Сильні виконавці» та «Претенденти». Візуальне розміщення на діаграмі відображає силу поточної пропозиції за вертикальною віссю та якість стратегії за горизонтальною. Додаткове кільце навколо маркера постачальника відображає оцінку відгуків клієнтів: один ореол вказує на відгуки вище середнього рівня, подвійний — на винятково високий рівень задоволеності. Оцінювання розглядається як відправна точка, результати якої доцільно адаптувати до конкретних пріоритетів організації з використанням інтерактивних інструментів порівняння [7].



Рис.2.1. Порівняння рішень SASE

У групі лідерів окремо виділяється Netskope. Цей постачальник спочатку позиціонувався як хмарний брокер безпеки доступу (CASB), а згодом розширив портфель за рахунок безпечного веб-шлюзу (SWG), DLP та повноцінного рішення SASE після придбання Infot у 2022 році. Стратегічне бачення Netskope орієнтоване на вирішення нових викликів, пов'язаних зі штучним інтелектом, криптовалютами, хмарними середовищами та Інтернетом речей. Технологічний стек включає єдину платформу та приватну глобальну мережу (NewEdge), де активно застосовуються технології ШІ, у тому числі для контролю використання genAI. Дорожня карта розвитку є деталізованою та узгодженою зі стратегічними пріоритетами. Партнерська екосистема та служба підтримки демонструють рівень, співставний з іншими провідними постачальниками, хоча модель ціноутворення лишається відносно складною і вищою за середньоринкову. З функціонального погляду Netskope характеризується потужними можливостями виявлення та класифікації даних, а також виявлення загроз для кінцевих точок, мережесегментів і як приватних, так і публічних хмарних середовищ. Інструменти сканування здатні виявляти специфічні типи документів (наприклад, контракти щодо злиття та поглинання, персональні ідентифікатори). Єдина консоль адміністратора забезпечує інтегроване керування широким спектром сервісів, а спектр варіантів розгортання, включно з локалізованими сервісами, активно розширюється. За відгуками клієнтів цінується централізація адміністративних інтерфейсів, хоча вказується на потребу в більш прозорій комунікації змін функціональності. Netskope розглядається як доцільний вибір для організацій, яким потрібна багатофункціональна централізована платформа мережевої безпеки для локальних і хмарних середовищ [19].

Palo Alto Networks, яка історично відома створенням одного з перших міжмережесегментів нового покоління (NGFW), інтегрувала мережеві й безпекові продукти в єдину платформу Strata Cloud Manager (SCM). Ця платформа керує рішенням Prisma SASE та його компонентами, до яких належать Prisma Access, обладнання ION, клієнт GlobalProtect та Prisma Access Browser. Стратегія постачальника орієнтована на поточні стратегічні та тактичні потреби клієнтів, а дорожня карта характеризується деталізованістю, регулярністю релізів і

прозорістю, що є важливим для партнерських мереж реселерів і постачальників керованих послуг. Спільнота користувачів підтримується через різні канали взаємодії. Водночас модель ціноутворення може бути складною для обґрунтування. Рішення Prisma SASE вирізняється розвинутим ZTNA, інтегрованим у клієнт GlobalProtect, а також швидким прогресом у розвитку функцій CASB і DLP. Для аналізу широкого спектра SaaS-ресурсів та сервісів genAI активно використовується ШІ, що дозволяє виявляти ризики для даних, включно з аналізом зображень, і застосовувати контекстно-залежні обмеження доступу. Для досягнення повної послідовності глобальних сервісів необхідні додаткові інвестиції в розширення типів обладнання, типів підключень та стандартизацію політик на рівні PoP. Клієнтські відгуки підкреслюють високу цінність можливостей SCM з точки зору візуалізації й керування даними, але вказують на зростання витрат через ускладнення ліцензійної моделі. Рішення Palo Alto Networks особливо релевантне для організацій у високорегульованих галузях, чутливих до захисту даних.

Компанія Zscaler, заснована у 2007 році, стала одним із піонерів хмарної безпеки та суттєво зміцнила позиції під час масштабного переходу до віддаленої роботи. Згодом охоплення розширилося від захисту віддалених співробітників до забезпечення безпеки та мережевих сервісів для віддалених локацій загалом. Стратегія базується на накопиченій експертизі в галузі безпеки та підтримується активною спільнотою й розвиненою партнерською мережею, що сприяє впровадженню моделей Zero Trust. Наявна партнерська екосистема дозволяє збирати зворотний зв'язок та уточнювати бачення SASE, яке наразі частково орієнтується на функціональний паритет з конкурентами. Модель ціноутворення поступово спрощується. З функціонального погляду Zscaler розвиває уніфікований клієнт ZTNA, який інтелектуально маршрутизує трафік через SWG, CASB та засоби керування цифровим досвідом. Забезпечуються розвинуті можливості звітності й діагностики, що важливо для відповідності нормативним вимогам. Водночас обмежений спектр мережевого обладнання та варіантів підключення, навіть з урахуванням нещодавнього додавання SD-WAN, створює обмеження для оптимального відведення трафіку від перевантажених центрів обробки даних.

Відгуки клієнтів позитивно оцінюють рух до уніфікованої платформи, але фіксують проблеми з продуктивністю внаслідок перевантаження окремих PoP. Zscaler вважається доцільним для великих підприємств та державних установ, особливо за наявності вимог FedRAMP.

До групи «сильних виконавців» віднесено, зокрема, Cato Networks. Цей постачальник ще до формалізації терміна SASE у 2017 році інтегрував функції WAN-керування з хмарними засобами фільтрації трафіку, міжмережевими екранами й іншими функціями безпеки, створивши ранню конвергентну модель. Стратегічне бачення характеризується орієнтацією на клієнта, врахуванням як поточних потреб, так і майбутніх викликів, включно з III та квантовими технологіями. Служба підтримки відзначається розвиненою системою угод про рівень сервісу, а партнерська програма відповідає очікуванням ринку, хоча потребує посилення офлайн-взаємодії та чіткішої пріоритизації в дорожній карті. Єдина консоль Cato Management Application забезпечує інтегроване керування всіма компонентами SASE з уніфікованим користувацьким інтерфейсом. Узгоджене розподілення функцій безпеки та мережі на PoP дозволяє ефективно контролювати SSE та мережеві сервіси з поглибленим моніторингом. За більшістю параметрів безпеки Cato демонструє рівень, зіставний з конкурентами, хоча в окремих аспектах (відсутність корпоративного браузеру й обмежений контроль доступу до даних) спостерігається відставання. Клієнти відзначають високу зручність консольного керування, але вказують на тенденцію пріоритизації нових функцій над усуненням стандартних недоліків. Рішення Cato Networks є релевантним для організацій, які прагнуть отримати узгоджений набір мережевих і безпекових сервісів в межах однієї інтегрованої консолі.

Versa Networks, що походить із сегмента SD-WAN, інтегрувала можливості SSE в єдине рішення, сформувавши платформу SASE, яка широко використовується постачальниками послуг та телекомунікаційними компаніями. Стратегія компанії ґрунтується на розвитку спеціалізованих інтерфейсів і функціоналу для сервіс-провайдерів, включно з практикою вбудовування представників виробника до команд підтримки партнерів. Водночас бачення не повною мірою відповідає динаміці потреб як сервіс-провайдерів, так і

корпоративних замовників, а модель ціноутворення залишається складною. Операційна система Versa (VOS) забезпечує інтегрований мережевий і безпековий функціонал, може розгортатися на різних апаратних платформах, а консоль Concerto забезпечує уніфіковане керування всіма сервісами. Компанія декларує прагнення максимального наближення принципів Zero Trust до периферії. Розширені функції SWG та значна частина можливостей DLP перебувають у стадії розвитку, що зумовлює відставання в захисті даних порівняно з лідерами ринку. За відгуками клієнтів, єдиний інтерфейс спрощує налаштування політик, однак основний акцент у відгуках робиться на мережевих, а не на безпекових можливостях. Versa Networks є доцільною для великих розподілених середовищ та сервіс-провайдерів.

Fortinet, який має тривалу історію в галузі мережевої безпеки, поєднав мережеві та безпекові функції в операційній системі FortiOS, що використовується на маршрутизаторах, комутаторах, точках доступу та спеціалізованих пристроях безпеки. Останніми роками локальні системи керування та операційні середовища розширено до хмарних рішень. Стратегічне бачення Fortinet охоплює поточні завдання та майбутні технологічні зрушення (ШІ, IoT, квантові технології), проте темпи інновацій іноді відстають від ринкових. Консолідація систем керування в межах FortiSASE розпочата відносно недавно, а частина нових функцій має базовий характер. Недостатня деталізація дорожньої карти викликає питання щодо реалізації заявлених планів, хоча низька вартість і проста модель ціноутворення залишаються конкурентною перевагою. Fortinet пропонує широкий спектр апаратних рішень та варіантів підключення для віддалених об'єктів, з локалізованими брандмауерами в прошивці. Для повної реалізації функціональності SASE все ще необхідне використання додаткових інструментів (FortiCloud, FortiManager). Компанія забезпечує базовий рівень відповідності новим вимогам SASE, але відстає у сферах управління цифровим досвідом, розширеного контролю доступу до даних, агентного ШІ та єдиної консолі. Клієнтські відгуки підкреслюють економічну ефективність та уніфікованість апаратної платформи, але містять зауваження щодо якості підтримки. Fortinet

доцільно розглядати як варіант для організацій, орієнтованих на вартісну ефективність і побудову захищених локальних мереж із елементами SASE.

Cloudflare еволюціонувала від хмарного «брандмауера» та мережі доставки контенту (CDN) до постачальника глобальної мережі та кіберзахисних сервісів, а з 2020 року — до рішень SASE (Cloudflare One). Стратегія компанії орієнтована на розробницькі спільноти і платформений підхід з компонуємими архітектурними блоками. Разом із тим не в повній мірі враховуються майбутні потреби щодо контролю безпеки для IoT та операційних технологій. Служба підтримки демонструє високу надійність при обробці великого обсягу трафіку, однак складніше адаптується до спеціалізованих вимог віддалених галузевих сегментів. Партнерська екосистема є значною, але має потенціал для подальшої диференціації каналів. Глобальна магістраль Cloudflare забезпечує високу продуктивність, оптимальний вибір маршрутів, можливість зберігання даних на рівні країни та використання виділених вихідних адрес. Водночас спостерігається відставання в окремих функціях периферійних мереж: агент ZTNA має обмежену зрілість, спектр апаратних рішень і сервісів для віддалених майданчиків є відносно вузьким, а можливості DLP та управління цифровим досвідом — менш розвинені, ніж у провідних конкурентів. Клієнти відзначають технічну інтуїтивність і простоту впровадження платформи, але вказують на обмежену гнучкість дизайну мережевих рішень для віддалених локацій. Cloudflare є придатною для організацій із високою часткою розробницьких команд, яким потрібні гнучкі структурні блоки для адаптації архітектури SASE.

SonicWall, один із давніх учасників ринку захищених мереж, увійшов до сегмента SASE через придбання Banyan Security у 2024 році. Раніше портфель компанії включав VPN-брандмауери, маршрутизатори, комутатори та точки доступу, побудовані на основі міжмережевих екранів. Стратегія SonicWall фокусується на поєднанні зрілих брандмауерних функцій у компактні, економічно ефективні рішення, орієнтовані на малий і середній бізнес, а також на освітні та державні установи. Підхід до SASE є еволюційним, з акцентом на інтеграції SD-WAN та SSE в межах програмної платформи SonicPlatform, при цьому значна частина сервісної підтримки делегується партнерським каналам. Дорожня карта

має обмежений характер і орієнтується переважно на задоволення базових потреб. З функціонального боку SonicWall пропонує широкий спектр обладнання та SD-WAN-підключень з локалізованими брандмауерними сервісами, тоді як хмарний компонент Cloud Secure Edge забезпечує середній рівень ZTNA і узгоджений набір SSE-сервісів, але з відносно малою кількістю PoP. Управління SSE та мережевими функціями розділено між двома консолями, що ускладнює формування повністю уніфікованої платформи. Функції SWG, CASB і звітності відстають від більш розвинених рішень. Клієнти високо оцінюють співвідношення вартості й функціональності, хоча емпірична база відгуків обмежена. SonicWall є доцільним вибором для місцевих органів влади, освітніх закладів та малих і середніх підприємств, які потребують базового SASE-функціоналу за конкурентною ціною [19].

Оцінювання здійснювалося за трьома головними категоріями. Поточна пропозиція, що відображається позицією на вертикальній осі діаграми, характеризує зрілість та повноту функціоналу. Стратегія, що відображається на горизонтальній осі, включає бачення розвитку та інноваційний потенціал. Відгуки клієнтів ураховуються через маркери навколо позначок постачальників, з виокремленням постачальників з відгуками вище середнього та винятково високим рівнем задоволеності. Для кожного постачальника розглянуто як свіжі інтерв'ю з референсними клієнтами, так і результати попередніх опитувань.

До звіту включено лише ті рішення, які відповідають низці критеріїв корпоративного рівня. Вимоги стосуються наявності повного набору основних функцій SASE і підтвердженого досвіду підтримки великих організацій; можливості придбання SASE-рішення як окремого продукту з власним артикулом і ціновою моделлю; мінімального рівня доходу від продукту SASE (не менше 75 млн доларів США за останні чотири квартали); значного рівня присутності у свідомості корпоративних клієнтів (регулярні згадки в запитах, консультаціях, рекомендаціях та конкурентних зіставленнях); наявності власного стеку технологій безпеки, який обов'язково включає продукт ZTNA та принаймні SWG чи хмарний шлюз безпеки, що постачаються безпосередньо, а не через партнерства; наявності пристрою для віддалених майданчиків із можливістю фізичного підключення до

WAN, балансування навантаження каналів або функцій маршрутизації, а також єдиного інтерфейсу та консолі керування для мережевих і безпекових сервісів.

Звіт не охоплює повністю весь ландшафт постачальників SASE. Окремі постачальники, відомі на ринку, не потрапили до цього оцінювання з різних причин. Зокрема, для Broadcom відсутня достатня інтеграція між продуктами VMware SD-WAN (VeloCloud) та Symantec, а інтерес клієнтів до її SASE-пропозицій зменшився після придбання VMware. Cisco, попри широкий портфель, ще не забезпечила достатній рівень інтеграції компонентів Umbrella, Secure Access, ThousandEyes, Viptela, Meraki, Duo та інших елементів у єдину платформу SASE. Hewlett Packard Enterprise (HPE) не продемонструвала порівняного рівня інвестицій в інтеграцію компонентів EdgeConnect (SD-WAN/SD-Branch) та SSE, а також залучення клієнтів у сегменті SASE на рівні постачальників, включених до оцінки. Додаткову інформацію про ширший перелік учасників і загальну характеристику ринку наведено в окремому звіті щодо ландшафту граничних послуг безпечного доступу.

Методологія Forrester Wave™ базується на стандартизованій процедурі оцінювання постачальників технологічних ринків. На першому етапі формується початковий список постачальників, після чого застосовуються критерії включення для звуження вибірки до репрезентативної підмножини. Далі збираються детальні дані про продукти й стратегії за допомогою анкет, демонстрацій, брифінгів та інтерв'ю з клієнтами (постачальники можуть запропонувати до трьох референсних клієнтів; додатково враховуються наявні відгуки з інших досліджень). На основі зібраних даних та експертних знань аналітиків здійснюється оцінювання за системою відносних рейтингів, де кожен постачальник порівнюється з іншими в межах дослідження. Чітко фіксується дата, станом на яку приймаються до уваги подані матеріали; для цього звіту останні дані надано до 26 червня 2025 року. До публікації постачальникам надається можливість перевірити коректність фактичних тверджень, не впливаючи на аналітичні висновки. Постачальники, які відповідали критеріям включення, але відмовилися від участі або надали часткову інформацію, відображаються в загальній картині згідно з політикою участі, з

позначенням їх позиції поруч з учасниками, що повністю пройшли процедуру оцінювання [7].

2.2. Архітектура рішення SASE

Безпечний доступ до сервісів на межі (Secure Access Service Edge, SASE) визначається як хмароорієнтована платформа, що консолідує базові мережеві та функції інформаційної безпеки в єдиній архітектурі. Така платформа оптимізує доступ до ресурсів і підвищує рівень захисту, інтегруючи програмно-визначені глобальні мережі (SD-WAN), безпечний веб-шлюз (SWG), брокер безпеки доступу до хмари (CASB), брандмауер як послугу (FWaaS) та мережевий доступ з нульовою довірою (ZTNA). Сукупність цих компонентів забезпечує комплексний захист користувачів, пристроїв і даних незалежно від їх розташування та середовища доступу. Хмарний характер підходу забезпечує гнучкість і масштабованість, необхідні для адаптації до динаміки сучасного цифрового середовища [9].

