Павлов К.К. Сравнительный анализ эффективности ZTNA и SASE для защиты распределённых удалённых рабочих мест // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 197–201

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ZTNA И SASE ДЛЯ ЗАЩИТЫ РАСПРЕДЕЛЁННЫХ УДАЛЁННЫХ РАБОЧИХ МЕСТ

Павлов К.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1),e-mail: kkpavlov2004@gmail.com

В работе проводится сравнительный анализ двух современных моделей кибербезопасности – Zero Trust Network Access (ZTNA) и Secure Access Service Edge (SASE), используемых для защиты распределённых удалённых рабочих мест. Рассматриваются принципы функционирования, преимущества и ограничения каждой технологии, а также их применимость в условиях возросшей цифровой мобильности сотрудников. Автор подчёркивает ключевые различия между подходами «нулевого доверия» и конвергентной облачной безопасности, определяя оптимальные сценарии использования ZTNA и SASE для повышения уровня защиты организации.

Ключевые слова: ZTNA, SASE, удалённые рабочие места, безопасность сети, виртуализация, облачные сервисы, zero trust, корпоративная кибербезопасность.

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF ZTNA AND SASE FOR THE PROTECTION OF DISTRIBUTED REMOTE WORKPLACES

Pavlov K.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1),, e-mail: kkpavlov2004@gmail.com

This paper presents a comparative analysis of two modern cybersecurity models – Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) – used to protect distributed remote workplaces. The study examines the operational principles, advantages, and limitations of each approach, with particular attention to their relevance in the context of increasing employee mobility and decentralization of corporate infrastructures. Key distinctions between the zero-trust paradigm and converged cloud-based security are highlighted. The paper identifies optimal use cases for both ZTNA and SASE and outlines how these technologies enhance organizational security and resilience in remote-work environments.

Keywords: ZTNA, SASE, remote workplaces, network security, cloud security, zero trust, corporate cybersecurity.vulnerabilities, connection security.

Рост числа распределённых команд, массовый переход на удалённую работу и расширение использования облачных сервисов приводят к фундаментальным изменениям в организации корпоративной сетевой инфраструктуры. Такой переход невозможен без глубокого изменения подходов к нормативному регулированию облачной среды, поскольку, как отмечается в исследованиях, «для широкого и эффективного внедрения технологий нужны методические и нормативные документы, разъясняющие правовые рамки применения этих технологий, имеющиеся проблемы и риски и способы их минимизации» [7]. На

протяжении десятилетий основным способом удалённого безопасного подключения сотрудников оставались виртуальные частные сети (VPN). Однако VPN создают прямой доступ пользователя ко внутренней сети, что приводит к риску бокового перемещения злоумышленника в случае компрометации устройства или учётной записи. Кроме того, VPN не масштабируются под сотни и тысячи распределённых пользователей, требуют значительных аппаратных ресурсов и плохо адаптируются к облачной архитектуре [1]. В ответ на эти вызовы появились подходы, основанные на распределённой безопасности и принципе «ноль доверия»: Zero Trust Network Access (ZTNA) и Secure Access Service Edge (SASE). Оба решения предназначены для замены или расширения функциональности VPN, но отличаются масштабом, архитектурой и задачами. Сегодня они становятся ключевыми технологиями при защите гибридных и удалённых рабочих мест. В этих условиях всё более широкое распространение получают архитектуры Zero Trust Network Access (ZTNA) и Secure Access Service Edge (SASE), которые предлагают альтернативу традиционным VPN, перераспределяя функции аутентификации, контроля доступа и анализа трафика между облаком и конечными устройствами [2].

ZTNA опирается на концепцию Zero Trust – модель, полностью отвергающую предположение о безопасном внутреннем периметре. Согласно Zero Trust, каждая попытка доступа должна быть проверена, независимо от источника соединения. Пользователь, устройство, сеть и контекст – всё должно пройти повторную аутентификацию и оценку риска [3].

