https://www.cloudflare.com/learning/access-management/what-is-sase/

Что такое SASE? | Технология безопасного пограничного доступа

Технология безопасного пограничного доступа, часто встречающаяся под аббревиатурой SASE (Secure access service edge) - это разновидность IT-модели, сочетающая функционал сетевых сервисов и сервисов безопасности.

Модель SASE

Задачи обучения

Прочитав эту статью вы:

- сможете дать определение понятию безопасного пограничного доступа (SASE)
- узнаете, какие сервисы входят в объем SASE?
- узнаете отличие между SASE и традиционной сетевой архитектурой
- изучите преимущества внедрения систем SASE

Сопутствующий контент

Модель безопасности в условиях «нулевого» доверия

Шлюз информационной безопасности

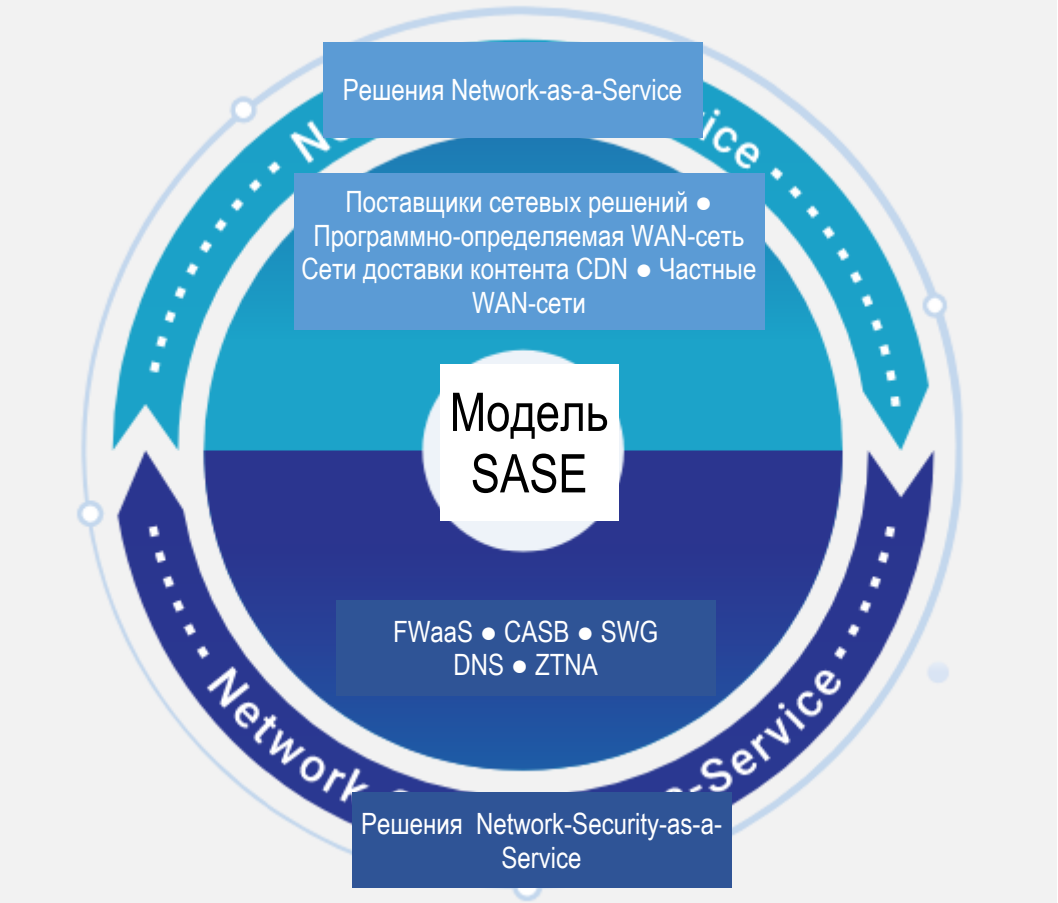
Что такое IAM?

Контроль доступа

Концепция программно-определяемого периметра (SDP)

Что такое SASE?

Технология безопасного пограничного доступа (SASE) реализована в модели безопасности на базе облачных ресурсов, в рамках которой объединен функционал программно-определяемых сетей (software-defined networking) и функции сетевой безопасности, весь этот пакет сервисов обеспечивается одним и тем же провайдером. Сама по себе аббревиатура SASE была предложена в 2019 году институтом Гартнера - глобальным исследовательским и консалтинговым агентством.