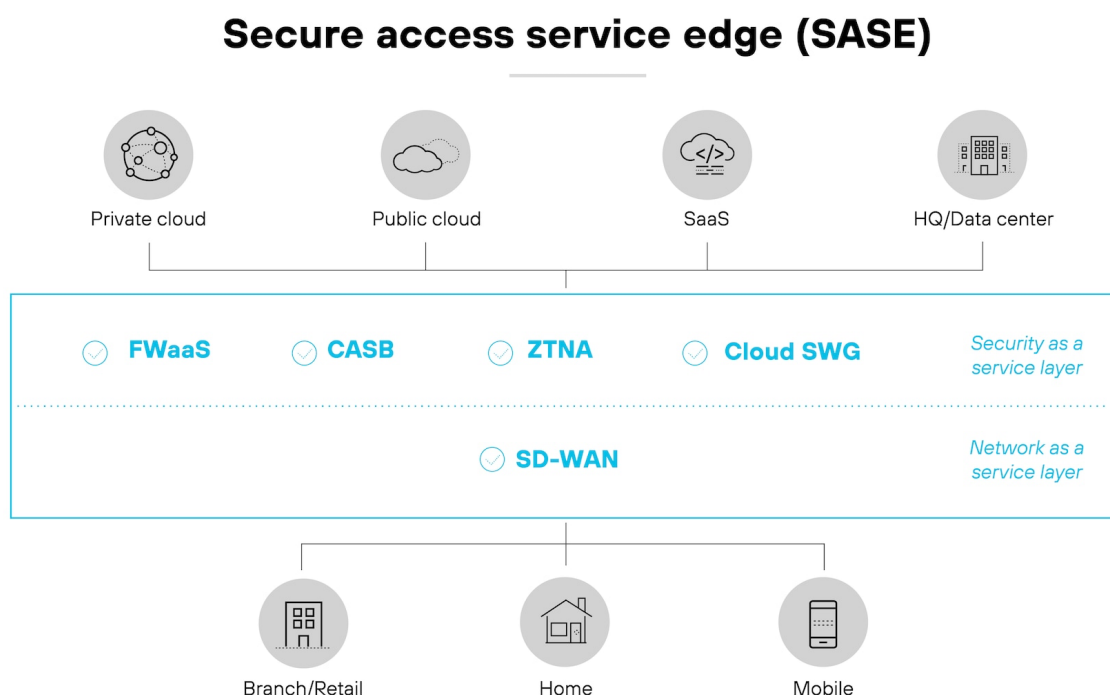


Рис.2.2. Платформа SASE

Необхідність впровадження SASE зумовлюється структурними обмеженнями традиційних моделей мережевої безпеки. Перехід до віддалених і

гібридних форматів роботи, а також масове використання хмарних сервісів виявили недостатність локальних апаратних рішень і фрагментованих точкових засобів захисту. Застарілі периметрові архітектури ускладнюють захист розподіленої робочої сили, яка отримує доступ до хмарних застосунків з різних географічних локацій і типів пристроїв. Використання хмарних засобів безпеки в рамках SASE дає змогу усунути «сліпі зони», сформувати єдиний контур контролю та забезпечити послідовний рівень захисту в масштабах усього підприємства.

Особливе значення SASE набуває в контексті безпечного віддаленого доступу. Умови широкого поширення віддаленої та гібридної роботи висувають вимогу до надання детального, ідентифікаційно-орієнтованого контролю доступу до корпоративних ресурсів. У моделі SASE автентифікація та авторизація ґрунтуються на ідентичності, контексті й ризиковому профілі, що забезпечує доступ до конфіденційних даних виключно авторизованим суб'єктам незалежно від місця їх перебування. Одночасно інтеграція з хмарними середовищами забезпечує необхідну видимість і контроль над хмарним трафіком, зменшуючи ризики витоків даних і несанкціонованого доступу.

Конвергенція мережевих і безпекових функцій в архітектурі SASE істотно спрощує управління інфраструктурою. Замість розрізнених засобів захисту та окремих мережевих рішень формується єдина керована платформа, яка знижує операційну складність, зменшує потребу в ручному усуненні несправностей та дає змогу IT-підрозділам зосереджуватися на стратегічних завданнях замість рутинної експлуатації. Вбудована хмарна модель також полегшує адаптацію до еволюційних змін загроз: завдяки централізованому оновленню політик та механізмів виявлення нові вразливості й техніки атак можуть враховуватися значно оперативніше, ніж у традиційних, суто локальних архітектурах.

Окремою вимогою сучасних організацій є забезпечення прийняттого рівня користувацького досвіду. Архітектура SASE враховує цей аспект шляхом оптимізації маршрутизації та продуктивності мережі, зокрема для віддалених користувачів. Завдяки поєднанню SD-WAN, хмарних точок присутності та контекстно-орієнтованого доступу до застосунків підвищуються стабільність підключення, швидкодія сервісів та загальний рівень продуктивності.

Функціональна модель роботи SASE

Архітектура SASE надає гібридним і віддаленим користувачам захищений доступ до корпоративних програм, даних і сервісів незалежно від фізичного розташування ресурсів. Захист гібридної моделі роботи досягається поєднанням хмарних сервісів безпеки з розширеними мережевими можливостями, що забезпечують безперервний контроль доступу «від краю до краю». У межах конвергентної архітектури SASE IT-підрозділ отримує централізовану видимість та можливість керування гібридним середовищем завдяки єдиному простору налаштувань, автоматизованій конфігурації мережі та послідовному управлінню політиками безпеки.

До хмарних сервісів безпеки SASE належать такі компоненти, як CASB (Cloud Access Security Broker), FWaaS (Firewall as a Service), SWG (Secure Web Gateway) та ZTNA (Zero Trust Network Access). Їх доповнює мережевий компонент SD-WAN, який забезпечує інтелектуальну маршрутизацію трафіку, використання декількох каналів зв'язку та оптимізацію продуктивності. Сукупне функціонування цих компонентів формує цілісний механізм контролю доступу й фільтрації трафіку.

Components of SASE

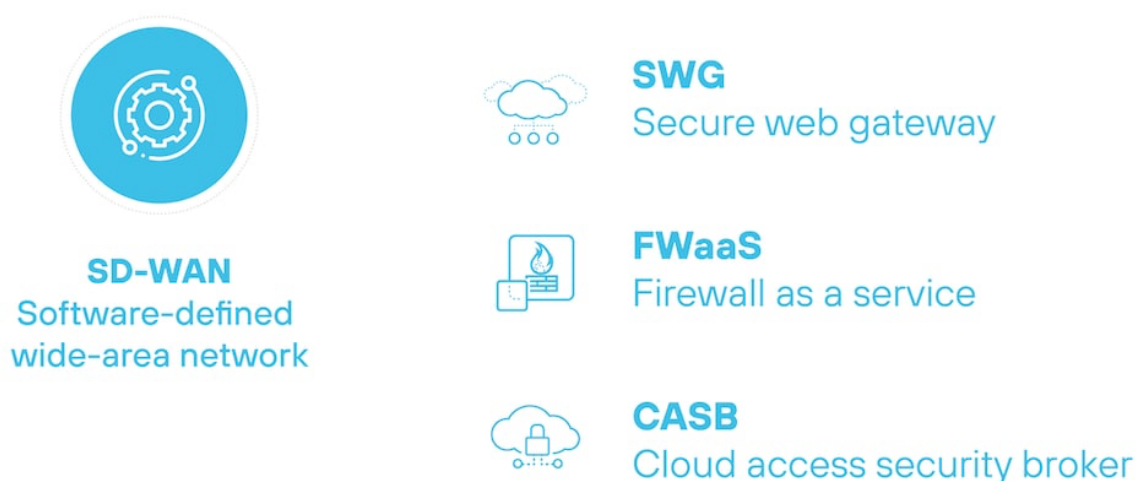


Рис.2.3. Компоненти SASE

Ефективність архітектури SASE визначається саме безперервною інтеграцією її складових. Безпечний веб-шлюз (SWG) виконує роль фільтраційного та захисного бар'єра між користувачами й мережею Інтернет. У його функціональність входять аналіз і фільтрація веб-трафіку, блокування шкідливого вмісту, запобігання доступу до ресурсів з високим ризиком, а також протидія фішинговим атакам, завантаженню шкідливих програм та іншим веб-орієнтованим загрозам.

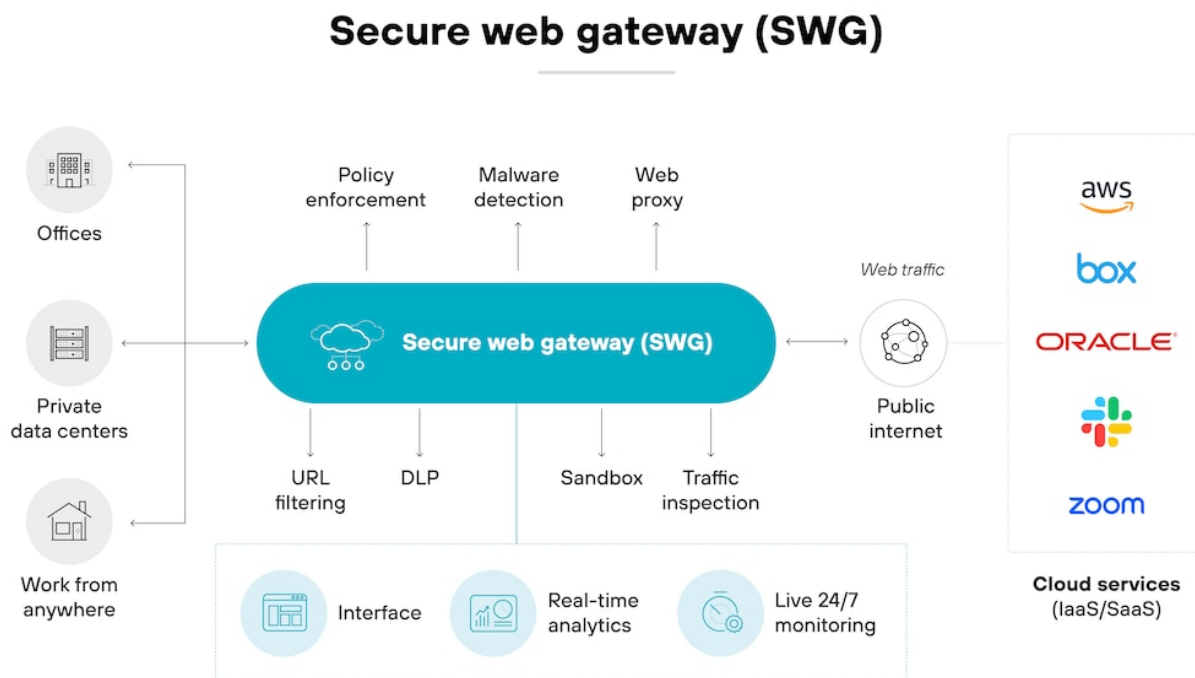


Рис.2.4. Архітектура SWG

Брокер безпеки доступу до хмари (CASB) забезпечує прозорість і контроль над використанням хмарних застосунків. Він виконує завдання контролю дотримання політик безпеки, запобігання втраті даних і підтримки регуляторної відповідності під час доступу до сервісів типу SaaS. CASB застосовує політики безпеки на шляху між користувачем і хмарним застосунком, виконує аналіз хмарних ресурсів та дозволяє оцінювати ризики, пов'язані з використанням тих чи інших хмарних сервісів. У поєднанні з API-орієнтованим доступом можливе поглиблене аналізування вмісту, який передається до хмарних застосунків (наприклад, завантажених файлів або повідомлень).

CASB (cloud access security broker)

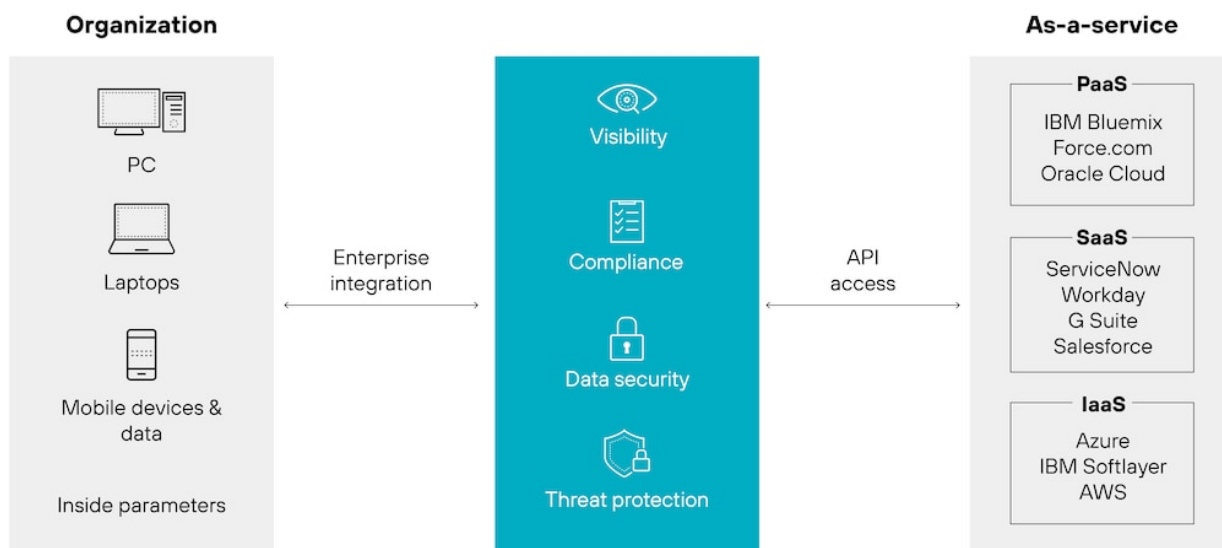


Рис.2.5. Архітектура CASB

Мережевий доступ з нульовою довірою (ZTNA) реалізує суворий контроль доступу на основі ідентичності та контексту. У межах цього підходу не вважається довіреним жоден користувач або пристрій за замовчуванням, незалежно від розташування. Надання доступу до ресурсів здійснюється лише після успішної перевірки та оцінки контекстних параметрів (тип пристрою, місцезнаходження, ризикові сигнали тощо). У результаті мінімізується ризик несанкціонованого доступу та латерального переміщення в мережі, а доступ обмежується конкретними застосунками або сервісами, на відміну від класичних VPN, що часто відкривають доступ до цілих мережевих сегментів.

Zero Trust network access (ZTNA)

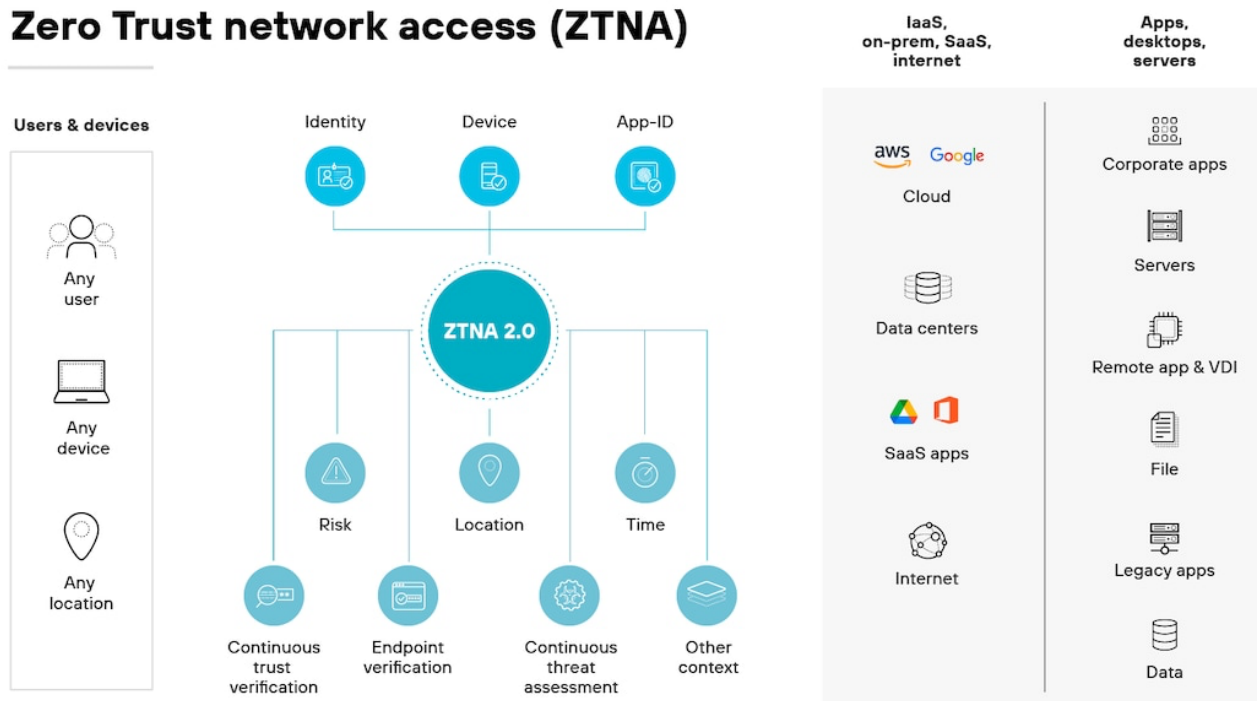


Рис.2.6. Архітектура ZTNA

Брандмауер як послуга (FWaaS) забезпечує функціональність міжмережевого екрану нового покоління в хмарній формі. Трафік аналізується на рівні застосунків, виявляються й блокуються загрози, застосовуються політики безпеки незалежно від фізичного розташування користувача або ресурсу. Хмарна модель FWaaS забезпечує масштабованість і гнучкість, дає змогу динамічно адаптувати конфігурацію до змін навантаження та структури мережі.

