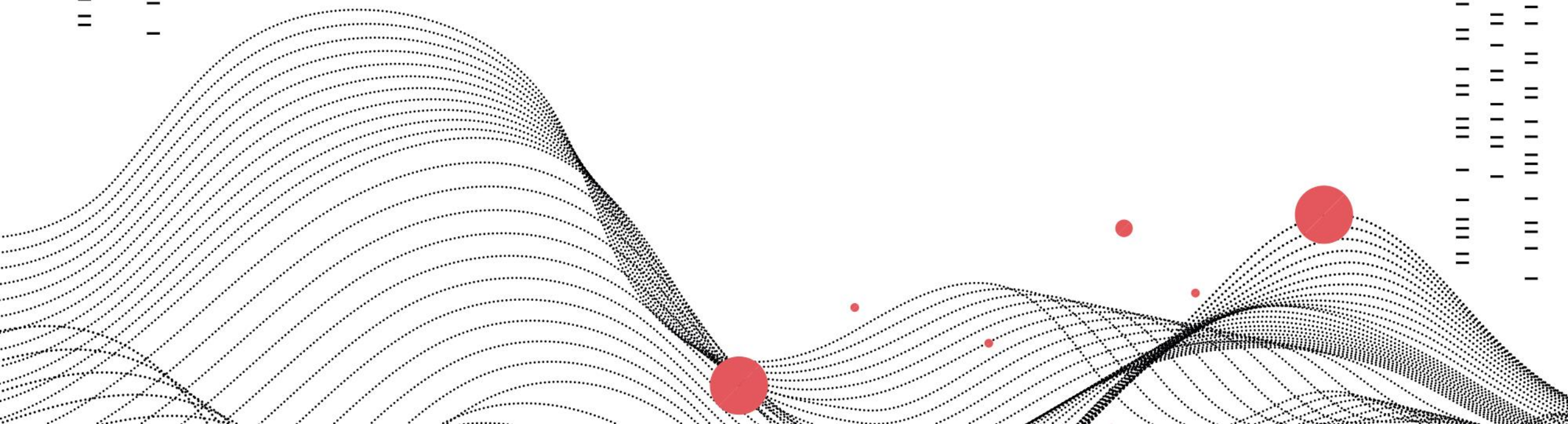
Zero Trust Network Access, (ZTNA)

Сетевой доступ с «нулевым доверием»



Содержание

Введение

- Сетевой доступ с «нулевым доверием» (Zero Trust Network Access, ZTNA) — концепция, о которой в последнее время говорят многие эксперты по информационной безопасности
- На протяжении десятилетий философия сетевой безопасности была сосредоточена на защите внутренней сети от внешних угроз. Это работало для привязанных к офису сотрудников, потому что стены помещений определяют периметр для охраны. Но сотрудники становились непрошеными гостями за пределами периметра, если пытались получить доступ к корпоративным ресурсам. Традиционная защита, конечно, позволяет обеспечить удаленную работу, но весьма неуклюже.
- Даже лучшие практики хорошо работавшие вчера рано или поздно устаревают вследствие развития технологий следующего поколения, в том числе получающих развитие в результате кризисных явлений. В 2020 году драйвером для изменений стал вирус COVID-19.
- Организации отреагировали на пандемию COVID-19, обязав своих сотрудников работать из дома, чтобы соблюдать социальную дистанцию. Отсутствие физического доступа к своим офисным ресурсам вынудило удаленных сотрудников использовать свои домашние сети и устройства для выполнения своей работы

Введение

- Предприятия вынуждены были переосмыслили безопасность периметра, потому что пользователи с рабочими устройствами располагаются произвольно. Периметр сети в этом случае перемещается туда, где находится пользователь. Парадигма сетевой безопасности, которая разработана для защиты мобильного персонала, — это сеть без периметра, или архитектура с нулевым доверием (Zero Trust Architecture, ZTA).
- Нулевое доверие обсуждается в сообществе информационной безопасности с тех пор, как в 2005 году международная группа **Jericho Forum** опубликовала своё видение этой темы. Фактически интерес к ZTA существовал и до пандемии. Сейчас он набрал новые обороты, технологии ZTA становятся мейнстримом. Отчёт **PulseSecure** «2020 Zero Trust Progress» показал, что к концу года около 75 % предприятий планируют внедрить ZTA. С другой стороны, почти половине специалистов по информационной безопасности не хватает опыта и уверенности для внедрения новой модели.
- Что же такое Zero Trust Network Access (ZTNA) — идея, концепция, технология, инструмент или же «хайп» и маркетинговая уловка, придуманная вендорами для стимуляции продаж? Существует ли отдельный, новый класс решений Zero Trust или же все постулаты этой концепции можно реализовать при помощи уже существующих продуктов?

Было….


Корпоративный «рай» под защитой периметра
Дикие «джунгли» снаружи…

Стало…

Модель нулевого доверия

- Нулевое доверие — это подход к цифровой безопасности, основанный на законе ограничения доступа к конфиденциальным данным и на отсутствии доверия к пользователю, устройству или учетной записи по умолчанию. Каждое подключение в рамках бизнеса должно проверяться и авторизовываться.
- Концепция нулевого доверия это ответ на эволюцию проблем цифровой безопасности, выходящих за рамки того, что может обеспечить традиционная модель безопасности периметра, основанная на предположении, что угрозы исходят извне сети и что всем внутренним пользователям, устройствам и приложениям можно доверять. В рамках традиционной модели организации могут просто развернуть брандмауэры, виртуальные частные сети (VPN) и средства контроля доступа к сети (NAC), чтобы удерживать компьютерных преступников за пределами сети, предоставляя при этом внутренним пользователям неограниченный доступ к сети.
- Развитие технологий привело к тому что еще до появления COVID-19 многие организации в процессе цифровой трансформации перенесли часть своих активов в облачную инфраструктуру, которая находится вне непосредственного контроля ИТ-отдела. Они также расширили удаленный доступ для поставщиков, подрядчиков, продавцов и штатных сотрудников, стремясь повысить свою гибкость и адаптируемость к завтрашним бизнес-задачам.
- Увеличение числа удаленных работников вынудило организации перенести еще больше рабочих нагрузок в облако, чтобы обеспечить все эти удаленные подключения, что привело к увеличению числа сетевых взаимодействий требующих проверки.

Модель нулевого доверия

- Парадигма сетевой безопасности с нулевым доверием (ZTA) — это не столько топология сети и физическое местоположение, сколько стратегия и руководящие принципы. Идея состоит в том, чтобы заменить предположение о доверии предположением о недоверии: каждый представляет собой угрозу, а сеть непрерывно находится под атакой.
- Чтобы упредить или ограничить бреши в защите, доверие сокращают до уровня данных, а не пользователей или элементов инфраструктуры. Принципы Zero Trust применимы для защиты всех корпоративных активов. Пословица «доверяй, но проверяй», которая выступает синонимом безопасности периметра, превращается в нечто иное: «сначала проверяй, потом доверяй, а затем перепроверяй и продолжай перепроверять».
- ZTA кажется логичным развитием принципов защиты, так же как смартфоны стали новой формой стационарного телефона. Как и в случае с внедрением новой технологии, речь идёт о компонентах и периферийных устройствах, а также о психосоциальных конструкциях, лежащих в основе принципов проектирования. Психоанализ в области ZTA — понимание корней доверия. Доверие — человеческая черта, которая развивается ещё во младенчестве. Когда люди впервые организовали сетевую безопасность, они положились на эту концепцию и создали периметр, в пределах которого все доверяли друг другу и имели общий доступ к ресурсам. Однако борьба с киберпреступностью и распределённый характер работы заставляют переходить к парадигме недоверия. ZTA характеризует недоверие как позитивное качество, которое особенно значимо в глобальном контексте развития.

