SASE: нова концепція кібербезпеки

Нова архітектура безпеки з'явилася два роки тому і швидко набуває популярності.

У світі кібербезпеки постійно виникають нові концепції та підходи. SASE (Secure Access Service Edge) — це архітектура, яка поєднує програмно-визначувану мережу (SD-WAN) і функції захисту (антивірус, DLP, брокер хмарного доступу CASB, хмарний мережевий екран за моделлю FWaaS тощо). Все це надається як єдиний сервіс і має на меті зменшити складність мережі, підвищити її продуктивність, забезпечити більш захищений доступ і в цілому покращити безпеку.

В цілому вважається, що за SASE майбутнє, тому ключові виробники як мережевих, так і безпекових рішень вже пропонують такі розробки.

«СіБ» розібрався, як влаштований SASE, у чому його реальні переваги – до того, як ця концепція остаточно стане мейнстримом (або відімре).

SASE виросла з SD-WAN

SASE означає щось на кшталт «безпечного крайового доступу» (в англомовних матеріалах незмінно підкреслюється, що цей термін вимовляється як sassy — «нахабний»). Термін означає хмарну платформу, яка поєднує інструменти безпеки і програмно-визначуваних мереж.

Причиною появи такого концепту стали усі ті явища, які відбуваються у корпоративних мережах протягом останніх років. По-перше, це поширення хмарних сервісів, зокрема моделі SaaS. Чимдалі більше даних і корпоративних програм переносяться у хмару, що є зручним і дозволяє ефективно розпоряджатися коштами. По-друге, завдяки Інтернету компанії можуть набирати персонал залежно від потрібних навичок, а не від місця проживання, а загалом через пандемію тренд на віддалену роботу тільки посилився. Завдяки ж мобільним пристроям доступ до корпоративних ресурсів можливий з будь-якої точки світу. Усе це обумовлює потребу забезпечити комунікації, які були б одночасно надійними і захищеними.

Концепція SD-WAN, яка набула поширення у 2010-х роках, дозволила позбутися регіональних мереж на базі MPLS, які є дорогими, складно розширюваними і до того ж мають «ефект тромбона», тобто увесь трафік з віддалених точок спрямовується у головний офіс або корпоративний дата-центр і вже звідти в Інтернет. SD-WAN — це більш проста і надійна архітектура, яка використовує різні типи каналів доступу (наприклад, оптичні та 4G) і здійснює балансування трафіка між ними. Динамічний вибір шляху залежно від стану цих каналів (джитеру, затримки, коефіцієнта втрати пакетів тощо) або наперед заданих правил забезпечує дотримання якості послуг. Наприклад, критичний трафік завжди отримує пріоритет у розподілі пропускної здатності, а також йому можна жорстко призначити найбільш якісні канали.

SD-WAN, однак, може не все. Використання Інтернету замість власних або операторських виділених ліній не підвищує якість на надійність зв'язку. Окрім того, SD-WAN не розрахована на підтримку рухомих користувачів, оскільки створювалася для сполучення фіксованих майданчиків. Нарешті, SD-WAN не має власних механізмів безпеки, а тому необхідні додаткові системи кіберзахисту і сторонні сервіси, такі як CASB (брокер безпечного доступу до хмар).

Тому з'явилась ідея уніфікованого сервісу, який об'єднує SD-WAN і кіберзахист у загальній хмарній платформі.

SASE в «розтині»

Архітектура SASE представлена на **рис. 1** і складається з кількох основних компонентів. Насамперед це хмара SASE: єдиний сервіс, який забезпечує зв'язок і функції захисту. Точки присутності SASE PoPs — це віртуальні вузли хмари, які містять усе необхідне (сервери, канали, ПО) для доставки послуг SASE. Ці точки є симетричними, взаємозамінними, багатоклієнтськими і є інтегральною складовою корпоративної мережі, яку обслуговують. Край SASE використовується як точка входу для користувачів і включає в себе пристрій SW-WAN, якщо йдеться про підключення корпоративної мережі, маршрутизатори й мережеві екрани, а також програмні агенти для мобільних пристроїв. Нарешті, система управління відповідає за конфігурування і налаштування політик безпеки, а також за моніторинг мережі у реальному часі.