Firewall as a service (FWaaS), also known as a cloud firewall

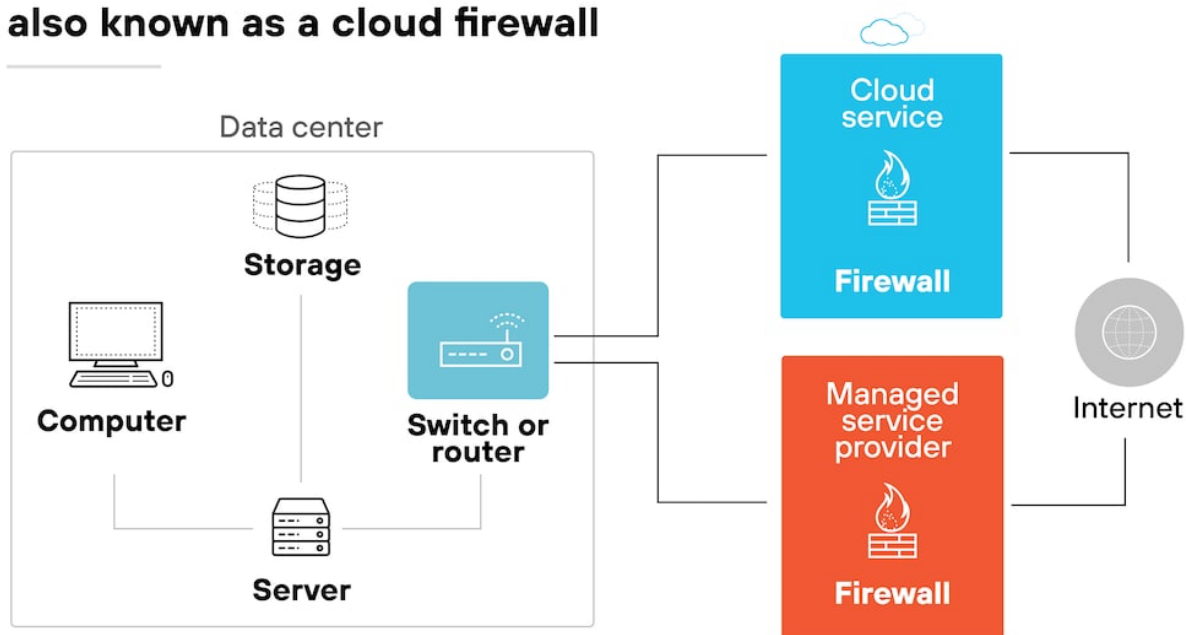


Рис.2.7. Архітектура FWaaS

Програмно-визначена глобальна мережа (SD-WAN) оптимізує мережеве підключення, інтелектуально маршрутизуючи трафік між декількома каналами зв'язку. SD-WAN підвищує продуктивність критично важливих застосунків, оптимізує використання наявних каналів та забезпечує стабільний користувацький досвід, у тому числі для віддалених працівників, що звертаються до ресурсів у хмарних середовищах.

SD-WAN architecture

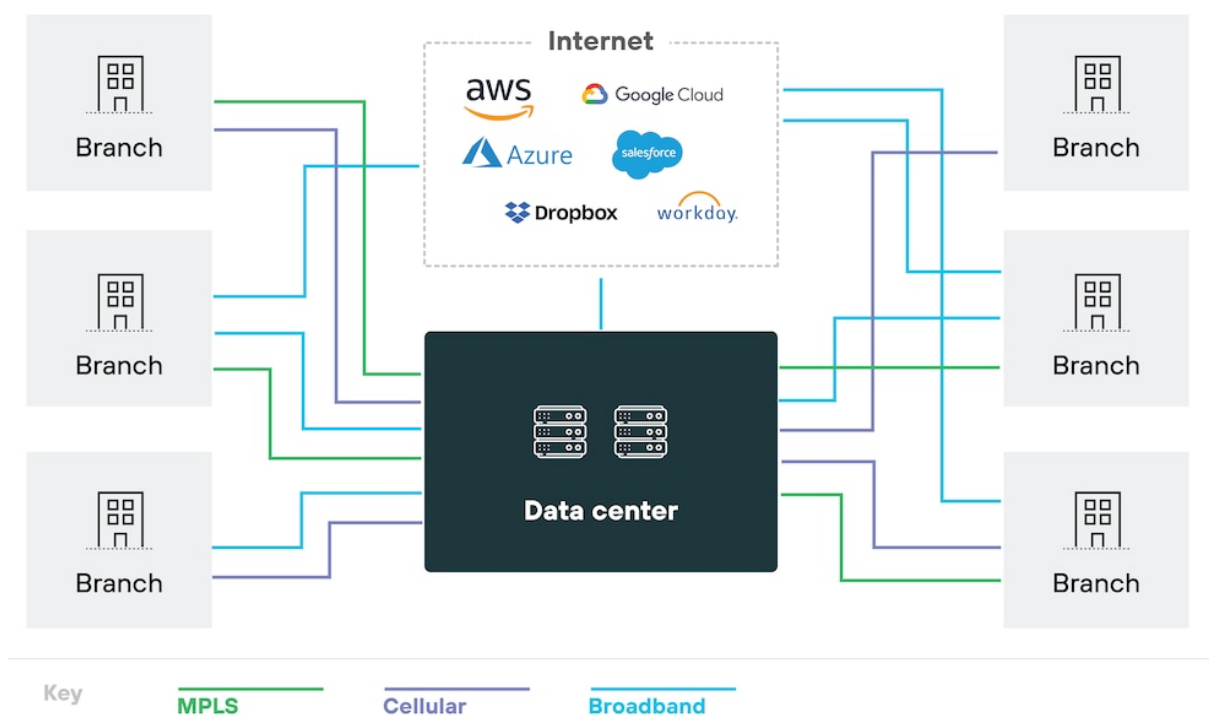


Рис.2.8. Архітектура SD-WAN

Усі ці компоненти інтегруються в рамках централізованого управління. SASE консолідує управління мережевими й безпековими функціями на єдиній хмарній платформі. Це спрощує адміністрування, підвищує узгодженість застосування політик та забезпечує цілісне уявлення про стан мережі, користувачів, пристроїв і застосунків.

SASE в контексті гібридної робочої сили та гібридної хмари

Архітектура SASE підтримує цілісний підхід до захисту, спрямований на безпечне підключення будь-якого користувача до будь-якої платформи в будь-якому місці. Гібридним працівникам забезпечується однаковий рівень захисту й доступності, незалежно від того, чи працюють вони в офісі, у віддаленій локації чи в умовах мобільного доступу. Конвергентні хмарні сервіси безпеки та мережеві сервіси формують єдиний контур управління, у межах якого продуктивність і безпека розглядаються як взаємопов'язані параметри.

Повністю конвергентні рішення SASE підвищують операційну ефективність завдяки спрощенню управління, уніфікації політик безпеки в усіх точках доступу

та реалізації принципів нульової довіри як базового підходу. Управління хмарною безпекою відбувається з урахуванням того, що політики та механізми контролю мають «супроводжувати» користувача незалежно від зміни пристрою, мережі або географічного розташування. Формується послідовна позиція безпеки, яка поширюється на користувачів, пристрої, застосунки та дані в масштабах усього підприємства.

Ключовими умовами досягнення позиції безпеки за моделлю нульової довіри є централізоване управління й повна видимість активності; єдина політика безпеки для всіх середовищ; поєднання мережевих функцій з можливостями глобальної мережевої інфраструктури; контекстно-орієнтована ідентифікація користувачів; використання хмарних сервісів для реалізації безпекових та мережевих функцій; наявність географічно розподілених точок присутності.

Підхід SASE також фокусується на кореляції користувацького досвіду з бізнес-результатами. Єдиний інтерфейс управління та уніфіковані показники дають змогу пов'язувати стан мережі, продуктивність застосунків і задоволеність кінцевих користувачів із ключовими показниками ефективності організації. Завдяки уніфікованому рішенню, яке замінює множину VPN і окремих систем захисту, досягається значне зниження операційної складності. Аналітичні засоби, попередньо підготовлені та динамічно сформовані звіти, детальне журналювання подій для користувачів, кінцевих точок і застосунків, а також моніторинг цифрового досвіду (Digital Experience Monitoring, DEM) забезпечують необхідну видимість для підтримання прийнятного рівня продуктивності та якості обслуговування.

Переваги SASE як архітектурного фреймворку

Фреймворк SASE забезпечує інтеграцію розширених мережевих і безпекових можливостей у єдине хмарне рішення. Така конвергенція створює низку відчутних переваг для розподілених підприємств. Посилення безпеки досягається за рахунок усунення прогалин, притаманних фрагментованим наборам точкових рішень, і шляхом впровадження узгоджених політик у різних середовищах. Централізована реалізація доступу за принципом нульової довіри гарантує, що доступ до ресурсів

отримують лише перевірені користувачі та пристрої, що знижує ймовірність несанкціонованих вторгнень.

Складність управління значною кількістю інструментів безпеки та мережових функцій зменшується через уніфікацію в межах однієї платформи. Це спрощує адміністрування, зменшує накладні витрати та звільняє ресурси ІТ-команд для стратегічних ініціатив. Хмарний характер рішень SASE дає змогу перейти від капітальних витрат на апаратне забезпечення та ліцензії до моделей, побудованих на операційних витратах, зокрема підписних або використання-орієнтованих моделей ліцензування. Таким чином забезпечується прогнозованість витрат і знижується загальна вартість володіння.

Поліпшення продуктивності мережі відбувається завдяки використанню SD-WAN, яка оптимізує маршрутизацію трафіку та визначає пріоритети для критично важливих застосунків. Це особливо важливо для віддалених працівників, які отримують доступ до хмарних ресурсів через різні мережові канали. Підвищена продуктивність безпосередньо впливає на продуктивність праці та кінцеві бізнес-результати.

У контексті безпеки SASE надає повний спектр сервісів — від запобігання загрозам до політик NGFW на будь-якому «краю» мережі — з підтримкою доступу за принципом нульової довіри як базової моделі. Об'єднання ключових мережових і безпекових функцій у межах єдиної платформи дозволяє подолати «розростання» точкових продуктів, зменшити як капітальні, так і операційні витрати й спростити архітектуру. Використання хмарної інфраструктури забезпечує можливість безпечного підключення користувачів до Інтернету, застосунків і корпоративних ресурсів незалежно від їхнього місцезнаходження.

Security Service Edge (SSE) як складова SASE

Security Service Edge (SSE) розглядається як хмарна служба безпеки, що забезпечує безпечний веб-доступ, автентифікований доступ до приватних застосунків і захищений доступ до SaaS-сервісів. SSE зазвичай включає FWaaS, SWG, ZTNA та CASB. FWaaS надає функції міжмережевого екрану наступного покоління (включно з IPS, захистом від шкідливого ПЗ, веб-захистом, протидією спаму, можливостями «пісочниці») через хмару. SWG перевіряє веб-активність

кінцевих користувачів і застосовує узгоджені політики безпеки (зокрема, DLP, глибоку перевірку SSL, фільтрацію URL та DNS-фільтрацію). ZTNA забезпечує безпечний віддалений доступ до застосунків та даних на основі чітко визначених політик контролю доступу, надаючи доступ лише до певних сервісів або застосунків, а не до всієї мережі. CASB формує єдину площину керування політиками для використання хмарних сервісів, контролює типи доступу до застосунків і аналізує контент, що передається до хмарних середовищ [10].

SASE виконує функцію конвергентного фреймворку, що дозволяє організаціям прискорювати трансформацію, спираючись на підхід нульової довіри, підтримуючи гібридні формати роботи, спрощуючи операції й знижуючи витрати. Архітектура SASE забезпечує узгоджені політики безпеки як у локальних середовищах, так і в публічних і приватних хмарах, знижуючи наслідки потенційних кібератак через контроль доступу на основі ідентичності.

Надання SASE як хмарного сервісу спрощує адаптацію для кінцевих користувачів і IT-фахівців, сприяє переходу до моделей операційних витрат і дозволяє гнучко керувати витратами завдяки використанню підписних схем або тарифікації на основі використання. Географічно розподілені точки присутності забезпечують низьку затримку й оперативний доступ до сервісів мережевої безпеки для віддалених користувачів. Повністю інтегровані рішення SASE зменшують складність IT-операцій завдяки централізованому управлінню, уніфікованим політикам безпеки та використанню аналітики загроз на основі штучного інтелекту, яка доповнює роботу команд безпеки та управління мережею.

У співвідношенні між SASE та SSE (Security Service Edge) SASE розглядається як комплексний фреймворк, що включає SD-WAN, SWG, CASB, NGFW та ZTNA і формує єдиний підхід до захисту всієї мережевої архітектури, включно з доступом користувачів, захистом даних і запобіганням загрозам. SSE, у свою чергу, є підмножиною SASE та зосереджується переважно на аспектах безпеки доступу до Інтернету, хмарних сервісів і приватних застосунків. Таким чином, SSE покриває критичні безпекові потреби, тоді як SASE поєднує функції оптимізації мережевої інфраструктури з розширеними механізмами захисту.

Ефективність рішень SASE безпосередньо залежить від ступеня інтеграції їхніх мережових та безпекових компонентів. Для досягнення належних характеристик усі елементи — підключення, мережа та безпека — мають взаємодіяти як єдина система. Повністю конвергентні платформи, що поєднують хмарні сервіси безпеки з розширеними мережевими можливостями, дають змогу реалізувати підхід нульової довіри без зниження продуктивності або деградації користувацького досвіду. На ринку, що швидко розвивається, лише обмежена кількість постачальників пропонує такі цілісні рішення; значна частина гравців надає часткові реалізації або набори партнерських продуктів із обмеженим ступенем взаємної інтеграції. З огляду на те, що SASE покликаний підвищувати рівень безпеки організацій, критично важливими залишаються детальна видимість і контроль як основа для проактивного управління доступом користувачів з будь-якого місця.

У процесі вибору та оцінки рішень SASE особливу увагу приділяється наявності єдиної, повністю конвергентної платформи від одного постачальника. Такий підхід спрощує операції завдяки централізованому хмарному управлінню, зручнішому впровадженню та використанню аналітики загроз на основі штучного інтелекту. Повноцінне рішення SASE має забезпечувати єдину систему, що об'єднує мережові та безпекові сервіси, уніфікований агент для реалізації послідовної політики безпеки, захищений доступ до Інтернету та внутрішніх ресурсів, гнучкий і безпечний доступ до публічних хмар, захищений доступ до SaaS-застосунків, економічно ефективну модель споживання та спрощену адаптацію, централізоване управління хмарними сервісами, механізми корпоративного рівня захисту з ШІ-орієнтованою аналітикою загроз, географічно розподілені точки присутності, а також підтримку з боку постачальників із високою фінансовою стійкістю та глобальними каналами збуту [16].

Узагальнено SASE розглядається як зміна парадигми в захисті мережевої інфраструктури, що виходить за межі можливостей традиційних локальних пристроїв і фрагментованих засобів безпеки. Конвергентний підхід, який поєднує мережу та безпеку в єдиній хмарній платформі, створює передумови для послідовної реалізації принципів нульової довіри, підвищення продуктивності,

зменшення складності та оптимізації витрат, що є ключовими вимогами до захисту сучасних розподілених організацій.

2.3. Аналіз основних функцій та можливостей SASE

Безпечний доступ до сервісів на межі (Secure Access Service Edge, SASE) розглядається як хмарно орієнтована архітектура, що інтегрує мережеві та функції кібербезпеки в єдину платформу-послугу. У типовій реалізації SASE поєднуються програмно визначена глобальна мережа (SD-WAN), безпечний веб-шлюз (SWG), брокер безпеки хмарного доступу (CASB), брандмауер як послуга (FWaaS) і мережевий доступ з нульовою довірою (ZTNA). Об'єднання цих компонентів у хмарі дає змогу спростити управління мережевою інфраструктурою, уніфікувати політики безпеки та забезпечити масштабований захист користувачів, пристроїв і даних у розподілених середовищах.

Сучасне бізнес-середовище формується в умовах децентралізації IT-інфраструктури, масового впровадження хмарних сервісів, віддаленої та гібридної роботи, а також мобільного доступу до ресурсів. У результаті дані та користувачі більше не обмежуються межами локального офісу, а традиційні периметрові моделі безпеки втрачають ефективність. За даними галузевих досліджень, переважна більшість робочих навантажень розміщується на хмарних платформах, тоді як виключно локальні рішення становлять лише незначну частку, що свідчить про системний перехід до хмарної інфраструктури. Аналітичні прогнози вказують на те, що ринок рішень класу SASE зростає високими темпами й у середньостроковій перспективі досягатиме багатомільярдних обсягів, при цьому очікується одночасне співіснування моделей з одним і кількома постачальниками.

У таких умовах SASE виконує функцію інфраструктурного фреймворку, що вбудовує засоби безпеки безпосередньо в мережеву тканину. Кожен запит доступу до ресурсів розглядається як об'єкт політики безпеки, незалежно від місця розташування користувача, пристрою чи застосунку. Інтеграція механізмів захисту в єдиній платформі створює передумови для централізованого керування політиками, зменшення адміністративного навантаження, підвищення

узгодженості контролів і забезпечення запобігання загрозам у режимі, наближеному до реального часу, у всіх середовищах розгортання.

Гнучкість і масштабованість хмарної моделі SASE роблять її ключовим елементом для захисту розподілених ресурсів на тлі триваючої цифрової трансформації та зростання складності кіберзагроз.

Архітектура SASE поєднує мережеві та безпекові функції як сервіс у єдиному хмарному рішенні на мережевому краї. Доступ гібридних і віддалених користувачів до корпоративних ресурсів забезпечується через географічно розподілені хмарні шлюзи (PoP), а не через зворотне тунелювання трафіку до центральних центрів обробки даних. Такий підхід зменшує затримку, знижує навантаження на центральну інфраструктуру та покращує стійкість мережі.

Усі запити до застосунків і даних проходять наскрізну перевірку на рівні хмарних сервісів безпеки. Контроль здійснюється на всіх портах і протоколах, що забезпечує повну видимість трафіку та єдине застосування політик незалежно від того, чи ресурс розміщено в локальному центрі обробки даних, у публічній хмарі чи в SaaS-сервісі. Периметр безпеки в такій моделі перестає бути статичним фізичним кордоном й перетворюється на узгоджений набір хмарних можливостей, які можуть розгортатися там і тоді, де це необхідно.