Модель безопасности SASE является работающей на облачных ресурсах альтернативой традиционной «веерной» модели сетевой инфраструктуры, которую еще называют модель «спицы на втулке». Такая традиционная модель подразумевает, что пользователи во множестве своих точек местонахождения («спицы») связаны через централизованные центры обработки данных («втулка»). В рамках традиционной модели построения сети данные и приложения размещаются в ядре - централизованном дата-центре. Для получения доступа к этим ресурсам пользователи, филиалы и приложения подключаются к этому единому дата-центру, будучи объединенными рамками локальной частной сети или

вторичной сети, которая подключена к основной сети через выделенную защищенную линию или виртуальную частную сеть - VPN.

Будучи достаточно простой по сути своей, традиционная «веерная» модель имеет ряд недостатков, в частности, она плохо приспособлена для решения проблем, связанных с безопасностью работы облачных сервисов, например, Software-as-a-Service (SaaS), а также не обеспечивает потребностей растущего числа пользователей, работающих удаленно. По мере того, как все большее количество разнообразных приложений, рабочих функций и конфиденциальных корпоративных данных переносится в облако, организациями приходится переосмысливать свою концепцию проверки сетевого трафика и управления политикой безопасного пользовательского доступа в сеть. Не представляется больше целесообразным осуществлять маршрутизацию всего трафика через единый дата-центр (принцип «тромбона»), учитывая, что большая часть приложений и данных уже перенесены в облако, это лишь чревато ненужными задержками. Эти задержки особенно остро будут ощущаться пользователями, работающими удаленно (а таких немало), при попытке подключения к корпоративной информационной сети через VPN, при этом пользователи сталкиваются с определенными рисками безопасности, когда осуществляют доступ к корпоративным информационным ресурсам через незащищенное соединение.

В модели SASE механизмы управления безопасностью сети размещены на периметре сети - в пограничной с облаком зоне - в отличии от традиционной модели, где управление безопасностью осуществляется централизованно, через единый дата-центр. Вместо того, чтобы множить облачные сервисы, требующие индивидуальной конфигурации и управления, модель SASE обеспечивает стандартизированный набор сетевых сервисов и сервисов безопасности, которые позволяют создать хорошо защищенную и эффективно организованную сетевую архитектуру в зоне соединения сети и облака (пограничная сетевая зона). Внедрение для защиты периметра сети политики управления доступом в условиях «нулевого» доверия, основанной на аутентификации личности пользователя, позволяет организациям существенно раздвинуть границы сетевого периметра, включив в них и работающих удаленно пользователей, и отдельные филиалы, мобильные устройства или приложения. Это, в свою очередь, делает ненужным использование VPN-сетей и файерволов, обеспечивая более тщательный контроль

реализации политики безопасности сети. Для этого модель SASE должна быть интегрирована уже в готовую единую глобальную сеть, в рамках которой вся комбинация сетевых сервисов и сервисов безопасности будет максимально приближена к конечному пользователю.

Почему модель SASE необходима?

Давайте представим традиционную архитектуру сети в виде кирпичной кладки, намертво скрепленной раствором. Предположим, Боб хочет проверить баланс своего счета, прежде чем оплатить стоимость аренды. Для этого ему нужно совершить визит в банк и подтвердить свою личность сотруднику банка. Каждый месяц ему приходится совершать такую поездку в банк, и вся процедура повторяется из раза в раз, а поездка обходится недешево в плане затрат времени и сил, особенно, если Боб живет далеко от банка.

Сходная ситуация наблюдается и в аппаратно-определяемом варианте сетевой архитектуры, в этом варианте все решения, связанные с безопасностью и предоставлением доступа, принимаются на уровне стационарного корпоративного дата-центра, а не в рамках облака. Добавление облачных сервисов в традиционную модель сетевой архитектуры сходно с тем, что Боб получил бы возможность проверять баланс своего счета по звонку в банк. Это немного удобнее, чем садиться за руль и ехать через весь город, но здесь потребуется совершенно другой процесс авторизации (например, вместо предъявления удостоверения личности, Боба могут попросить представить по телефону целый ряд других данных для подтверждения его личности). Перед банком встает необходимость управления всем процедурами авторизации для того, чтобы представленная в ходе этих процедур клиентами конфиденциальная информация была в безопасности.