Модель нулевого доверия

- Принцип предоставления сетевого доступа с «нулевым доверием», или Zero Trust Network Access (ZTNA), основан на идентификации, аутентификации и проверке клиентских устройств для предоставления доступа к приложениям на основе ролей. ZTNA позволяет управлять доступом не только удалённых пользователей, но и локальных, тем самым стирая границы периметра безопасности. Доступ к приложениям предоставляется только после проверки устройства и пользователя, а также оценки безопасности на основе контекста с помощью тегов Zero Trust..
- ZTNA изначально позиционировалась как альтернатива классическому удалённому доступу, но впоследствии стала эффективной и для локальных сотрудников, например при реализации BYOD (Bring Your Own Device) или IoT.
- Можно сказать, что ZTNA является логическим продолжением VPN, решая его классические проблемы, такие как отсутствие идентификации и оценки безопасности устройства, с которого осуществляется доступ, предоставление сотрудникам полного доступа к сети, который потом сужается правилами, и непрозрачность для пользователей (требуются дополнительные программы и настройки).
- ZTNA обеспечивает ряд преимуществ. Повышается защищённость сети, контролируется соответствие подключаемых устройств и их стеков безопасности принятым требованиям. Применение ZTNA позволяет организовать доступ к приложениям (в том числе облачным) вне зависимости от их расположения и уменьшить площадь атаки за счёт предоставления гранулированного доступа. Для пользователей повышается удобство использования приложений из любой точки мира, становятся прозрачными подключение и использование технологии единого входа (SSO).

Экскурс в историю

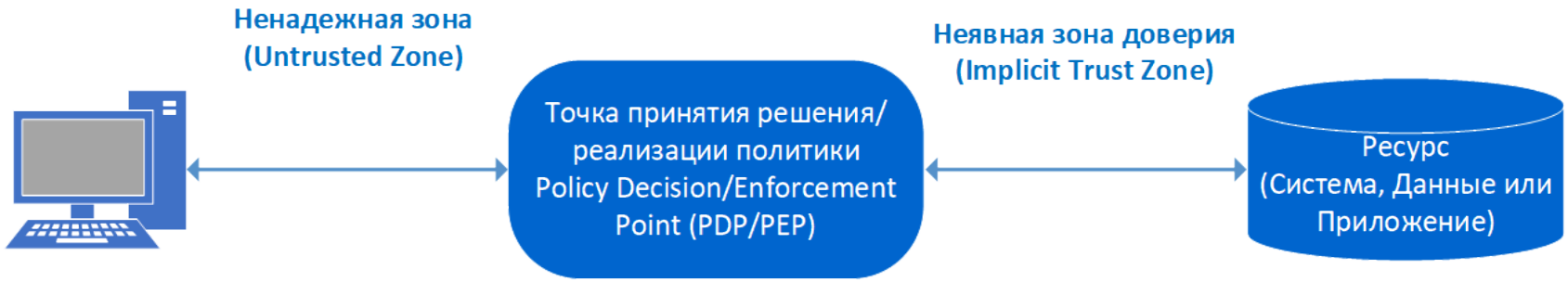
- 2005 год - международная группа Jericho Forum опубликовала своё видение темы нулевого доверия
- 2007 год - Агентство оборонных информационных систем (DISA) и Министерство обороны США опубликовали работу, посвященную безопасной стратегии предприятия. Данная стратегия, получившая название «Черное ядро», предусматривала переход от модели безопасности на основе периметра к модели, ориентированной на безопасность отдельных транзакций.
- В 2010 году главный аналитик Forrester Research Джон Киндерваг сформулировал термин «нулевое доверие».
- 2012 год – после того как НАТО подверглась более чем 2500 кибератакам, правительство США призвало федеральные агентства перейти на модель нулевого доверия.
- 2015 год - правительство США снова обеспокоилось проблемами безопасности после крупнейшей утечки данных федеральных служащих.
- 2019 год – опубликован первый проект архитектуры с нулевым доверием (Zero Trust Architecture, ZTA) от Национального Института Стандартов и Технологий США (National Institute of Standards and Technology – NIST).
- 2020 год - NIST опубликовал черновик второй редакции документа, в котором рассматриваются основные логические компоненты архитектуры ZTA. Технологии ZTA становятся мейнстримом

ZERO TRUST ARCHITECTURE. NIST SP 800-207 (2nd DRAFT)

Для развертывания модели Zero Trust необходимо распределить минимальные привилегии доступа и максимально детализировать пакеты с данными - определить «защищаемое пространство» (наиболее важные и ценные данные и ресурсы), и зафиксировать маршруты трафика по отношения к этим ресурсам.

После определения связей между ресурсами, инфраструктурой и сервисами, создаются микро периметры — межсетевые экраны на уровне сегментов корпоративных сетей. Пользователи, которые могут удаленно проходить микро периметры, могут находиться в любой точке мира и использовать различные устройства.

В модели пользователю (или устройству) необходимо получить доступ к корпоративному ресурсу через «контрольно-пропускной пункт». Пользователь проходит проверку через точку принятия решения о доступе на основе политики безопасности (**Policy Decision Point, PDP**) и через точку реализации политики (**Policy Enforcement Point, PEP**), отвечающую за вызов PDP и правильную обработку ответа.



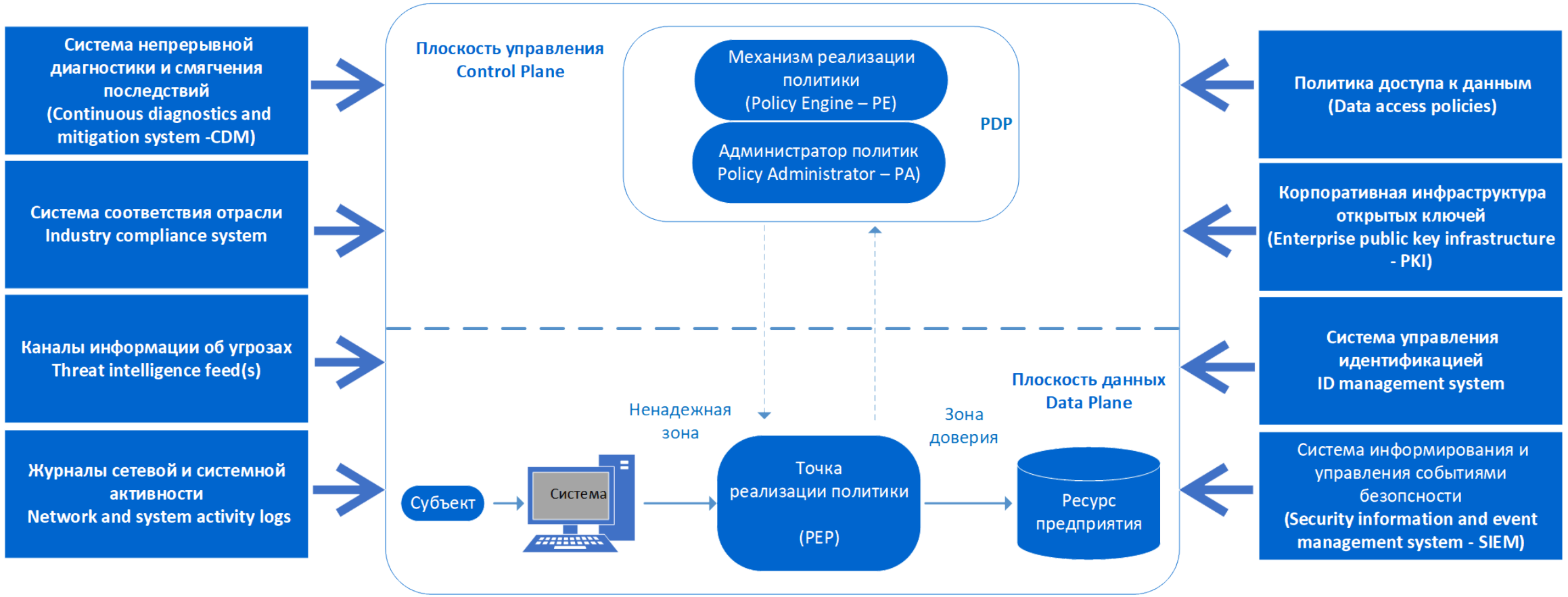
Точка применения политики должна быть как можно ближе к приложению. PDP/PEP не может применять дополнительные политики за пределами своего местоположения в потоке трафика.