Таким чином, SASE замінює традиційний підхід побудови периметра навколо центру обробки даних із використанням різнорідних локальних пристроїв безпеки на єдину платформу з централізованим управлінням, що адаптується до змін бізнес-вимог, еволюції загроз та появи нових технологій.

SASE застосовується для вирішення низки типових завдань сучасних організацій. Одним із ключових сценаріїв є підтримка гібридної робочої моделі. Хмарна платформа SASE забезпечує масштабовану, еластичну та низьколатентну інфраструктуру, оптимізовану під конкретні застосунки, і використовує засоби моніторингу цифрового досвіду (Digital Experience Monitoring, DEM) для детальної видимості факторів, що впливають на продуктивність користувачів. Поєднання мережевих і безпекових компонентів у межах однієї архітектури покращує виявлення загроз, зменшує фрагментацію контролів і спрощує управління, що є критичним для стійкої роботи гібридної робочої сили.

Другим важливим сценарієм є підключення й захист філій та роздрібних точок. Архітектура SASE, спираючись на SD-WAN наступного покоління, оптимізує пропускну здатність, забезпечує динамічний розподіл трафіку між каналами та застосовує контекстно залежні політики безпеки ближче до місця виникнення трафіку. Підтримка DEM дає змогу підтримувати стабільний користувацький досвід, а централізоване управління політиками знижує витрати на мережу й безпеку та спрощує роботу з постачальниками. Водночас узгоджені політики й реалізація принципів нульової довіри забезпечують захист даних і застосунків незалежно від фізичного розташування.

SASE відіграє ключову роль у підтримці хмарних і цифрових ініціатив. Консолідація функцій безпеки в хмарній платформі усуває обмеження апаратних підходів, спрощує розгортання в філіях і покращує керованість. Розширені механізми SD-WAN збільшують доступну пропускну здатність, забезпечують глибшу аналітику мережевого трафіку та сприяють підвищенню продуктивності критично важливих застосунків. Компоненти, що використовують штучний інтелект і машинне навчання, покращують виявлення загроз, а динамічні брандмауери забезпечують контекстний аналіз вмісту й контроль потоків даних, включно з трафіком від пристроїв Інтернету речей [16].

Ще одним значущим напрямом застосування є забезпечення глобальної зв'язності. SASE покладається на розподілену мережу хмарних точок присутності, які розміщуються в різних регіонах і країнах. Користувачі підключаються до найближчої точки присутності, що мінімізує відстань передавання даних, знижує затримку та забезпечує стабільну продуктивність і надійність мережі незалежно від географії.

Важливим сценарієм є також міграція з MPLS-мереж на SD-WAN у межах архітектури SASE. Традиційні MPLS-рішення характеризуються високою вартістю, обмеженою гнучкістю та тривалими циклами розгортання. Використання Інтернет-каналів для побудови захищених, високопродуктивних накладених мереж у рамках SD-WAN дає змогу перейти до більш масштабованої й економічно ефективної моделі. У результаті підвищується гнучкість і стійкість мережі,

оптимізується продуктивність локальних і хмарних застосунків, а процес розгортання істотно прискорюється порівняно з класичними MPLS-підходами [18].

Застосування SASE надає низку системних переваг. Забезпечується цілісна видимість гібридного мережевого середовища організації, включно з центрами обробки даних, головними офісами, філіями, віддаленими майданчиками та публічними й приватними хмарами. Ця видимість охоплює користувачів, дані та застосунки й доступна через уніфікований інтерфейс.

Завдяки класифікації трафіку на рівні застосунків (L7) зникає необхідність складної кореляції портів і сервісів, підвищується прозорість використання застосунків і посилюється контроль за їхнім доступом. Об'єднання моніторингу та звітності в єдиній платформі дає змогу мережевим і безпековим командам ефективніше співвідносити події та сповіщення, прискорювати діагностику інцидентів і скорочувати час реагування.

Перенесення значної частини функцій у хмару зменшує операційну складність і витрати на підтримку множини точкових рішень. Пріоритизація послідовного захисту даних у всіх периферійних локаціях через єдині політики зменшує ризики, пов'язані із «сліпими зонами» та несинхронністю налаштувань. Економічний ефект досягається за рахунок можливості розширювати мережевий і безпековий стек на всі локації без пропорційного зростання капітальних і операційних витрат.

Єдине комплексне управління знижує адміністративне навантаження та скорочує час, необхідний для навчання й утримання персоналу. Консолідація функцій у межах однієї хмарної платформи зменшує потребу в інтеграції різномірних продуктів. Інтеграція можливостей SD-WAN (балансування навантаження, агрегація каналів, резервування) покращує продуктивність і надійність мережі, а засоби DEM оптимізують користувацький досвід без потреби у додатковому програмному чи апаратному забезпеченні на кінцевих точках.

Впровадження SASE супроводжується низкою організаційних і технологічних викликів. Необхідним є переосмислення ролей у межах ІТ-підрозділів, зокрема у гібридних хмарних середовищах, де тісна взаємодія

мережевих і безпекових команд стає критичною. Це може потребувати перегляду традиційних меж відповідальності.

Висока інтеграційна здатність SASE водночас ускладнює навігацію в ландшафті постачальників, оскільки пропонуються як повністю конвергентні рішення, так і часткові комплекси та партнерські зв'язки. Забезпечення повного покриття вимог, особливо за наявності великої кількості філій, іноді потребує комбінування хмарних і локальних компонентів.

Додатковим фактором є потреба формування довіри до хмарно орієнтованої моделі безпеки в професійній спільноті, зокрема в контексті критичних і гібридних сценаріїв. Відбір і інтеграція продуктів SASE в організаціях зі структурно розділеними ІТ-командами можуть вимагати комбінування кількох рішень для окремого задоволення мережевих і безпекових потреб. Перехід до хмарної моделі здатний зробити частину наявних інструментів надлишковою, тому постає завдання ідентифікації та усунення дублюючих засобів для уникнення фрагментації функцій. Успішність впровадження значною мірою залежить від узгоджених дій фахівців із мереж та безпеки, оскільки їхній сумарний досвід забезпечує коректне зіставлення компонентів SASE зі стратегічними цілями організації.

Гнучкість архітектури SASE зумовлює її придатність до інтеграції з різними технологічними доменами, зокрема 5G, Інтернетом речей та платформами запобігання витоку даних (DLP).

У випадку 5G спостерігається істотне зростання швидкостей передавання даних і зменшення затримок, а також поступовий відхід від традиційних мережевих архітектур. Це породжує нові вимоги до безпеки мобільних середовищ. Використання SASE як централізованого рівня безпеки, через який маршрутизується 5G-трафік, дозволяє забезпечувати узгоджені політики й підвищувати операційну ефективність. Компонент SD-WAN додатково оптимізує маршрути та підвищує стійкість, формуючи захищену високопродуктивну платформу для розподіленого доступу до корпоративних ресурсів [20].

В контексті Інтернету речей традиційні моделі, що залежать від централізованих мереж провайдерів, призводять до ускладненої маршрутизації й

підвищеної затримки, особливо за умов масового розміщення пристроїв у багаторегіональних хмарах. SASE забезпечує централізований контроль політик і оптимізує маршрутизацію, поєднуючи віртуалізовані мережеві та безпекові сервіси. Переміщення контролю ближче до джерел даних через розподілені точки присутності дає змогу автентифікувати доступ на основі атрибутів пристрою, зменшувати затримку, зміцнювати безпеку IoT-середовища та враховувати регіональні вимоги до обробки даних.

У сфері захисту даних SASE компенсує обмеження традиційних систем DLP, які часто виявляються недостатньо гнучкими для роботи з високо розподіленими IT-ландшафтами. Консолідація DLP-можливостей з іншими засобами захисту в єдиній хмарній інфраструктурі дає змогу застосовувати точні політики безпеки безпосередньо до даних у процесі їх переміщення мережами й хмарними сервісами. Підвищується видимість і керованість конфіденційною інформацією, формується більш стійка модель захисту, здатна адаптуватися до динамічних кіберзагроз і складних інфраструктурних конфігурацій.

Узагальнюючи, SASE постає як архітектурний фреймворк, що конвергує мережу та безпеку, забезпечує реалізацію принципів нульової довіри, підвищує продуктивність, знижує складність і створює основу для інтеграції з іншими ключовими технологіями в сучасних розподілених IT-середовищах [11].

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ НА ОСНОВІ РІШЕННЯ SASE

3.1. Варіант розгортання системи забезпечення безпеки на базі Netskope SASE

Ефективна імплементація SASE передбачає структурований багатокроковий підхід. На початковому етапі формуються передумови координації, зокрема організовується тісна взаємодія мережових і безпекових команд. Враховуючи історичні відмінності у пріоритетах (продуктивність проти захисту), доцільним є створення міжфункціональної групи, що включає представників ІТ, інформаційної безпеки, комплаєнсу й ключових бізнес-підрозділів, а також використання експертної підтримки постачальників та консультантів.

На наступному етапі розробляється гнучка дорожня карта впровадження. Інтеграція сервісів SASE відбувається поступово, узгоджуючись з поточними ІТ-ініціативами та бізнес-пріоритетами. Розгортання може починатися з модернізації SD-WAN чи підвищення рівня безпеки в окремих сегментах, використовуючи SASE як засіб як конвергенції, так і поступового розвитку архітектури.

Паралельно забезпечується підтримка керівництва. Обґрунтування доцільності впровадження ґрунтується на оцінці рентабельності інвестицій, порівнянні поточних витрат на мережу й безпеку з очікуваними після переходу до SASE, врахуванні економії від зменшення простоїв і вартості підвищеної гнучкості. Важливим аргументом виступає комплексний характер захисту в умовах ескалації загроз. У процесі реалізації проєктів результати доцільно вимірювати за чітко визначеними показниками.

Далі формулюються конкретні цілі впровадження, адаптовані до специфіки організації, аналізується поточна мережева конфігурація, визначаються «вузькі місця» та проводиться аудит наявних компетенцій і технологій, що дозволяє оцінити готовність до переходу.

На етапі вибору й розгортання відбираються рішення SASE, сумісні з існуючою інфраструктурою, з пріоритетом повної інтеграції з поточними інструментами. Доцільним є поетапне впровадження з використанням пілотних зон або обмежених груп користувачів, що дозволяє отримувати зворотний зв'язок і коригувати конфігурацію до масштабування.

Після розгортання здійснюється безперервний моніторинг роботи платформи, оцінюється її ефективність, проводиться оптимізація налаштувань з урахуванням відгуків, технологічних трендів і змін у вимогах організації. Формуються сталі механізми підтримки, що забезпечують стабільне функціонування рішення.

Клієнт Netskope підтримує взаємодію з кількома сервісами платформи, зокрема Netskope Private Access, Cloud Firewall, SWG, Endpoint DLP, Endpoint SD-WAN та DEM. У випадку Private Access клієнт встановлюється на основні платформи (Windows, macOS, Linux, iOS, Android, ChromeOS) і спрямовує трафік приватних застосунків до відповідних шлюзів доступу; альтернативою є доступ через браузер. Для хмарного брандмауера клієнт перенаправляє як веб-, так і невеб-трафік: HTTP(S) потоки доставляються на проксі Netskope, а інші протоколи – на компонент Cloud Firewall, після чого виконується аналіз згідно з налаштованими політиками, а події відображаються в консолі адміністратора. Принципи роботи та взаємодії клієнта з конфігураціями керування трафіком додатково проілюстровані на схемах, що демонструють структуру SSL-тунелю, завершення його на хмарному проксі та розповсюдження конфігурацій серед клієнтів [12].

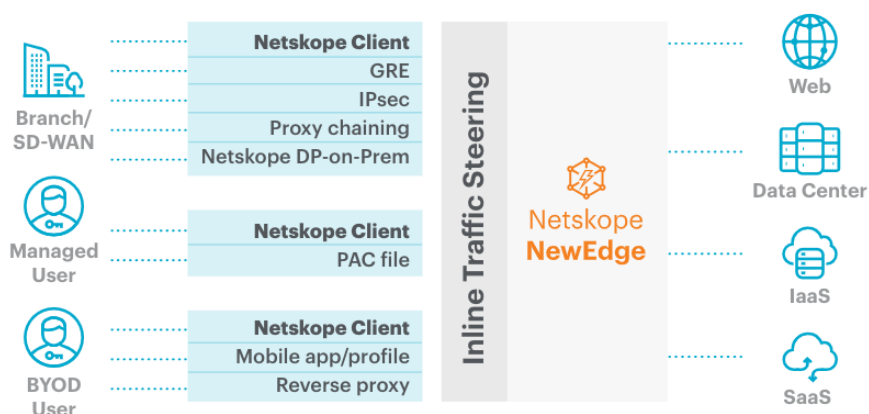


Рис.3.1. Варіант розгортання клієнта Netskope

У підсумку описана послідовність дій забезпечує повний цикл швидкого розгортання Netskope: від інтеграції каталогів користувачів і налаштування мережевої інфраструктури до розгортання клієнта, визначення профілів керування, обхідних маршрутів, параметрів клієнта та впровадження базового набору політик безпеки. Такий підхід дає змогу отримати централізовану видимість та контроль над доступом до веб-ресурсів і хмарних сервісів із будь-якого місця розташування користувачів та кінцевих пристроїв.

Швидкий запуск платформи Netskope у корпоративному середовищі передбачає виконання двох базових дій: інтеграцію облікових записів користувачів з платформою та розгортання клієнта Netskope на кінцевих пристроях. Інтеграція з наявною службою ідентифікації (наприклад, Azure AD або Okta через SCIM-інтерфейс чи синхронізація з локальною службою Active Directory за допомогою інструмента імпорту каталогів) забезпечує передавання до Netskope повного набору атрибутів ідентифікації. Це дає змогу пов'язувати трафік з конкретними користувачами та застосовувати політики доступу, орієнтовані на ці атрибути (зокрема, реалізовувати винятки для окремих груп, таких як підрозділи маркетингу чи IT). Паралельно розгортання клієнта Netskope на робочих станціях і мобільних пристроях створює основний канал спрямування трафіку в хмару Netskope, де здійснюється аналіз і примусове виконання політик. Клієнт є малоресурсним, оскільки оброблення трафіку переноситься до хмарної інфраструктури, а стандартна конфігурація орієнтована на перехоплення веб-трафіку без необхідності додаткових налаштувань одразу після інсталяції [14].

Першим етапом розгортання є отримання доступу до консолі адміністратора Netskope. Консоль забезпечує централізоване керування політиками, перегляд журналів та інцидентів, а також налаштування всіх сервісів хмарної платформи. Доступ до неї здійснюється за унікальною для кожного тенанта URL-адресою у форматі <https://tenant-name.goskope.com> (або з регіональними доменами au.goskope.com, eu.goskope.com тощо). Типовий вигляд панелі керування, де відображаються основні показники та розділи конфігурації, ілюструється на

рисунку з панеллю керування консолі адміністратора Netskope. Увійти до консолі можливо за обліковими даними адміністратора, які надаються під час створення тенанта; у разі їх відсутності доступ відновлюється через службу підтримки або команду супроводу облікового запису.

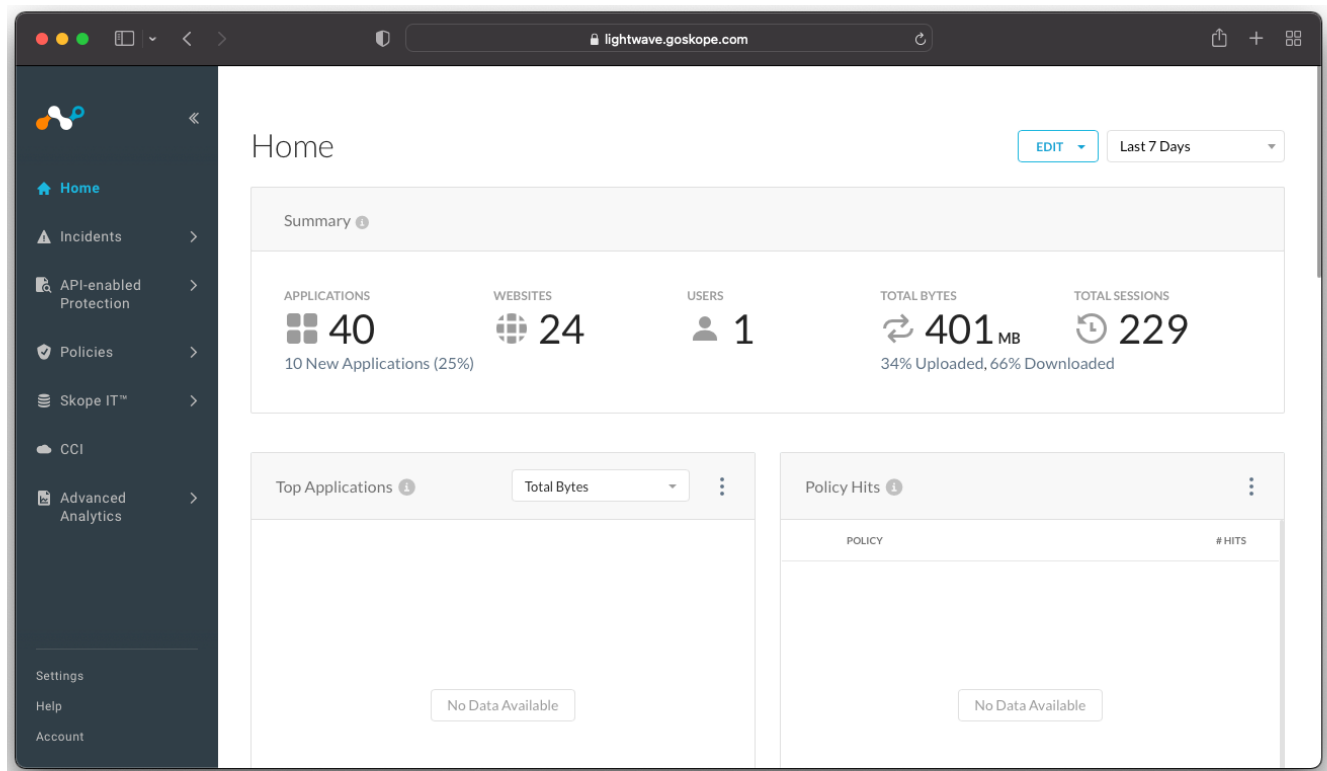


Рис.3.2. Консоль адміністратора Netskope

URL-адреса для входу в консоль адміністратора унікальна. Подальшим кроком є створення та розмежування ролей адміністраторів. У розділі налаштувань адміністратора відкривається сторінка керування адміністраторами, де додаються нові облікові записи керування, для яких вказуються адреси електронної пошти та ролі доступу.

