Изибаев Дмитрий Вадимович, бакалавр
Уфимский университет науки и технологий
Izibaev Dmitry Vadimovich
Ufa University of Science and Technology

АРХИТЕКТУРНЫЕ ПРИНЦИПЫ И ТЕХНОЛОГИЧЕСКИЕ МЕХАНИЗМЫ РЕАЛИЗАЦИИ КОНЦЕПЦИИ «НУЛЕВОГО ДОВЕРИЯ» В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ
ARCHITECTURAL PRINCIPLES AND TECHNOLOGICAL MECHANISMS FOR IMPLEMENTING THE ZERO TRUST CONCEPT IN CLOUD INFRASTRUCTURES

Аннотация. Систематизированы подходы к обеспечению информационной безопасности облачных сред на основе архитектуры «нулевого доверия» (Zero Trust Architecture). Проанализирована логика функционирования компонентов управления и исполнения политик согласно стандарту NIST SP 800-207. Детализированы механизмы контекстно-зависимой верификации субъектов, учитывающие состояние оконечных устройств и параметры сессий в реальном времени. Рассмотрены технологические аспекты микросегментации на уровне программно-определяемых сетей. Проведено сопоставление протоколов ZTNA и традиционных средств удаленного доступа. В заключении сформулированы технологические преимущества и системные ограничения внедрения модели Zero Trust в распределенных вычислительных инфраструктурах.

Abstract. The paper systematizes approaches to ensuring information security in cloud environments based on the Zero Trust Architecture (ZTA). The logic of the functioning of control and enforcement components according to the NIST SP 800-207 standard is analyzed. Context-aware verification mechanisms taking into account device posture and session parameters in real time are detailed. Technological aspects of microsegmentation at the software-defined network level are considered. A comparison of ZTNA protocols and traditional remote access tools is conducted. In conclusion, the technological advantages and systemic limitations of implementing the Zero Trust model in distributed computing infrastructures are formulated.

Ключевые слова: Нулевое доверие, Zero Trust, NIST SP 800-207, ZTNA, облачная безопасность, микросегментация, информационная безопасность.

Keywords: Zero Trust, NIST SP 800-207, ZTNA, cloud security, microsegmentation, information security.

Введение

Трансформация подходов к защите облачных вычислительных сред обусловлена необходимостью обеспечения безопасности ресурсов в условиях отсутствия фиксированного сетевого периметра. Традиционные модели, предполагающие наличие зоны доверия внутри локальной сети, заменяются концепциями, ориентированными на идентификацию и непрерывную проверку контекста. Архитектура «нулевого доверия» (Zero Trust Architecture, ZTA) постулирует отказ от априорного доверия к любому субъекту вне зависимости от его сетевого местоположения. Публикация стандарта NIST SP 800-207 в 2020 году заложила методологическую базу для перехода к данной модели, определив требования к динамическому управлению доступом на основе оценки рисков [1].

Функциональные компоненты управления и исполнения политик

Логическая структура архитектуры нулевого доверия базируется на строгом разделении плоскости управления (Control Plane) и плоскости данных (Data Plane). Ключевым элементом принятия решений является Движок политик (Policy Engine). Этот компонент функционирует как аналитический узел, который на основе установленных правил безопасности и входящей телеметрии выносит вердикт о возможности предоставления доступа. В отличие от классических систем управления доступом, Движок политик оперирует

динамическими переменными, анализируя не только учетные данные, но и внешние факторы риска. Это позволяет системе адаптироваться к изменениям в инфраструктуре и блокировать запросы, имеющие признаки аномального поведения, еще до момента фактического взаимодействия с ресурсом [1, 2].

Второй важный компонент, Администратор политик (Policy Administrator), отвечает за техническую реализацию решений, принятых Движком. Он инициирует создание временных каналов связи и управляет аутентификационными токенами. Функционирование Администратора политик в изолированной плоскости управления предотвращает возможность прямой компрометации механизмов принятия решений со стороны потенциального нарушителя, находящегося в плоскости данных. PA гарантирует, что каждое соединение является краткосрочным и строго целевым, что исключает возможность несанкционированного расширения полномочий субъекта в процессе сессии [3].

Исполнительным механизмом в этой структуре выступает Точка обеспечения соблюдения политик (Policy Enforcement Point). Данный компонент располагается на пути следования трафика и выполняет функции интеллектуального шлюза. В облачных архитектурах PEP часто реализуется в виде набора микросервисов или распределенных брокеров доступа. Он терминирует соединение, инспектирует пакеты на соответствие установленным правилам и при необходимости мгновенно разрывает связь. Таким образом, PEP обеспечивает физическую или логическую изоляцию целевого ресурса, делая его недоступным для обнаружения и взаимодействия до момента успешного прохождения всех этапов верификации в плоскости управления [4].

Механизмы контекстно-зависимой аутентификации

Центральной технологией обеспечения безопасности в модели Zero Trust является контекстно-зависимая аутентификация. Данный подход заменяет статическую проверку пароля на комплексный анализ параметров сессии. Важнейшим фактором здесь выступает телеметрия оконечного устройства (Device Posture). Система проверяет целостность программной среды, наличие актуальных обновлений безопасности и активность средств защиты. Если устройство характеризуется высоким уровнем риска (например, из-за обнаружения уязвимостей в операционной системе), доступ к чувствительным облачным сервисам ограничивается даже при вводе корректных идентификаторов пользователя [2, 5].

