safe-t

ZoneZero®

Perimeter Access Orchestration (управление доступом к периметру) Нулевое доверие — это правильный путь!

В мире цифровой трансформации число сценариев удаленного доступа к любой организации растет по экспоненте. Сегодня и крупные и небольшие организации имеют дело с большим числом требований к удаленному доступу:

- Предоставление сотрудникам и сторонним подрядчикам доступа к внутренним ресурсам
- Возможность для внутренних пользователей использовать внутренние ресурсы, подключаясь через корпоративную сеть
- Удаленный доступ к облачным приложениям и внутренним унаследованным приложениям
- Интеграция многофакторной аутентификации (MFA) и осведомленность о личности пользователя во всех сценариях удаленного доступа

Решение ZTNA (Zero Trust Network Access — Нулевое доверие при доступе к сети) помогает организациям внедрить более эффективный способ обеспечения безопасности, основанный на принципе «никогда не доверяем, всегда проверяем». Тем не менее, между потенциалом технологий ZTNA и фактическим использованием, возможностями, внедрением и результатами до сих пор есть значительный разрыв.

Проблемы внедрения решений ZTNA

Путь к принципу Zero Trust (нулевого доверия) зачастую оказывается более сложным и требовательным к ресурсам, чем ожидалось, особенно когда существующая инфраструктура организации не совместима с концепцией Zero Trust.

Для достижения уровня Zero Trust Network Access (нулевого доверия при доступе к сети) требуются:

- Разделение плоскости данных и плоскости управления
- Улучшенный механизм аутентификации пользователей
- Доступ на уровне приложения

Это позволит вам как минимум реализовать стратегию минимальных прав доступа, постоянно и правильно выполнять аутентификацию пользователей, а также строго контролировать и применять политики.

Решения Software Defined Perimeter (SDP) известны как лучший способ создания этой схемы доступа. Они интегрируется с поставщиками идентификации и многофакторной аутентификации для выполнения этих функций.

Однако схемы доступа VPN и не веб-приложений (SMB, SSH, SFTP и т. д.) по-прежнему являются жизненно важной частью среды организации. Поскольку решения SDP/MFA обычно несовместимы с такой существующей средой, организации полагают, что для ZTNA потребуется длительное время, необходимое для замены существующих инфраструктур на решения SDP.

В результате огромный потенциал ZTNA не реализуется, и процент перехода на этот принцип остается низким.

safe-t

Решение – платформа для управления доступом ZoneZero Perimeter Access Orchestration Platform

Благодаря прозрачному и простому развертыванию Safe-T мы обеспечиваем инновационную и уникальную возможность реализации принципа ZTNA в VPN, брандмауэрах и сервисах приложений корпоративных сетей, помогая «бесшовно» интегрировать решение в унаследованную инфраструктуру и сервисы аутентификации.

Понимая потребность в решениях ZTNA, которые эффективно и полностью соответствуют всем сценариям и требованиям к удаленному доступу, компания Safe-T усовершенствовала решение ZTNA, создав первую в истории платформу управления доступом к периметру, которая включает следующие модули:

- Внедрение классического SDP от Safe-T, безопасный доступ для приложений (SAA) — безклиентный модуль ZTNA
- Интеграция с самыми распространенными VPN — добавление функций ZTNA в существующие VPN
- Поддержка постоянной аутентификации и переход от двухфакторной аутентификации (2FA) к действительно многофакторной аутентификации (MFA)
- Контроль доступа к приложениям для внутренних и внешних пользователей
- Непрерывный мониторинг, контроль требований и формирование отчетов о действиях пользователей/приложении

Новая платформа Safe-T ZoneZero поддерживает существующие решения VPN, избавляет от необходимости менять структуру сети и процедуру доступа, а также позволяет организациям поддерживать все сценарии доступа:

Все типы пользователей

- Люди — управляемые/неуправляемые
- Приложения, API
- Подключенные устройства

Все местоположения пользователей

- Внешние / удаленные пользователи
- Внутренние пользователи

Все типы приложений и местоположений

- Веб-приложения
- Собственные приложения
- Облачные и локальные

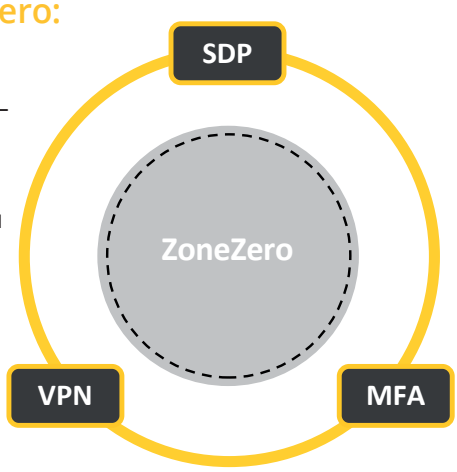
Если вы заинтересованы во внедрении нового решения SDP, хотите повысить безопасность унаследованного доступа к VPN или добавить многофакторную аутентификацию (MFA) в любой VPN, сервис или приложение, ZONEZERO® позволит вам управлять всей схемой доступа на одной целостной и простой в использовании платформе.