ZERO TRUST ARCHITECTURE. NIST SP 800-207 (2nd DRAFT)

Семь основных принципов ZT и ZTA, которые должны учитываться при построении безопасной системы..

1. Все источники данных и услуг считаются ресурсами. Сеть может состоять из устройств разного класса. Личные устройства могут считаться ресурсами, если они могут получить доступ к данным и услугам.
2. Все коммуникации защищены независимо от их местоположения в сети. Доверие не может быть связано с местоположением. Коммуникации должны быть максимально безопасными и обеспечивать конфиденциальность и аутентификацию источника.
3. Доступ к отдельным корпоративным ресурсам предоставляется для каждой сессии. Аутентификация и авторизация для одного ресурса не дают доступ к другому.
4. Доступ к ресурсам определяется динамической политикой, основанной в т.ч. на состоянии идентификации клиента, приложения и других атрибутов (например отклонений в модели использования приложения).
5. Предприятие обеспечивает максимально безопасное состояние всех своих устройств, и отслеживает эти активы, для обеспечения безопасности..
6. Все ресурсы аутентификации и авторизации являются динамическими и строго контролируются на основе постоянной переоценки доверия к текущей связи. Предполагается, что предприятие имеет все необходимые системы управления учетными данными, активами и доступом, включая многофакторную аутентификацию (МФА).
7. Предприятие собирает максимум информации о текущем состоянии сетевой инфраструктуры и коммуникаций и использует её для повышения безопасности, создания и применения политик.

КОМПОНЕНТЫ АРХИТЕКТУРЫ. NIST SP 800-207 (2nd DRAFT)

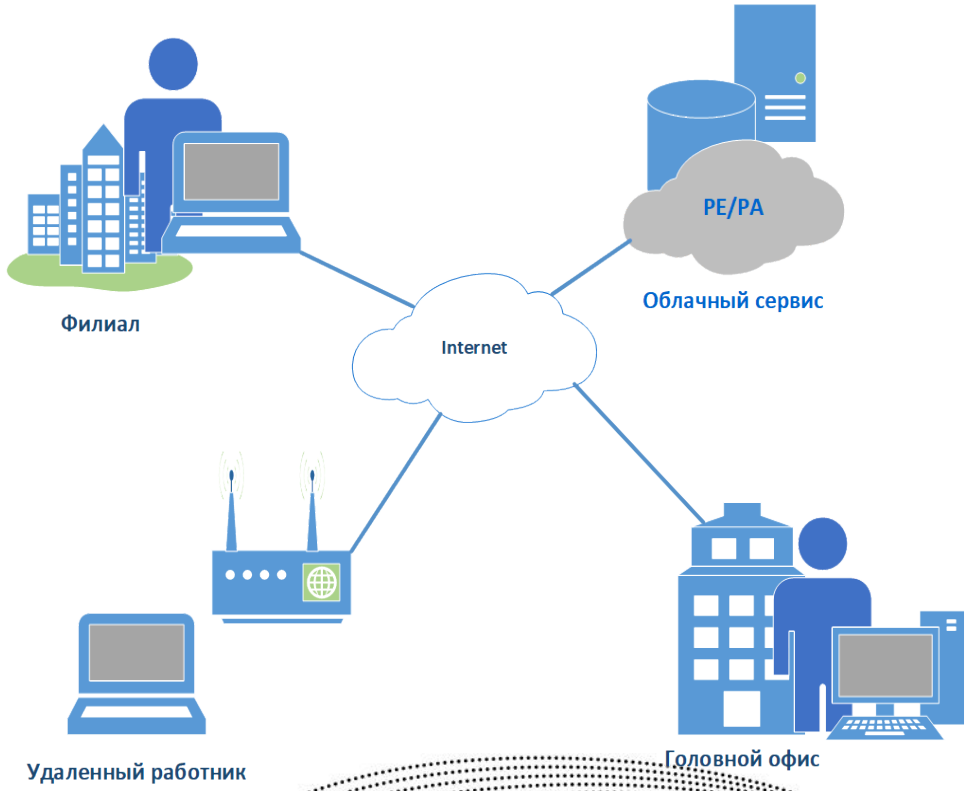


КОМПОНЕНТЫ АРХИТЕКТУРЫ. NIST SP 800-207 (SECOND DRAFT)

- **Policy Engine (PE),** отвечает за решение о предоставлении доступа к ресурсу для данного субъекта на основе политики и входные данных из внешних источников (например, службы анализа угроз);
- **Policy Administrator (PA)**, отвечает за установление и/или закрытие канала связи между субъектом и ресурсом. При создании канала он связывается с Policy Enforcement Point (PEP).
- **Точка применения политики (PEP)** отвечает за включение, мониторинг и, в конечном итоге, завершение соединений между субъектом и корпоративным ресурсом.
- **Система непрерывной диагностики и устранения последствий (CDM):** собирает информацию о текущем состоянии корпоративных активов и применяет обновления к компонентам конфигурации и ПО.
- **Отраслевая система соответствия**: это гарантирует, что предприятие будет соответствовать любому нормативному режиму, под который оно может подпадать
- **Веб-канал(ы) аналитики угроз:** предоставляет информацию из внутренних или внешних источников, которая помогает механизму политик принимать решения о доступе.
- **Политики доступа к данным:** это атрибуты, правила и политики доступа к корпоративным ресурсам..
- **Инфраструктура открытых ключей предприятия (PKI)**: эта система отвечает за создание и регистрацию сертификатов, выдаваемых предприятием ресурсам, субъектам и приложениям..
- **Система управления идентификаторами**: отвечает за создание, хранение и управление учетными записями корпоративных пользователей и идентификационными.

Сценарии развертывания. NIST SP 800-207 (2nd DRAFT)

ZTA берет свое начало в организациях, которые географически распределены и/или имеют высоко мобильную рабочую силу. Тем не менее, любая корпоративная среда может быть спроектирована с учетом принципов нулевого доверия. Не исключен период, когда компоненты ZTA и сетевая инфраструктура на основе периметра будут одновременно работать на предприятии



