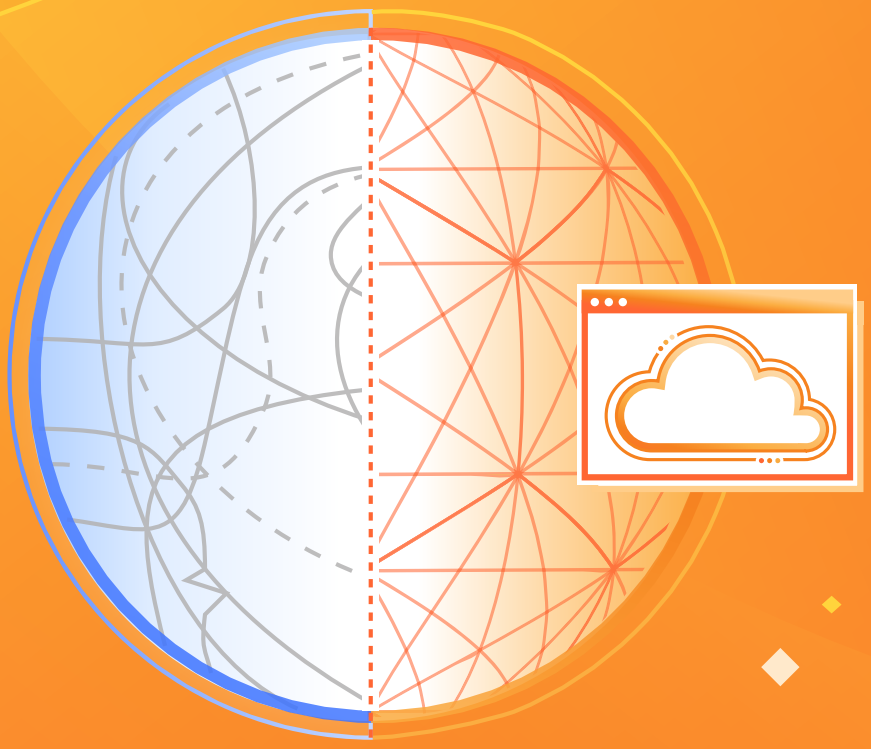
CLOUDFLARE

СПРАВОЧНЫЙ ДОКУМЕНТ

Разработка стратегии модернизации вашей сети



Содержание

Устаревшие сети: препятствие для цифровой модернизации

Гибкость имеет решающее значение для достижения успеха в мире, где условия ведения бизнеса могут измениться в мгновение ока. Но гибкость — это не просто вопрос управления и принятия решений. Гибкость также зависит от способности организации осуществлять изменения. Системы должны создаваться таким образом, чтобы они могли гибко подстраиваться и адаптироваться, при этом без разрушений собственной структуры. Бизнес должен быть способен перестроиться на новые модели доходов, поддерживать новые приложения и соединять людей по всему миру.

Гибкость — один из основных желаемых результатов проектов цифровой модернизации, поскольку организации перестраиваются для получения конкурентных преимуществ. Это особенно актуально в отношении традиционной корпоративной сети, которая играет решающую роль в обеспечении связи и обеспечении совместной работы. Корпоративная сеть по-прежнему упорно сопротивляется изменениям, и на это есть веские причины. Она была разработана с тем, чтобы противостоять потрясениям системы, а изменения требуют больших затрат и усилий.

Иногда изменения можно предвидеть, поскольку они происходят с течением времени, например, влияние облака на центр обработки данных. В сетевых технологиях внешние рыночные силы приводят к быстрым, иногда одномоментным изменениям. Например, пандемия преподнесла болезненные уроки того, как трудно некоторым компаниям быстро наращивать мощности для удаленной работы, поддерживать производительность сотрудников и управлять расходами в свете того, сколько бюджетных средств расходовалось на неработающие сети в пустых офисах.

Несмотря на все эти трудности, также стало очевидно, что некоторые компании смогли не только адаптироваться, но и процветать. Это был вопрос не только способности руководства принимать правильные деловые решения, но и возможностей бизнеса по преобразованию и реализации. Директорам по ИТ необходимо разработать стратегии реагирования на изменения, обеспечить переоснащение для удовлетворения будущих потребностей и превратить ИТ в ускоряющий, а не тормозящий фактор изменений.