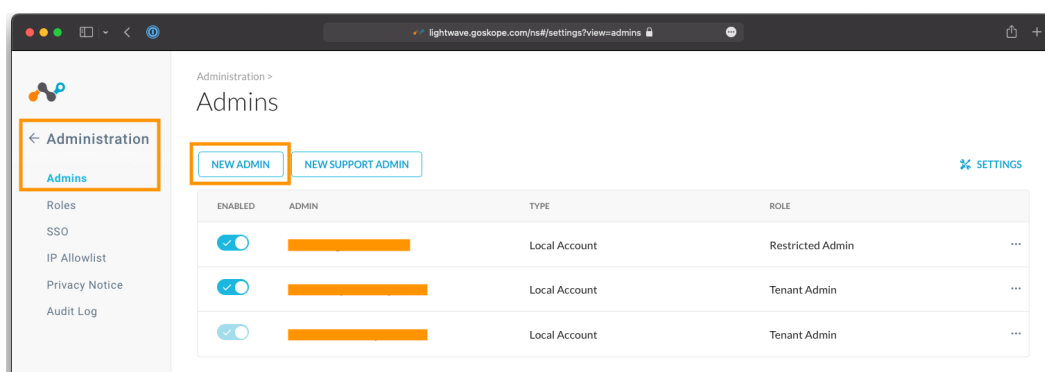


Рис.3.3. Сторінка керування адміністратором

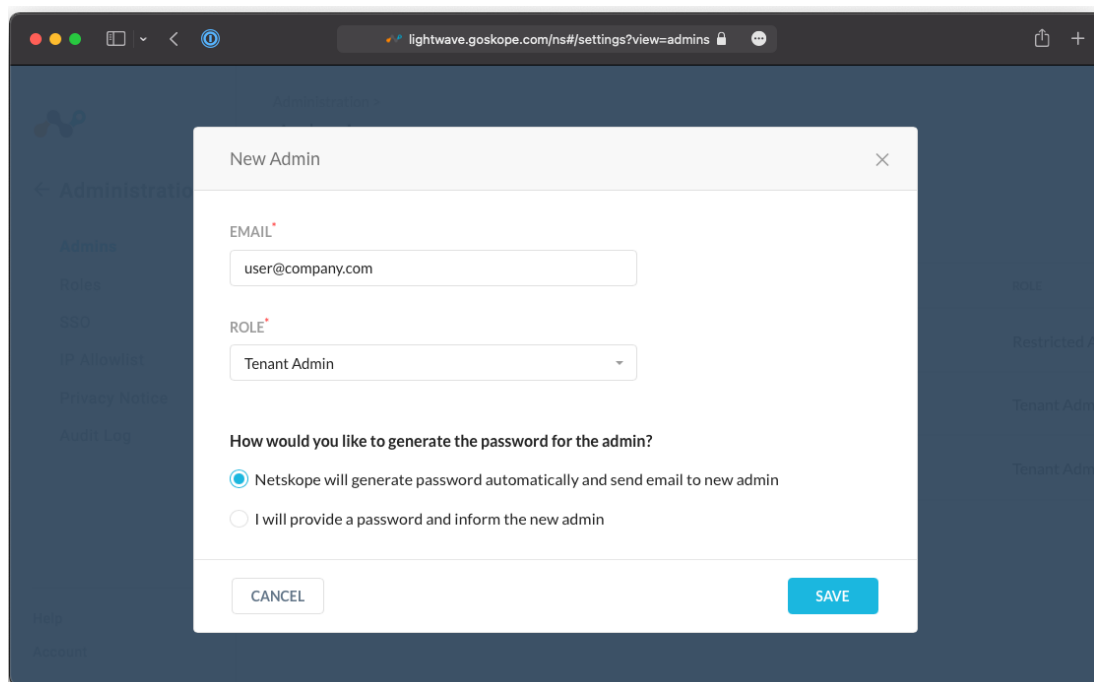


Рис.3.4. Додавання нового адміністратора

В інтерфейсі на рис.3.3. та рис.3.4. керування адміністраторами та формою додавання нового адміністратора, продемонстровано процес призначення ролей з повними правами (tenant administrator) або обмеженим доступом лише для читання. Для підвищення рівня безпеки рекомендується інтегрувати автентифікацію адміністраторів з корпоративним постачальником SSO, що налаштовується в окремому підрозділі консолі, а також застосувати білий список IP-адрес для доступу до порталу адміністратора. На рисунку зі списком дозволених IP-адрес зазвичай демонструється форма, де задаються довірені вихідні адреси для доступу до консолі.

Ключовим елементом є інтеграція з постачальником ідентифікації (IdP). У цьому режимі каталог користувачів та груп з Azure AD, Okta, JumpCloud або локального Active Directory синхронізується з Netskope для подальшого використання в політиках доступу. Рекомендованим механізмом є протокол SCIM, який забезпечує автоматизований обмін даними про користувачів і групи між IdP та Netskope [11].

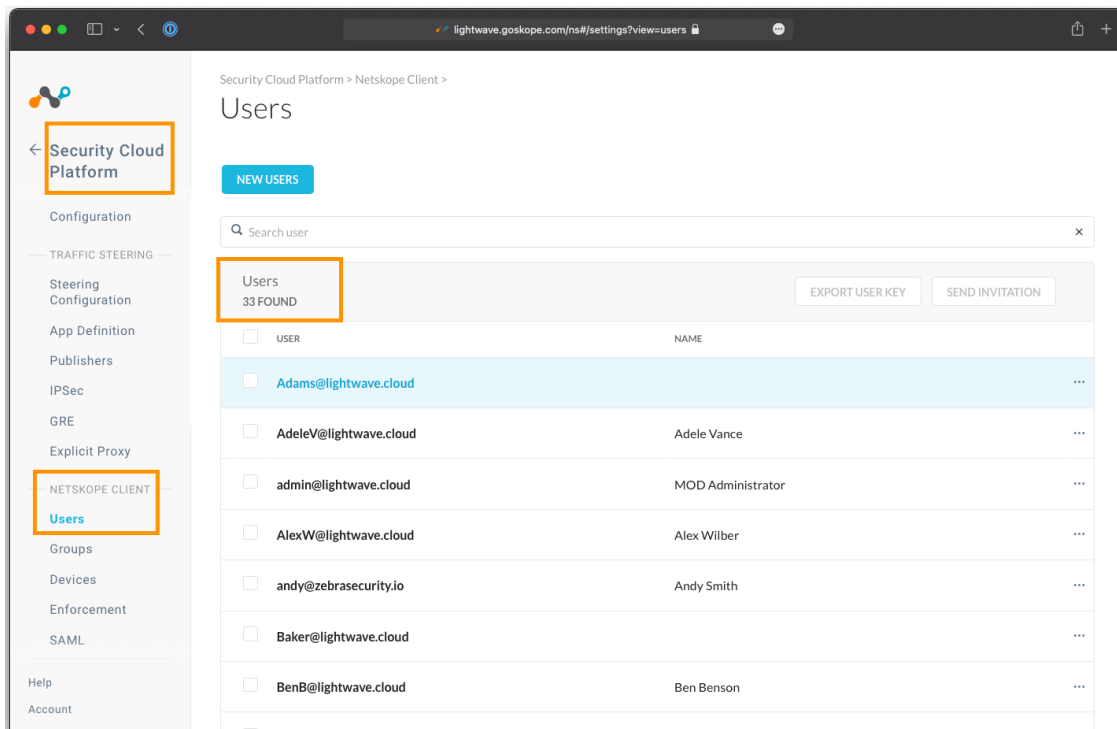


Рис.3.5. Керування користувачами

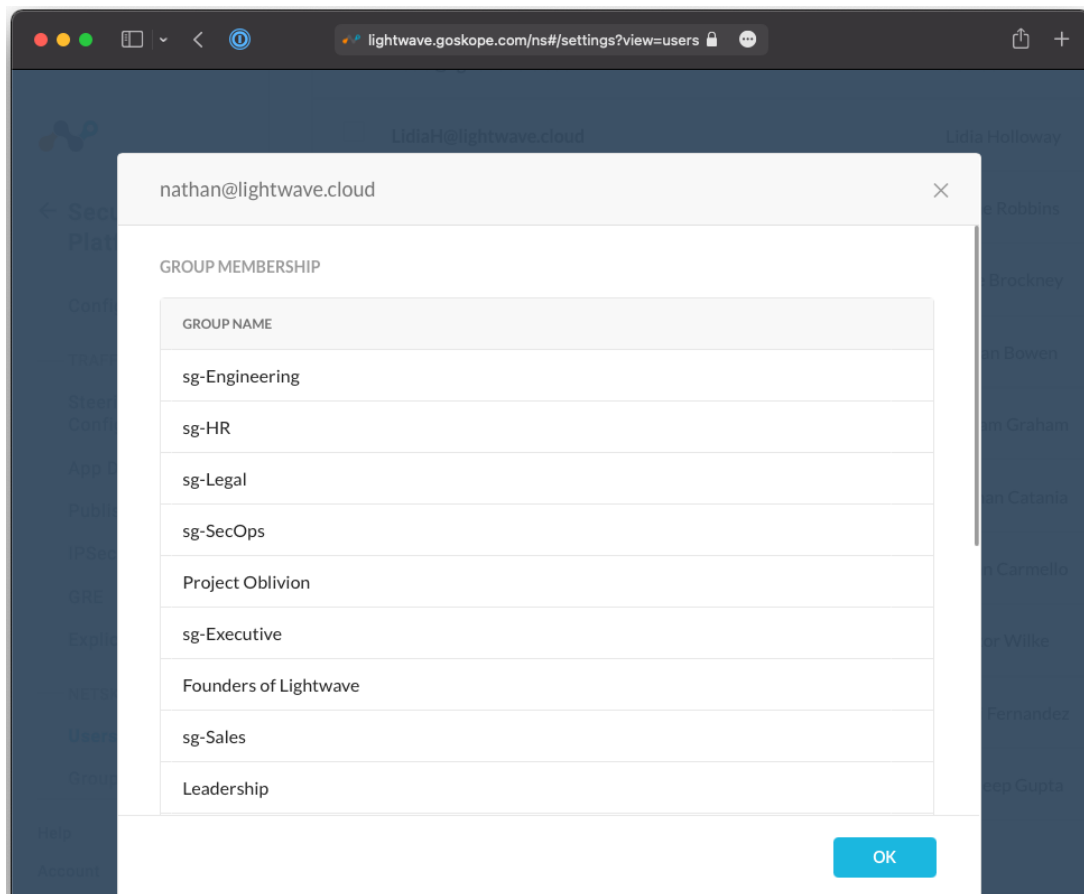


Рис.3.6. Групи користувачів

У консолі відображаються актуальні атрибути користувачів, а при відкритті картки конкретного запису видно, до яких груп і організаційних одиниць він належить. Якщо використовуються локальні каталоги без хмарного IdP, можливе застосування інструмента імпорту каталогів для синхронізації облікових записів з Active Directory або JumpCloud, а для невеликих організацій – ручне створення або імпорт користувачів через CSV-файл.

Перед розгортанням клієнта Netskope необхідно перевірити політики мережесхематизованих брандмауерів. Забезпечується дозвіл вихідних з'єднань клієнта до хмари Netskope (зокрема, TCP-з'єднання до діапазону IP-адрес платформи та DNS-запити до служб, що використовуються для геолокації та вибору найближчого центру обробки даних). Одночасно трафік до хмари Netskope має бути виключений з будь-яких механізмів розшифрування SSL на периметрі, оскільки взаємодія клієнта з хмарою захищена закріпленими сертифікатами, що унеможливорює перехоплення за схемою «людина посередині».

У середовищах, де використовується VPN у режимі повного тунелю, налаштовується обхід трафіку Netskope у VPN-конфігурації. Рекомендованим підходом є перехід до режиму розділеного тунелю, коли внутрішній трафік (адресні простори RFC1918 та інші внутрішні маршрути) передається через VPN, а трафік до Інтернету прямує безпосередньо й перехоплюється клієнтом Netskope. У такому разі діапазон IP-адрес хмари Netskope виключається з VPN-тунелю, щоб забезпечити пряме підключення клієнта до найближчого центру обробки даних.

Наступним кроком створюється та налаштовується профіль керування трафіком (steering configuration), який визначає, який трафік перехоплюється клієнтом та спрямовується до хмари Netskope, а який передається напряму.

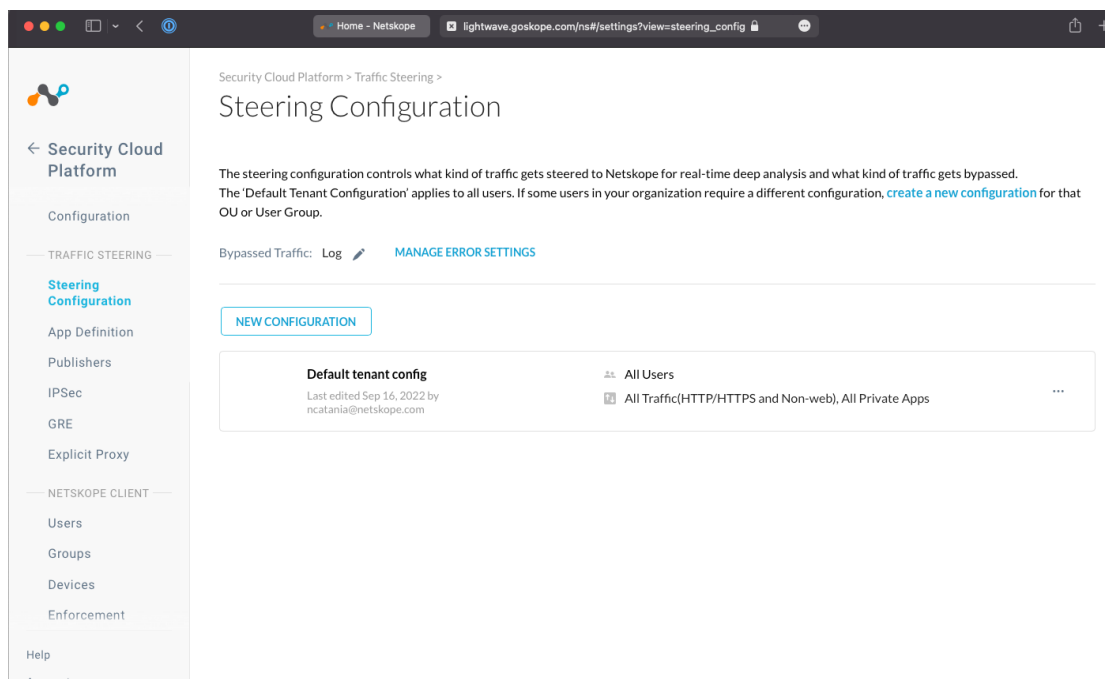


Рис.3.8. Конфігурації керування трафіком

У консолі адміністратора вибирається базовий профіль за замовчуванням або створюється новий, орієнтований на певні групи користувачів (наприклад, ІТ-підрозділ для тестування змін). Рекомендується вмикати журналювання обходженого трафіку, щоб зберегти видимість операцій, що не піддаються аналізу в хмарі.

Під час редагування профілю задається режим перехоплення: лише хмарні додатки, весь веб-трафік HTTP(S) або весь трафік (включно з невебовим), що залежить від придбаних ліцензій (CASB, SWG, Cloud Firewall, Private Access). За необхідності встановлюється прапорець керування приватними застосунками для сценаріїв NPA. Також можуть бути визначені нестандартні порти та увімкнене динамічне керування, яке змінює поведінку клієнта залежно від того, чи використовується корпоративна мережа, чи віддалений доступ.

У конфігурації керування окремо задаються обхідні шляхи. Розрізняються обхід керування, коли трафік повністю минає хмару Netskope, та обхід розшифрування SSL, коли трафік передається в хмару, але не піддається SSL-інспекції. З міркувань безпеки рекомендовано надавати перевагу обходу SSL у

випадках, коли застосунок використовує закріплення сертифікатів, але зберігається потреба в базовій видимості та фільтрації.

New Configuration [X]

NAME: USER GROUP:

TRAFFIC STEERING | NON-STANDARD PORTS

What kind of traffic do you want to steer to Netskope?

☐ Enable Dynamic Steering ⓘ

▼ **Info about traffic steering**

Cloud Apps Only - Steer only selected applications to Netskope for deep analysis. You can make exceptions and allow special accommodations for custom applications.