Предприятие с филиалами и удаленными работниками

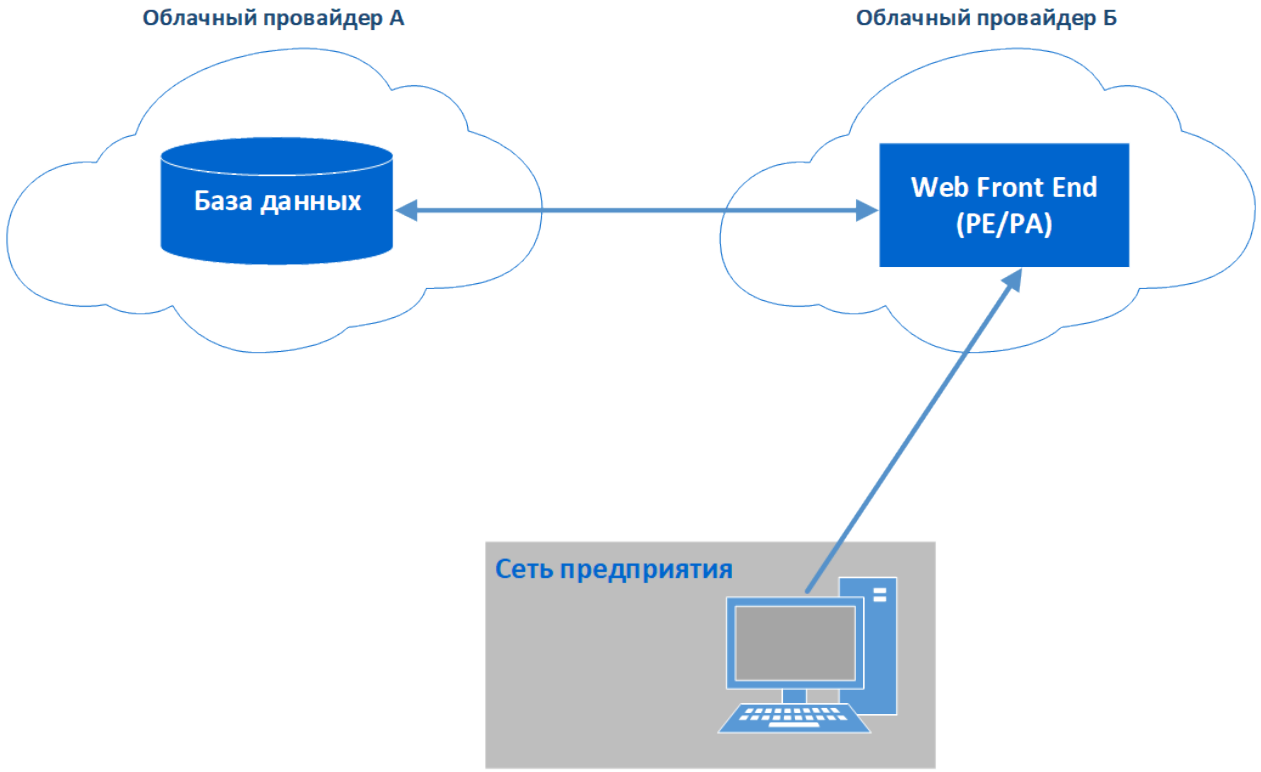
Предприятие с одной штаб-квартирой и географически разнесенными местоположениями, которые не соединены корпоративным физическим сетевым подключением.

У удаленных сотрудников есть доступ к корпоративным ресурсам для выполнения своих задач. Сотрудники могут работать удаленно используя как корпоративные так и личные устройства.

В этом случае PE/PA часто размещаются как облачная служба с конечными активами, имеющими установленный агент.

Размещение PE/PA в локальной сети предприятия может вызывать дополнительные задержки в сети, поскольку удаленные офисы и работники должны отправлять весь трафик в корпоративную сеть для доступа к приложениям, размещенным в облачных службах.

Сценарии развертывания. NIST SP 800-207 (2nd DRAFT)



Мульти облачное предприятие

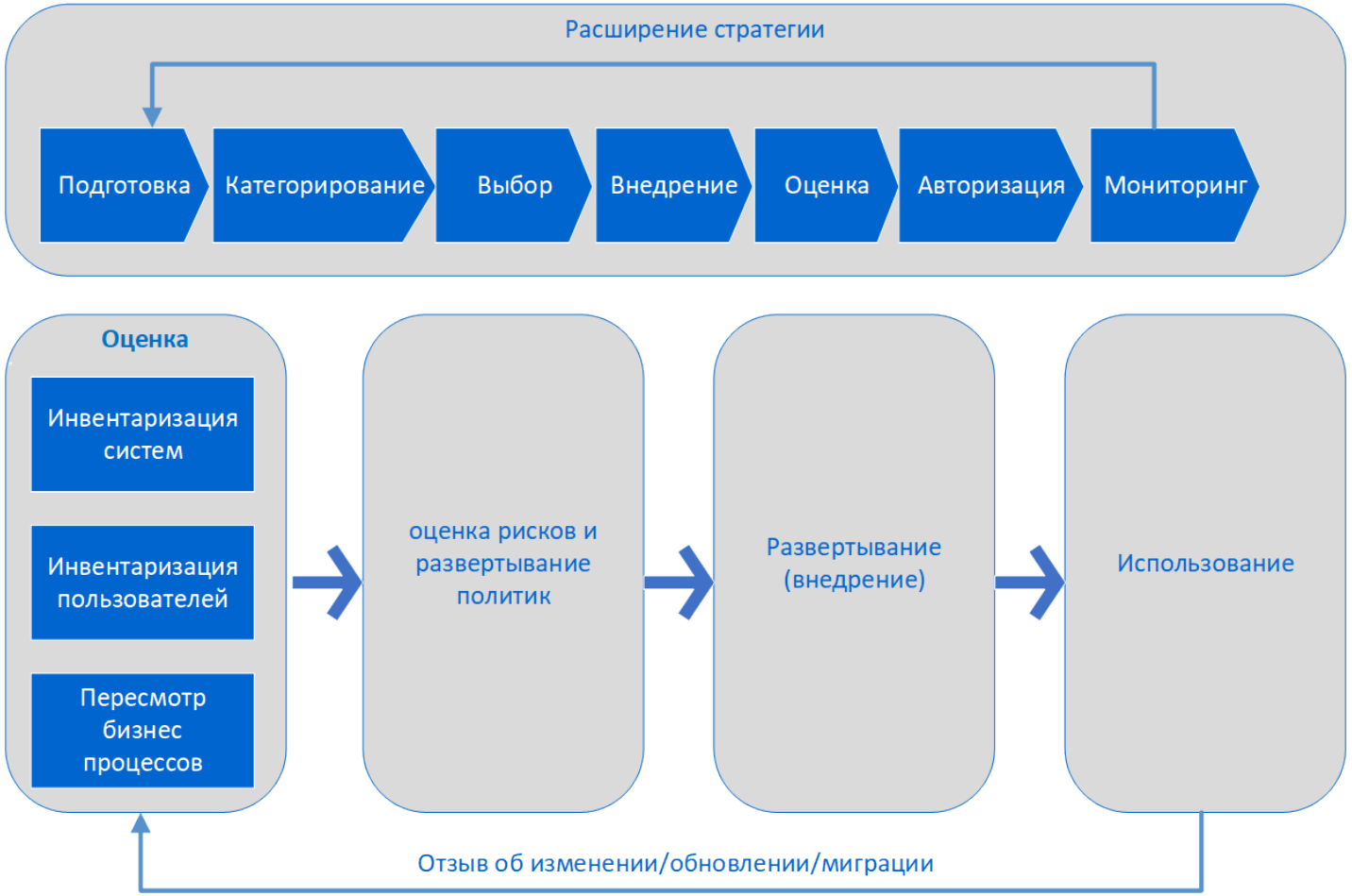
В этом случае предприятие имеет локальную сеть, но использует двух или более поставщиков облачных услуг для размещения приложений и данных.

Иногда приложение размещается в облачной службе, отдельной от источника данных.

Для повышения производительности и простоты управления приложение, размещенное в облачном провайдере А, должно иметь возможность напрямую подключаться к источнику данных, размещенному в облачном провайдере В, а не заставлять приложение туннелировать обратно через корпоративную сеть.

PE и PA могут быть службами, расположенными либо в облаке, либо даже у третьего поставщика облачных услуг. Затем клиент (через портал или локально установленный агент) напрямую обращается к PEP.

Шаги по внедрению ZTA в архитектурную сеть на основе периметра. NIST SP 800-207 (2nd DRAFT)



Для перехода на ZTA организация должна иметь подробные сведения о своих активах (физических и виртуальных), пользователях (включая привилегии пользователей) и бизнес-процессах. Неполное знание будет приводит к сбою бизнес-процесса, когда система отклоняет запросы из-за недостаточности информации. Это особенно важно, если в организации работают неизвестные развертывания «теневых ИТ».