Возможности ZoneZero:

- Обеспечивает действительное разделение плоскости данных и плоскости управления
- Применяет политики уровня приложений для внешних (VPN)/внутренних пользователей сети
- Интегрирует многофакторную аутентификацию (MFA) в любой VPN
- Решение основано на запатентованной технологии обратного доступа Safe-T

Преимущества ZoneZero:

- Достижение уровня ZTNA
- «Бесшовная» интеграция — быстрое развертывание
- Оптимизация стоимости развертывания и владения
- Централизованное управление



51 John F Kennedy Parkway, Short Hills, NJ | 888-304-5010
www.safe-t.com

safe-t

ZoneZero® VPN

В течение более 20 лет технологии VPN являются основой безопасности сетей. И хотя VPN прошли проверку временем, теперь мы знаем, что по-настоящему безопасная архитектура основана на концепции доступа к сети с нулевым доверием (Zero Trust Network Access), которая не поддерживается инфраструктурой VPN. Многие организации хотели бы использовать решения Software Defined Perimeter (SDP), которые поддерживают ZTNA, но сталкиваются с ограничениями существующей инфраструктуры.

Решение ZoneZero VPN от Safe-T меняет подход к безопасному доступу, действительно обеспечивая разделение плоскости данных и плоскости управления, мониторинг и усиление политики в слое приложения, а также интеграцию MFA в любое приложение или сервис. Все это выполняется в существующей инфраструктуре.

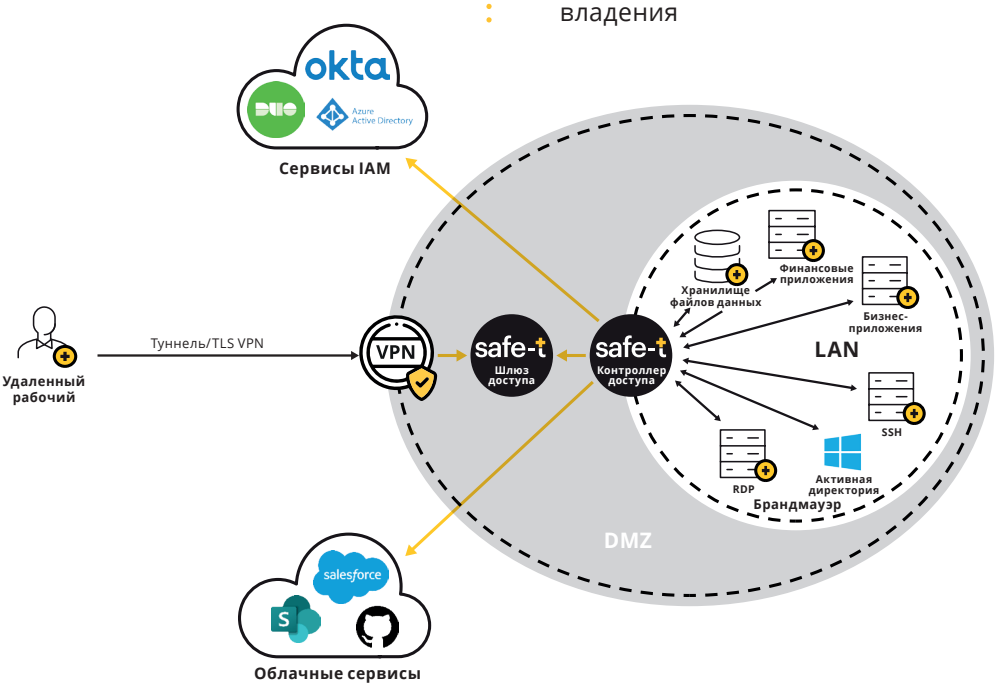
Этот продукт является частью платформы ZoneZero Perimiter Access Orchestration, обеспечивающей централизованное управление всеми технологиями доступа, помогая организациям достичь уровня Zero Trust Network Access (ZTNA).

