2GC ZTNA

Может ли ZTNA и 2GC заменить ваш VPN?

Введение

Безопасный и бесперебойный удаленный доступ способствует развитию бизнеса, повышая производительность удаленных пользователей и сокращая время, затрачиваемое ИТ-командами на создание и поддержание связи между пользователями и приложениями благодаря гибкости и отказоустойчивости. И всё же удаленный доступ остаётся проблемой для многих организаций.

Когда-то давно VPN предлагали простой способ подключения нескольких удаленных пользователей к корпоративным сетям на короткие периоды времени. Однако по мере того, как рабочая сила становилась всё более распределенной, а организациям требовалось поддерживать безопасную связь с удаленными пользователями в течение более длительных периодов времени, недостатки этого подхода стали очевидны: от низкой производительности и повышенных рисков безопасности до проблем с масштабируемостью.

По мере роста потребностей в удаленном доступе организации всё чаще отказываются от традиционных реализаций VPN в пользу более безопасных и производительных решений удаленного доступа. Сетевой доступ, или ZTNA, создает безопасные границы вокруг определенных приложений, частных IP-адресов и имен хостов, заменяя разрешенные по умолчанию VPN-подключения политиками запрета по умолчанию, которые предоставляют доступ на основе идентификатора и контекста.

В 2020 году примерно 5% всего удаленного доступа обслуживалось преимущественно ZTNA. Из-за ограничений традиционного VPN-доступа и необходимости обеспечения более точного доступа и контроля сеанса ожидается, что к 2024 году это число возрастет до 40%. ZTNA предлагает предприятиям ряд явных преимуществ — и расширенные функциональные возможности — по сравнению с VPN, многие организации сочли это неполной заменой инфраструктуры VPN. Но поскольку ZTNA становятся более надежными, а VPN-сети - более проблематичными, и это быстро меняется. В этом документе сравниваются решения для удаленного доступа VPN и ZTNA, чтобы осветить их преимущества и ограничения, а также пролить свет на наиболее важные аспекты проектов миграции. Это объясняет как Cloudflare предлагает ZTNA и рекомендует ряд действий по переводу устаревшей VPN инфраструктуры для более быстрого и безопасного подключения с нулевым доверием для удаленных пользователей.

ПОДХОД №1: УСТАРЕВШАЯ VPN

На протяжении десятилетий VPN позволяли организациям подключать своих удаленных пользователей к корпоративным сетям с определенной степенью конфиденциальности и безопасности. Вместо доступа к конфиденциальной информации через общедоступный Интернет, где любой злоумышленник может перехватить или украсть данные, VPN позволяют пользователям безопасно получать доступ к внутренним ресурсам через зашифрованное соединение.

Двумя наиболее распространенными способами реализации VPN являются клиентские VPN и бесклиентские SSL-VPN. У каждого из них есть свои преимущества и проблемы:

<table>
<tr>
<td rowspan="2"><u>Клиентские VPN</u> подключают удаленных пользователей к частной сети через зашифрованный туннель. Это соединение устанавливается через программное приложение или клиент, который требует от пользователей однократной аутентификации с помощью имя пользователя и пароль для получения постоянного доступа к любому ресурсу в этой сети.</td>
<td><u>Выгода</u>:

После подключения свободное перемещение в боковом направлении упрощает пользователям быстрый доступ к множеству ресурсов путем доступа к приложениям и подключения к внутренним хостам.</td>
</tr>
<tr>
<td>Задачи:

• Не предназначен для пользователей в роуминге и мобильных устройств. По мере того, как пользователи перемещаются, их ноутбуки и мобильные устройства легко повторно подключаются по мере изменения беспроводных сетей от местоположения к местоположению. Однако VPN клиенты не умеют плавно обрабатывать эти переподключения, требующие от пользователей неоднократного принудительно перезапускать VPN-клиент и повторно аутентификация, приводящая к снижению производительности и создание ИТ-заявок.