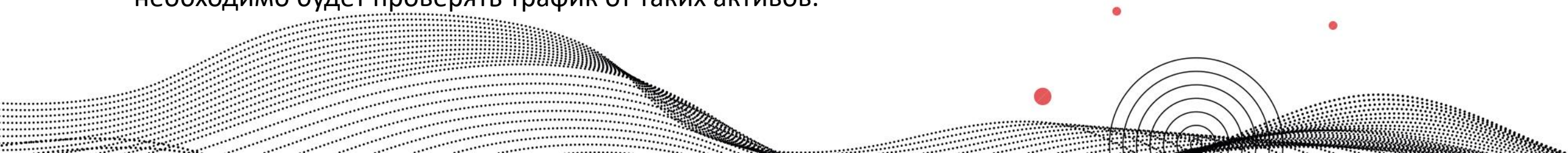
Шаги по внедрению ZTA можно сопоставить с шагами, описанными в документе Risk Management Framework (RMF [SP800-37] - Структура управления рисками для информационных систем и организаций - NIST Special Publication 800-37 Revision 2)

Шаги по внедрению ZTA в архитектурную сеть на основе периметра. NIST SP 800-207 (2nd DRAFT)

- **Подготовка:** Выполнение основных действий на уровне организации, бизнес-процесса и ИС организации, для подготовки к управлению рисками безопасности и конфиденциальности с использованием структуры управления рисками.
- **Категоризация**: Определения неблагоприятного воздействия на организационные операции и активы, отдельных лиц и других организации в отношении потери конфиденциальности, целостности и доступности ИС и информации которая обрабатывается, хранится и передается этими системами.
- **Выбор:** Выбор, адаптация и документирование средства контроля для защиты ИС и организации, соизмеримых с риском для операций и активов организации, отдельных лиц и других организаций
- **Внедрение:** Внедрение средств контроля в планы обеспечения безопасности и конфиденциальности для ИС и организации, документирование в базовой конфигурации деталей реализации средств контроля.
- **Оценка:** Определение правильности реализации элементов управления, работают ли они должным образом и дают ли желаемый результат в отношении соответствия требованиям безопасности и конфиденциальности для ИС и организации.
- **Авторизация:** Обеспечение организационной подотчетности старшего должностного лица относительно существования риска безопасности и конфиденциальности для операций и активов организации.
- **Мониторинг:** Поддержание постоянной ситуационной осведомленности о состоянии безопасности и конфиденциальности ИС и организации для поддержки управления рисками.

РИСКИ РЕАЛИЗАЦИИ ZERO TRUST. NIST SP 800-207 (2nd DRAFT)

1. **Нарушение процесса принятия решений ZTA**: При ошибках настройки PE и PA взаимодействие между корпоративными ресурсами не происходит. Компоненты PE и PA должны быть правильно настроены и контролироваться, а любые изменения конфигурации должны регистрироваться и подлежать аудиту.
2. **Отказ в обслуживании или нарушение работы сети:** Ресурсы предприятия не могут подключаться без разрешения PA. Если нарушен доступ к PEP или PA (например, DoS-атака, перехват маршрута, действия хостинг провайдера) это нарушит работу предприятия..
3. **Украденные учетные данные/внутренняя угроза:** ZTA повышает устойчивость к атакам с использованием украденных учетных данных ценных учетных записей (фишинг, социальная инженерия и т.д.) и предотвращает боковое перемещение скомпрометированных учетных записей или активов по сети Тем не менее, злоумышленник с действительными учетными данными (или злонамеренный инсайдер) может по-прежнему иметь доступ к ресурсам, доступ к которым предоставлен учетной записи.
4. **Недостаточная видимость в сети:** Согласно концепции ZTA весь трафик в сети проверяется, регистрируется и анализируется для выявления и реагирования на потенциальные атаки на предприятие. Однако, как уже упоминалось, часть (возможно, большая часть) трафика в корпоративной сети может быть непрозрачной для традиционных инструментов сетевого анализа уровня 3. При развертывании ZTA необходимо будет проверять трафик от таких активов.



РИСКИ РЕАЛИЗАЦИИ ZERO TRUST. NIST SP 800-207 (2nd DRAFT)

5. **Хранение сетевой информации:** Если сетевой трафик и метаданные сохраняются для создания контекстных политик, судебной экспертизы или последующего анализа, эти данные становятся целью для злоумышленников. Так же, как сетевые диаграммы, файлы конфигурации и другие документы по сетевой архитектуре, эти ресурсы должны быть защищены. Если злоумышленник сможет успешно получить доступ к сохраненной информации о трафике, он сможет получить представление об архитектуре сети и идентифицировать активы для дальнейшей разведки и атаки.
6. **Привязка к закрытым форматам данных:** ZTA использует различные источников данных для принятия решений о доступе. Источники данных могут не придерживаться общего открытого стандарта взаимодействия и обмена информацией. Это может привести к тому, что предприятие будет привязано к подмножеству поставщиков из-за проблем с совместимостью и может быть не в состоянии перейти к новому поставщику без чрезмерных затрат..
7. **Использование сущностей, не являющихся физическими лицами (NPE):** Для решения проблем безопасности в корпоративных сетях развертываются системы искусственного интеллекта и другие программные агенты. Эти компоненты зачастую взаимодействуют с ZTA вместо администратора-человека. Самый большой риск при использовании автоматизированных технологий для применения я политик — это возможность ложных срабатываний и ложных отрицательных результатов.

Можно ли построить систему с нулевым доверием

?

МОЖНО ЛИ ПОСТРОИТЬ СИСТЕМУ С НУЛЕВЫМ ДОВЕРИЕМ

- Действительно ли системы доступа с нулевым доверием соответствуют декларируемой концепции?
- Возможно ли построение архитектуры, в которой ко всем пользователям будут применяться одинаковые правила, или появление привилегированных аккаунтов неизбежно?
- Как моделировать угрозы в сети, где нет доверенных подключений — ведь ZTNA исходит из того, что события уже развиваются по худшему из возможных сценариев?

Концепция сетевого доступа с нулевым доверием, появившаяся как адаптация традиционного подхода к современным реалиям, является очень перспективной. Внедрение принципов Zero Trust Network Access (ZTNA) в корпоративную инфраструктуру позволяет сохранять высокий уровень безопасности несмотря на всё более «расползающиеся» границы сетевого периметра в условиях развития облачных технологий и дистанционной работы.

Вендоры решений и сервисов в сфере информационной безопасности отреагировали на рост интереса к модели сетевого доступа с нулевым доверием и выпустили продукты её реализующие. Таким образом, на мировом рынке сейчас представлено большое количество таких решений. В основном это — облачные сервисы, которые организуют защищённый доступ пользователей и устройств к корпоративным ресурсам.

МОЖНО ЛИ ПОСТРОИТЬ СИСТЕМУ С НУЛЕВЫМ ДОВЕРИЕМ

На рынке распространены два подхода к развёртыванию модели сетевого доступа с нулевым доверием:

- с установкой на устройства локального агента
- без установки на устройства локального агента

В первом случае пользователь или устройство самостоятельно инициирует подключение с помощью заранее установленного на устройство дополнительного программного обеспечения (агент). Агент отвечает за аутентификацию, установку соединения, шифрование, мониторинг состояния и т. п.

Такой подход является наиболее близким к модели программно определяемого (динамически изменяемого в зависимости от различных условий) периметра (Software Defined Perimeter, SDP), разработанного для управления доступом с помощью аутентификации и динамически создаваемых возможностей подключения.

К преимуществам ZTNA с использованием агентов следует отнести наличие полного контроля над устройствами, а также сложность подключения не верифицированного устройства.

С другой стороны, это же является и недостатком, потому что накладывает дополнительные ограничения: либо агент должен быть совместим с различными операционными системами и их версиями, либо для доступа к корпоративным ресурсам организация должна предоставлять устройства с поддерживаемыми версиями ОС и своевременно устанавливать на них обновления безопасности.