Помимо состояния оборудования, анализируются геопространственные и поведенческие характеристики запроса. Учет местоположения позволяет идентифицировать попытки несанкционированного доступа из нетипичных регионов. Анализ времени запроса и характера обращения к данным помогает выявлять аномальную активность, свойственную автоматизированным атакам или компрометации учетных записей. Контекстно-зависимая верификация позволяет реализовать принцип адаптивного доверия, при котором права доступа динамически корректируются в зависимости от текущего уровня угрозы. Это значительно повышает точность идентификации и минимизирует риски, связанные с человеческим фактором [1, 6].

Микросегментация в программно-определяемых сетях

Для предотвращения горизонтального распространения угроз (lateral movement) внутри облачной среды применяется стратегия микросегментации. В отличие от традиционного разделения сети на широкие сегменты, микросегментация предполагает создание индивидуальных защитных барьеров вокруг каждой рабочей нагрузки, приложения или микросервиса. В современных центрах обработки данных эта логика реализуется на уровне программно-определяемых сетей (SDN), что позволяет гибко управлять политиками безопасности без привязки к физической топологии. Использование виртуальных сетевых функций дает возможность изолировать трафик на прикладном уровне, ограничивая взаимодействие только разрешенными протоколами и портами [7].

Реализация микросегментации опирается на идентификаторы сервисов, а не на статические IP-адреса. Это критически важно для динамических облачных сред, где жизненный цикл контейнеров и виртуальных машин может быть крайне коротким. Политики безопасности формулируются в терминах логических групп и меток, что обеспечивает их автоматическую применимость при масштабировании ресурсов. Программно-определяемый периметр скрывает внутреннюю структуру сети от внешнего и внутреннего сканирования. В результате потенциальный злоумышленник, получивший доступ к одному из узлов, остается локализованным в рамках единственного сегмента, что кратно снижает вероятность масштабной утечки данных [1, 3].

Сравнение ZTNA и традиционных протоколов удаленного доступа

Технологическая эволюция методов удаленного доступа привела к появлению протоколов Zero Trust Network Access (ZTNA), которые фундаментально отличаются от традиционных виртуальных частных сетей (VPN). Основное различие заключается в уровне предоставления доступа: VPN функционирует на сетевом уровне (Layer 3), предоставляя пользователю адрес во внутренней сети и потенциальную видимость всех соседних ресурсов. ZTNA работает на прикладном уровне (Layer 7), устанавливая изолированное соединение «пользователь-приложение». Это исключает возможность сетевой разведки со стороны удаленного субъекта и соответствует принципу минимальных привилегий [8].

С точки зрения производительности в облачных конфигурациях ZTNA также демонстрирует преимущества. VPN-инфраструктура часто требует концентрации трафика на центральных шлюзах, что создает избыточные задержки. ZTNA использует архитектуру распределенных облачных брокеров, обеспечивая оптимальную маршрутизацию трафика напрямую к облачному ресурсу. Кроме того, ZTNA обеспечивает непрерывную проверку сессии, в то время как VPN-соединение часто остается доверенным в течение всего времени активности туннеля. Однако ZTNA требует более сложной интеграции с системами управления идентификацией (IAM) и тщательного описания прав доступа к каждому отдельному приложению [3, 8].

Заключение

Применение архитектуры нулевого доверия в облачных вычислительных средах обеспечивает высокий уровень гранулярности контроля и минимизацию поверхности атаки. Основные преимущества модели заключаются в возможности адаптивного управления доступом на основе контекста и эффективном сдерживании внутренних угроз посредством микросегментации. Вместе с тем внедрение Zero Trust сопряжено с рядом системных сложностей. К ним относятся высокая трудоемкость первичной настройки динамических политик, потенциальное увеличение задержек при постоянной инспекции трафика и проблемы совместимости с устаревшими программными комплексами, не поддерживающими современные методы аутентификации. Эффективная реализация ZTA требует комплексного подхода, сочетающего технологические решения с развитой культурой управления идентификацией. Дальнейшие исследования будут направлены на автоматизацию процессов анализа рисков для упрощения администрирования масштабных гибридных облаков.

Список литературы:

1. NIST Special Publication 800-207. Zero Trust Architecture. – Gaithersburg: National Institute of Standards and Technology, 2020. – 59 p.

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture: Strategy and Implementation // IEEE Security & Privacy. – 2021. – Vol. 19, № 2. – P. 38–48.

3. Teerakanok S., Uruanda M., Atighetchi M. A Survey on Zero Trust Architecture: Challenges and Future Directions // Computers & Security. – 2022. – Vol. 118. – 102713.

4. Gilman E., Barth D. Zero Trust Networks: Building Secure Systems in Untrusted Networks. – O'Reilly Media, 2017. – 248 p.

5. Buck C., Olenberger C., Schweizer A. et al. Never Trust, Always Verify: A Taxonomy of Zero Trust Architecture // Communications of the Association for Information Systems. – 2021. – Vol. 49. – P. 301–321.

6. Stallings W. Zero Trust Security: Principles and Practice. – Addison-Wesley, 2022. – 320 p.

7. Vyas S., Gupta M. Micro-segmentation and Zero Trust: A Review of Modern Network Security // International Journal of Cloud Applications and Computing. – 2021. – Vol. 11, № 4. – P. 56–74.

8. Dixon M., Al-Hamdani A. From VPN to ZTNA: A Paradigm Shift in Secure Remote Access // Journal of Cyber Security Technology. – 2022. – Vol. 6, № 1. – P. 12–29