Традиционная «веерная» инфраструктура на момент своего создания не была рассчитана на работу с облачными сервисами. В ее основе фиксированный и защищенный периметр сети, сформированный вокруг основного дата-центра, эта модель эффективна лишь в том случае, если большая часть данных и приложений остается внутри этого периметра. При переходе к облаку для IT-специалистов становится сложнее управлять различными сервисами безопасности и политикой контроля доступа.

С другой стороны, модель SASE работает по аналогии с банковским приложением, установленным на мобильном устройстве Боба. Вместо того, чтобы лично ехать в банк или тратить время на телефонный звонок, Боб может в электронном виде пройти авторизацию и быстро получить доступ к информации о балансе своего счета из любой точки мира. И это становится возможным не только для Боба, но и для любого клиента банка, независимо от его местонахождения.

Модель SASE приближает сервисы по обеспечению безопасности сети и контроля доступа к конечному пользователю путем переноса ключевых процессов в облако, она функционирует в глобальной сети для минимизации времени задержки при работе этих ключевых процессов.

Какие возможности включает в себя модель SASE?

Пакеты сервисов в рамках модели SASE: возможности программно-определяемых WAN-сетей с богатым функционалом сервисов сетевой безопасности, которые в полном объеме доставляются и управляются с единой облачной платформы. Пакет функционала SASE включает в себя следующие 4 базовых компонента обеспечения безопасности:

1. *Шлюзы веб- безопасности (SWG):* Они также известны как шлюзы безопасности Интернет-каналов. Позволяют предотвратить кибер-атаки и утечку данных путем фильтрации нежелательного контента, содержащегося в веб-трафике, блокируют действия неавторизованных пользователей и способствуют реализации корпоративной политики безопасности. Шлюзы информационной безопасности могут быть внедрены в любом месте, что делает их идеальным вариантов для организации работы сотрудников «на удаленке».
2. *Агент по управлению безопасным доступом в облако (CASB):* Агент CASB выполняет несколько функций обеспечения безопасности для облачных сервисов: выявляет теневую активность (неавторизованный корпоративные IT-системы), защищает конфиденциальные данные с помощью систем DLP и систем контроля доступа, обеспечивает соответствие с требованиям регламентов по защите данных и прочее.
3. *Контроль доступа в сеть в условиях «нулевого» доверия (ZTNA):* Платформы контроля доступа ZTNA блокируют внутренние ресурсы, защищая их от возможности публичного доступа, и помогают обезопасить систему от потенциальных утечек данных. Это достигается путем запроса аутентификации в режиме реального времени для разрешения доступа каждому отдельно взятому пользователю к любому защищенному приложению.
4. *Решения на базе сетевых экранов Firewall-as-a-Service (FWaaS):* Концепция FWaaS подразумевает использование сетевых защитных экранов (файерволов) как сервиса, получаемого из облака. Сетевые экраны FWaaS защищают облачные платформы, инфраструктуру и приложения от кибер-атак. В отличие от традиционных сетевых экранов, FWaaS не является физическим устройством, а представляет собой набор сервисов безопасности, в числе которых фильтрация URL-адресов, функция предотвращения вторжений и единое управление политиками безопасности в рамках всего сетевого трафика.

В зависимости от поставщика и потребностей организации, это ключевые функции могут быть объединены и интегрированы с любым количеством сервисов безопасности, от защиты веб-приложений и API (WAAP) с изоляцией удаленных браузеров до рекурсивных DNS-серверов, защиты точек беспроводного доступа

Wi-Fi, механизмов сетевой обфускации/дисперсии, граничные вычисления (edge computing) и т.д.

Какие преимущества внедрения систем SASE

Модель SASE обеспечивает целый ряд преимуществ по сравнению с традиционной моделью сетевой безопасности, основанной на концепции дата-центра, лежащего в ядре всей системы.