МОЖНО ЛИ ПОСТРОИТЬ СИСТЕМУ С НУЛЕВЫМ ДОВЕРИЕМ

Другой подход — это предоставление решений на основе ZTNA в формате облачных сервисов или услуг. В этом случае создаётся логическая граница доступа вокруг корпоративных ресурсов в облачной инфраструктуре или центре обработки данных (ЦОД) таким образом, что они оказываются скрытыми от внешнего пользователя. Доступ сотрудников, контроль сетевого трафика, сканирование подключаемых систем осуществляются с помощью посредника, например брокеров безопасного доступа в облако — (Cloud Access Security Broker - CASB)

Преимущества архитектуры ZTNA как облачного сервиса — это быстрота и лёгкость развёртывания, относительная дешевизна, централизованное управление, хорошая масштабируемость, отсутствие необходимости устанавливать дополнительное программное обеспечение (соответственно, это снимает ограничения на подключаемые устройства и удобно при организации принципов BYOD или дистанционной работы сотрудников).

К недостаткам следует отнести отсутствие контроля над субъектами доступа в режиме реального времени, что несколько снижает уровень защищённости. Также отсутствие предустановленных агентов повышает возможности осуществления атак типа «отказ в обслуживании».

РЕАЛИЗАЦИЯ ZTNA НА ПРАКТИКЕ

Для полной интеграции принципов нулевого доверия в корпоративную инфраструктуру нужно, по сути, полностью её перестроить: изменить архитектуру внутренней сети, поменять оборудование, принятые стратегии безопасности, может быть, даже подход сотрудников к работе с ресурсами предприятия. Этот процесс невозможен для большинства крупных компаний, поскольку не только занимает продолжительное время, но и является крайне дорогостоящим.

Другой вариант — модернизировать существующую инфраструктуру на основе уже имеющихся ресурсов и возможностей. Для успешного внедрения принципов ZTNA прежде всего нужно обновить стратегию информационной безопасности предприятия в целом и каждый её элемент для соответствия принципам нулевого доверия. Затем анализ компонентов ИТ-инфраструктуры покажет, какое оборудование и уже реализованные технологии могут быть использованы для построения сетевого доступа с нулевым доверием, а что нужно заменить.

Согласно исследованию Gartner, ожидалось, что к 2023 году 60 % компаний уйдут от использования VPN для доступа к корпоративным ресурсам и станут применять решения на основе сетевого доступа с нулевым доверием. Компания PulseSecure в отчёте «2020 Zero Trust Access Report» сообщает, что около 72 % организаций-респондентов планируют использовать идеи нулевого доверия для снижения рисков в информационной безопасности.

РЕАЛИЗАЦИЯ ZTNA НА ПРАКТИКЕ

Ряд вендоров предлагают решения для реализации принципов ZTNA в двух основных вариантах: как облачный сервис и как отдельное самостоятельное решение, которое, в большинстве случаев можно интегрировать с публичной облачной инфраструктурой. Кроме того, ZTNA является одним из ключевых компонентов Secure Access Service Edge (SASE) — комплексного подхода к обеспечению облачной безопасности, предложенного исследовательской компанией Gartner в 2019 году.

Вендор	Решение
Akamai	Enterprise Application Access (EAA)
Cato Networks	CATO SASE Platform (Software Defined Perimeter - SDP)
Cisco	Cisco Zero Trust (Duo/Secure Workload/SD Access)
Citrix	Citrix Secure Workspace Access
Cloudflare	Cloudflare Access
Google	BeyondCorp
ForcePoint	ForcePoint Private Access (компонент SASE-сервиса Dynamic Edge Protection)
InstaSafe	InstaSafe Secure Access
Netskope	Netskope Private Access
Netfoundry	Zero Trust Networking Platform

Вендор	Решение
Symantec (Broadcom)	Symantec Secure Access Cloud
Thales	SafeNet Trusted Access
Versa	Versa Secure Access
Zscaler	Zscaler Private Access
Microsoft	Azure Active Directory (AD) Application Proxy
Ivanti (Pulse)	Ivanti Neurons for Zero Trust Access (Pulse SDP)
Safe-T	ZoneZero
Verizon	Verizon SDP
Check Point	Check Point Harmony Connect (CloudGuard Connect)
Fortinet	FortiSASE (SASE)
Palo Alto Networks	Prisma Access (SASE)

Среди Российских продуктов, позволяющих хотя бы частично интегрировать принципы ZTNA можно отметить «ИнфоТеКС», «Код Безопасности» и «UserGate»

ЧТО ТАКОЕ SECURE ACCESS SERVICE EDGE (SASE)

Периферийный (пограничный) сервис безопасного доступа (Secure Access Service Edge - SASE) — это модель облачной архитектуры, которая объединяет сетевые функции и функции безопасности как услуги и предоставляет их как единую облачную службу. Концептуально SASE расширяет возможности сети и безопасности за пределы того, где они обычно доступны.

Помимо ZTNA обязательными компонентами SASE являются система SD-WAN (Software-Defined Wide Area Network), шлюз безопасности (Secure Web Gateway, SWG), решение для безопасного доступа к облаку (CASB) и облачный межсетевой экран (Firewall-as-a-Service, FWaaS).

Зачем нужен SASE?

Корпоративные сети все больше зависят от облачных приложений для ведения бизнеса и поддержки распределенных рабочих процессов для поддержки удаленных и мобильных пользователей. Корпоративная сеть быстро вышла за границы обычной сети, что привело к постоянно расширяющейся поверхностью атаки .

Сети развиваются достаточно быстро, чтобы поддерживать рабочие процессы удаленных конечных точек, но большинство инструментов безопасности не поспевают за ними, что делает решения, основанные только на VPN, устаревшими. Чтобы организации оставались конкурентоспособными, все конечные точки должны быть защищены и управляться с помощью тех же политик безопасности и сети, что и их локальная инфраструктура, независимо от того, где они расположены.

ЧТО ТАКОЕ SECURE ACCESS SERVICE EDGE (SASE)

SASE — это не отдельный продукт, а набор решений, которые можно комбинировать исходя из потребностей предприятия.

При правильной реализации подход SASE позволяет организациям:

- организовывать безопасный доступ к корпоративным приложениям и приложениям SaaS независимо от того, где находятся пользователи, рабочие нагрузки, устройства или приложения..
- быстро перемещать данные между центрами обработки, филиалами, гибридными и мультиоблачными средами .

SASE предлагает:

- **Гибкую, согласованную безопасность:** широкий спектр услуг по обеспечению безопасности, от предотвращения угроз до политик NGFW , на любой периферии, доступ к сети с нулевым доверием, знание того, кто и что находится в сети и возможность защищать активы в любом месте сети.
- **Снижение сложности:** упрощение архитектуры за счет объединения ключевых сетевых функций и функций безопасности в единое легко управляемое решение.
- **Оптимизированную производительность:** легкое и безопасное подключениея к Интернету, приложениям и корпоративным ресурсам, где бы они ни находились.

ЧТО ТАКОЕ SASE НА ПРИМЕРЕ РЕШЕНИЯ FORTINET

FortiSASE — это масштабируемая облачная система защиты, которая обеспечивает гибкий, безопасный доступ в любое время и для работы из любого места. Используя возможности FortiOS и Fortinet Security Fabric, FortiSASE обеспечивает беспрепятственное взаимодействие между облачным NGFW, веб-безопасностью, IPS, DNS и песочницей. Вместе эти аспекты позволяют системе выполнять все функции SASE.