Web Traffic - Steer all web traffic (HTTP and HTTPS) to Netskope for deep analysis. You can make exceptions for traffic that have personal or private content.

All Traffic - Steer all traffic (web and non-web) to Netskope for deep analysis. You can make exceptions for traffic that have personal or private content.

DNS ⓘ

☐ Steer DNS traffic

PRIVATE APPS ⓘ

☐ Steer private apps

STATUS

☒ Disabled

Рис.3.9. Налаштування для конфігурації рульового керування

На вкладці винятків профілю керування, можна визначити програми, домени, категорії, мережеві розташування джерела і призначення, а також країни, для яких трафік не має перехоплюватися або не має розшифровуватися. Практикою рекомендується налаштувати принаймні обхід сторінок входу постачальника SSO, VPN-шлюзів та агентів інших систем безпеки, які застосовують власне закріплення SSL [9].

Паралельно налаштовуються профілі конфігурації клієнта Netskope.

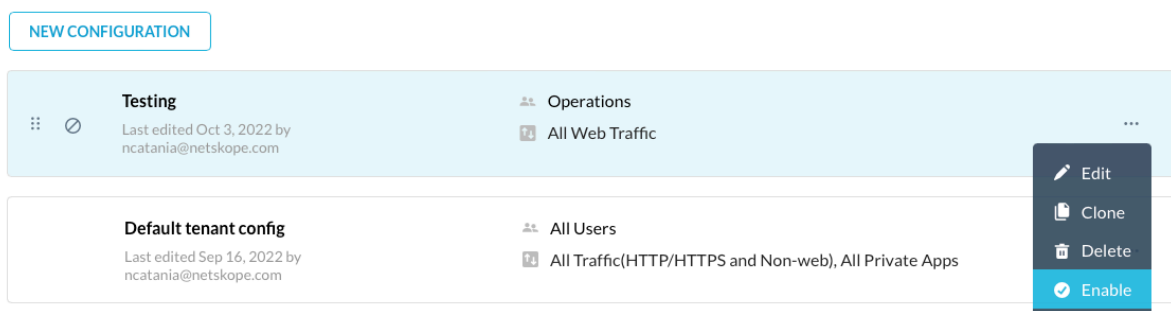


Рис.3.10. Профілі керування

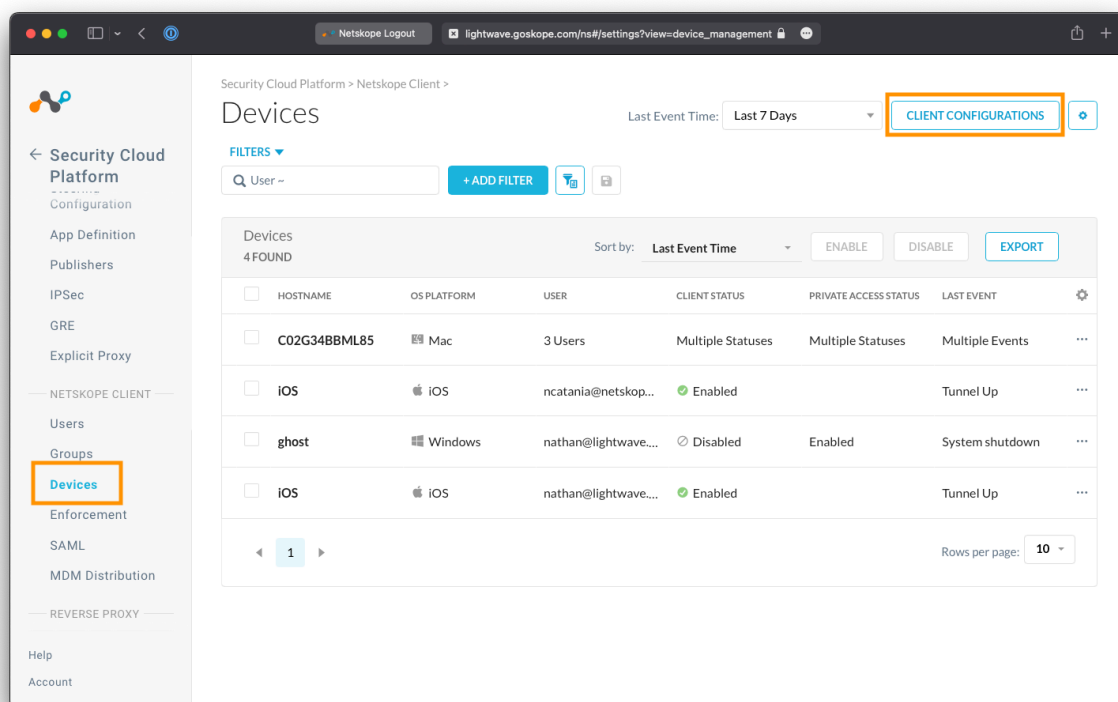


Рис.3.11. Список усіх пристроїв, на яких було розгорнуто клієнт Netskope

У розділі керування пристроями, задаються глобальні або групові параметри роботи клієнта: політика автоматичного оновлення (доцільно орієнтуватися на стабільні Golden Release-версії), рівень журналювання, поведінка під час інсталяції, а також параметри захисту від несанкціонованого втручання.

Client Configuration

DEFAULT TENANT CONFIG

TRAFFIC STEERING INSTALL & TROUBLESHOOT **TAMPERPROOF**

☒ Allow disabling of Clients

☐ Hide Client Icon on System Tray

☒ Password protection for client uninstallation and service stop ⓘ

ADMIN PASSWORD

.....

☐ Fail Close ⓘ

CANCEL SAVE

Рис.3.12. Налаштування захисту від несанкціонованого доступу

На рис.3.12. із вкладкою захисту від несанкціонованого доступу відображаються налаштування, що обмежують можливість користувача самостійно вимикати клієнт або видаляти його без пароля. У виробничих середовищах рекомендується блокувати вимкнення клієнта для звичайних користувачів та застосовувати парольний захист операцій деінсталяції, одночасно залишаючи окремий більш гнучкий профіль для ІТ-команди з метою діагностики.

Розгортання клієнта Netskope на кінцевих точках може виконуватися декількома способами. У невеликих або тимчасових сценаріях (наприклад, під час пілотного впровадження) може використовуватися механізм запрошення електронною поштою: користувач отримує лист із унікальним посиланням, яке містить токен реєстрації, завантажує інсталятор і проходить автоматичну реєстрацію клієнта в тенанті.

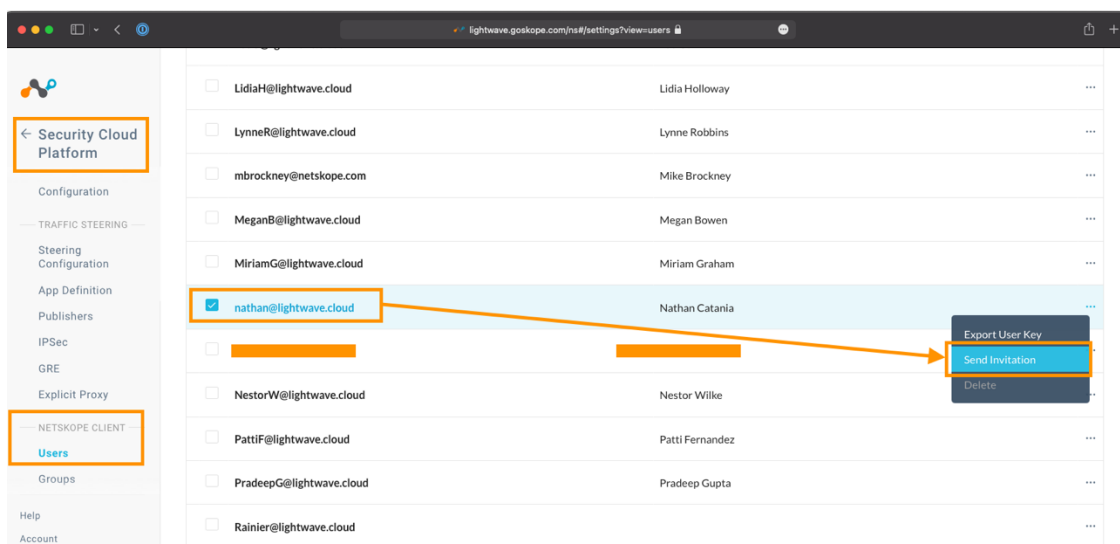


Рис.3.13. Запрошення електронною поштою користувачеві

Netskope New User Onboarding for "nathan@lightwave.cloud"

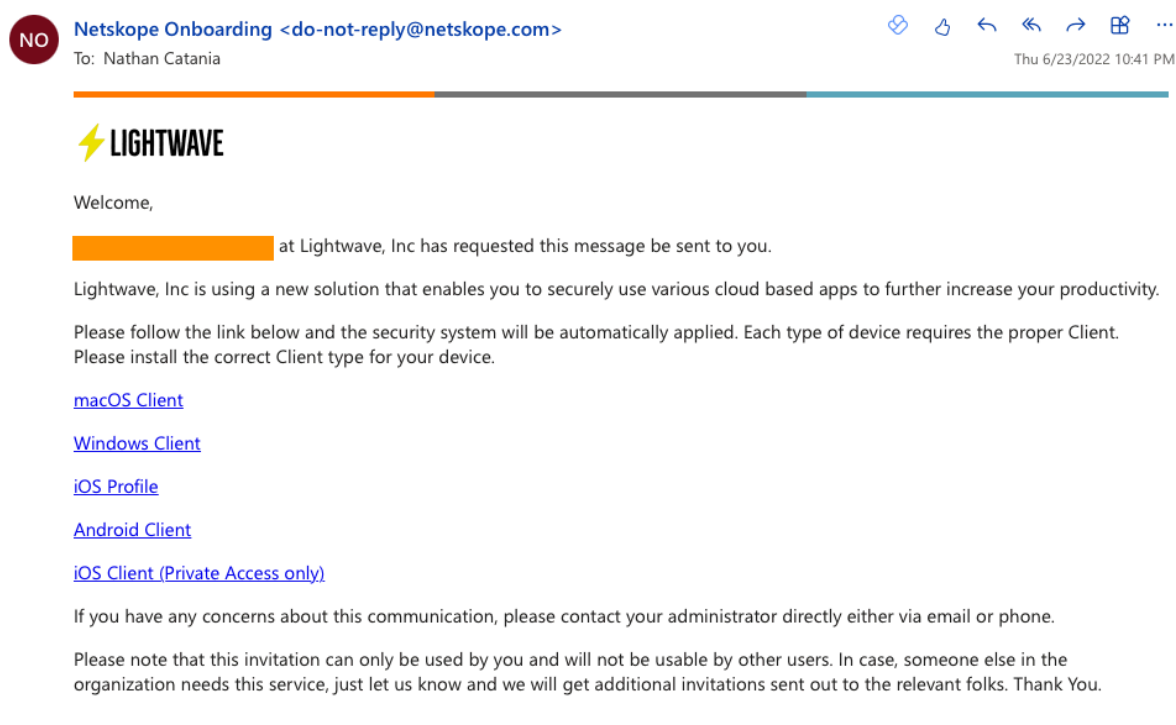


Рис.3.14. Приклад запрошення електронною поштою, яке отримує користувач

Для масштабного виробничого розгортання доцільним є пакування клієнта для систем керування кінцевими точками (SCCM, Microsoft Intune, JAMF, Workspace ONE та інші) з використанням параметрів командного рядка для вказання ідентифікатора організації та хосту тенанта.

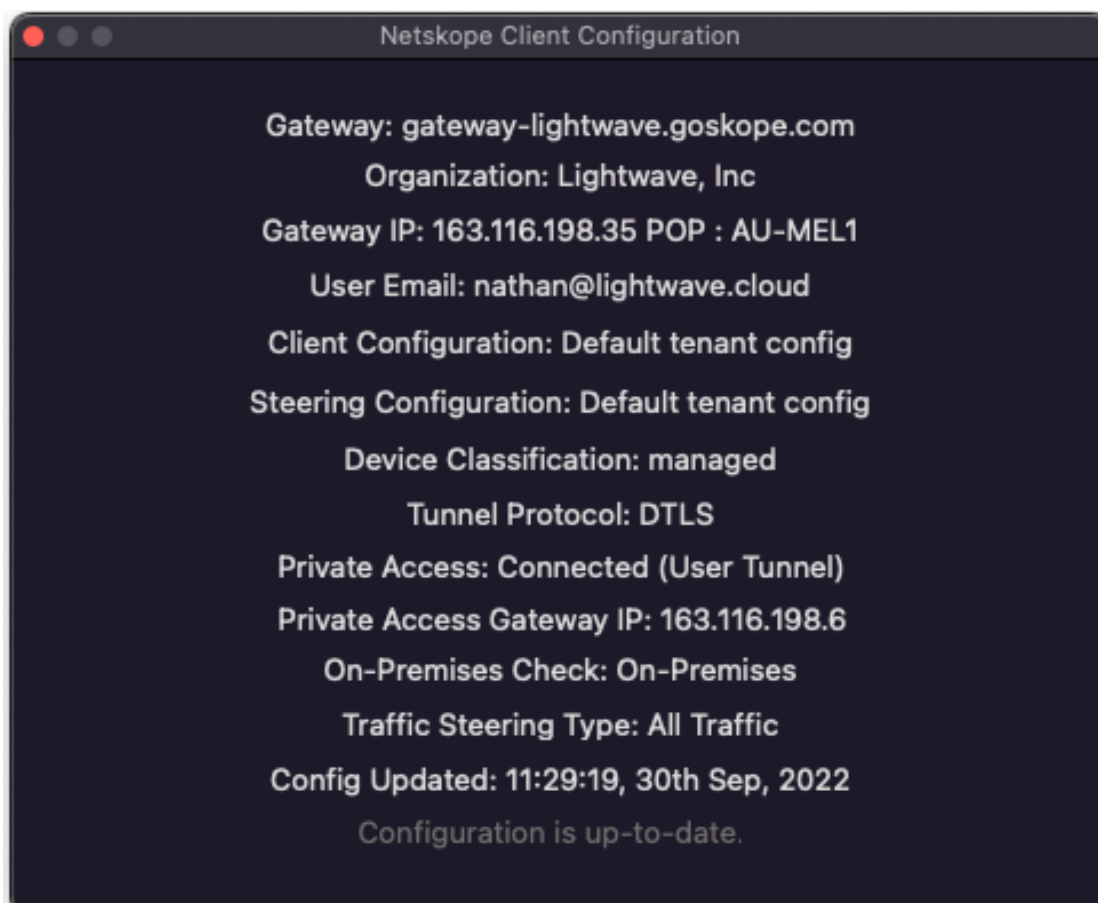


Рис.3.15. Панель конфігурації клієнта Netskope

У цьому варіанті клієнт встановлюється без участі користувача, не потребує прав локального адміністратора й може бути застосований до багатокористувацьких середовищ (наприклад, Citrix).

Через те, що клієнт Netskope перехоплює значну частину мережевого трафіку, окремі засоби захисту кінцевих точок можуть помилково класифікувати його процеси як потенційно небажані. Тому процес клієнта, відповідальний за перехоплення та переспрямування трафіку, має бути доданий до списків винятків антивірусів та інших агентів безпеки.

Після розгортання клієнта виконується перевірка коректності керування трафіком. На настільних операційних системах (Windows, macOS, Linux, ChromeOS) наявність та стан клієнта відстежуються за піктограмою у системному треї або рядку меню; різні стани (увімкнено, вимкнено, помилка) мають окремі позначення. Додаткові відомості про підключення, активного користувача, IP-адресу шлюзу Netskope, POP-вузол, статус пристрою (керований/некерований),

застосовані профілі конфігурації та протокол тунелювання (TLS або DTLS) відображаються у вікні «Конфігурація» клієнта, що продемонстровано на окремому рисунку. На мобільних пристроях для перевірки використовується наявність і активність VPN-профілю Netskope, а у випадку інсталяції через електронне запрошення додатково необхідно позначити кореневий сертифікат Netskope як довірений у налаштуваннях ОС.

Для підтвердження факту маршрутизації трафіку через хмару Netskope використовується спеціальний тестовий ресурс notskope.com, інтерфейс якого показано на рисунку з веб-сторінкою перевірки.