• Плохая видимость. С помощью этого метода инфраструктура VPN завершает работу зашифрованного туннеля от VPN-клиента за Хотя эти подключения регистрируются, для конкретных приложений не существует централизованных журналов, показывающих, к каким приложениям пользователи получили доступ или какие действия они выполнили взято из приложения.</td>
</tr>
</table>

Бесклиентные SSL-VPN-порталы позволяют нескольким удаленным пользователям подключаться к нескольким браузерным приложениям. Это соединение становится возможным с помощью веб-сервера, встроенного в сетевое устройство под управлением службы VPN.	**Выгода**: Вместо использования клиента на устройстве, любой веб-браузер может использовать SSL-сертификат портала для установления зашифрованного HTTPS-соединения с поддержка подрядчиков на неуправляемых устройствах. **Задачи**: • **Соображения безопасности**. Большинство настроек VPN в центре обработки данных предоставляют пользователям полный доступ, что создает проблему для организаций, которые этого не делают хотите, чтобы внештатные сотрудники, например подрядчики, получали неограниченный доступ к конфиденциальным ресурсам и приложениям. • **Не создан для поддержки большого числа одновременных пользователей.** В отличие от современных облачных сервисов, веб-сервер портала не может быть эластично масштабирован для удовлетворения растущего спроса. Вместо этого необходимо и сбалансировать нагрузку для масштабирования портала, который часто является дорогостоящим, сложным и неэффективно, поскольку остальные функции устройства могут использоваться недостаточно. • **Бесклиентные порталы SSL-VPN подвергают атакам брандмауэр Порты и веб-серверы.** Для того, чтобы позволить веб-серверу, на котором размещен портал, получать доступ к внутренним приложениям, администраторы должны открывать входящие порты брандмауэра, подвергая их внешним атакам. Как открытые порты, так и Сам веб-сервер должен быть защищен от DDoS-атак и атак веб-приложений, что требует более сложной конфигурации и более высоких затрат на для обеспечения безопасности этого метода подключения.

Хотя VPN обеспечивают базовый уровень конфиденциальности для удаленных пользователей, они не были разработаны с учетом безопасности или масштабируемости. Традиционно, организации использовали VPN для подключения нескольких удаленных пользователей к корпоративной сети на короткие периоды времени. Однако по мере того, как удаленная работа становится все более распространенной, проблемы с VPN начинают множиться:

- **Пользователи сталкиваются с низкой производительностью.**
  Если инфраструктура VPN не имеет возможностей для обработки пропускной способности трафика и параллельных подключений, создаваемых их сотрудниками, пользователи сталкиваются с замедление их интернет-соединения. Кроме того, если расположенном виртуальные частные сети являются большом расстоянии от пользователя и сервер приложений они пытаются открыть, полученное время создает задержки.
- **Корпоративные сети остаются уязвимыми для атак**. VPN обычно используют модель "замок" и "ров", при которой пользователю предоставляется неограниченный доступ ко всем корпоративным ресурсам после подключения к сети. Без встроенного метода ограничения доступа к критически важной инфраструктуре и данным организации вынуждены настраивать дорогостоящие, сложные службы безопасности, такие как следующее поколение брандмауэры и контроль доступа к сети — или оставлены уязвимыми для боковых действий злоумышленников перемещение, приводящее к более крупным утечкам данных.

Проблема размещенных VPN-сервисов

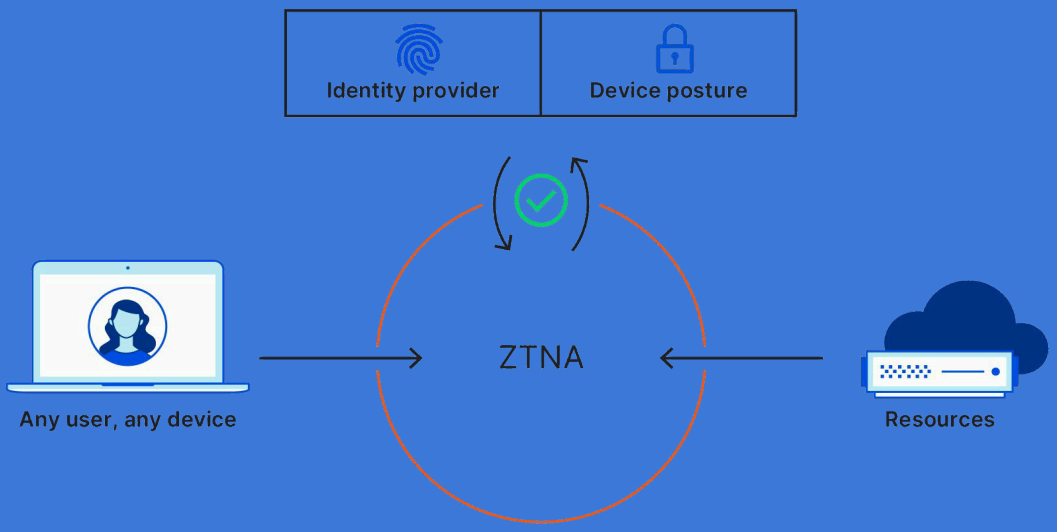
Некоторые поставщики перенесли сеть устройство, на котором работает служба VPN, в общедоступное облако, где оно работает как виртуальное машина в одном или нескольких центрах обработки данных.
VPN может быть как в комплекте, так и без него с дополнительными Службы безопасности.