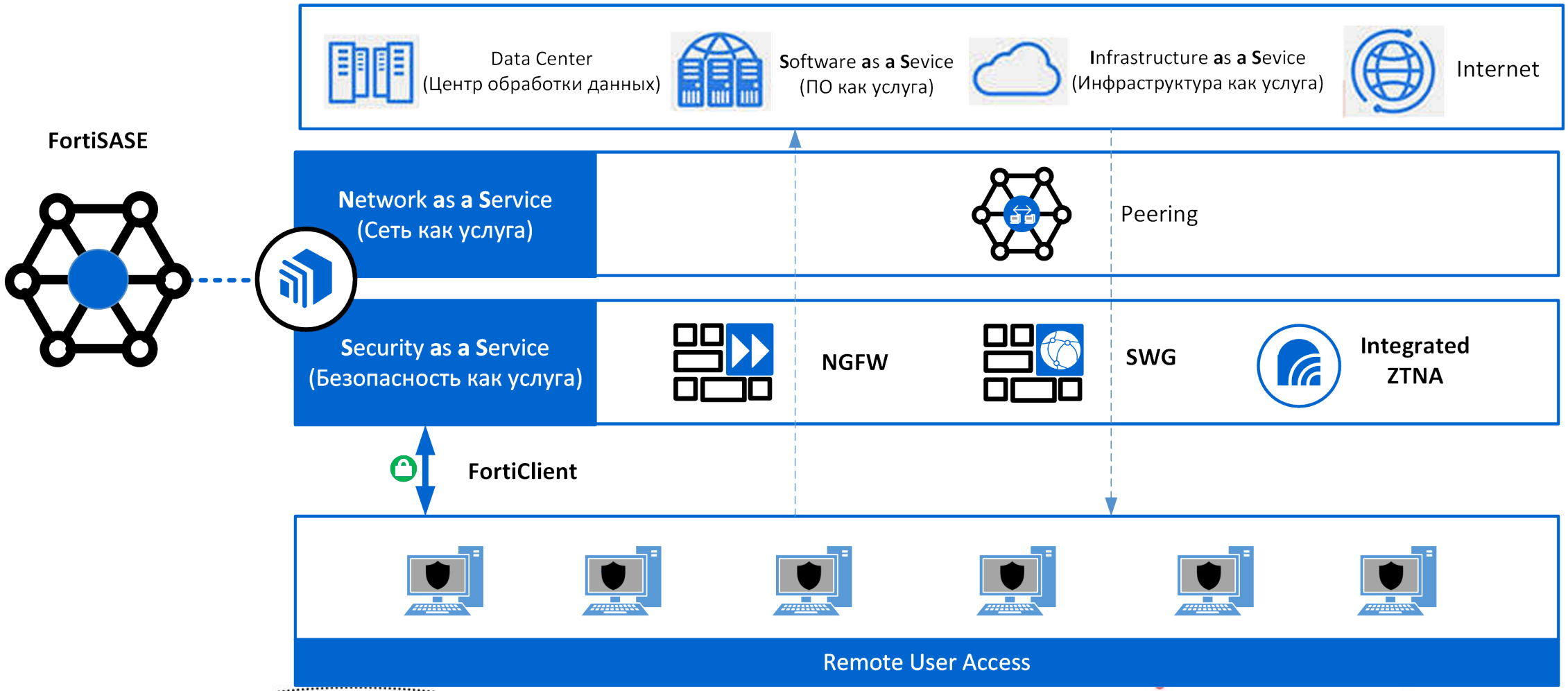
Система SASE от Fortinet помогает обеспечить безопасность всех периферийных устройств, решая многие проблемы масштабируемости и сетевой инфраструктуры, которые возникают в крупных распределённых организациях, чьи рабочие процессы тесно связаны с продуктами IaaS / SaaS. Fortinet предлагает комплексное решение SASE, которое легко интегрируется с SD-WAN, использует межсетевой экран Fortinet и шлюз Secure Web Gateway (SWG), обеспечивая корпоративным организациям многоуровневую безопасность.

Fortinet предоставляет комплексное решение SASE, которое легко интегрируется с SD-WAN, использует межсетевой экран Fortinet и шлюз Secure Web Gateway (SWG), обеспечивая корпоративным организациям многоуровневую безопасность.

Решение Fortinet SASE не использует общедоступные облачные службы и предоставляется заказчикам на основе собственной многопользовательской гибкой облачной архитектуры.

Для эффективной работы все компоненты SASE взаимодействуют как одна интегрированная система обеспечивающая возможности подключения, обмена данными по сети и элементы безопасности

ЧТО ТАКОЕ SASE НА ПРИМЕРЕ РЕШЕНИЯ FORTINET



ЧТО ТАКОЕ SASE НА ПРИМЕРЕ РЕШЕНИЯ FORTINET

Агент FortiClient нулевого доверия с многофакторной аутентификацией (MFA)

Функции	Описание
Централизованное управление через EMS или FortiClient Cloud	• Централизованное развертывание (в т.ч. удаленное) и контролируемое обновление FortiClient. • Панель управления уязвимостями для снижения поверхностью атаки организации. Уязвимые конечные точки идентифицируются для административных действий. • Интеграция с Windows AD синхронизирует структуру AD с EMS. Для управления конечными точками используются одни и те же организационные единицы (OU). Статус точки в реальном времени показывает информацию об активности и событиях безопасности.
Централизованные журналы и отчеты	Централизованное ведение журналов упрощает составление отчетов о соответствии и анализ безопасности с помощью ForiSIEM или другого продукта SIEM.
Dynamic Security Fabric Connector	EMS создает виртуальные группы на основе состояния безопасности конечной точки. Эти группы используются в политике брандмауэра FortiGate для динамического контроля доступа и соблюдение политик безопасности.
Агент уязвимости и исправление	Агент уязвимости и исправления выявляет уязвимые конечные точки и помогает устранять уязвимости, с целью уменьшения поверхности атаки. Приоритет отдается неисправленным уязвимостям ОС и программного обеспечения.
SSL VPN с MFA	Secure Socket Layer (SSL) Виртуальная частная сеть (VPN) с MFA обеспечивает простой в использовании зашифрованный туннель, который может проходить практически через любую инфраструктуру.
IPsec VPN с MFA	IP Secure (IPSec) VPN с MFA обеспечивает простой в использовании зашифрованный туннель, обеспечивающий высочайшую пропускную способность VPN.
Веб-фильтрация FortiGuard	Отслеживает все действия веб-браузера для обеспечения веб-безопасности и приемлемой политики использования. Профиль веб-фильтрации конечной точки синхронизируется с FortiGate для согласованного применения политик безопасности в т.ч. для сайтов HTTPS с зашифрованным трафиком.
Раздельное туннелирование	Поддерживается в туннелях ZTNA и VPN, позволяет оптимизировать взаимодействие с пользователем.
Единый вход (SSO)	SSO интегрируется с управлением идентификацией и доступом FortiAuthenticator для обеспечения единого входа.

РЕАЛИЗАЦИЯ ZTNA НА ПРИМЕРЕ РЕШЕНИЯ FORTINET

Решение Fortinet позволяет использовать как облачную, так и локальную ZTNA, причем последняя позволяет организации владеть, контролировать и управлять своей инфраструктурой и политиками самостоятельно в собственной среде. Для организаций, которые не полностью доверяют облаку, беспокоятся о потере критически важных функций или не могут перейти в облако по причинам соответствия, решение Fortinet Universal ZTNA позволяет использовать все преимущества ZTNA.

Иными словами универсальное решение ZTNA применимо к гибридным сетям, которым необходимы как облачная, так и локальная компоненты.

