УДК 004.771

РЕФЕРЕНСНАЯ АРХИТЕКТУРА ЗАЩИЩЁННОГО УДАЛЁННОГО ДОСТУПА НА БАЗЕ SASE/ZTNA: КОМПОНЕНТЫ, ПОТОКИ ДОСТУПА И АРТЕФАКТЫ TOGAF

Наталья Викторовна Картечина
кандидат сельскохозяйственных наук, доцент
kartechnatali@mail.ru
Никита Алексеевич Улыбышев
студент
avtocad68@yandex.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. Статья описывает универсальную (vendor-neutral) референсную архитектуру защищённого удалённого доступа к корпоративным приложениям на основе SASE/ZTNA и принципов Zero Trust. Рассмотрены основные компоненты (идентичность, MFA, доверие к устройству, enforcement, коннекторы, журналирование), типовые потоки доступа и практичный набор артефактов TOGAF для документирования и планирования внедрения.

Ключевые слова: референсная архитектура, ZTNA, SASE, Zero Trust, IdP, posture check, SIEM, TOGAF артефакты.

1. Цели и границы референсной архитектуры

Цель: обеспечить безопасный доступ удалённых пользователей к корпоративным приложениям по принципам:

– явная аутентификация и авторизация;

– минимальные привилегии;

– контекстный контроль и постоянная проверка;

– сквозной аудит.

Граница решения: фокус на доступе к корпоративным приложениям (private apps и SaaS). Функции SASE вроде SWG/CASB/FWaaS рассматриваются как расширения, часто используемые совместно.

2. Слои архитектуры (в логике TOGAF)

2.1 Business Architecture: роли и сценарии

Типовые роли:

– Пользователь (стандартный доступ к рабочим приложениям);

– Подрядчик/партнёр (ограниченный доступ, повышенная чувствительность);

– Администратор (привилегированные операции, требования PAM);

– Служба ИБ/ИТ (политики, мониторинг, реагирование).

Типовые сценарии:

– доступ к web-приложениям;

– доступ к внутренним API/сервисам;

– доступ к административным интерфейсам (RDP/SSH/консоли);

– доступ из «недоверенных» сетей.

2.2 Application Architecture: классы приложений

– SaaS/Web (обычно проще интегрируются через SSO);

– Private web/apps (публикуются через ZTNA + коннектор);

– Legacy (могут потребовать проксирования или специальных методов);

– Privileged endpoints (нуждаются в PAM/записи сессий).

2.3 Data Architecture: «данные о доверии»

Для принятия решения ZTNA использует:

– атрибуты пользователя (роль, группа);

– атрибуты устройства (управляемость, EDR, шифрование, патчи);

– контекстные атрибуты (гео, время, IP, риск);

– события аудита (policy-id, result, reason).

3. Компоненты референсной Technology Architecture

Набор компонентов можно выразить через типовые функциональные блоки:

– Identity Provider (IdP) / Directory – идентичность, группы, SSO;

– MFA/Strong Auth – усиленная аутентификация, предпочтительно устойчивые к фишингу механизмы там, где возможно;

– Device Trust (MDM/UEM + EDR) – состояние устройства (posture);

– Policy Decision Point (PDP) – движок политик, принимает решения;

– Policy Enforcement Point (PEP) – применяет решения (агент/прокси/edge);

– App Connector / Gateway – соединение с приложениями, часто через исходящие подключения;

– Observability – журналирование/телеметрия;

– SIEM/SOAR – корреляция событий и реагирование;

– PAM (для админов) – JIT-доступ, запись сессий.