При огромных инвестициях в создание локальных сетей модернизация — непростое решение. Чтобы в полной мере реализовать преимущества модернизации сети, необходимо понять, чего именно мы хотим достичь — и тогда мы сможем определить, что должно измениться.

Понимание пути

При рассмотрении передовых методов проектирования сетей за последние годы становится понятно, почему существует так много сложностей. На протяжении десятилетий организации создавали и укрепляли свои сети, добавляя все новые и новые технологии. С каждым новым поколением сетевых технологий и каждым нововведением сеть становилась все сложнее. Не было самой возможности стремиться к простоте, и зачастую добавление новых технологий еще больше усложняло обеспечение скорости, отказоустойчивости и безопасности.

Благодаря облачным сетевым сервисам и сервисам безопасности мы сейчас стоим перед лицом принципиально новых изменений в проектировании корпоративных сетей. Используя облачные сервисы в качестве расширения сети, организации могут решать новые задачи, расширять охват и обеспечивать безопасность приложений далеко за пределами центра обработки данных. Это дает возможность значительно упростить сеть, поскольку предоставление услуг стоится на базе существующих подключений к точке присутствия поставщика облачного сервиса и не нужно разрывать соединения для подключения очередного устройства. Сетевое соединение между локальной сетью и облачным сервисом остается прежним, а сервисы подключаются и используются внутри облачного пространства.

Проблема состоит в том, что не все облачные сетевые платформы и платформы безопасности построены одинаково, и не всегда легко понять, что отличает одну платформу от другой. Многие из них имеют ограниченный потенциал роста на пути модернизации. Чтобы понять различия, необходимо определить цели модернизации сети, чтобы не заменять один источник сложности другим.

Четыре ключевых маршрута сетевого трафика

При оценке масштаба вашего проекта модернизации сети следует учитывать, что ваша сеть охватывает большое количество точек соприкосновения, некоторые из которых пересекают одну и ту же инфраструктуру (например, трафик проходит входящий, исходящий маршруты и маршрут с востока на запад через вашу основную сеть), а некоторые из них работают за ее пределами (например, ваше сетевое общедоступное облако).

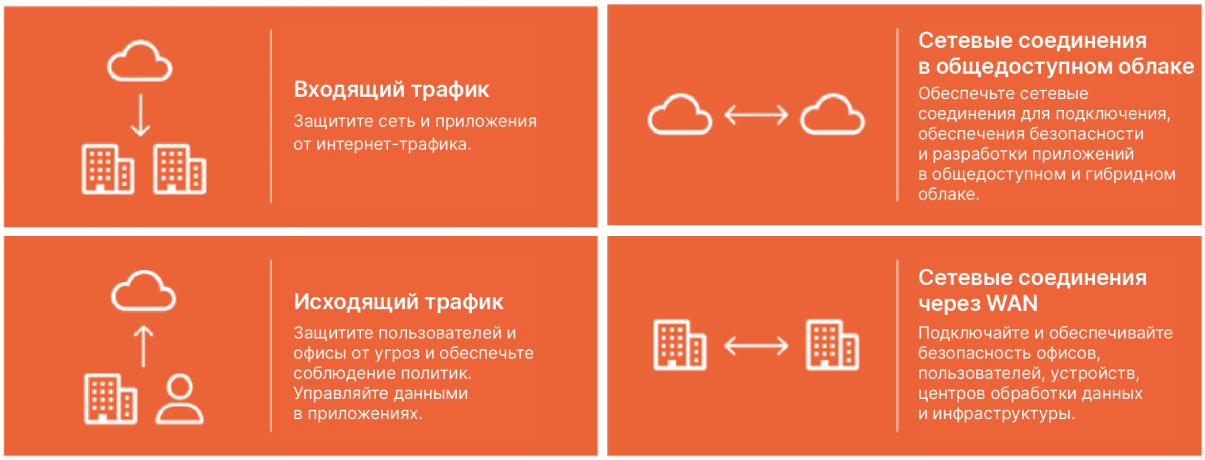
Входящий трафик. Учитывая, что некоторые участки вашей непосредственно взаимодействуют с Интернетом, необходимы средства безопасности входящего трафика, которые защитят от попыток злоумышленников вывести из строя или использовать в своих целях ресурсы компании, но при этом будут пропускать трафик от легитимных пользователей. Традиционную защиту периметра можно преодолеть. В ней должны быть возможности для борьбы с распределенными атаками типа «отказ в обслуживании».

