

Magic WAN

Magic WAN упрощает путь к SASE благодаря возможности многоточечного подключения

Эволюция сетевых архитектур

Интернет — новая корпоративная сеть

Поскольку гибридная работа стала новой нормой, а приложения перемещаются в облако, ИТ-команды сталкиваются со следующим:

- **Сложность сети.** Предоставление MPLS и настройка точечных решений занимает слишком много времени
- **Бреши в безопасности.** Прямой выход в Интернет не соответствует политикам безопасности и приемлемого использования, подвергая риску пользователей и данные
- **Высокие затраты.** MPLS-линии и решения на основе точек безопасности сопряжены с лишними расходами
- **Низкое удобство использования.** Перенаправление трафика на периметр обеспечения безопасности приводит к сетевым задержкам

Magic WAN упрощает сетевое подключение филиалов, мультиоблачных VPC и центров обработки данных к платформе SASE [Cloudflare One](#), обеспечивая безопасное, производительное и экономичное подключение для решения задач гибридной работы и мультиоблака для ИТ-команд.

В отличие от негибкой, дорогостоящей сети [MPLS](#) или сложных развертываний [SD-WAN](#), построенных на локальных межсетевых экранах, Magic WAN использует подход «легкий филиал, тяжелое облако» для расширения или замены вашей текущей архитектуры. Такое решение является более простым в развертывании и масштабируется в соответствии с меняющимися бизнес-требованиями благодаря встроенной системе безопасности.



Magic WAN подключает физические или виртуальные сетевые локации к платформе SASE Cloudflare. Примеры физических площадок включают филиалы, заводские цеха, магазины розничной торговли, головные офисы или центры обработки данных. Примеры виртуальных местоположений включают общедоступные облачные сервисы, такие как AWS, Azure, GCP и OCI.



Улучшенная операционная гибкость

Централизованно управляйте сетями и сетевой безопасностью с помощью единой консоли администратора. Доставка трафика на основе возможностей сетевого подключения благодаря полностью автоматической конфигурации.



Обеспечение безопасности за счет внутренних, а не внешних средств

Получите облачно-ориентированную защиту от DDoS-атак, межсетевой экран, функциональные возможности SSE и Zero Trust — все компоненты глубоко интегрированы и предоставляются как услуга.



Сокращение затрат на сеть

Максимально сократите углеродный след своих филиалов и перенесите сетевые функции в облако, чтобы снизить зависимость от дорогостоящих развертываний MPLS и отказаться от SD-WAN.

Основные варианты использования для Magic WAN

Оптимизация сетевого сервиса

- **Упрощение сетевого подключения филиалов** — Замените разнородный набор проприетарных каналов и сетевых устройств для безопасной маршрутизации трафика между филиалами и центрами обработки данных. Упростите соединение между объектами с помощью Anycast IPsec.
- **Упрощение гибридного и мультиоблачного подключения** — У организаций есть приложения в облаках разных поставщиков (например, AWS, GCP, Azure, Oracle, IBM), а также в локальных центрах обработки данных. Используйте централизованные средства контроля для маршрутизации и защиты трафика в различных средах.

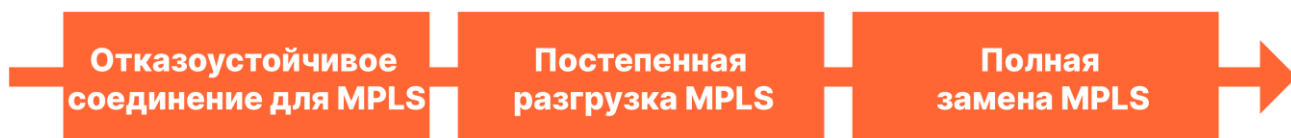
Повышение безопасности без ущерба для производительности

- **Безопасность в сети WAN** — Обеспечьте безопасность соединений за счет применения политики сетевой безопасности между локациями (филиалами, центрами обработки данных и т. д.) с помощью облачного межсетевого экрана и элементов управления SWG.
- **Масштабирование производительности WAN** — Использование MPLS является дорогостоящим, негибким и медленным решением. Переход на Cloudflare обеспечивает более экономичное и гибкое развертывание со встроенными средствами обеспечения безопасности.

Подход к развертыванию Magic WAN

Трансформация сети — это целый путь

Magic WAN обеспечивает производительность и надежность подключения к Интернету и помогает организациям отказаться от устаревших сетевых архитектур. Начните с поэтапного развертывания Magic WAN и заменяйте технологии постепенно. Принцип «легкий филиал, тяжелое облако», принятый в Cloudflare, сочетает в себе широкие возможности подключения на последней миле и производительность, надежность и безопасность на средней миле и таким образом помогает обеспечивать и защищать сетевые подключения в гибридной рабочей среде. Наша архитектура поддерживает развертывание вместе с существующей инфраструктурой для миграции в удобном для вас темпе.