Як зазначається у книжці *Secure Access Service Edge (SASE) for Dummies*, виданій компанією ***Cato Networks***, хоча SASE є цілком новою і повністю хмарною архітектурою, самі технології та послуги, які лежать в її основі, не є новими, вони просто надаються через уніфіковане хмарне рішення за моделями Network-as-a-Service та Security-as-a-Service.

З мережевого боку, як зазначалось, SASE включає функціональність SD-WAN, яка забезпечує підключення філій та дата-центрів до хмари. Кожен крайовий пристрій підключений до SASE інтернет-каналами, а в точці присутності трафік класифікується і пріоритезується відповідно до встановлених правил. Понад те, PoP автоматично фіксує втрату пакетів і у разі погіршення ситуації ініціює переключення на інший канал.

Проте SASE — це не лише SD-WAN, а й транспортна мережа, яка лежить «під нею». Існують провайдери SASE, які володіють власними точками присутності, що поєднані каналами, орендованими у операторів зв'язку першого рівня. Ця «глобальна приватна опорна мережа» здатна забезпечувати роботу багатьох накладених WAN. Таким чином, клієнту залишається лише «дійти» до PoP-провайдера, який бере на себе відповідальність за якість послуг, здійснюючи постійний моніторинг каналів і автоматичний вибір оптимальних маршрутів. Корпоративні ресурси, власні ЦОД і віддалені користувачі приєднуються до PoP безпечними тунелями.

Також провайдер SASE опікується безпечним доступом до хмарних інструментів, що досягається завдяки інтеграції його мережі з основними постачальниками хмарних послуг, як-от AWS, Microsoft чи Google.

Таким само чином провайдер надає набір послуг захисту, з яких клієнт обирає потрібні. Наприклад, Firewall-as-a-Service (FWaaS), що дозволяє позбутися апаратних пристроїв у різних будівлях компанії. Як підкреслює Cato Networks, FWaaS не просто «заліплює» мережеві екрани «хмарною ізоляційною стрічкою», а взагалі робить непотрібним сам формфактор окремого мережевого екрану, оскільки відтепер функції безпеки, такі як контентна фільтрація, запобігання вторгненням, захист від зловмисного ПЗ, виявлення та знешкодження загроз, доступні будь-де. До цього додаються загальні переваги моделі SaaS, зокрема те, що провайдер бере на себе регулярне оновлення ПЗ до останніх версій. SASE також підтримує можливості захисту від зловмисного ПЗ наступного покоління (Next-generation antimalware — NGAM). Вони включають в себе глибокий аналіз пакетів, розпізнавання типів файлів,