Исходящий трафик. Для подключений к Интернету и облачным приложениям требуются политики, обеспечивающие защитные меры для безопасного использования в бизнесе, такие как защита от угроз и кражи данных. Учитывая изменчивость местоположения пользователя, организации внедряют сочетание технологий защиты исходящего трафика, которые включают в себя локальные устройства, такие как межсетевые экраны (когда пользователь находится в сети), DNS-резолверы, а также облачные прокси-серверы, такие как SWG и CASB (для удаленных пользователей).

Сетевое взаимодействие на основе WAN. Сети WAN, а также границы, которые они охватывают, включая кампусы и филиалы, перестраиваются для поддержки облачных инициатив и устройств с поддержкой Интернета вещей (IoT). Таким образом, традиционная топология сети отменяет перенаправление трафика на центр обработки данных в пользу архитектуры прямого доступа в Интернет. С быстрым развитием сетевых технологий в этих областях обеспечение безопасности, наоборот, стало более сложным. Во многих случаях внутренние пути трафика по-прежнему зависят от развертываемых на периферии устройств безопасности, что препятствует прогрессу трансформации организации.

Сетевое взаимодействие на основе общедоступного облака. Поскольку организации размещают свои приложения в нескольких облаках, становится все труднее устанавливать и поддерживать конфигурации сети и безопасности на двухточечной основе. Настройка сети и управление ею требует времени и ресурсов — времени, которое лучше потратить на разработку проектов.

Для каждого из этих путей трафика есть ряд технологий, которые организации внедряют в своей сети или используют из облака. Учитывая, что проекты модернизации затрагивают различные пути трафика, необходимо планировать полную модернизацию сети по всем четырем направлениям, чтобы избежать архитектурных ошибок, которые будут ограничивать достижимые преимущества трансформации или требовать использования нескольких разрозненных технологий для охвата всех возможных вариантов развития событий.