Сравнение Cloudflare One с MPLS и SD-WAN

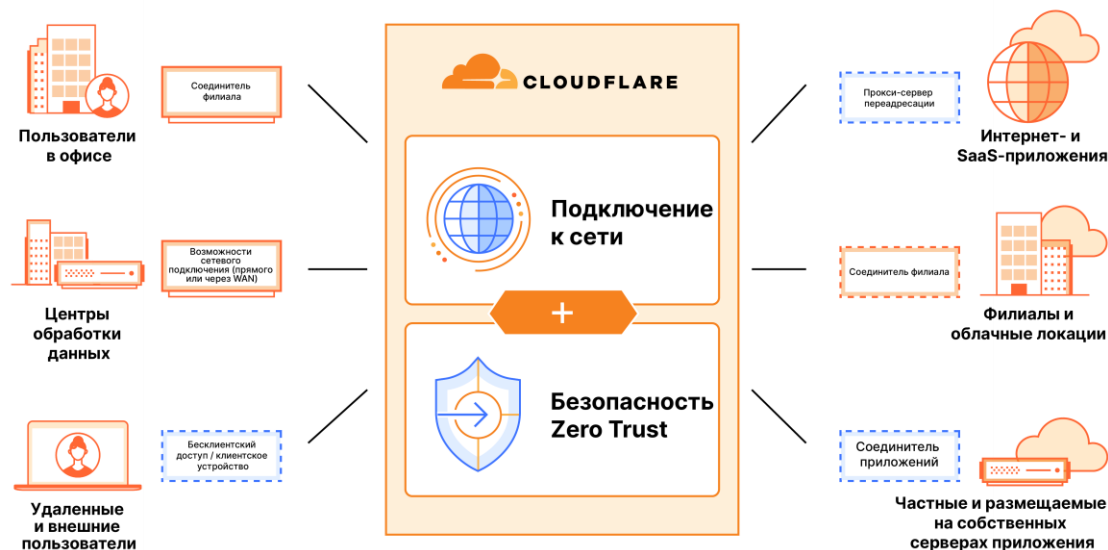
По мере того как приложения перемещаются в облако, а организации переходят на гибридную работу, традиционные сетевые архитектуры сталкиваются со снижением уровня производительности и безопасности. Перенаправление трафика снижает производительность и удобство использования, а разрешение локального интернет-соединения снижает согласованность и эффективность безопасности. Ни один из этих сценариев не является желательным, и в результате при проектировании сетей приходится идти на компромиссы, в результате которых организационные и индивидуальные потребности остаются неудовлетворенными.

Совсем недавно в SD-WAN были добавлены наложения для управления трафиком с целью предложить альтернативу MPLS. Однако безопасность SD-WAN во многом зависит от периферийных устройств, в результате чего командам приходится объединять множество аппаратных, виртуализированных и облачных инструментов. Как следствие, дополнительная сложность сводит на нет многие предполагаемые преимущества.

Платформа SASE от Cloudflare объединяет безопасность и сетевое взаимодействие в нашем облаке connectivity cloud и позволяет организациям использовать нашу сеть как расширение своей собственной. Упрощенное управление, надежная производительность, современная безопасность на основе Zero Trust и снижение совокупной стоимости владения одновременно возможны только при использовании по-настоящему обновленного подхода к SASE.

Критерии	Сервис MPLS/VPN	SD-WAN	SASE с Cloudflare One
Конфигурирование Установка, настройка и управление новым объектом	Посредством MSP через запрос на обслуживание	Упрощенная координация и управление с помощью централизованного контроллера	Автоматизированная координация через портал SaaS; централизованная информационная панель
Контроль трафика на последней миле Балансировка трафика, качество обслуживания (QoS) и аварийное переключение	Охватывается соглашениями об уровне обслуживания MPLS	Выбор наилучшего пути доступен в устройстве SD-WAN	Минимальное развертывание на собственной инфраструктуре для контроля принятия решений на местном уровне
Контроль трафика на средней миле Распределение трафика по загруженному пути средней мили	Охватывается соглашениями об уровне обслуживания MPLS	«Туннель „Спагетти“» и при этом отсутствие контроля над средней милей	Интегрированное управление трафиком и управление частной магистральной сетью в одном и том же интерфейсе
Облачная интеграция Сетевой сервис для миграции в облако	Централизованное интернет-соединение	Децентрализованное интернет-соединение	Собственный сетевой сервис с Cloud Network Interconnect
Безопасность Фильтрация входящего и исходящего интернет-трафика на предмет вредоносного ПО	Разнородный набор инструментов управления аппаратными средствами	Разнородный набор инструментов управления аппаратными средствами и/или программным обеспечением	Нативная интеграция с инструментами безопасности пользователей, данных, приложений и сети
Затраты Максимизация рентабельности инвестиций в сеть	Высокие затраты на аппаратное обеспечение и сетевой сервис	Оптимизированные затраты на сетевой сервис за счет увеличения затрат на аппаратные средства и программное обеспечение	Снижение затрат на аппаратные средства и сетевой сервис для максимального увеличения окупаемости инвестиций