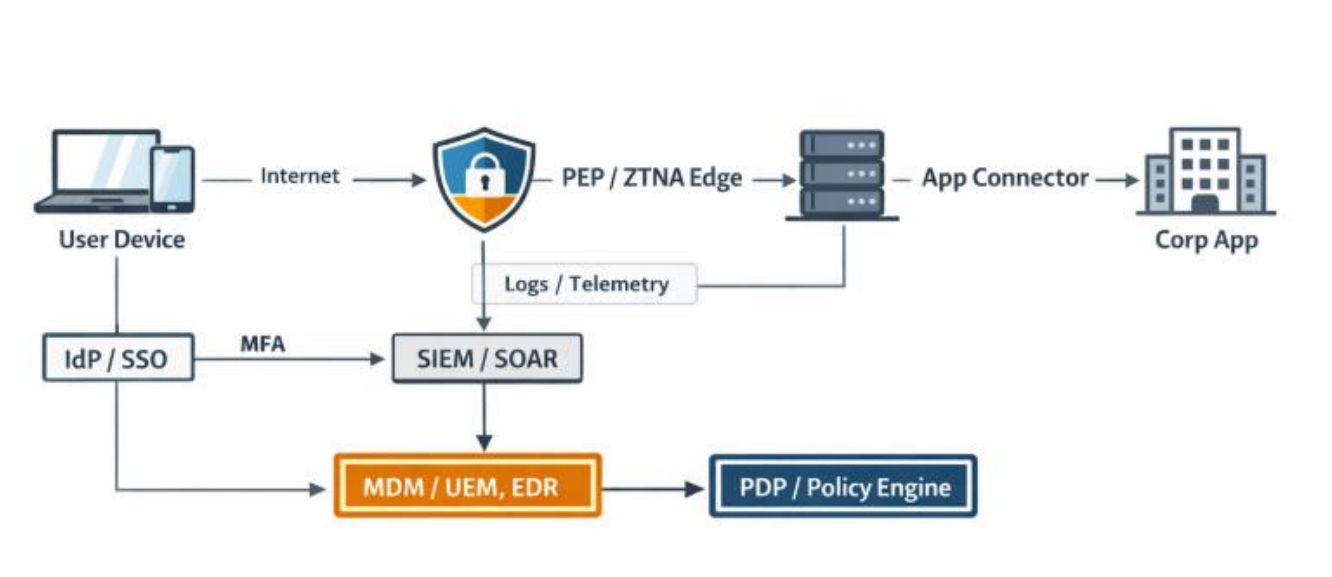

Рисунок 1 – Референсная архитектура ZTNA/SASE (ASCII-схема).

4. Типовые потоки доступа

4.1 Поток 1: доступ пользователя к приложению

Последовательность доступа:

1) Пользователь инициирует доступ к приложению (портал/агент/браузер);

2) PEP перенаправляет на IdP (SSO) → выполняется MFA при необходимости;

3) PDP собирает атрибуты: роль, группы, posture, риск, гео/время;

4) PDP принимает решение: allow/deny/step-up/ограничение;

5) PEP устанавливает соединение к приложению через коннектор;

6) Событие пишется в журнал: user, device, app, policy, decision, reason.

4.2 Поток 2: непрерывная проверка (continuous verification)

В течение сессии возможны «тригеры»:

– изменение posture (EDR выключен);

– смена географии/IP;

– рост риск-скоринга;

– выявление аномалии.

Реакции политики:

– запрос step-up MFA;

– принудительное завершение сессии;

– снижение привилегий (например, запрет скачивания).

5. Политическая модель: как описывать правила доступа

Удобная форма записи политики (вендорно-независимая):

Policy = Subject + Resource + Conditions + Action + Obligations

– Subject: роль/группа/уровень доверия;

– Resource: приложение, URL-путь, API, административный порт;

– Conditions: compliant device, гео, время, risk-score, тип сети;

– Action: allow/deny/step-up MFA/read-only;

– Obligations: запись сессии, повышенное логирование, DLP.

Пример:

– P-01: Если роль = «Employee» и device = compliant, то allow к App-Web.

– P-02: Если роль = «Contractor», то allow только к App-Portal, запрет download, session-timeout 30m.

– P-03: Если роль = «Admin», то доступ только через PAM + запись сессии + JIT 1h.

6. Артефакты TOGAF: что включить в архитектурное описание

В описание архитектуры следует добавлять:

1) Context Diagram (границы решения) – пользователи, IdP, ZTNA, приложения, SIEM.

2) Capability Map (карта возможностей).

3) Catalog требований (security requirements).

4) Матрица трассируемости (требование → компонент/контроль).

5) Roadmap (этапы внедрения).