- *Стандартизированные процессы внедрения и управления* Модель SASE объединяет точечные решения безопасности в рамках одного облачного сервиса, освобождая организации от необходимости взаимодействовать с несколькими поставщиками, что позволяет им тратить меньше средств, внутренних ресурсов и времени, занимаясь настройкой и обслуживанием физической инфраструктуры.
- *Упрощенное управление политикой безопасности* Вместо управления несколькими политиками безопасности в рамках отдельных решений, модель SASE позволяет организации устанавливать, контролировать, настраивать и внедрять единую политику контроля доступа для всех точек местоположения, всех пользователей, устройств и приложений с единого портала.
- *Контроль доступа в сеть в условиях «нулевого» доверия на основе аутентификации личности пользователя* В основе модели SASE лежит концепция безопасности в условиях «нулевого» доверия, это подразумевает, что пользователь не получит доступ к приложениям и данным до авторизации, даже если он уже находится внутри защитного периметра частной сети. При определении политики контроля доступа в рамках модели SASE учитывается не только личность пользователя, но и прочие факторы: местоположение пользователя, время суток, корпоративные стандарты безопасности, политика обеспечения соответствия нормативным требованиям и непрерывная оценка риска/уровня доверия.
- *Маршрутизация трафика с оптимизацией времени задержки* Существует целый ряд сервисов, крайне чувствительных к задержке доставки контента (например, видео-конференции, стриминговые каналы, онлайн-игры и пр),

соответственно, для поставщиков этих сервисов любое увеличение времени задержки является серьезной проблемой. Модель SASE помогает снизить время задержки путем маршрутизации сетевого трафика через глобальную сеть, в рамках которой обработка трафика производится по месту нахождения пользователя. Оптимизация процесса маршрутизации поможет определить самую быструю траекторию доставки трафика в обход проблемных с точки зрения скорости зон и с учетом прочих факторов.

Важно отметить, что все варианты реализации модели SASE выглядят одинаково. При наличии ряда общих характеристик - политики контроля доступа на базе авторизации личности пользователя, сетевых услуг безопасности и облачной архитектуры - существуют значительные отличия, которые зависят от специфики организации. К примеру, в отдельно взятом варианте реализации модели SASE может отдаваться предпочтение архитектуре с одним арендатором, нежели со множеством арендаторов, могут быть предусмотрены механизмы контроля доступа в сеть для Интернета Вещей и периферийных устройств, могут содержаться дополнительные ресурсы безопасности, делаться акцент на минимизацию количества аппаратных/виртуальных устройств для обеспечения функционирования сервисов безопасности и пр.

Как компания Cloudflare оказывает поддержку при внедрении модели SASE?

Предлагаемая компанией Cloudflare модель SASE может применяться с такими продуктами, как Cloudflare for Infrastructure и Cloudflare for Teams, оба этих продукта работают на базе единой глобальной платформы, обслуживающей более 25 миллионов сетевых Интернет-объектов. Продукт Cloudflare имеет уникальную архитектуру, представляя собой интегрированную платформу с пакетом сетевых сервисов и сервисов безопасности, в зону охвата которой входит более 200 городов. Эта платформа устраняет необходимость для организации заниматься закупкой и управлением целым набором точечных решений для работы в облаке.

Cloudflare for Infrastructure представляет собой созданный компанией пакет сервисов безопасности и управления сетью, которые обеспечивают безопасность, ускоряют и делают более надежной работу любой внутренней, гибридной или облачной системы. Неотъемлемой часть продукта Cloudflare for Infrastructure

является Cloudflare Magic Transit. Этот инструмент защищает инфраструктуру сети от угроз DDoS-атак и атак сетевого уровня, а также работает совместно с Cloudflare Web Application Firewall (WAF) для защиты против вредоносных кодов, эксплуатирующих уязвимости сети (эксплойтов). Продукт Magic Transit функционирует на базе глобальной сети Cloudflare, что позволяет ускорить прохождение легитимного трафика, сократить время задержки и оптимизировать пропускную способность сети. Более подробная информация о продукте Cloudflare Magic Transit.

Продукт Cloudflare for Teams обеспечивает безопасность корпоративных данных двумя разными способами: с помощью Cloudflare Access - продукта для контроля доступа в сеть в условиях «нулевого» доверия, и Cloudflare Gateway - сервиса с функционалом фильтрации запросов в системе DNS, обеспечивающего защиту от вредоносных программ (malware) и фишинга. Продукт Cloudflare Access делает ненужными традиционные VPN-сети и обеспечивает безопасный доступ на базе авторизации пользователя к внутренним сетевым приложениям и данным, независимо от местонахождения пользователя. Продукт Cloudflare Gateway защищает корпоративные данные и данные пользователей путем фильтрации и блокировки вредоносного контента, выявляя компрометированные устройства и используя технологию изоляции браузера для того, чтобы помешать срабатыванию вредоносного программного кода на других устройствах пользователей. Более подробная информация о продукте Cloudflare for Teams.