Направление трафика на платформу SASE Cloudflare



Magic WAN Connector позволяет легко подключить ваши сетевые локации к Cloudflare. Используйте программное обеспечение Branch Connector, предварительно установленное и настроенное на аппаратном устройстве, сертифицированном Cloudflare, для упрощенного развертывания, или разверните программное обеспечение на физических или виртуальных устройствах Linux в вашей среде.

Часть растущего семейства гибких возможностей сетевого подключения

Первым шагом к использованию [SASE](#) является подключение — создание безопасного пути от вашей существующей сети до ближайшего местоположения, где можно применить политики безопасности на основе Zero Trust. Cloudflare предлагает широкий набор возможностей сетевого подключения для обеспечения такого подключения, включая варианты клиентского и бесклиентского доступа для пользователей, работающих в гибридном формате, туннели прикладного уровня, создаваемые путем развертывания облегченных программных соединителей, подключение сетевого уровня с помощью GRE с поддержкой Anycast или туннели IPsec, а также физическое или виртуальное соединение как для частных центров обработки данных, так и для общедоступных облаков.

Чтобы еще больше упростить внедрение SASE, Magic WAN Connector можно развернуть в любой физической или облачной сетевой локации, чтобы обеспечить автоматическое подключение к оптимальному центру обработки данных Cloudflare, используя существующее подключение к Интернету на участке «последней мили» и устраняя необходимость для ИТ-команд вручную настраивать сетевое оборудование для подключения.

Возможности программного обеспечения и технические характеристики аппаратных средств