Может показаться, что размещение VPN в облаке решает некоторые проблемы масштабируемости, присущие аппаратным устройствам VPN. Однако, это также сопряжено с некоторыми серьезными безопасность и масштабируемость.

Например, рассмотрим организацию, которая использует полноценный NGFW (брандмауэр следующего поколения), который сочетает в себе VPN с брандмауэром и дополнительной безопасностью функциональные возможности. Поскольку NGFW предлагается в виде комплексной услуги, невозможно независимо масштабировать какую-либо конкретную Масштабирование одной функции требует масштабирования всей службы; для этого необходимо подключить больше виртуальных машин для балансировки нагрузки небольшого объема вычислений, выполняемых в каждом из них ВМ. Это не только непрактично и громоздкое решение, но и, вероятно, повлечет за собой высокие затраты, поскольку удаленная работа организации потребности в доступе продолжают расширяться.

ПОДХОД №2: ДОСТУП К СЕТИ С НУЛЕВЫМ УРОВНЕМ ДОВЕРИЯ

Система безопасности с нулевым доверием позволяет преодолеть многие проблемы, связанные с VPN. Она основана на принципе, согласно которому ни одному пользователю или устройству внутри сети или за ее пределами нельзя доверять по умолчанию. Чтобы снизить риск утечек данных, внутренних атак и других угроз, подход с нулевым доверием проверяет подлинность и регистрирует каждый вход в систему и запрос, требует строгой проверки всех пользователей и устройств, ограничивает информацию, к которой может получить доступ каждый пользователь и устройство в зависимости от личности и контекста, а также добавляет сквозное шифрование для изоляции приложений и данных в сети.



Как и в случае с VPN, существует несколько способов настройки ZTNA:

- Бесклиентная (или инициируемая сервисом) ZTNA: Этот подход использует существующий веб-браузер вместо клиентского программного обеспечения для создания безопасного соединения и аутентификации пользовательских устройств. Изначально бесклиентный ZTNA ограничивался приложениями с протоколами HTTP/HTTPS, но совместимость с другими протоколами быстро развивается.

  Преимущества: Бесклиентный ZTNA использует соединение с обратным прокси-сервером для предотвращения прямого доступа к приложениям. Он блокирует доступ пользователей к приложениям и данным, к которым у них нет разрешения на просмотр, и предоставляет администраторам больший контроль и гибкость в управлении.

- Клиентская (или инициируемая конечной точкой) ZTNA: В этом случае программное обеспечение устанавливается на пользовательское устройство перед установкой зашифрованного соединения между управляющим агентом и авторизованными приложениями.

Преимущества: Клиентская ZTNA позволяет администраторам более точно определить состояние устройства, его местоположение и контекст рисков, связанных с доступом пользователей к приложениям. Этот метод не ограничен протоколами HTTP/HTTPS и может использоваться для доступа к широкому кругу приложений, включая те, которые работают на протоколах SSH, RDP, VNC, SMB и других TCP-соединениях.

Проблемы внедрения ZTNA

Хотя ZTNA обеспечивает явные преимущества перед традиционными VPN, это не безупречный подход к обеспечению доступа к сети для удаленных пользователей. По мере того, как предприятия взвешивают все "за" и "против" внедрения нулевого доверия, они могут столкнуться с одной или несколькими из следующих проблем:

Решения на самом деле не облачные. Если продавец не предлагает облачного ZTNA, то это означает, что их клиентам необходимо развертывать программное обеспечение в собственных данных центрах. В этом случае пользователи лишаются ключевых преимуществ, таких как мгновенная масштабируемость и неограниченная пропускная способность.	**Продавцы могут не предлагать клиентские и бесклиентские варианты ZTNA.** Это ограничивает ценность для организаций, которым необходимо подключать пользователей к приложениям, не использующим протокол HTTP, таким как удаленные рабочие столы, SSH-приложения или файлообменники.	**Конфигурация может быть сложной и отнимать много времени.** Продавцы, которые не предлагают поддержку оркестрации и автоматизации политик (с помощью инструментов, таких как Terraform), могут требовать от администраторов дополнительных инструкций работы, помимо уже существующей конфигурации, которая происходит на стороне поставщика удостоверений.