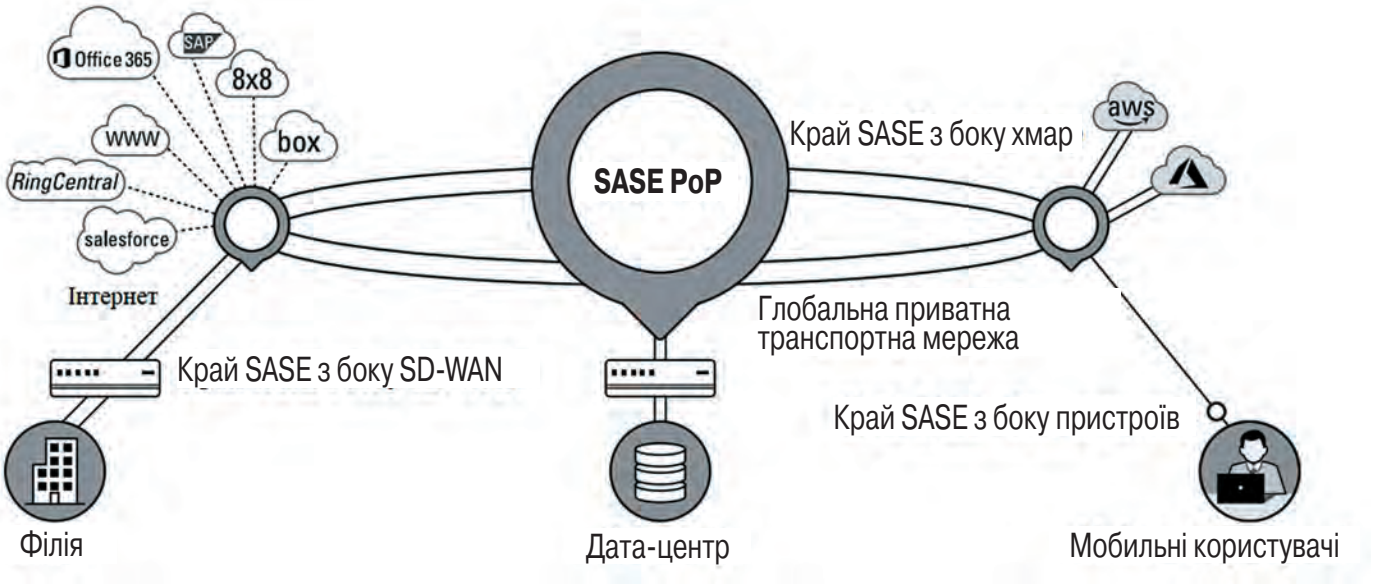

Рис. 1. Загальна схема SASE (джерело: Cato Networks)

що передаються по мережі (це дозволяє виявляти потенційно шкідливі файли і нейтралізувати техніки обходу, які використовують злочинці), а також багатошарові засоби виявлення і знешкодження загроз, такі як сигнатурний ті евристичний аналіз, штучний інтелект.

Система запобігання вторгненням (IPS) теж пропонується як окремий хмарний сервіс. Він включає поведінковий і репутаційний аналіз, протокольну валідацію (перевірку відповідності пакетів протоколам зв'язку для блокування атак через аномальний трафік), доручення в пошуковий механізм інформації про нові вразливості, блокування зв'язку злочинного ПО з керівними центрами, підтримання політик доступу з використанням географічного розташування (наприклад, блокування трафіка з певних країн чи до них). Усе бере на себе провайдер, який також відповідає за створення і оновлення сигнатур.

Зрештою, SASE підтримує концепцію мережевого доступу з нульовою довірою (Zero-Trust Network Access — ZTNA), яка покликана убезпечити роботу віддалених та мобільних працівників. Зазвичай для цього використовується VPN, що вимагає наявності мережевих екранів або VPN-концентраторів, а це збільшує затримку. Окрім того, під'єднавшись по VPN, користувач отримує доступ до усіх корпоративних ресурсів, що збільшує ризик поширення зловмисного ПО та/або витоку даних. В SASE користувач входить у корпоративну мережу без пристроїв-посередників з використанням багатофакторної автентифікації, при цьому він отримує доступ лише до дозволених ресурсів, а постійна перевірка трафіка забезпечує своєчасне виявлення загроз.

Не всі SASE однакові

В цілому вже є певний набір ознак і функцій, яким повинні відповідати SASE. Організація ***Enterprise Management Associates (EMA)***, яка у лютому цього року випустила порівняльний звіт рішень, які можна зустріти на ринку, розділила функції SASE на три групи. До основних належать SD-WAN, захищений веб-шлюз (SWG), ZTNA, FWaaS, вміння визначати чутливі дані (у тому числі зашифровані) і зловмисне ПЗ, а також стабільна робота на лінійній швидкості. Окрім того, ще є рекомендовані функції, наприклад, захист застосунків і API (WAAP), ізоляція браузера (тобто відокремлення діяльності користувача в Інтернеті від корпоративної інфраструктури), мережева пісочниця тощо. Нарешті, є додаткові можливості, такі як захист хотспотів Wi-Fi, приховування архітектури мережі від зловмисників (Network obfuscation, захист крайових обчислень та поведінковий аналіз користувачів (UEBA).