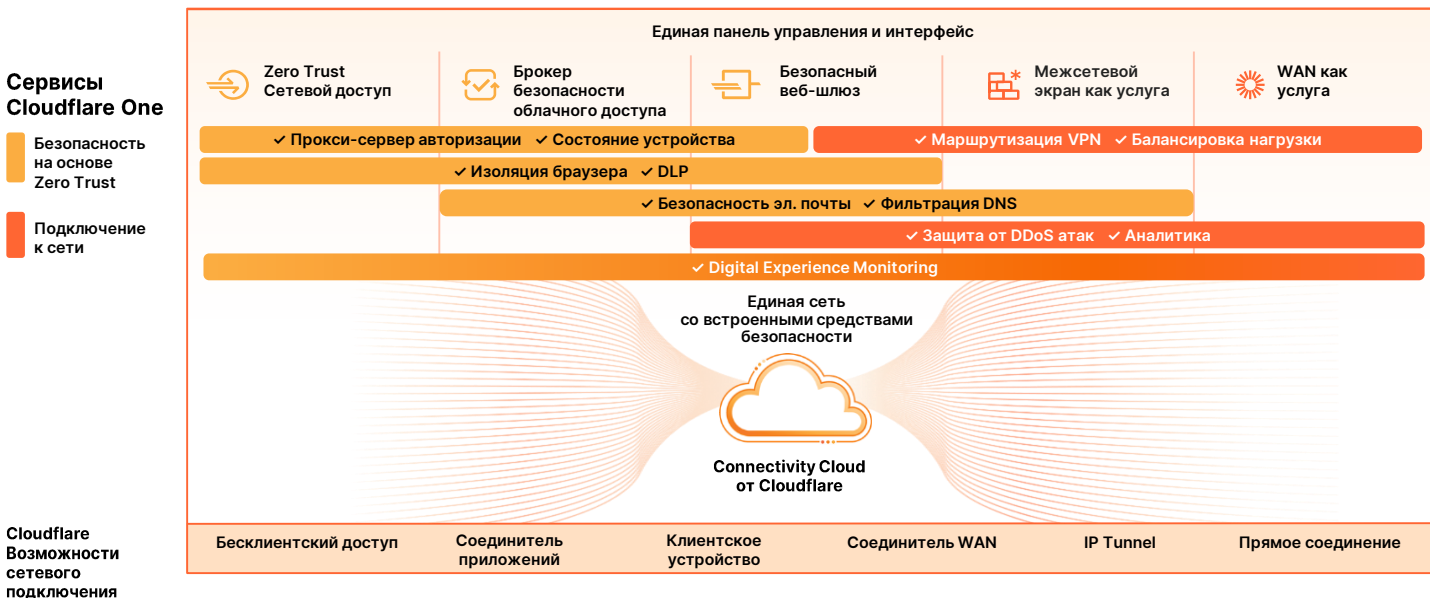
Возможности программного обеспечения Magic WAN ¹	
Установка WAN Connector	Устройства абонентского оконечного оборудования с возможностью автоматической настройки по принципу «подключи и работай», которые централизованно управляются через панель управления/API Cloudflare. Автоматически настраивайте туннели и маршруты IPsec для направления трафика в сеть Cloudflare для обеспечения связи и функций безопасности. Автоматические обновления программного обеспечения (в течение периода обслуживания, определяемого клиентом).
Конфигурирование объекта WAN Connector	Поддержка WAN/LAN для конфигураций на основе статических IP или DHCP. Поддержка VLAN и сегментации локальной сети.
Подход «легкий филиал, тяжелое облако»	Балансировка нагрузки и аварийное переключение на локальном легком WAN Connector с высокой доступностью в нескольких каналах WAN на основе проверок работоспособности. Сервисы безопасности, такие как межсетевой экран и возможности Zero Trust SSE, предоставляются из облака connectivity cloud Cloudflare.
Интеграция сторонних сервисов	Настройте конечные точки туннеля Anycast IPsec или GRE с помощью существующих облачных VPC, таких как Amazon AWS Transit Gateway, или абонентского оконечного оборудования, такого как SD-WAN, межсетевой экран и устройства-маршрутизаторы. Настраивайте статические маршруты с пересылкой пакетов ECMP в сеть Cloudflare.
Встроенные средства безопасности	Встроенный межсетевой экран уровня L3 и обнаружение вторжений; бесшовная интеграция с другими возможностями SSE/безопасности и возможностями сетевого подключения, такими как безопасный веб-шлюз уровней L4-7, клиент устройства, соединитель приложений и т. д.
Возможности мониторинга и управления	Обнаружение и маршрутизация трафика на основе приложений. Контроль пропускной способности. Возможности мониторинга/аналитика для показателей туннеля, трафика и устройств доступны через информационную панель, API, журналы или GraphQL. Управление через информационную панель Cloudflare, API или Terraform.
Magic WAN Connector: спецификации аппаратных средств ²	
Спецификации устройств	• Порты: (6x 1G медь RJ45) + (2x 10G SFP+) + (2x USB 3.0 Тип A) • Размеры: 8,1x7,9x2,0 дюйма; 1,5RU; Вес: 2,87 фунта • Варианты монтажа: настольное размещение, настенный монтаж или крепление в стойку (с лотком) • TPM: 2.0, весь мир, кроме Китая • СРУ (ЦП): Denverton 4-х ядерный C3558 • Диск: M.2 120 SSD с 16G eMMC Flash • RAM: 8 ГБ DDR4 • Wi-Fi и Bluetooth: 802.11ac, 2x2 MIMO, макс. режим передачи данных: 866,7 Мбит/с • Вентилятор: один

¹ Всю документацию по функциям Magic WAN можно найти в [документации Cloudflare](#)

² Аппаратные средства, сертифицированные Cloudflare с предустановленным программным обеспечением Magic WAN: [Dell VEP 1425](#), продается через партнера (поставляется с креплением в стойку)

Сетевое подключение и путь к SASE

Cloudflare connectivity cloud обеспечивает простоту развертывания, отказоустойчивость сети и скорость инноваций, необходимые для того, чтобы оставаться на шаг впереди при консолидации специализированных продуктов и объединении единой ИТ-стратегии.



Cloudflare One позволяет организациям любого размера выполнить [переход на SASE](#): подключить любой источник и место назначения трафика к безопасной, быстрой и надежной глобальной сети, где применяются все функции безопасности, а трафик оптимизируется на пути к месту назначения, как внутри частной сети, так и в общедоступном Интернете.

Независимо от того, переносит ли ваша организация трафик из готовых развертываний MPLS или SD-WAN либо впервые модернизирует сеть, Magic WAN может помочь вам упростить этот процесс. Cloudflare One объединяет в себе средства безопасности на основе Zero Trust и WAN как услугу, то есть вы можете использовать его и как основу для SASE от одного поставщика, и как дополнение к решениям других поставщиков на пути к внедрению SASE.

Давайте обсудим возможности сетевого подключения для вашей организации

Запрос семинара



Узнать больше о [платформе SASE от Cloudflare](#)