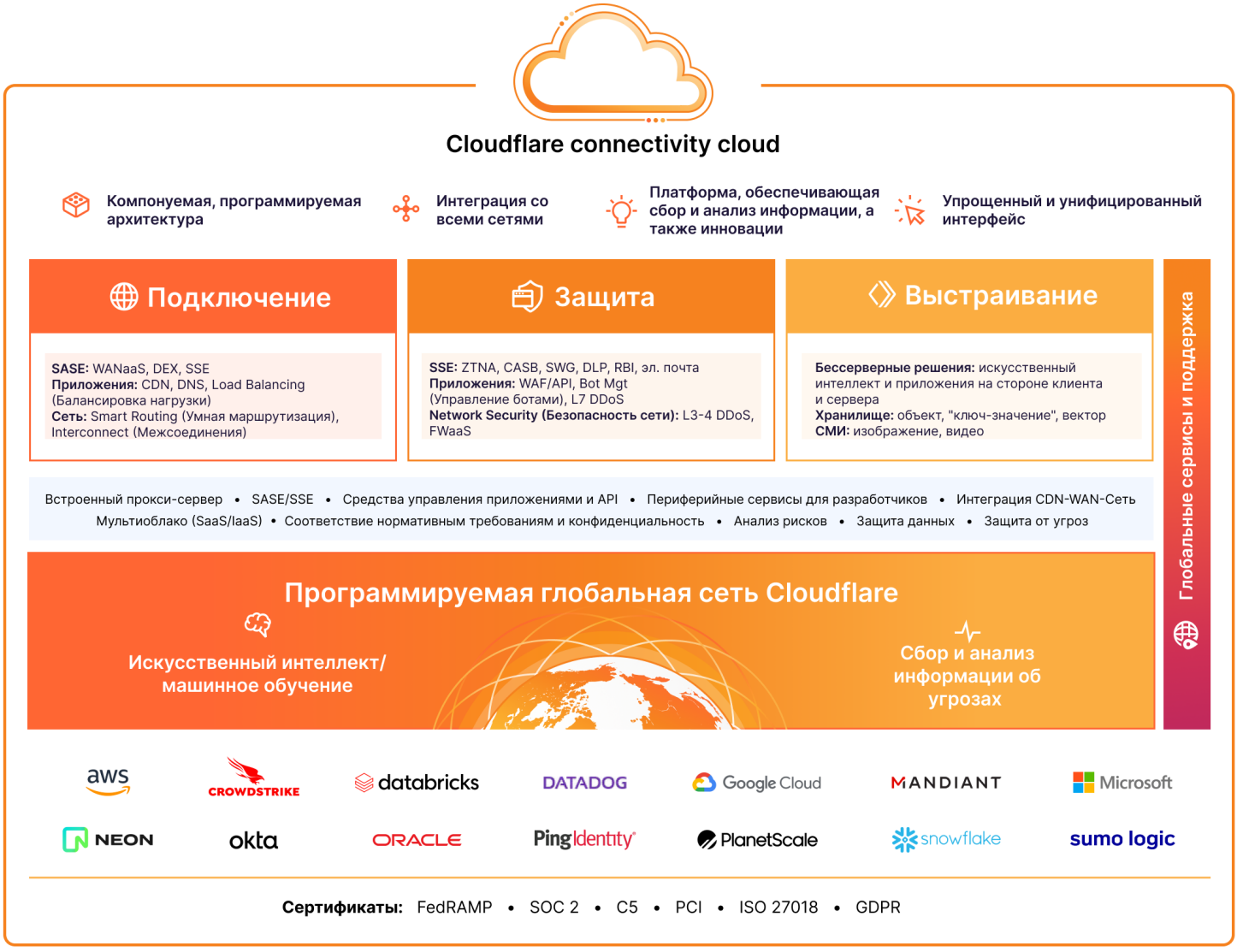


Connectivity cloud от Cloudflare

Рассмотрите возможность использования облака connectivity cloud от Cloudflare для модернизации вашей сети. Оно построено на основе философии использования компонуемой программируемой архитектуры для предоставления сетевых услуг и услуг безопасности всем вашим пользователям, на всех участках облачно-ориентированной бизнес-инфраструктуры и во всех приложениях. В результате облако connectivity cloud учитывает как текущие, так и будущие потребности вашего пути модернизации.

Благодаря Cloudflare вы можете добавлять функциональные возможности и поддерживать новые варианты использования, включая сервисы, а не добавляя устройства. Подключение к центру обработки данных Cloudflare Anycast остается прежним — вы при этом настраиваете и развертываете сервисы из единого интерфейса управления для обработки трафика. Вы можете удовлетворить текущие потребности, одновременно развернув платформу для поддержки будущих вариантов использования и всего процесса модернизации сети.

Используйте нашу глобальную инфраструктуру, вместо того чтобы создавать свою. Ваша организация получит выгоду от молниеносной скорости, обеспечиваемой глобальной сетью Cloudflare. Благодаря прямым соединениям почти со всеми поставщиками услуг и облачными провайдерами, сеть Cloudflare может охватить 95 % пользователей Интернета во всем мире в течение примерно 50 мс.



Ключевые варианты использования модернизации сети

Чтобы начать работу, начните с вариантов использования, которые оказывают влияние на бизнес и приносят наиболее значимую выгоду для вашей организации. Порядок, в котором они перечислены, не особенно важен, поскольку ваши приоритеты уникальны для вашего бизнеса. Тут важно скорее учитывать краткосрочные потребности, а также создавать архитектуру, которая будет поддерживать процесс модернизации вашей сети, независимо от того, какой путь вы выберете.