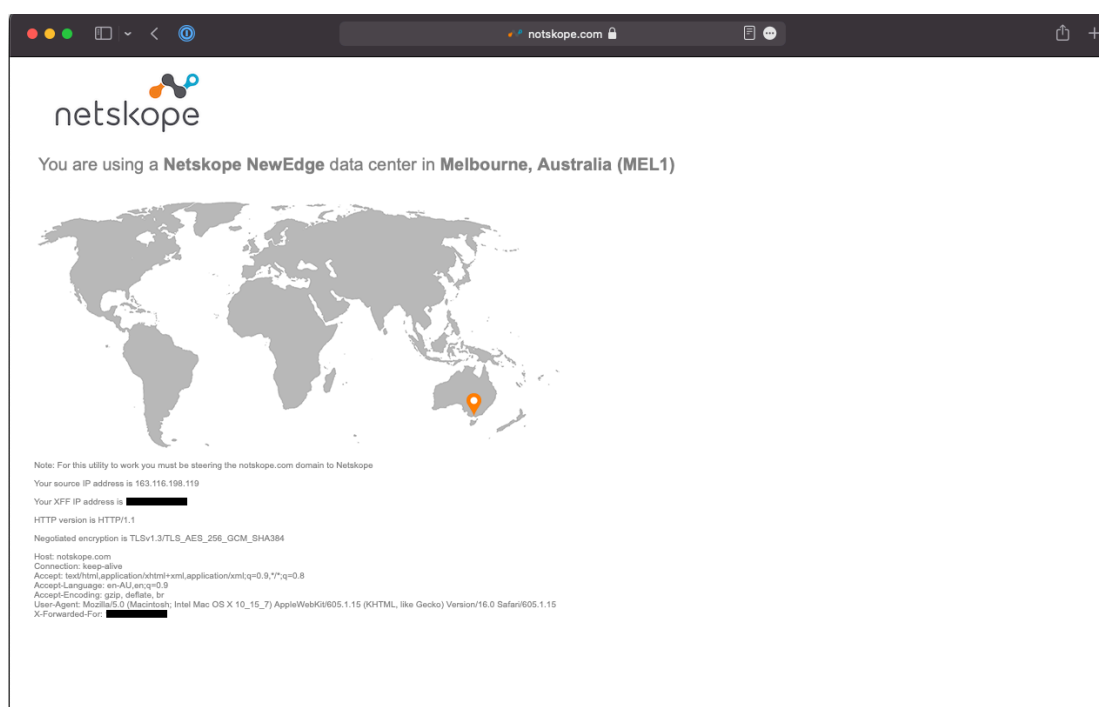


Рис.3.16. Інтерфейс тестового ресурсу notskope.com

Під час успішного проходження трафіку через хмару на цій сторінці відображається інформація про POP-вузол і пов'язаний тенант. Додатково, для перевірки SSL-інспекції, аналізується ланцюжок сертифікатів на будь-якому не обійденому HTTPS-ресурсі (наприклад, notskope.com або www.wikipedia.org): наявність проміжного сертифіката виду ca.<tenant-name>.goskope.com означає, що вміст проходить через проксі Netskope [14].

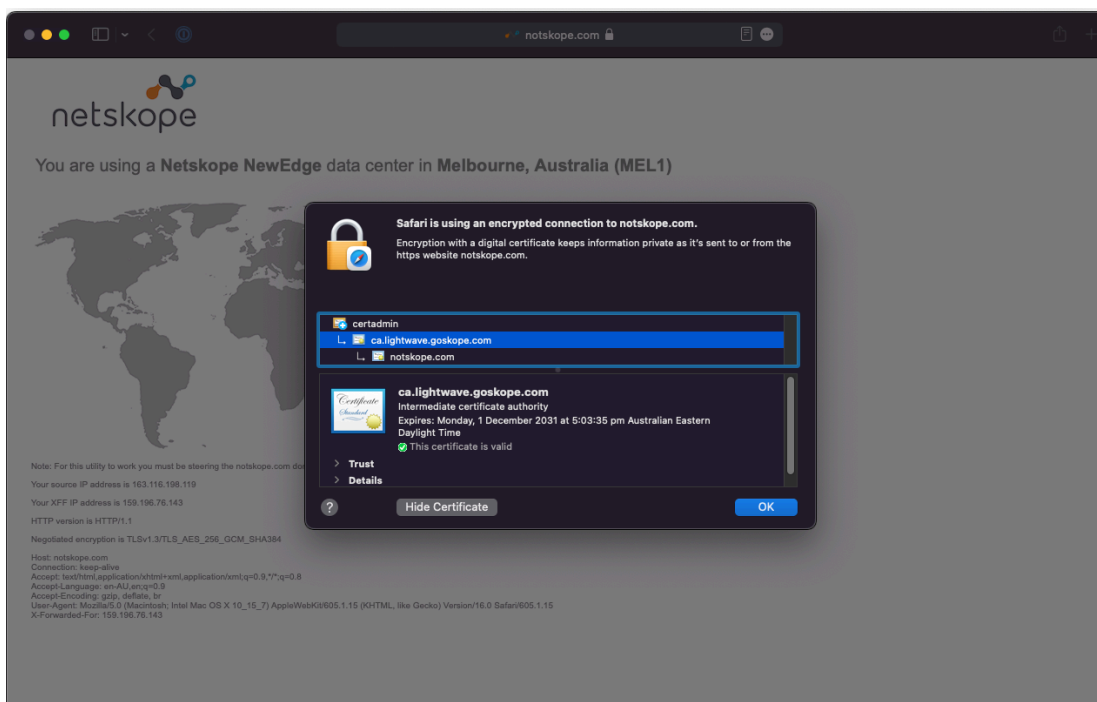


Рис.3.17. Перевірка сертифіката SSL

Після завершення базового розгортання доцільно переглянути та адаптувати стандартні політики, що входять до початкової конфігурації Netskope. Типово вони включають глобальне блокування небажаних сайтів (контент для дорослих, P2P), сповіщення з вимогою обґрунтування доступу до невідомих або нових доменів, блокування шкідливих і фішингових ресурсів та обов'язкову перевірку завантажень на наявність шкідливого ПЗ. Для подальшого удосконалення рекомендується розширити перелік глобально заблокованих категорій (наприклад, онлайн-реклама), розробити політики інструктажу для «небізнесових, але відносно безпечних» сервісів (стримінг, розваги), а також поступово впроваджувати складніші правила на основі індексу довіри до хмари (Cloud Confidence Index), DLP-профілів та атрибутів екземплярів застосунків. Використання CCI, процес маркування ключових бізнес-застосунків як санкціонованих та подальше застосування цих міток у політиках також пояснюється в окремому блоці з рисунками, де проілюстровано перегляд результатів оцінювання хмарних сервісів [11].

3.2. Система захисту інформаційних ресурсів організації на базі Netskope SASE

Політики захисту в режимі реального часу (Real-time Protection Policies) у платформі Netskope SASE є основним механізмом примусового виконання правил безпеки «на льоту» для хмарних застосунків, веб-ресурсів і приватних сервісів, які обслуговуються через хмару Netskope Security Cloud. У межах загальної архітектури SSE ці політики відповідають за інлайн-контроль даних і загроз, доповнюючи інші сервіси платформи (DLP, Threat Protection, Cloud Firewall, Private Access) та забезпечуючи послідовне застосування єдиного набору правил до всього трафіку, що проходить через хмарний проксі.

Конфігурація політик Real-time Protection виконується у веб-консолі адміністратора на сторінці Policies Real-time Protection, де відображається таблиця з усіма поточними політиками, їхнім типом, станом, дією та порядком оброблення. На екрані відображається таблиця з усіма поточними політиками, їхнім типом, станом, дією та порядком оброблення, передбачені елементи керування зміною порядку (зокрема перетягуванням), панель фільтрів для відбору політик за різними критеріями та кнопка «New Policy» для створення нового правила.

У діалоговому вікні пропонується вибір типу політики, що визначає контекст її застосування: доступ до хмарних застосунків, веб-трафік, політики хмарного брандмауера, політики доступу до приватних застосунків (Netskope Private Access), політики Threat Protection та DLP-політики.

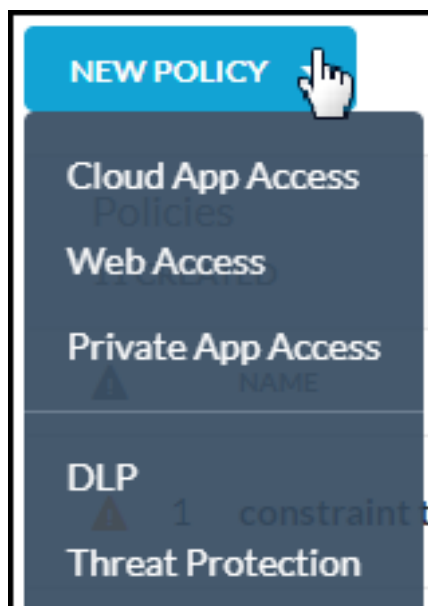


Рис.3.18. Створення нової політики безпеки

Після натискання кнопки створення відкривається діалогове вікно, у якому обирається тип політики, що визначає контекст її застосування: політики для хмарних застосунків, веб-трафіку, хмарного брандмауера, доступу до приватних застосунків (Netskope Private Access), а також політики Threat Protection і DLP-політики. Вибраний тип визначає доступний набір умов і профілів, які можуть бути прив'язані до правила, зокрема профілі Threat Protection для протидії шкідливому програмному забезпеченню та DLP-профілі для контролю витоку даних.

Структура будь-якої політики Real-time Protection є уніфікованою і базується на послідовному заповненні кількох логічних блоків: параметрів джерела (Source), параметрів призначення (Destination), набору активностей (Activities) та секції дій із прив'язкою відповідних профілів безпеки. Наприклад, для політики Threat Protection, що блокує завантаження потенційно шкідливих файлів, у блоці Source може бути вказано конкретного користувача чи групу, у блоці Destination — категорію, яка відповідає всьому веб-трафіку, а в Activities — операцію «завантаження». У секції дій для такої політики зазвичай обирається профіль Threat Protection і дія «Block» для всіх рівнів критичності виявлених загроз.

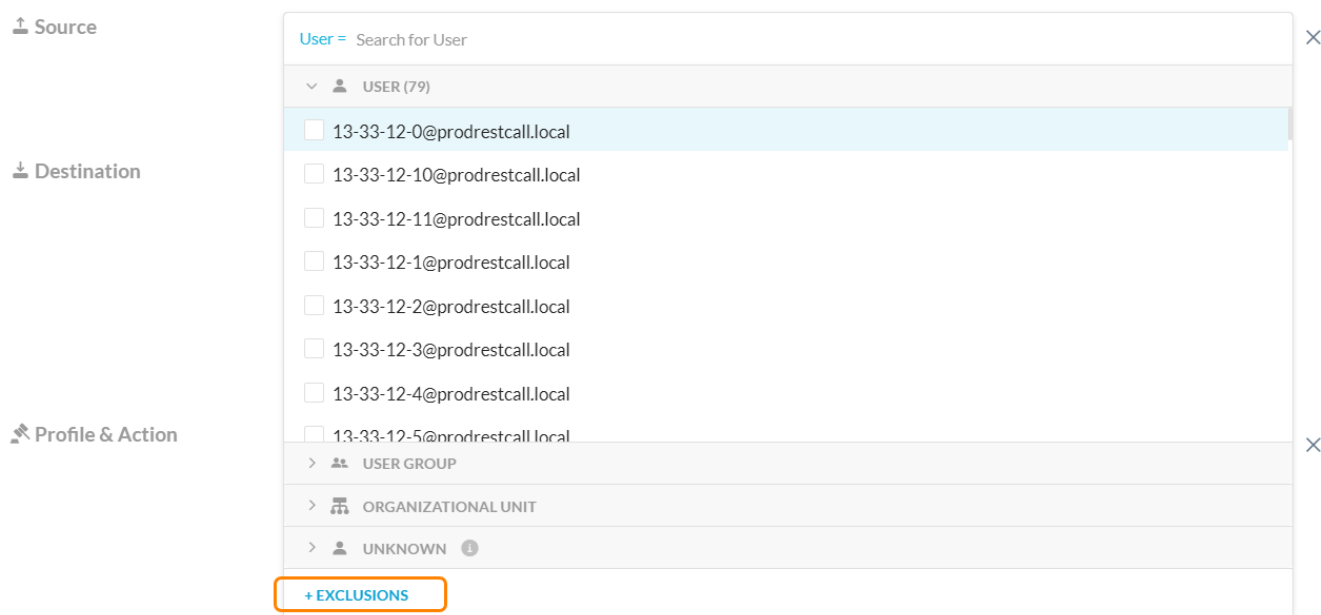


Рис.3.19. Атрибути ініціатора трафіку

У блоці Source визначаються атрибути, які характеризують ініціатора трафіку. До них належать користувач, група або організаційна одиниця каталогу, тип пристрою, операційна система, спосіб доступу (клієнт Netskope, Secure Forwarder, браузерний доступ, мобільний клієнт, NPA) та мережеве розташування, що може описувати сегменти корпоративної мережі чи VPN-з'єднання. Платформа підтримує профілі Network Location, що дає змогу виділяти окремі довірені й недовірені мережі та будувати диференційовані політики для трафіку з офісу, домашніх VPN-тунелів або публічних точок доступу.

Activities and actions available are dependent on the type of profile and applications you selected.

Source

User = student01@training.securenomics.com

ADD CRITERIA ▾

Destination

Application ▾

Application = Microsoft Office 365 OneDrive for Business

Activities = Select

ADD CRITERIA & CONSTRAINTS ▾

Profile & Action

Action: Allow ▾

ADD PROFILE ▾

Policy Name

Student01 - Allow OneDrive Storage

Group: 2 . Student Policies ▾

POLICY DESCRIPTION

Allow access to corporate OneDrive Traffic

+ EMAIL NOTIFICATION

Status

☒ Enabled

+ POLICY SCHEDULE

Рис.3.20. Приклад налаштування політики безпеки

Налаштування блоку Destination визначає, до яких ресурсів застосовується політика. У цьому блоці задаються категорії веб-сайтів, конкретні хмарні застосунки, їхні екземпляри (наприклад, корпоративний і особистий тенанти), а також додаткові атрибути, пов'язані з оцінкою ризику через Cloud Confidence Index [13].

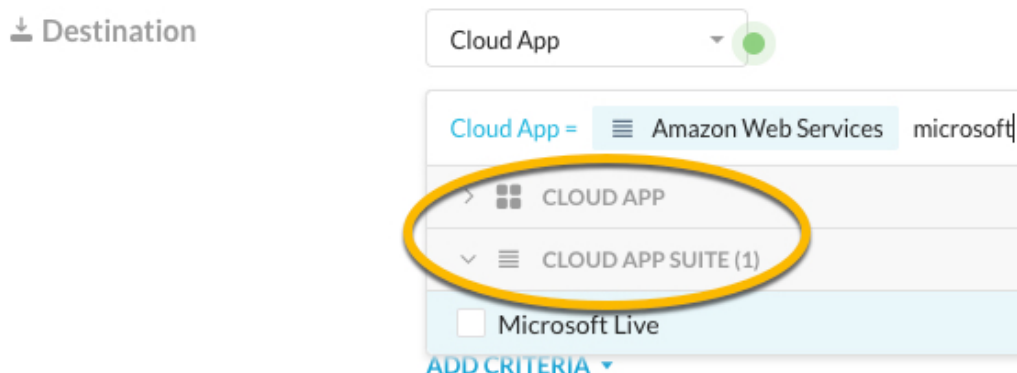


Рис.3.21. Визначення ресурсів до яких застосовується політика

Підтримується динамічна класифікація, що аналізує текстовий вміст сторінок і автоматично визначає категорії раніше невідомих URL-адрес, завдяки чому політики коректно спрацьовують навіть для нових або маловідомих сайтів. У формі налаштування Destination адміністратор бачить список обраних категорій, застосунків і тегів екземплярів, що дає наочне розуміння, до яких саме ресурсів буде застосовано правило.

Блок Activities визначає, які саме дії користувача в межах обраних застосунків або сайтів контролюються політикою. Для веб- і хмарного трафіку зазвичай розрізняють щонайменше три базові типи активності: завантаження даних з Інтернету, вивантаження даних до Інтернету та перегляд (browse). Для окремих категорій застосунків підтримується ширший набір детальніших дій, таких як створення, редагування, спільний доступ або видалення об'єктів. У вікні редагування активностей для вибраного застосунку відкривається перелік доступних дій, і адміністратор позначає ті з них, які мають бути під контролем у межах конкретної політики.

У секції дій політики задається реакція системи на подію, що відповідає умовам у полях Source, Destination та Activities. Доступні дії включають дозвіл доступу, блокування, режим «user alert» або «coaching» із відображенням попереджувальної сторінки та вимогою підтвердження, а також обхід (bypass) або карантин для окремих сценаріїв. У цій секції прив'язуються профілі, налаштовані в розділі Profiles: DLP-профілі для виявлення конфіденційних даних, профілі Threat Protection для аналізу файлів на наявність шкідливого ПЗ, а також профілі

Quarantine, Legal Hold та HTTP Header. Шаблони користувацьких і електронних сповіщень конфігуруються в окремому розділі Templates і застосовуються до обраних дій, визначаючи зовнішній вигляд сторінок блокування та текстів повідомлень, які бачить користувач або адміністратор.

The screenshot displays the configuration interface for DLP (Data Loss Prevention) rules. It is divided into two main sections: 'Destination' and 'Profile & Action'.

Destination Section:

- Email Outbound App:** A dropdown menu with 'Email Outbound App' selected.
- Email Outbound =:** A text field containing 'Microsoft Office 365 Exchange'.
- Activities =:** A text field containing 'Send'.
- ADD CRITERIA & CONSTRAINTS:** A blue link with a downward arrow.

Profile & Action Section:

- DLP Profile =:** A text field containing 'drm_label_based_profile (custom)'.
- Action:** A dropdown menu with 'Alert' selected.
- Set action for each profile:** A checkbox that is checked.
- Continue policy evaluation after match:** An unchecked checkbox.
- + ADD TRAFFIC ACTION:** A blue link.

Рис.3.22. Налаштування DLP профілей та дій

Інтеграції з Threat Protection і DLP надається особлива увага. Файли можуть скануватися на наявність шкідливого коду в режимі реального часу в рамках політик Real-time Protection, підтримується використання додаткових списків хешів для блокування чи дозволу окремих файлів, а також взаємодія із засобами захисту кінцевих точок для автоматизованого реагування. DLP-політики прив'язують один або кілька DLP-профілів до транзакцій у хмарних застосунках і на веб-ресурсах, що дозволяє виявляти й блокувати передавання чутливих даних, зокрема із застосуванням методів точного співставлення, аналізу вмісту класифікаторами й відбитками файлів.