6.1 Пример Capability Map

Таблица 1

Карта возможностей (упрощённо)

Домен	Возможность	Описание результата
Identity	SSO + MFA	Централизованная аутентификация
Device Trust	Posture контроль	Доступ зависит от состояния устройства
Access Control	App-level segmentation	Доступ выдаётся к приложению, не к сети
Monitoring	Central logging	Наблюдаемость и аудит
Response	SOAR/Playbooks	Автоматизация реагирования

6.2 Пример матрицы «угрозы-меры»

Таблица 2

Threat/control mapping

Угроза	Риск	Контроль (ZTNA/SASE)	Подтверждение
Кража пароля	Несанкционированный доступ	MFA, risk-based access	Логи IdP + policy decision
Компрометация устройства	Доступ злоумышленника	Posture (EDR/MDM), terminate	Posture events + session logs
Lateral movement	Распространение атаки	App-level segmentation	Нет сетевого доступа «широко»
Слабый аудит	Невозможность расследования	Центр логирования, SIEM	Полные события доступа

7. Нефункциональные требования (NFR), которые нельзя пропускать

Частые NFR для удалённого доступа:

– Доступность: отказоустойчивость PDP/PEP/коннекторов;

– Производительность: задержка до edge/PoP, влияние проксирования;

– Совместимость: поддержка legacy-протоколов и разных типов приложений;

– Наблюдаемость: полнота логов, корреляция, хранения;

– Управляемость: жизненный цикл политик, управление исключениями, контроль изменений.

8. Универсальная дорожная карта внедрения (результат TOGAF-подхода)

– Baseline: инвентаризация приложений и сценариев удалённого доступа;

– Классификация приложений по критичности/готовности;

– Пилот ZTNA на ограниченном наборе приложений;

– Интеграция posture + SIEM (политики становятся контекстными);

– Расширение на критичные приложения и отдельно – привилегированный доступ (PAM);

– Оптимизация и сокращение VPN до исключений.

9. Выводы

ZTNA в составе SASE реализует Zero Trust на практике: доступ становится транзакцией, управляемой политикой и контекстом, а не фактом «входа в сеть». Референсная архитектура должна описывать не только компоненты, но и потоки доступа, модель политик, NFR и набор артефактов TOGAF, обеспечивающих воспроизводимость и управляемость внедрения.

Список литературы

1. Грищенко В. В., Кузнецов А. А. Управление доступом и идентификацией в информационных системах: учебное пособие. СПб.: Питер, 2020. 304 с.

2. Макаренко С. И. Информационная безопасность распределённых и облачных систем: учебное пособие. М.: Инфра-М, 2022. 392 с.

3. Лапонина И. В., Киселёв А. А., Румянцев К. Е. Архитектура защищённых корпоративных сетей: учебное пособие. М.: МГУ им. М. В. Ломоносова, 2022. 288 с.

4. Зегжда П. Д., Полянский А. А. Архитектура и управление безопасностью информационных систем. М.: Горячая линия – Телеком, 2021. 456 с.

5. Барт Д., Гилман Э., Морильо К., Райс Р. Сети с нулевым доверием. Построение безопасных систем в ненадёжных сетях: практическое руководство / пер. с англ. СПб.: БХВ-Петербург, 2022. 336 с.

6. The Open Group. TOGAF® Standard. 10-е изд.: руководство / пер. с англ. / М.: ДМК Пресс, 2023. 820 с.

7. National Institute of Standards and Technology (NIST). Zero Trust Architecture: SP 800-207. 2020.

8. Методические рекомендации по защите информации в распределённых информационных системах // ФСТЭК России – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g

9. TOGAF. ADM Overview // The Open Group – URL: https://www.opengroup.org/togaf

UDC 004.771

REFERENCE ARCHITECTURE FOR SECURE REMOTE ACCESS BASED ON SASE/ZTNA: COMPONENTS, ACCESS FLOWS, AND TOGAF ARTIFACTS

Natalya V. Kartechina
candidate of agricultural sciences, associate professor
kartechnatali@mail.ru
Nikita Al. Ulybyshev
student
avtocad68@yandex.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. This article presents a vendor-neutral reference architecture for secure remote access to corporate applications based on SASE/ZTNA and Zero Trust

principles. It describes key components (identity, MFA, device trust, enforcement, connectors, logging), typical access flows, and a practical set of TOGAF artifacts for documenting the architecture and planning implementation.

Keywords: reference architecture, ZTNA, SASE, Zero Trust, IdP, posture check, SIEM, TOGAF artifacts.

Статья поступила в редакцию 25.02.2026; одобрена после рецензирования 20.03.2026; принята к публикации 31.03.2026.

The article was submitted 25.02.2026; approved after reviewing 20.03.2026; accepted for publication 31.03.2026.