

Защита распределенных рабочих мест

Последовательная защита на единой унифицированной плоскости управления для всех запросов из любой локации

Перенесите безопасность в облако

Снижение сложности и рисков для офисов с помощью Cloudflare

Поскольку сотрудники работают в офисах и удаленно, сегодня многие организации пересматривают методы обеспечения безопасности офисов, независимо от того, полагаются ли они на устройства в центрах обработки данных или разрешают прямой незащищенный доступ в Интернет.

Их новым приоритетом является обеспечение последовательной защиты и удобства для пользователей внутри сети и за ее пределами. В большинстве случаев это означает перенос средств управления с разрозненных инструментов, таких как VPN, веб прокси-серверы и межсетевые экраны, на единую облачную платформу безопасности.

Cloudflare предлагает организациям модернизировать офисную безопасность с помощью двух распространенных вариантов использования.

Рекомендуемый вариант использования:

Безопасный доступ к приложениям с Zero Trust для замены VPN

Применяйте детализированные политики с учетом идентификации для каждого приложения вместо бокового перемещения по корпоративной сети.



- **Шаг 1:** Интеграция с вашим сервисом (-ами) авторизации
- **Шаг 2:** Защитите любое веб-приложение через браузер
- **Шаг 3:** Обеспечьте безопасность сред SSH, VNC и RDP через браузер



Объедините филиалы и удаленный доступ в одной реализации, чтобы обеспечить согласованные политики и свести к минимуму количество необходимых поставщиков. Разверните ZTNA, чтобы дополнить или заменить устаревшую VPN, что позволит ограничить инвестиции в устаревшие технологии.¹

Gartner®

Рекомендуемый вариант использования:

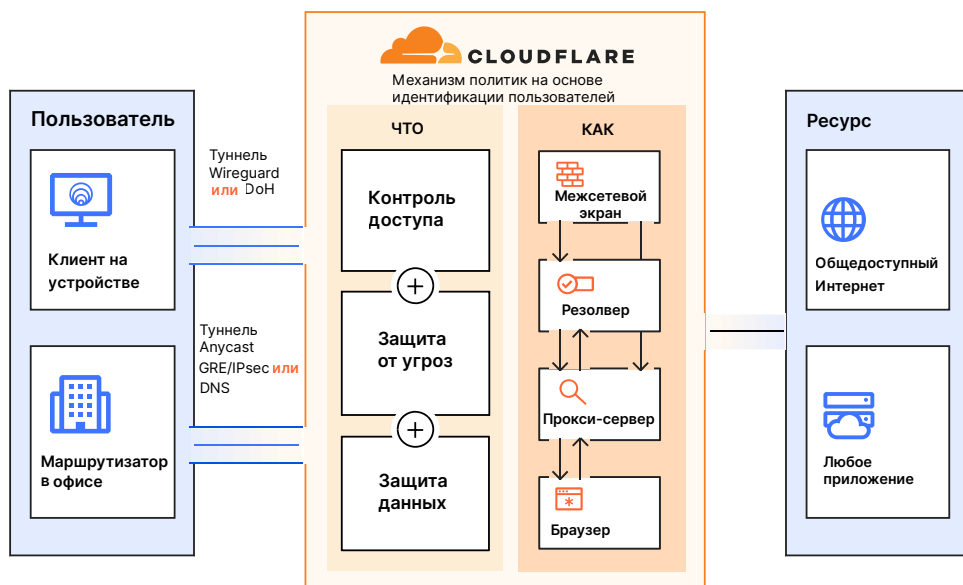
Фильтрация доступа в Интернет для последовательной безопасности и быстрого времени окупаемости

Сначала защитите офисных пользователей с помощью фильтрации DNS, а затем и более комплексных проверок во всех локациях. Больше не нужно перенаправлять трафик через локальные устройства безопасности в центры обработки данных.



- **Шаг 1:** Направьте DNS-трафик в глобальную сеть Cloudflare
- **Шаг 2:** Настройте фильтрацию DNS на основе локации для защиты от программ-шантажистов, фишинга и других интернет-угроз
- **Шаг 3:** Контролируйте потоки данных, применяя правила в отношении HTTP, сети и изоляции браузера с неограниченной проверкой TLS 1.3.

Как это работает



Бесклиентское развертывание для проверки доступа и фильтрации DNS-запросов из офисов.

Развертывание с помощью клиентского устройства Cloudflare, чтобы обеспечить расширенные возможности мониторинга и контроля для каждого пользователя и устройства.

Рисунок 1: Проверка, фильтрация, изоляция и проверка офисного трафика за один проход с помощью [Cloudflare Zero Trust](#)

Гибкие возможности сетевого подключения из любого источника

Начните с использования Cloudflare для разрешения DNS через сетевые маршрутизаторы. Со временем вы можете направлять трафик L3 в нашу глобальную сеть через туннели GRE или IPsec или использовать существующий метод маршрутизации SD-WAN.

Кроме того, вы можете развернуть клиент Cloudflare для фильтрации и проверки DNS и HTTP на управляемых устройствах.

Быстрое применение политик, созданное для глобального масштабирования

Все функции обеспечения безопасности, производительности и надежности встроены для работы на каждом сервере в каждом центре обработки данных в наших 275+ локациях и 100+ странах.

Масштаб нашей сети означает, что средства защиты всегда применяются рядом с офисами и конечными пользователями, где бы они ни находились, на высокой скорости с проверкой в один проход.

Другие варианты использования для изучения в течение следующих шести-двенадцати месяцев



Восстановите контроль над приложениями SaaS

Выявляйте и снижайте риски, связанные с теневыми ИТ, которые сотрудники используют в офисах и дома.

Предотвращайте утечки данных и нарушения нормативных требований с помощью политик CASB, реализуемых через ту же единую информационную панель Cloudflare. [Узнайте как.](#)



Разгрузка трафика MPLS

Замените дорогостоящие, устаревшие и медленные частные соединения MPLS.

Упростите устаревшую архитектуру WAN, используя глобальную сеть Cloudflare для управления трафиком между филиалами, центрами обработки данных и сервисами общедоступного облака. [Узнайте как.](#)

1. Gartner Hype Cycle for Network Security, 2021 г. | GARTNER и HYPE CYCLE являются зарегистрированными товарными знаками и знаками обслуживания Gartner, Inc. и/или аффилированных с ней компаний в США и других странах и используются здесь с разрешения владельца. Все права защищены.