	Проекты модернизации
Подключение филиалов Сократите затраты, повысьте удобство использования	• Переход от MPLS к connectivity cloud • Переход от SD-WAN к connectivity cloud
Защита своей общедоступной инфраструктуры Расширьте срок отдачи от инвестиций в FW, DMZ	• Сокращение нагрузки на межсетевые экраны сетевого уровня • Перенос защиты DMZ в connectivity cloud
Упрощение корпоративной сети Внедрите Zero Trust для повышения безопасности и снижения капитальных затрат	• Уменьшение DMZ-сегментов или полный отказ от них • Замена VPN на ZTNA • Устранение повышенного доверия в локальной сети (LAN) • Ускорение подключения для слияний и поглощений
Объединение и защита облаков Используйте лучшее из каждого облака в своих приложениях	• Создание и защита приложений • Использование сервисов для разработчиков (для централизации основных функций)

Подключение филиалов

Основным компонентом сетевого взаимодействия WAN является соединение небольших объектов, таких как филиалы или магазины, работа которых зависит от подключения пользователей и устройств к приложениям. Традиционная архитектура на основе звездообразной топологии соединяла объекты с центром обработки данных с помощью дорогих каналов MPLS, но с растущей потребностью в поддержке облачных приложений все больше организаций используют архитектуры с прямым выходом в Интернет и широкополосной связью.

Предполагалось, что SD-WAN обеспечит более высокую надежность сетевого соединения, но ее взаимодействие со средствами обеспечения безопасности несовершенно. Большинство архитектур SD-WAN полагаются на мощные периферийные устройства и локальные межсетевые экраны для обеспечения соблюдения политики безопасности в структуре SD-WAN, а интеграцию SSE/SASE применяют только для исходящего трафика.

Используйте connectivity cloud от Cloudflare для подключения филиалов и поддерживайте полный путь миграции, независимо от того, дополняете ли вы устаревшие сервисы или заменяете их. Cloudflare использует архитектуру, основанную на философии «легкая периферия / тяжелое облако», для предоставления сетевых сервисов и сервисов безопасности. Упростите межобъектное соединение между сетевыми локациями — филиалами, торговыми точками или заводскими цехами — с помощью Magic WAN от Cloudflare. Данное решение обеспечивает безопасное и эффективное подключение и маршрутизацию для всей корпоративной сети, снижая затраты и сложность эксплуатации. В целях обеспечения безопасности Cloudflare Magic Firewall легко развертывается вместе с Magic WAN, что позволяет применять политики управления сетью независимо от направления «север/юг» или «восток/запад» при прохождении трафика через сеть Cloudflare.

Защита своей общедоступной инфраструктуры

К корпоративной сети и DMZ-сегментам можно обращаться из Интернета, поэтому нужны защитные меры, которые будут препятствовать действиям злоумышленников. В идеальном мире традиционные сетевые межсетевые экраны должны проверять и отклонять весь нежелательный трафик, но в реальности каждый экран имеет ограничения (доступная пропускная способность, загруженность вычислительных ресурсов, количество сеансов и т. д.). Успех злоумышленника зависит от масштаба, а именно от того, сможет ли он создать достаточный эффект, чтобы подавить способность компании работать на разных уровнях сетевых протоколов.

И дело не только в объеме трафика. Сам факт наличия входящих каналов открывает поверхность атаки для неаутентифицированного/предварительно аутентифицированного трафика. Недостатками приложений и операционных систем может воспользоваться злоумышленник, даже не имеющий учетной записи в системе. Подстановка учетных данных, использование известных имен пользователей и паролей, полученных в результате других вредоносных действий, также представляет собой серьезный источник риска. Применяя принципы Zero Trust к приложениям в DMZ, организации могут уменьшить воздействие со стороны Интернета и по возможности устранить его.

Организации могут улучшить защиту своей сети, применяя принципы глубоко эшелонированной защиты для поглощения вредоносного трафика от общедоступной инфраструктуры организации. Cloudflare Magic Transit со встроенным Magic Firewall, развернутым через сеть Cloudflare Anycast, действует как «входная дверь» в организацию, фильтруя вредоносный и ненужный трафик и доставляя только чистый входящий трафик.

Когда межсетевые экраны сетевого уровня осуществляют нейтрализацию DDoS-атак на устройстве, соединение все равно необходимо обработать, и только потом оно будет разорвано. С Cloudflare наша сеть транслирует префикс клиента, тем самым притягивая трафик, который в противном случае направлялся бы на межсетевой экран по периметру. Благодаря Anycast мы эффективно поглощаем DDoS-атаки, распределяя нагрузку по всем нашим центрам обработки данных. Участники ботнета видят ближайшую точку присутствия Anycast, который обрабатывает трафик в соответствии с политиками Magic Transit и Magic Firewall.