Порядок оброблення політик Real-time Protection є критично важливим для коректного функціонування системи. Політики опрацьовуються послідовно зверху вниз, і перше правило, умови якого відповідають поточній транзакції, визначає остаточну дію; подальші правила вже не розглядаються. Тому правила з більш вузькими умовами (наприклад, для окремих груп користувачів або критичних застосунків) доцільно розміщувати вище за загальноорганізаційні політики, а блокувальні політики з винятками — вище за ширші дозволяльні правила. Зміни в конфігурації політик набувають чинності лише після виконання команди

застосування змін; у верхній частині інтерфейсу зазвичай відображається попередження про наявність незастосованих змін та кнопка для їх публікації.

Для зручності адміністрування реалізовано можливості фільтрації та групування політик за різними атрибутами. Можна відібрати, наприклад, лише ті правила, що застосовуються до певного користувача, обмежити перелік політик за типом, дією чи групою збереження. Над таблицею політик розташована панель фільтрів і засоби швидкого пошуку, які полегшують аналіз і налагодження в умовах великої кількості правил.

More Specific to Less Specific

	NAME	SOURCE ⓘ	DESTINATION	PROFILE	ACTION	# ALERTS ⓘ
Threat	1 [Threat] Block Security Risk Category - BP	Any	Security Risk	None	Block High Med Sev Malware	0
	2 [Threat] Block Malware - BP	Any	Abortion, Adult Content - Other, Adult Content - Pornography, Advocacy... Download, Upload	Test Profile	High: Block High Med Sev Malware	0
	3 [Threat] Allow Security Risk Category Exception - BP	Any	Security Risk Exception	None	Allow	0
Utility	4 [Utility] Policy Sync - 002	jforrest@netskope.com	Netskope	None	User Alert How To Test A Real-Time Protection Policy Chan...	3
	5 [Utility] Block DNS over HTTPS - BP	Any	DNS Over HTTPS	None	Block Default Template	0
RBI	6 [RBI] Allow Uncategorized Internal Domains - BP	Any	Netskope Domains	None	Allow	0
	7 [RBI] Forward to RBI Ericom - BP	Any	Uncategorized, Ericom, Parked Domains, Newly Registered Domain	None	Forward To Proxy Ericom RBI	0
CASB	8 [CASB] Allow Test Instances	Any	Microsoft Office 365 Suite-j4hax, Microsoft Office 365 OneDrive for...	None	Allow	0
Web	19 [Web] Block AUP Policy Categories - BP	Any	Company AUP Category	None	Block Default Template	0
	20 [Web] Block Gambling - Miscat Demo	Any	Gambling	None	Block Miscategorization Example	5

Рис.3.23. Групування політик

Перевірка коректності роботи налаштованих політик виконується шляхом генерації контрольних подій і аналізу журналів. Після створення політики Threat Protection із блокуванням тестового файлу EICAR здійснюється спроба завантажити цей файл, а далі в розділі SkopeIT → Alerts перевіряється факт спрацювання політики, фіксується назва правила, рівень критичності та результат роботи сканера. Аналогічним чином перевіряються DLP- і веб-політики: після зміни конфігурації ініціюється тестова транзакція (наприклад, вивантаження

документа з конфіденційними даними до несхваленого хмарного сервісу або доступ до сайту із забороненої категорії), а в інтерфейсі SkopeIT верифікується, яке саме правило Real-time Protection спрацювало й яку дію було виконано.

The screenshot displays the Skope IT Alerts interface. On the left, a table lists alerts with columns for TIME, NAME, ALERT, and ACTION. A red box highlights the first row of the table. On the right, the 'Alert Details' panel provides comprehensive information about the selected alert.

TIME	NAME	ALERT	ACTION
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	DLP	useralert
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	DLP	useralert
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	DLP	useralert
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	DLP	useralert
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	policy	block
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	policy	block
8/12/24, 12:16 PM	EICAR...	Malware	Detecti...
8/12/24, 12:16 PM	Student01 - Warn on Sensitive Information	policy	block

Alert Details

8/12/24, 12:16 PM

DLP

Alert Name: Student01 - Warn on Sensitive Information
Action: useralert

GENERAL

App Tags: Enterprise
Appsuite: Office365
Browser Version: 129.0
Device Classification: not configured
Incident Id: 697404699262834710
Instance Tags:
Managed App: no
Page Site: Microsoft Office 365 Sharepoint Sites
Protocol: HTTPS/1.1
Src Time: Mon Aug 12 12:16:00 2024
True Type Id: 230
CustomInstance: OneDrive_Corporate_Instance
Instance Name: OneDrive_Corporate_Instance
Type: nspolicy
Alert Severity: unknown
Policy Name: Student01 - Warn on Sensitive Information
Alert Generated: yes
Access Method: Client
Traffic Type: CloudApp
Request ID: 2906466855458112000
MD5: 43302ca9e68d3f3360e68b45fadee8de
Browser Session ID: 5618513008292163147
Transaction ID: 697404699262834710
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
Parent ID: /personal/student01_training_securenomics_com/Documents

Рис.3.24. Інформація про подію в журналі

Важливим аспектом є узгодження політик Real-time Protection із політиками SSL Decryption. Для низки сценаріїв, зокрема коли застосунок використовує закріплення сертифікатів, доцільно застосовувати політику «SSL Do Not Decrypt» замість повного обходу трафіку, щоб зберегти видимість подій і можливість застосування базових дій Real-time Protection без глибокого аналізу вмісту. У засобах керування політиками можна налаштувати узгоджені набори правил Real-time Protection і SSL Decryption для тих самих призначень, що дозволяє гнучко балансувати між вимогами сумісності та рівнем контролю [14].

Отже, налаштування політик Real-time Protection у платформі Netskope SASE охоплює послідовне визначення атрибутів джерела, призначення, активностей, дій і пов'язаних профілів, коректне розміщення правил у порядку оброблення,

узгодження їх із політиками розшифрування SSL, а також регулярну перевірку спрацювань через журнали SkopeIT. Графічний інтерфейс платформи відображає всі ці кроки у вигляді послідовних екранів — від загального списку політик і майстра створення нового правила до форм заповнення блоків Source, Destination та Activities, конфігурації дій із прив'язкою профілів і шаблонів сповіщень та елементів керування застосуванням змін, що істотно полегшує практичне засвоєння й повсякденне адміністрування.

3.3. Рекомендації щодо захисту інформаційних ресурсів організації

Захист інформаційних ресурсів організації зазвичай розглядається як цілісна система, що охоплює дані, інформаційні системи, сервіси, мережеву інфраструктуру та пов'язаних з ними користувачів. Основна увага приділяється забезпеченню конфіденційності, цілісності й доступності інформації з урахуванням критичності бізнес-процесів та рівня загроз для конкретної організації.

Важливою передумовою є наявність зрозумілої нормативно-організаційної бази. Політика інформаційної безпеки, положення про доступ до інформації, правила використання хмарних сервісів, віддаленого доступу та особистих пристроїв формують рамки, у межах яких функціонують технічні засоби захисту. У цих документах фіксується розподіл ролей і відповідальності, статус окремих категорій даних, підходи до їх обробки, зберігання та знищення. Технічна архітектура безпеки розглядається як механізм реалізації визначених у документах вимог.

З погляду контролю доступу інформаційні ресурси пов'язуються з системами керування ідентичністю та правами. У практиці організацій переважають централізовані служби каталогів, рольові моделі доступу, багатофакторна автентифікація для критичних операцій і віддалених підключень. Окремо акцентується регулярний перегляд наданих прав, обмеження надмірних привілеїв і усунення «зайвих» облікових записів, що знижує ймовірність несанкціонованого доступу як з боку зовнішнього зловмисника, так і через внутрішні зловживання.

Мережевий вимір безпеки пов'язується із сегментацією інфраструктури, мінімізацією довіри між сегментами та фільтрацією трафіку. Критичні сервери, системи управління та сховища даних ізолюються від відкритих мереж і робочих станцій користувачів за допомогою міжмережових екранів, систем виявлення й запобігання вторгненням, спеціалізованих шлюзів для веб-трафіку та електронної пошти. Веб-канали й пошта розглядаються як ключові шляхи доставки шкідливого ПЗ та фішингу, тому тут застосовуються механізми аналізу вмісту, перевірки вкладень і блокування небажаних категорій ресурсів.

Захист кінцевих точок трактується як окремий шар, що доповнює мережеві засоби. Антивірусні й EDR-платформи, централізоване керування оновленнями, обмеження встановлення програмного забезпечення, контроль використання зовнішніх носіїв та мобільних пристроїв знижують імовірність компрометації робочих станцій. Наявність журналювання подій на кінцевих точках та уніфікованих політик безпеки спрощує подальший аналіз інцидентів і відстеження ланцюжка дій зловмисника.

Окремий блок підходів стосується безпосередньо даних. Замість орієнтації лише на «периметр» дедалі більше уваги приділяється класифікації інформації, шифруванню при зберіганні й передаванні, керуванню доступом на рівні документів, а також застосуванню технологій запобігання витоку даних (DLP). Такі системи відстежують переміщення чутливих відомостей через електронну пошту, веб-канали, хмарні сховища й зовнішні носії, формують картину типових порушень і дають змогу обмежувати небажані операції з даними.

Система захисту інформаційних ресурсів доповнюється безперервним моніторингом і реагуванням на інциденти. Централізований збір журналів від мережових пристроїв, серверів автентифікації, критично важливих бізнес-систем, засобів захисту кінцевих точок створює єдину подієву базу. На її основі будуються кореляційні правила, моделі аномальної поведінки та сценарії атак, що дозволяє виявляти інциденти на ранніх етапах і підтримувати формалізований процес розслідування та усунення наслідків.

Людський фактор розглядається як наскрізний елемент системи. Захист інформаційних ресурсів неможливий без формування сталих моделей поведінки персоналу: обережного ставлення до обробки конфіденційних даних, коректної роботи з паролями та засобами багатофакторної автентифікації, критичного сприйняття підозрілих листів і запитів, усвідомлення наслідків використання несанкціонованих хмарних сервісів. Для технічних фахівців актуальними є знання щодо захисту мереж, хмарних платформ, виявлення загроз і реагування на інциденти.

У цьому загальному контексті SASE (Secure Access Service Edge) описується як один із сучасних підходів до реалізації мережевої та прикладної безпеки для розподілених середовищ. Такі рішення поєднують функції захищеного веб-шлюзу, контролю хмарних застосунків, хмарного міжмережевого екрана, сервісів доступу до внутрішніх ресурсів (ZTNA) і засобів захисту від загроз у єдиній хмарній платформі. Користувацький трафік, незалежно від місця перебування користувача, спрямовується через вузли постачальника SASE, де до нього застосовуються уніфіковані політики доступу, фільтрації та контролю даних, включно з DLP-механізмами для веб- і хмарних сервісів. Таким чином, SASE інтегрується в загальну систему захисту інформаційних ресурсів як технологічна основа для реалізації концепцій Zero Trust і «доступу, орієнтованого на застосунок», особливо в умовах активного використання SaaS-платформ і віддаленої роботи.

ВИСНОВКИ

У роботі проведено дослідження проблеми захисту інформаційних ресурсів організації в умовах розподілених, гібридних та хмароорієнтованих інфраструктур. Проаналізовано сучасний стан використання інформаційних систем, у яких дані, сервіси та користувачі розміщуються як у локальних дата-центрах, так і в хмарних середовищах. Виявлено основні загрози й вразливості, пов'язані з такою моделлю, зокрема ризики несанкціонованого доступу, витоку даних, компрометації облікових записів і використання неконтрольованих хмарних сервісів. Показано, що інформаційні ресурси організації потребують цілісного підходу до захисту, який охоплює мережевий рівень, кінцеві точки та прикладні сервіси.

Аналіз підходів до забезпечення безпеки показав, що традиційні периметрові моделі, побудовані навколо статичної межі корпоративної мережі, не відповідають вимогам сучасних організацій, де значна частина трафіку проходить поза класичним периметром. Зростаюча роль віддаленої роботи, використання SaaS-платформ і доступу з різних типів пристроїв вимагає переходу до моделей, заснованих на принципах Zero Trust, контекстно-орієнтованому контролі доступу та інлайн-аналізі трафіку.

Дослідження можливостей і функцій рішень класу SASE показало, що така архітектура є ефективним засобом для побудови єдиного контуру захисту інформаційних ресурсів. SASE поєднує функції захищеного веб-шлюзу, брокера безпеки доступу до хмари, сервісів приватного доступу, міжмережевого екрана як сервісу та засобів запобігання витоку даних у єдиній хмарній платформі. Це забезпечує інлайн-контроль трафіку, застосування уніфікованих політик доступу до внутрішніх і хмарних ресурсів, виявлення аномальної активності та блокування спроб компрометації даних у режимі, наближеному до реального часу.

У роботі проаналізовано можливості застосування платформи Netskope SASE для захисту інформаційних ресурсів організації. Розглянуто варіанти маршрутизації трафіку через глобальну інфраструктуру провайдера, механізми

класифікації та контролю хмарних сервісів, реалізацію політик Real-time Protection, DLP і Threat Protection для веб- та хмарного трафіку. Показано, що використання Netskope SASE дозволяє формувати єдиний набір правил доступу для різних категорій користувачів і ресурсів, незалежно від місця їх розташування, а також забезпечує деталізований контроль операцій над даними.

Завдяки інтеграції SASE з системами керування ідентичностями, засобами захисту кінцевих точок і платформами моніторингу подій безпеки досягається комплексний захист інформаційних ресурсів. Єдиний контур доступу та спостереження забезпечує реалізацію принципу мінімально необхідних привілеїв, зменшує площу атаки й спрощує виявлення та розслідування інцидентів. Узгодження політик SASE з внутрішніми регламентами організації створює передумови для керованого й відтворюваного процесу забезпечення безпеки.

Таким чином, впровадження технології забезпечення безпеки інформаційних ресурсів організації на основі рішень SASE є обґрунтованим і ефективним підходом до протидії сучасним кіберзагрозам. Застосування SASE дозволяє поєднати гнучкість і масштабованість хмарних сервісів із керованим, прозорим і стійким до атак механізмом захисту даних, що є ключовою умовою надійного функціонування інформаційних систем сучасних організацій.

.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST SP 800-60, Volume I, Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg, MD: NIST, 2008. Дата звернення: 30.10.2025.
2. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. TLP:CLEAR, October 2025. – European Union Agency for Cybersecurity, 2025.
3. 2025 Data Breach Investigations Report / C. David Hylander, Philippe Langlois, Alex Pinto, Suzanne Widup. – Verizon, 2025. – 116 p. – Режим доступу: <https://www.verizon.com/business/resources/reports/dbir/> (дата звернення: 30.10.2025)
4. What is an information asset?. TechTarget WhatIs.com. URL: <https://www.techtarget.com/whatis/definition/information-assets> (дата звернення: 22.11.2025).
5. Information Security: Principles, Threats, and Solutions. HackerOne Knowledge Center. URL: <https://www.hackerone.com/knowledge-center/principles-threats-and-solutions> (дата звернення: 14.11.2025).
6. Vulnerabilities, Threats & Risk Explained. Splunk Learn. URL: https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html (дата звернення: 14.11.2025).
7. Gartner Peer Insights. Single-Vendor SASE (Transitioning to SASE Platforms) Reviews and Ratings. URL: <https://www.gartner.com/reviews/market/single-vendor-sase> (дата звернення: 22.11.2025).
8. What is SASE? Secure Access Service Edge. Netskope. URL: <https://www.netskope.com/security-defined/what-is-sase> (дата звернення: 22.11.2025).
9. Secure Access Service Edge (SASE). Netskope. URL: <https://www.netskope.com/products/secure-access-service-edge> (дата звернення: 22.11.2025).

10. Understanding Security Service Edge (SSE) and SASE. Netskope. URL: <https://www.netskope.com/blog/understanding-security-service-edge-sse-and-sase> (дата звернення: 20.11.2025).
11. Netskope One SASE. Netskope. URL: <https://www.netskope.com/resources/data-sheets/netkope-one-sase> (дата звернення: 26.11.2025).
12. Netskope Security Cloud Platform. Netskope. URL: <https://www.netskope.com/wp-content/uploads/2022/10/netkope-security-cloud-platform-2.pdf> (дата звернення: 27.11.2025).
13. Netskope Security Cloud Features. Netskope. URL: <https://docs.netskope.com/en/netkope-security-cloud-features/> (дата звернення: 01.12.2025).
14. Netskope One – Cloud-native Converged Security & Networking. Netskope. URL: <https://www.netskope.com/netkope-one> (дата звернення: 29.11.2025).
15. A Guide to Secure Access Service Edge (SASE). Zayo. URL: <https://www.zayo.com/resources/a-guide-to-secure-access-service-edge-sase/> (дата звернення: 12.11.2025).
16. SASE: Secure Access Service Edge. Upright Security. URL: <https://uprightsecurity.com/services/sase/> (дата звернення: 20.11.2025).
17. What is SASE? A Guide to Secure Access Service Edge. Somerford Associates. URL: <https://www.somerfordassociates.com/blog/what-is-sase/> (дата звернення: 06.11.2025).
18. What is Secure Access Service Edge (SASE)? | SD-WAN. HPE Airheads Community. URL: <https://airheads.hpe.com/discussion/what-is-secure-access-service-edge-sase> (дата звернення: 01.11.2025).
19. Gartner SASE – The Future of Network Security is Now. Netskope. URL: <https://www.netskope.com/blog/gartner-sase-the-future-of-network-security-is-now> (дата звернення: 31.10.2025).

20. The pros and cons of Netskope SASE. TechTarget. URL: <https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-Netskope-SASE> (дата звернення: 01.11.2025).

ДЕМОНТРАЦІЙНІ МАТЕРІАЛИ (Презентація)