Возможности

- «Бесшовное» внедрение
- Интеграция MFA в любой VPN – Туннель/TLS
- Правила доступа на уровне приложения
- Постоянная аутентификация

Преимущества

- Позволяет использовать преимущества ZTNA в инфраструктуре VPN
- Не зависит от поставщика услуг
- Не препятствует работе пользовательского интерфейса
- Оптимальная стоимость развертывания и владения



ZoneZero VPN – «Бесшовное» внедрение ZTNA в существующие VPN

51 John F Kennedy Parkway, Short Hills, NJ | 888-304-5010
www.safe-t.com

safe-t

ZoneZero® MFA
(многофакторная аутентификация)

Одним из главных компонентов Zero Trust Network Access является улучшенная и постоянная аутентификация пользователя. Провайдеры идентификации и провайдеры многофакторной аутентификации усовершенствовали процесс аутентификации, но распространенный подход «на основе клиента» создает проблемы для интеграции и обслуживания. Более того, многие приложения не на базе веб по определению не совместимы с MFA.

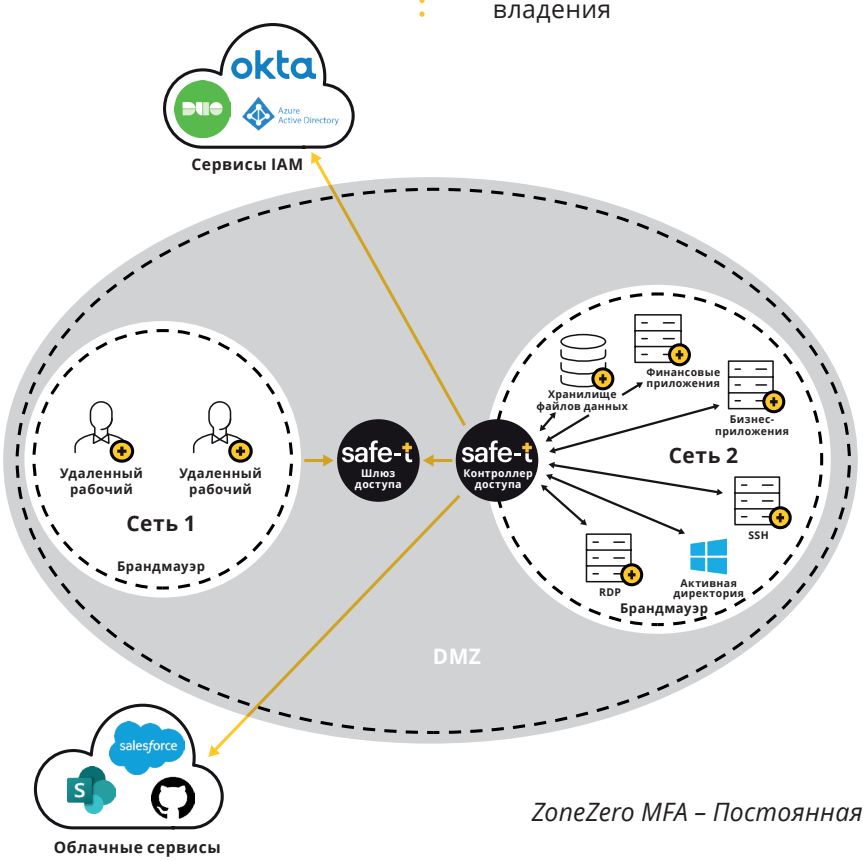
Централизованный подход решения ZoneZero MFA от Safe-T позволяет клиентам легко интегрировать многофакторную аутентификацию и информированность об идентификации во все сценарии доступа — для дистанционных и внутренних пользователей, VPN, веб и не веб приложений.

Возможности

- Встроенная MFA или интеграция со сторонними провайдерами MFA/ идентификации
- Поддержка постоянной аутентификации
- Контроль доступа к приложениям для внутренних пользователей
- Варианты использования «Пользователь > Приложение» и «Приложение > Приложение»

Преимущества

- Централизованный подход – без интеграции на стороне клиента
- «Бесшовная» интеграция – быстрое развертывание
- Переход от двухфакторной аутентификации (2FA) к действительно многофакторной аутентификации (MFA)
- Оптимальная стоимость развертывания и владения



ZoneZero MFA – Постоянная аутентификация

51 John F Kennedy Parkway, Short Hills, NJ | 888-304-5010
www.safe-t.com