Упрощение корпоративной сети

Упрощение обеспечивает ряд преимуществ в плане модернизации. Специалисты по ИТ могут сделать сеть более надежной, если в их проекте будет меньше компонентов, которые можно взломать, и более безопасной, применяя подход на основе Zero Trust и полный отказ для привилегий доступа.

Для упрощения вашей сети рассмотрите следующее:

Миграция из DMZ

Сетевые DMZ являются «узким местом» при эксплуатации, поскольку они особенно чувствительны к атакам нулевого дня (zero day). Злоумышленнику не требуется доступ к внутренней сети для связи с серверами в DMZ, поэтому организациям приходится сохранять бдительность, чтобы предотвратить злоупотребления и вредоносные действия.

Однако, хотя DMZ играли важную роль в прошлом, нужны ли они сегодня? Значение DMZ как элемента сетевой конструкции снижается, поскольку существуют альтернативные способы создания и размещения приложений.

- Для общедоступных приложений перенос рабочих нагрузок в общедоступное облако обеспечивает экономические и технические преимущества.
- Благодаря SaaS многие типы общедоступных и приватных приложений вообще не требуют запуска в инфраструктуре, управляемой клиентом.

Таким образом, с точки зрения безопасности и проектирования сети будет разумным задуматься о том, как уменьшить или устранить необходимость в DMZ. Это не только имеет смысл с операционной точки зрения, но и значительно упрощает архитектуру за счет устранения громоздкой сетевой инфраструктуры, такой как межсетевой экран, WAF и балансировщики нагрузки, которые ее поддерживают.

А как насчет приватных приложений, которые размещаются в DMZ для предоставления доступа сотрудникам, партнерам и подрядчикам? Было бы более безопасно изолировать их в приватной сети и предоставить доступ сотрудникам и партнерам, используя сетевой доступ с нулевым доверием (Zero Trust — ZTNA).

С помощью ZTNA можно эффективно уменьшить поверхность атаки, устранив входящий сетевой трафик в приложение. ZTNA использует контекстный доступ на основе брокера к ресурсам через облако connectivity cloud от Cloudflare, тем самым устраняя необходимость открывать порты в межсетевом экране сетевого уровня, одновременно предоставляя команде по ИБ полную информацию о том, кто к какому ресурсу имеет доступ.

Замена VPN на ZTNA

Дни использования VPN для доступа к приложениям сочтены. С точки зрения проектирования сети нецелесообразно привязывать пользователей к очень длинному туннелю для доступа к Интернету и облаку. Кроме того, подключение пользователей (и потенциально скомпрометированных конечных точек) к сети с помощью VPN представляет серьезную угрозу безопасности.

Доступ к приложениям также не является единственной функцией VPN. Существуют сценарии, в которых организациям требуется более широкое сетевое подключение к конечной точке, например при администрировании конечных точек и связи, инициируемой сервером. При таких вариантах традиционно используется сетевое подключение VPN в обоих направлениях, что ставило в тупик первые продукты ZTNA, представленные на рынке. Не имея альтернативы, организации использовали ZTNA и VPN параллельно.

Чтобы модернизировать сетевую инфраструктуру, организации могут консолидировать функции с помощью ZTNA от Cloudflare. Это связано с тем, что с помощью Cloudflare организации могут поддерживать как классические варианты использования ZTNA, так и двунаправленный трафик, инициируемый сервером. Эти функции помогают организациям сократить количество используемых приложений за счет исключения VPN, а также способствуют простоте и повышению безопасности.

Устранение повышенного доверия в локальной сети (LAN)

При гибридной работе становится все меньше различий между работой в офисе и в любом другом месте. И это особенно актуально, когда пользователи часто работают в общедоступных ненадежных сетях, которые встречаются в кафе и общих рабочих пространствах.

В некотором смысле открытая общедоступная сеть является воплощением Zero Trust: никто не имеет привилегированного доступа, и никто или ничто не обладает доверием. Если это в принципе может работать в общем рабочем пространстве, домашнем офисе и кафе, почему нельзя устранить доверие и внутри корпоративной сети?