EMA у цьому відношенні зазначає, що на дату публікації звіту дуже мало хто з виробників міг похвалитися підтримкою усіх базових можливостей SASE, хоча багато хто запланував розширення функціональності у своїх дорожніх картах. Кожна з компаній так чи інакше прагне грати на своїх сильних сторонах, і те, як вони реалізували архітектуру SASE, справляє величезний влив як на ефективність рішення, так і на вартість послуг і розташування точок присутності.

Приміром, рішення ***Palo Alto Networks*** — Prisma Access SASE – працює на базі хмар AWS і Google Cloud і використовує функціональність свого NGFW з обробкою трафіка в один прохід. Кожному клієнтові виділяється програмний вузол безпекової обробки (SPN), що здорожчує послугу, але забезпечує ізоляцію клієнтів один від одного і дозволяє уникнути негативного впливу на продуктивність. У ***Fortinet*** рішення SASE з'явилося після придбання компанії OPAQ і використовує крайові пристрої (мережевий екран і захищений веб-шлюз). ***Cato Networks***, навпаки, розміщує увесь стек функцій безпеки на серверах у колокації, а також агресивно розширює власну транспортну мережу.

Cloudflare, світовий провайдер послуг доставки контенту, послуговується власною мережею з понад 200 дата-центрів, де в один прохід відбувається фільтрація контенту і виконання безпекових перевірок. Аналогічно ***Zscaler*** використовує свою потужну хмарну інфраструктуру, вибудувану за ті роки, коли компанія надавала сервіс захищених веб-шлюзів. У ній в один прохід здійснюється дешифрування трафіка, його перевірка і вживання необхідних заходів, хоча функціональність SD-WAN забезпечують партнери, зокрема Aruba і VMware.

Cisco має пірінгові угоди з тисячами операторів, що забезпечує високошвидкісний доступ з низькою затримкою до програм, а рішення SASE базується на брендах, куплених у різний час: зокрема Meraki і Viptela (SD-WAN), Umbrella, Scansafe та ін. з безпекового боку, а також на власній службі кіберрозвідки Talos. Архітектура ***Aruba (HPE)*** Silver Peak включає в себе спеціалізовані пристрої, апаратні або віртуалізовані, які поєднують функції SD-WAN, сегментації та мережевого екрану, тоді як інші функції безпеки надають партнери (зокрема, клієнти мають змогу самостійно обирати рішення безпеки, які інтегруються з SD-WAN через систему управління Aruba Orchestrator). Партнери забезпечують і точки присутності. ***VMware*** і ***Versa*** пропонують клієнтам можливість користуватися послугами SASE локально або через хмарну підписку.

Загалом EMA нарахувала щонайменше 16 компаній, які активно просувають послуги SASE. Організація ділить їх на 4 групи: ті, що спеціалізуються на SASE (наприклад, Cato Networks і Versa Networks); компанії, що свого часу придбали виробників SD-WAN і рішень хмарної безпеки (це, наприклад, Cisco, HPE, Fortinet, Palo Alto); гравці, що мають партнерські відносини з провайдерами SD-WAN (Forcepoint, McAfee, Zscaler, Check Point тощо); і провайдери SDN, які розвинули в себе функції SASE (Cloudflare, Akamai).

Ідея набуває поширення

Між тим, уже досить помітно, що після усього лише двох років з часу (офіційної) появи терміну SASE ця ідея пустила коріння. У квітні організація ***Ponemon Institute*** оприлюднила результати дослідження, яке було проведене за спонсорської участі компанії ***Aruba*** і стосувалося реального використання архітектур SD-WAN, SASE і Zero Trust. Усього було опитано понад 1,8 тис. фахівців з різних сфер бізнесу із основних регіонів світу.