ПОДХОД CLOUDFLARE К УДАЛЕННОМУ ДОСТУПУ

Защита и масштабирование удаленного доступа должны быть непрерывным процессом, который не требует многоуровневых громоздких решений в области безопасности, компромиссных решений в области производительности или неоправданных затрат. Cloudflare позволяет командам обрабатывать все варианты использования удаленного доступа со следующими преимуществами:

- Простая адаптация без риска для пользователей и администраторов: Cloudflare легко интегрируется с существующими поставщиками идентификационных данных и платформами защиты конечных точек для обеспечения соблюдения политик нулевого доверия, которые ограничивают доступ к корпоративным приложениям и ресурсам.

- Гибкость для клиентского и бесклиентного развертывания ZTNA: Cloudflare предоставляет бесклиентную поддержку подключений к веб-приложениям, SSH, VNC (а вскоре и RDP), а также клиентскую поддержку приложений, отличных от HTTP, и частную маршрутизацию к внутренним IP-адресам.

Таблица 1. Как Cloudflare решает проблемы удаленного доступа

Проблема	Решение	Реализация Cloudflare
Трудно масштабировать	Глобальная периферийная сеть	Проблемы масштабируемости беспокоят как VPN, так и сервисы ZTNA. Необлачная инфраструктура усложняет доступ удаленных пользователям к приложениям и данным. Однако глобальная сеть Anycast Cloudflare не только позволяет установить соединения быстрее, чем VPN, но также гарантирует, что удаленные сотрудники любого размера могут безопасно и быстро подключаться к корпоративным ресурсам по мере необходимости — без необходимости дополнительной трудоемкой настройки со стороны администраторов.
Плохая совместимость с мобильные устройства	Легкий клиент	Решения VPN и ZTNA, использующие протоколы IPSec и SSL, часто имеют низкую производительность на мобильных и роуминговых устройствах. Однако клиент Cloudflare WARP использует более современный протокол Wireguard, который работает в пользовательском пространстве и поддерживает более широкий набор операционных систем. Это обеспечивает более быстрый пользовательский интерфейс по сравнению с традиционными вариантами. Клиент Cloudflare WARP можно настроить на устройствах с операционными системами Windows, macOS, iOS, Android и, скоро, Linux.
Нет интегрированного или слабого защита от DDoS	Ведущий в отрасли DDoS встроенная защита	Без встроенной защиты от DDoS организации часто вынуждены подключать дополнительные службы безопасности, что может вызвать проблемы с конфигурацией, масштабируемостью и безопасностью. Сеть Cloudflare, обладающая скоростью более 67 Тбит/с, предоставляет встроенную защиту от DDoS для любого режима ZTNA, защищая сети от крупномасштабных атак.
Ограничения протокола	Поддержка не-веб-приложений	✓ Совместимость режимов: бесклиентский ZTNA для SSH/VNC приложений; клиентский ZTNA для всех остальных приложений, не являющихся сетевыми.
Нет интегрированной	Встроенный сетевой	По мере роста корпоративных сетей увеличивается и уровень безопасности, что требует от организаций

сети брандмауэр	брандмауэр	постоянного балансирования между стоимостью, производительностью и безопасностью оборудования. Cloudflare позволяет администраторам применять политики сетевого брандмауэра на грани, предоставляя им детальный контроль над тем, какие данные разрешены для входа и выхода из их сети, а также улучшая видимость трафика через нее. ✓ Совместимость режимов: клиентский ZTNA
Отсутствие мелкозернистости и контроль	Встроенный безопасный Интернет шлюз (SWG)	Несанкционированное использование приложений может стать причиной серьезных проблем с безопасностью для организаций; без строгой политики пользователи могут получить доступ к конфиденциальным и другим корпоративным данным и злоупотребить ими. Объединив ZTNA с Secure Web Gateway (SWG), Cloudflare позволяет администраторам осуществлять более детальный контроль над правами доступа пользователей и устройств внутри приложений, что позволяет пользователю и группам на основе их ролей иметь доступ только к необходимым ресурсам. ✓ Совместимость режимов: клиентский ZTNA