Рассмотрим основные прицепы ZTNA:

1. Нулевое доверия по умолчанию: доступ не предоставляется автоматически, даже если пользователь уже находится внутри сети. Каждый запрос – отдельная проверка.

2. Минимизация прав доступа: пользователь получает доступ только к одному конкретному приложению, а не к целой сети. Это снижает вероятность lateral movement – бокового перемещения злоумышленников [4].

3. Непрерывная проверка контекста:

ZTNA анализирует:

- состояние устройства (patch level, антивирус, наличие шифрования),
- геолокацию,
- поведенческие факторы,
- сетевые аномалии [5].

4. Отсутствие прямых сетевых соединений: пользователь не подключается к корпоративной сети, а получает туннель только к конкретному приложению.

В преимущества данного подхода входит:

- высокая изоляция приложений;
- значительное снижение площади атаки;
- независимость от сетевой инфраструктуры;
- удобное масштабирование на небольшие команды;
- возможность быстрой интеграции с облаком.

Ограничения такого подхода:

- сложная миграция при наличии большого количества устаревших приложений;
- необходимость перестройки IAM и политики доступа;

- отсутствие единых инструментов сетевой безопасности.

ZTNA – является решение для организаций, которым требуется тонко настроенный, строго сегментированный доступ к критически важным ресурсам, особенно в средах с ограниченным числом удалённых пользователей.

SASE представляет собой более широкую архитектуру, чем ZTNA. Это не отдельный инструмент, а целостная экосистема безопасности, которая переносит сетевые и защитные функции в облако. SASE сочетает:

- SD-WAN,
- облачный межсетевой экран (FWaaS),
- защищённый веб-шлюз (SWG),
- брокер безопасности облачного доступа (CASB),
- встроенный механизм ZTNA,
- инспекцию и оптимизацию трафика [2].

Особенности CASE являются:

1. **Объединение сетевых и защитных функций в облаке**

Вся фильтрация и проверка трафика происходит в распределённых облачных точках присутствия, что снижает нагрузку на локальные ресурсы.

2. **Единая политика безопасности для всех пользователей**

Независимо от того, где находится сотрудник – в филиале, дома или в другом регионе.

3. **Широкий спектр интеграций**

SASE включает инструменты анализа угроз, DLP, защиту облачных сервисов, контроль теневых ИТ.

4. **Масштабируемость и производительность**

Поддержка тысяч пользователей по всему миру без необходимости увеличения мощности локальных дата-центров [5].

Преимущества и ограничения CASE

Преимущества:

- централизованное управление безопасностью;
- широкая функциональность «всё в одном»;
- улучшенная производительность благодаря глобальной оптимизации трафика;
- удобство для крупного бизнеса и распределённых филиальных сетей.

Ограничения:

- зависимость от качества интернет-соединения;
- необходимость готовности к активному использованию облачных сервисов;
- возможная сложность миграции при переходе от локальных решений.

SASE выступает идеальным вариантом для компаний, стремящихся к глобальной унификации управления безопасностью и снижению операционных затрат.

ZTNA и SASE часто воспринимают как альтернативы, но это некорректно. ZTNA – элементарная составляющая SASE, выполняющая узкую задачу контроля доступа. В то время как SASE расширяет её возможностями сетевой доставки и глубокой инспекции трафика (Таблица 1).

Таблица 1 – Сравнение подходов ZTNA и CASE

Критерий	**ZTNA**	**SASE**
Масштаб	Локальный, точечная защита приложений	Глобальный, защита всей сети
Подход	Zero Trust для доступа	Конвергентная безопасность и сеть
Основные функции	Контроль доступа, сегментация	FWaaS, SWG, CASB, SD-WAN, ZTNA
Инфраструктура	Чаще используется как дополнение	Полная облачная архитектура
Производительность	Зависит от конкретного сервиса	Оптимизируется через PoP
Применимость	Малый и средний бизнес	Средний и крупный бизнес

Рассмотрим практические сценарии применения подходов в рамках организация. Сценарий 1: Защита критически важных внутренних приложений. Компания может использовать ZTNA для обеспечения доступа только к внутренним ERP/CRM, огранивич боковое движение и минимизировав риски проникновения.