Чи розгорнула Ваша організація або чи планує розгорнути архітектуру безпеки SASE?

Рис. 2. Плани розгортання SASE серед організацій світу (за даними Ponemon Institute)

Дослідження показало, що рівень проникнення SASE найближчим часом зростатиме. Серед опитаних 10% повідомили, що SASE в них вже розгорнуто, 14% — що буде розгорнуто впродовж року, 25% — що такі плани є, але без конкретних термінів (**рис. 2**). Як видно, SASE таки стає мейнстрімом — лише третина респондентів заявила, що у них нема планів щодо впровадження цієї архітектури. Прикметно, що ті організації, які впевнені в дієвості своїх архітектур безпеки, активно запроваджують нові концепції — зокрема, серед високоефективних компаній SASE розгорнули вже 43%.

Загалом з SASE виявилися знайомі 45% опитаних (з Zero Trust — 62%). В регіональному розрізі з SASE найкраще знайомі в Північній Америці та EMEA (по 47% опитаних), а впроваджень найбільше знову-таки в Північній Америці 43%). При цьому більшість компаній (44%) схильні обирати виробників, які спеціалізується на таких рішеннях, тоді як 31% назвали виробників систем безпеки, у яких ці продукти є частиною більш широкого портфеля, а 25% обрали постачальників мережевих систем.

За даними ***Gartner***, наведеними у вересневому звіті *Magic Quadrant for WAN Edge Infrastructure*, до 2024 року 70% власників SD-WAN впровадять SASE (порівняно з 2021 роком). Компанія Netscaler оцінила, що загалом до 2024 року 40% компаній матимуть чіткі стратегії впровадження SASE.

EMA наводить ще переконливіші цифри: у їхніх опитуваннях щонайменше 75–78% респондентів були знайомі з SASE. При цьому анкетування фахівців з мережевих систем і з інформаційної безпеки виявило цікаві розбіжності: якщо серед «мережників», знайомих з SASE, 37% заявили, що їхні організації вже частково це впровадили, серед «безпечників» таких виявилося лише 14%. Оцінюванням або тестуванням займалися відповідно 28% і 8%. EMA це пояснює, зокрема, тим, що виробники SD-WAN найактивніше просувають свої рішення саме як SASE, чим і приваблюють IT-відділи компаній. З іншого боку, саме функціональність SD-WAN користувачі цінують найбільше (на другому місці багатофункціональний хмарний захист, на третьому безпечний віддалений доступ).

Згідно з прогнозом агенції ResearchAndMarkets, світовий ринок SASE найближчим часом зростатиме шаленими темпами — в середньому по 36,4% на рік — і до 2028-го сягне $11,29 млрд. Повідомляється, що минулого року найбільший попит на SASE демонстрував сектор IT і телекомунікацій. Markets&Markets наводить такі цифри: у 2021 році розмір ринку прогнозується на рівні $1,2 млрд, у 2026-му він становитиме $4,1 млрд при середньому зростанні 26,4% на рік. Ця компанія називає найбільшим споживачем банківсько-фінансовий сектор. Агенція Valuates Reports оцінює ринок минулого року у $2,668 млрд і прогнозує, що у 2027-му він збільшиться до $5,430 млрд, середнє зростання буде 10,4%. Усі три звіти називають ключовим фактором зростання пандемію COVID-19, яка посилила потребу в організації безпечного віддаленого доступу для персоналу, а також у хмарних продуктах і сервісах.

Наскільки реальні ці прогнози, можна буде побачити вже у найближчі роки, але якщо кажуть правду, що до-пандемічні порядки вже не повернуться, то потреба в SASE дійсно лише зростатиме.

Василь ТКАЧЕНКО, **СиБ**