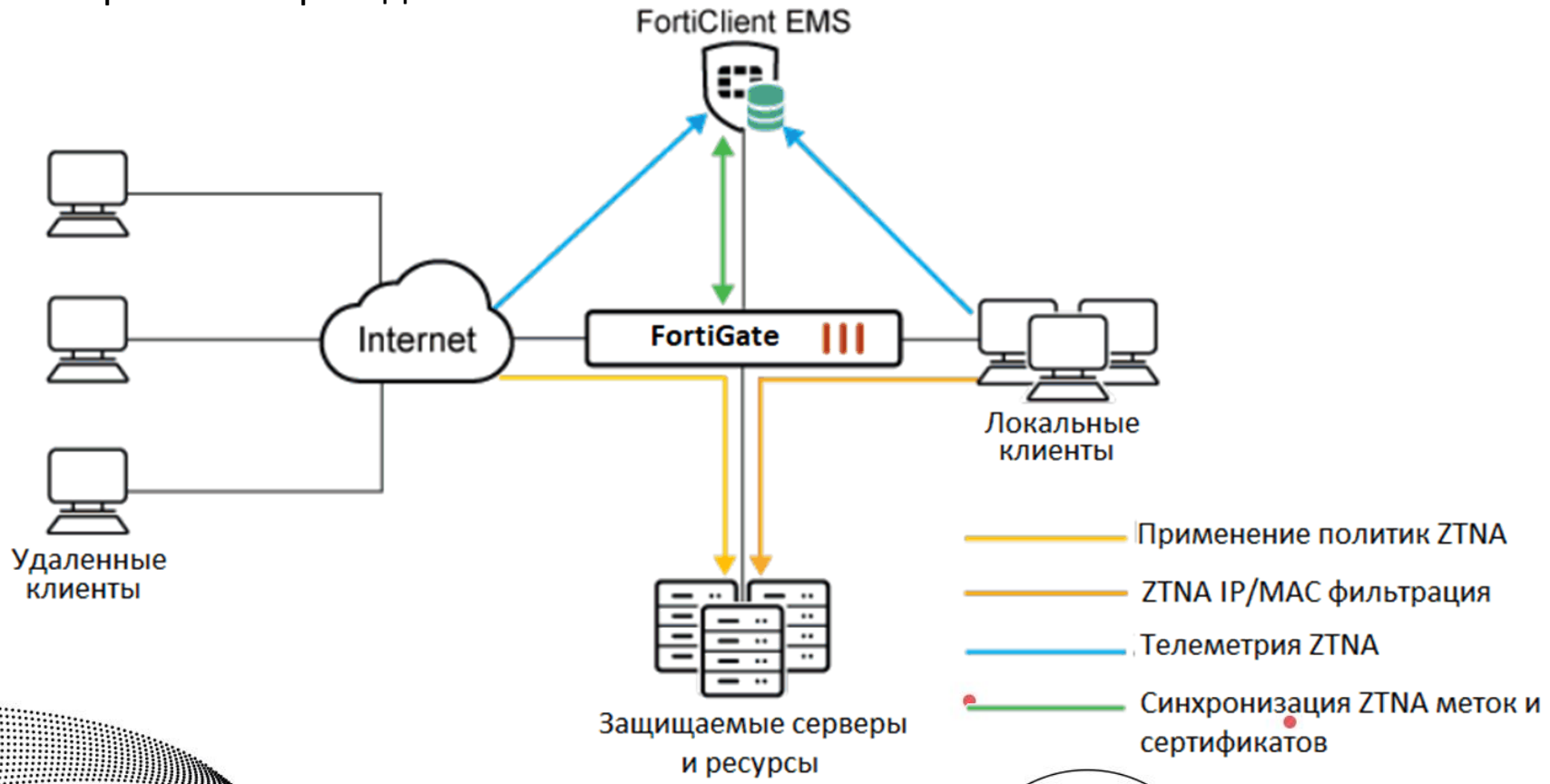
Решение от Fortinet позволяет работать как локально так и в облаке, поскольку сервисы ZTNA интегрированы в операционную систему FortiOS (начиная с OS версии 7), под управлением которой работают устройства FortiGate NGFW. FortiOS обеспечивает конвергенцию сети и безопасности, согласованную независимо от того, предоставляется ли она в виде устройства, виртуальной машины или облачной службы или контейнера.

В сочетании с универсальным агентом FortiClient это обеспечивает беспрепятственное развертывание, работу и архитектуру доступа к сети с нулевым доверием (ZTNA). Преимуществ решения, заключается в том, что FortiClient является как агентом VPN, так и агентом ZTNA. Архитектура Fortinet ZTNA отражает инфраструктуру VPN. Это важно, потому что зачастую к ZTNA обращаются как к средству улучшения ситуации с удаленным доступом и переходят от использования сети VPN к сети ZTNA.

РЕАЛИЗАЦИЯ ZTNA НА ПРИМЕРЕ РЕШЕНИЯ FORTINET

Две возможности в одном агенте (VPN и ZTNA) упрощают задачу. Можно начинаеть с использования только VPN для удаленного доступа, а потом раз за разом перемещать покрытие приложений на ZTNA, используя VPN для оставшихся требований доступа. Таким образом можно перейти к использованию ZTNA посредством контролируемого, осторожного и простого перехода.

Со своей стороны шлюзы безопасности FortiGate под управлением операционной системы FortiOS уже содержат все необходимые базовые компоненты для развертывания не облачного ZTNA решения



ЗАКЛЮЧЕНИЕ

Концепция ZTNA сегодня больше похожа не на законченный чертеж, а на карту с обозначенными ключевыми точками для путешествия. Согласно рекомендациям NIST, организации должны стремиться постепенно внедрять принципы нулевого доверия. И хотя многие организации уже имеют элементы ZTA в корпоративной инфраструктуре, еще долгое время большинство корпоративных инфраструктур будут работать в гибридном режиме с нулевым доверием/периметром.

Как уже отмечалось ранее, можно сказать, что ZTNA является логическим продолжением VPN, решая его классические проблемы, такие как отсутствие идентификации и оценки безопасности устройства, с которого осуществляется доступ, предоставление сотрудникам полного доступа к сети, который потом сужается правилами, и непрозрачность для пользователей (требуются дополнительные программы и настройки).

Архитектура сетевого доступа с нулевым доверием является частью концепции Zero Trust, однако технологическое содержание этого термина может меняться в зависимости от позиции вендора, системного интегратора или конкретного эксперта. Идеи, которые сейчас реализуются под вывеской ZTNA, появились в ИБ-продуктах более 10 лет назад, но оформлять их в единую маркетинговую «упаковку» стали сравнительно недавно. В общем случае создать модель Zero Trust на предприятии можно при помощи уже имеющихся на рынке инструментов, зачастую даже теми средствами, которые находятся в распоряжении организации. Концепция не привязана к конкретному вендору, но требует интеграции совместно работающих продуктов.

ВЫВОДЫ

Модель нулевого доверия — перспективное направление развития сетевой безопасности. Компаниям стоит постепенно внедрять её, пусть даже и временно совмещая с традиционным подходом по защите периметра.

Переход к архитектуре с нулевым доверием предполагает использование доступных технологий, но потребует времени — как в техническом плане, так и со стороны решения психосоциальных вопросов. Зато по окончании перехода организация получит преимущества за счёт сокращения количества инцидентов в сфере информационной безопасности вкупе с возможностью гибко управлять защитой в зависимости от изменений ИТ-инфраструктуры.

Отметим, однако, что несмотря на возрастающую популярность концепции нулевого доверия, остаются организации, для которых традиционный подход к обеспечению информационной безопасности не теряет своей актуальности, потому что в них невозможны или неприемлемы ни облачные сервисы, ни удалённый доступ: военные структуры, некоторые государственные предприятия, компании работающие с засекреченной информацией.

ИСТОЧНИКИ

1. Zero Trust Architecture Draft (2nd) NIST Special Publication 800-207
2. Risk Management Framework for Information Systems and Organizations. NIST Special Publication 800-37 Revision 2
3. Сетевой доступ с нулевым доверием — маркетинговый термин или реальный инструмент? Денис Сарычев - Обозреватель Anti-Malware.ru. Источник: https://www.anti-malware.ru/analytics/Technology_Analysis/What-is-Zero-Trust-Network-Access
4. Обзор мирового и российского рынков решений для организации сетевого доступа с нулевым доверием (ZTNA) Вера Холопова - Обозреватель Anti-Malware.ru. Источник: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-and-Global-ZTNA-market-overview
5. Обзор мирового рынка систем Secure Access Service Edge (SASE). Павел Лего - Обозреватель Anti-Malware.ru. Источник: https://www.anti-malware.ru/analytics/Market_Analysis/Secure-Access-Service-Edge
6. Периферийный сервис безопасного доступа (SASE). Источник: https://www.fortinet.com/ru/products/sase#

Благодарю за внимание!

Ронжин В.В
Специально для компании «NIHOL»
2023 г.