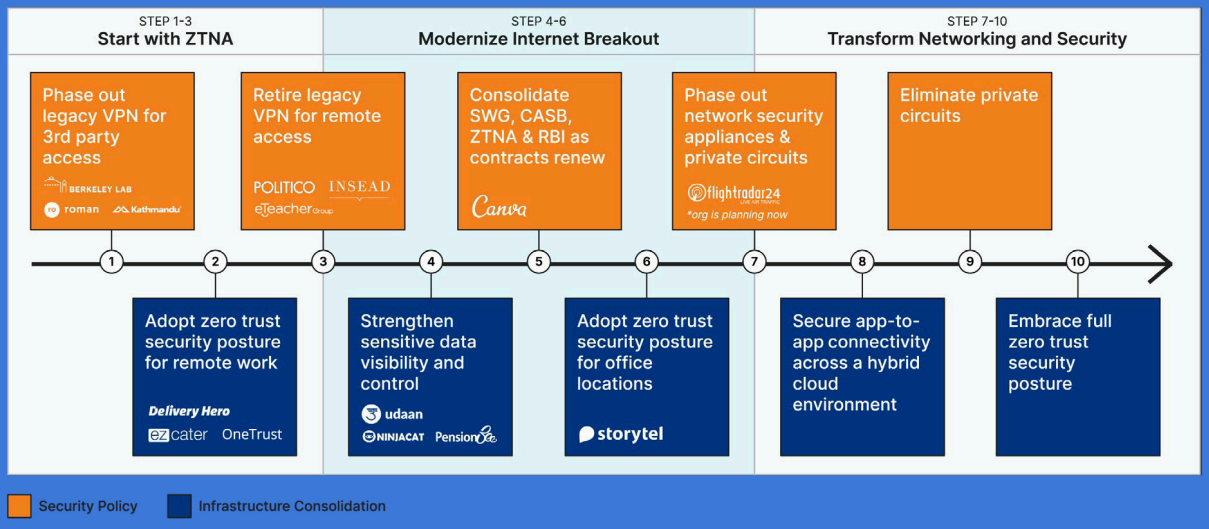
ЗАМЕНИТЕ СВОЙ СТАРЫЙ VPN НА ДОСТУП К СЕТИ С НУЛЕВЫМ УРОВНЕМ ДОВЕРИЯ

Обещания о нулевом доверии могут показаться руководителям ИТ-безопасности пустыми словами в разгар долгого и болезненного перехода к безопасности без использования VPN. Однако, замена вашего VPN сетью с нулевым доверием предлагает доступ без компромиссов в поддержке протокола или функциональности.

Рекомендуемый путь миграции зависит от бизнес-приоритетов вашего проекта:

- Если вашим приоритетом является более быстрое подключение к приложениям, сначала разверните клиентскую ZTNA для не веб-приложений.
- Если повышение безопасности правил доступа к вашим приложениям важнее, начните с веб-приложений.

Замена вашего VPN - это только первый шаг в полном преобразовании сети. Поскольку переход к модели SASE может быть сложным, мы разработали общий путь к обеспечению безопасности с нулевым уровнем доверия на основе подхода, принятого нашими клиентами.



ПРИЛОЖЕНИЕ

Модернизируйте свои интернет-сервисы

Внедрение ZTNA является важным шагом в развертывании пограничной службы безопасного доступа (SASE) модели. Cloudflare One - это комплексное решение "сеть как услуга" (NaaS), которое упрощает и обеспечивает безопасность корпоративных сетей для команд любого размера. С Cloudflare One организации могут:

- Использовать доступ с нулевым уровнем доверия: Замените широкие периметры безопасности индивидуальной проверкой каждого запроса к каждому ресурсу. Применяйте правила нулевого доверия при каждом подключении к вашим корпоративным приложениям, независимо от того, где находятся ваши пользователи.

- Обеспечивать безопасный интернет-трафик: Когда угрозы в Интернете распространяются быстро, средства защиты, которые вы используете для их предотвращения, должны быть более активными. Cloudflare One защищает удаленных сотрудников от угроз в Интернете и применяет политики, предотвращающие утечку ценных данных из вашей организации за счет принудительной изоляции браузера с нулевым уровнем доверия на любом сайте — с плавным, молниеносным взаимодействием с пользователем.

- Обеспечивать защиту и подключение офисов и центров обработки данных: Корпоративные сети стали чрезмерно сложным процессом, что означает, что пользовательскому трафику часто приходится проходить несколько переходов, чтобы добраться до куда ему нужно. С Cloudflare One предприятия могут защищать офисы и центры обработки данных с помощью единой облачной платформы.

Преобразуйте свою сеть

В ближайшее время предложения Cloudflare "Нулевое доверие" и "Глобальная сеть как услуга" объединятся в единое целое, что позволит вашим сотрудникам постоянно получать доступ к корпоративным ресурсам, где бы они ни работали. Сегодня ваши продукты VPN и глобальной сети позволяют вашим сотрудникам получать доступ к ресурсам, расположенным в вашей частной корпоративной сети, но они вынуждают вас по-другому управлять подключением и политиками безопасности. Теперь Cloudflare предоставляет единую плоскость управления, что дает вам больше гибкости при ее применении. Не доверяйте политикам безопасности для всего персонала и на рабочем месте без необходимости манипулировать несколькими точечными продуктами.