Сценарий 2: глобальная распределённая инфраструктура для корпораций с филиалами в разных странах оптимален SASE:

- единая политика;
- фильтрация трафика во всех точках присутствия;
- снижение нагрузки на корпоративные ЦОДы.

Сценарий 3: гибридная модель

Средний бизнес часто сочетает оба подхода:

- ZTNA — для внутренних приложений;
- SASE — для облачных ресурсов и интернета.

Такой подход позволяет адаптировать стратегию безопасности под разнообразные бизнес-процессы.

Текущий тренды внедрения ZTNA и CASE

Согласно аналитике ведущих компаний кибербезопасности:

- крупный бизнес чаще выбирает **SASE** благодаря масштабируемости и унификации процессов;
- средний бизнес комбинирует решения;
- малые компании предпочитают **ZTNA** как более доступное и быстрое в развёртывании [6].

ZTNA – является важным подходом Zero Trust, который становится обязательной частью корпоративной политики безопасности.

SASE превращается в облачную платформу, способную полностью заменить локальные средства безопасности и сетевую инфраструктуру.

Аналитические отчёты ведущих компаний в области кибербезопасности показывают, что крупные предприятия чаще выбирают SASE для глобальной масштабируемости и возможности централизованного управления распределёнными командами [6]. Средний бизнес стремится сочетать оба подхода, применяя ZTNA для защиты критичных внутренних ресурсов и SASE – для контроля внешних и облачных сервисов. Малые компании чаще внедряют ZTNA как более доступное и легко развёртываемое решение. Такое сочетание позволяет формировать гибкую модель безопасности, адаптированную к специфике организации.

ZTNA и SASE представляют собой эволюцию методов защиты распределённых рабочих мест. ZTNA обеспечивает строгую минимизацию доверия и эффективную сегментацию доступа, предотвращая распространение угроз в случае компрометации одного пользователя или устройства [4]. SASE предлагает более широкую архитектуру, в которой объединены сетевые и защитные функции, что создаёт единую облачную платформу для контроля трафика, предотвращения угроз и управления доступом [5]. В условиях возросшей цифровой мобильности именно совместное применение ZTNA и SASE обеспечивает наиболее высокий уровень безопасности и устойчивость корпоративной инфраструктуры к современным киберугрозам [6].

Список литературы

1. Бирих Э.В., Травкина Е.А. Сравнительный анализ подходов к безопасности технологий VPN и ZTNA // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом (Сборник материалов (тезисов) 53-й Международной конференции, Москва, 2024), 2024. – С. 72-74.
2. Gartner. The Future of Network Security Is in the Cloud. 2023.
3. John Kindervag. Zero Trust Architecture. Forrester Research, 2020.
4. NIST SP 800-207. Zero Trust Architecture. 2021.
5. Cisco. SASE and ZTNA Security Overview. 2023.
6. Palo Alto Networks. Global Remote Work Security Report, 2024.

References

1. Birikh E.V., Travkina E.A. Comparative Analysis of Approaches to VPN and ZTNA Security Technologies // Mobile Business: Prospects for the Development and Implementation of Radio Communication Systems in Russia and Abroad (Collection of Materials (Abstracts) of the 53rd International Conference, Moscow, 2024), 2024. – pp. 72-74.
2. Gartner. The Future of Network Security Is in the Cloud. 2023.
3. John Kindervag. Zero Trust Architecture. Forrester Research, 2020.
4. NIST SP 800-207. Zero Trust Architecture. 2021.
5. Cisco. SASE and ZTNA Security Overview. 2023.
6. Palo Alto Networks. Global Remote Work Security Report, 2024.