Захарова М.М. Сравнительный анализ эффективности стратегий ZTNA и традиционных VPN для защиты гибридной ИТ-инфраструктуры предприятия // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 95–98

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ СТРАТЕГИЙ ZTNA И ТРАДИЦИОННЫХ VPN ДЛЯ ЗАЩИТЫ ГИБРИДНОЙ ИТ-ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Захарова М.М.
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: efizmor@gmail.com

В статье проводится сравнительный анализ двух доминирующих архитектур безопасного удаленного доступа в условиях распределенной гибридной ИТ-инфраструктуры: традиционных виртуальных частных сетей (VPN) и модели Zero Trust Network Access (ZTNA). Анализ базируется на критериях безопасности, производительности, масштабируемости и соответствия требованиям современных гибридных рабочих сред. Рассматриваются базовые принципы, преимущества и ограничения каждой модели. Предлагается методика поэтапной миграции с VPN-ориентированной инфраструктуры на архитектуру Zero Trust.

Ключевые слова: Zero Trust, ZTNA, виртуальная частная сеть, гибридная инфраструктура, безопасность, периметровая модель, микросегментация, гранулярный доступ.

A COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF ZTNA AND TRADITIONAL VPN STRATEGIES FOR SECURING HYBRID ENTERPRISE IT INFRASTRUCTURE

Zakharova M.M.
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: efizmor@gmail.com

The article presents a comparative analysis of the two dominant secure remote access architectures in a distributed hybrid IT infrastructure: traditional Virtual Private Networks (VPN) and the Zero Trust Network Access (ZTNA) model. The analysis is based on security, performance, scalability, and compliance criteria with the requirements of modern hybrid work environments. The basic principles, advantages, and limitations of each model are considered. A methodology for a phased migration from a VPN-centric infrastructure to a Zero Trust architecture is proposed.

Keywords: Zero Trust, ZTNA, virtual private network, hybrid infrastructure, security, perimeter model, microsegmentation, granular access.

Введение

Распространение облачных сервисов, переход к гибридному формату работы и увеличение количества удаленных точек доступа обострили недостатки периметровой модели безопасности, к которой относятся традиционные VPN. Классические VPN, предоставляя избыточный уровень доверия после аутентификации, увеличивают риски латерального перемещения злоумышленника при компрометации учетных данных, что противоречит

требованиям защиты от целевых и APT-атак. В этих условиях концепция Zero Trust, основанная на принципе «никогда не доверяй, всегда проверяй», и её практическая реализация в виде ZTNA становятся объектом пристального внимания.[1]

Традиционные VPN-решения создают зашифрованный туннель между устройством пользователя и корпоративной сетью, предоставляя после успешной аутентификации доступ к сегменту сети. Данный подход отличается относительной простотой внедрения для базового удаленного доступа и широкой поддержкой на различных устройствах. [2] Однако модель характеризуется существенными недостатками: широкой поверхностью атаки после установления соединения, сложностями реализации гранулированного доступа и микросегментации, проблемами масштабирования в распределенных средах, а также потенциальным снижением производительности из-за туннелирования всего трафика через единый шлюз.

Архитектура ZTNA реализует принцип нулевого доверия, предоставляя доступ не к сети, а непосредственно к конкретным приложениям или сервисам на основе динамической оценки контекста: идентичности пользователя, состояния устройства, местоположения и других параметров. Ключевыми компонентами являются центральный контроллер (ZTNA Broker), осуществляющий авторизацию, и коннекторы, размещаемые рядом с защищаемыми ресурсами. Основные преимущества ZTNA включают минимальную площадь атаки за счет гранулированного доступа, постоянную проверку доверия, скрытие приложений от публичной сети, а также улучшенную производительность за счет установления прямых оптимизированных соединений, особенно с облачными ресурсами.[3]

Сравнительный анализ эффективности моделей проводится по следующим критериям: безопасность, производительность и пользовательский опыт, операционная эффективность.

В аспекте безопасности ZTNA демонстрирует стратегическое преимущество, устраняя неявное доверие, присущее VPN. Если VPN предоставляет доступ к сетевому сегменту после однократной аутентификации, то ZTNA реализует явное, постоянное доверие с проверкой каждого запроса. Это обеспечивает точный гранулированный контроль доступа к конкретным приложениям (микросегментация) вместо горизонтального расширения прав в сети. Как следствие, площадь атаки при компрометации конечной точки в модели ZTNA минимальна, в то время как при компрометации VPN-клиента злоумышленник потенциально получает доступ ко всей внутренней сети. Кроме того, ZTNA обеспечивает более высокую манёвренность и меньшее время на парирование инцидентов благодаря мгновенному применению изменений в политиках доступа.

С точки зрения производительности и пользовательского опыта ZTNA также предлагает более современный подход. Традиционное VPN-туннелирование всего трафика через корпоративный шлюз может создавать задержки, особенно при доступе к облачным приложениям (эффект backhauling). ZTNA устанавливает прямое безопасное соединение пользователя с приложением по оптимальному маршруту, что улучшает скорость отклика для распределенных ресурсов. Управление доступом в ZTNA централизовано через политики, не зависящие от сетевой топологии, что упрощает администрирование и масштабирование в динамичных гибридных средах по сравнению со сложным управлением большим количеством VPN-правил и шлюзов.[4]

На основе анализа предлагается 4-этапная модель миграции для типовой корпоративной инфраструктуры:

1. Инвентаризация и сегментация: каталогизация пользователей, устройств, приложений и данных; применение внутренней сегментации сети для снижения рисков на переходном этапе.

2. Внедрение сильной аутентификации: обязательное использование многофакторной аутентификации (MFA) для привилегированных пользователей и доступа к критичным активам.

3. Пилотное внедрение ZTNA для отдельных приложений: выбор низкорисковых, публичных или новых облачных приложений для развертывания ZTNA; параллельная работа с VPN.

4. Расширение и отказ от VPN: постепенный перевод сервисов на модель ZTNA с последующим мониторингом; финальный отказ от VPN для большинства сценариев.[5]

Таким образом, ZTNA демонстрирует стратегические преимущества для современных гибридных инфраструктур, обеспечивая более высокий уровень безопасности за счет отказа от концепции «доверенной внутренней сети» и реализации принципа минимальных привилегий. Традиционные VPN сохраняют актуальность для специфических задач, таких как доступ к legacy-системам, или в качестве резервного канала. Для новых проектов и облачных сервисов целесообразно сразу внедрять принципы Zero Trust. Для существующей инфраструктуры рекомендован плановый переход по предложенной модели с фокусом на сильную аутентификацию и детальную сегментацию ресурсов.

Список литературы

1. Защита информации в базах данных / Э. В. Бирих, Л. А. Виткова, В. В. Гореленко, Д. Б. Казаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 89-92.
2. Э. В. Бирих, Е. Ю. Рябов, Д. В. Сахаров / Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 103-107.
3. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.

4. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
5. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

References

1. Information Security in Databases /E.V.Birikh, L. A. Vitkova, V. V. Gorelenko, D. B. Kazakov // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of Scientific Articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 89–92.
2. E. V. Birikh, E. Yu. Ryabov, D. V. Sakharov / Methodology for Forming a Model of Information System Security Threats // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of Scientific Articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 103–107.
3. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. - pp. 92-95. - EDN YRPZWJ.
4. Selection of tools for dynamic security analysis of web applications for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Security. Inside. – 2024. – No. 1(115). – pp. 42-46. – EDN RLNHWK.
5. Research of methods for improving the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University. Technical sciences. – 2024. – Vol. 51, No. 3. – pp. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.