Устранение доверия не требует усовершенствования инфраструктуры сети, а, скорее, упрощает ее. Вместо того чтобы давать расширенные права доступа пользователям, прошедшим проверку, и использовать сетевые политики при подключении к ресурсам, гораздо безопаснее предположить, что вся сеть ненадежна. Если безопасность строится на базе SASE, организации могут получать доступ к нужным им приложениям с соответствующими мерами безопасности, не требуя какой-либо презумпции доверия к самой сети. Целью Zero Trust является не добавление доверия к сети, а его устранение до тех пор, пока мы не достигнем лучшего и более безопасного состояния без явных и чрезмерных разрешений из прошлого.

Ускорение подключения в случае слияний и поглощений

Организации используют слияния и поглощения для получения доступа к бизнес-ресурсам и возможностям, которые в противном случае были бы недоступны или доступны не сразу. Чтобы извлечь выгоду из этой возможности, организации должны действовать быстро, чтобы объединенная компания стала лучше, чем сумма ее частей. Однако компоненты ИТ не всегда способны к быстрому перемещению, поскольку приложения и базовая сетевая инфраструктура двух организаций редко взаимодействуют друг с другом с легкостью.

Чтобы ускорить подключение в случае слияния или поглощения, организации могут рассматривать доступ к приложениям как задачу, отдельную от сетевой интеграции. График разработки архитектуры конвергентной сети может растянуться на годы, но доступ к приложениям не обязательно должен зависеть от столь отдаленного этапа.

Ситуация в первый день работы фактически является сценарием Zero Trust, когда доверенные пользователи оказались в недоверенной сети, но все равно нуждаются в доступе к приложениям. Расширьте доступ с помощью Cloudflare One, который позволяет подключить новые подразделения не дожидаясь полного объединения сетей.

Объединение и защита облаков

По мере развития облачных технологий компоненты одного облака будут полезны для использования в другом. Точно так же, как со временем каждая организация станет мультиоблачной, со временем каждой организации потребуется управлять общедоступной облачной сетью. Разработка приложений, как правило, носит «родственный» характер, поскольку разработчики в разных подразделениях организации предпочитают инструменты, с которыми они наиболее знакомы. Разработка средств управления подключением между облаками, между тем, является сложной задачей, поскольку работа охватывает наборы инструментов, построенных на совершенно разных платформах.

Другим аспектом сложности мультиоблачных систем является область гибридных облаков. Гибридное облако сочетает в себе локальное частное облако и одно или несколько виртуальных. Такие сети иногда создаются с использованием выделенной сетевой инфраструктуры, такой как AWS Direct Connect, которая может быть дорогостоящей и ограничена только одним облаком.

Создавая мультиоблачные приложения, организации не всегда хотят нести расходы на выделенную сеть для каждого облака.

Вместо того чтобы создавать сетевые каналы (и обеспечивать в них безопасность) непосредственно между приложениями, используйте Cloudflare для организации и подключения общедоступных облачных сетевых сервисов. Мы считаем, что облако connectivity cloud от Cloudflare оптимально подходит для такой архитектуры, поскольку идеально расположено в качестве транзитного узла для трафика, проходящего между облаками через обширную сеть Cloudflare. Благодаря добавлению возможностей управления сетевой инфраструктурой на основе connectivty cloud, клиенты теперь также могут организовывать настройку подключения рабочих нагрузок через Cloudflare.

Наша общедоступная облачная сеть выходит за рамки просто координации базовой системы. Наша архитектура делает еще один шаг вперед, предоставляя сервисы для разработчиков, которые помогают создавать и интегрировать мультиоблачные приложения. Платформа для разработчиков предоставляет обширную экосистему фундаментальных технологий, построенных на основе открытого исходного кода и открытых стандартов. Вы сможете использовать все элементы платформы для разработчиков или только те, которые вы выберете, не ограничиваясь конкретными сервисами в данном облаке.

Следующие шаги

Чтобы сделать следующий шаг на пути к модернизации сети, свяжитесь с Cloudflare, и мы поможем вам разработать стратегию. Мы тесно сотрудничали с тысячами клиентов, когда они переводили свою архитектуру в облако connectivity cloud от Cloudflare.

Подробнее на сайте
http://www.cloudflare.com

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/ru-ru/

REV:BDES-5483.2024JAN30