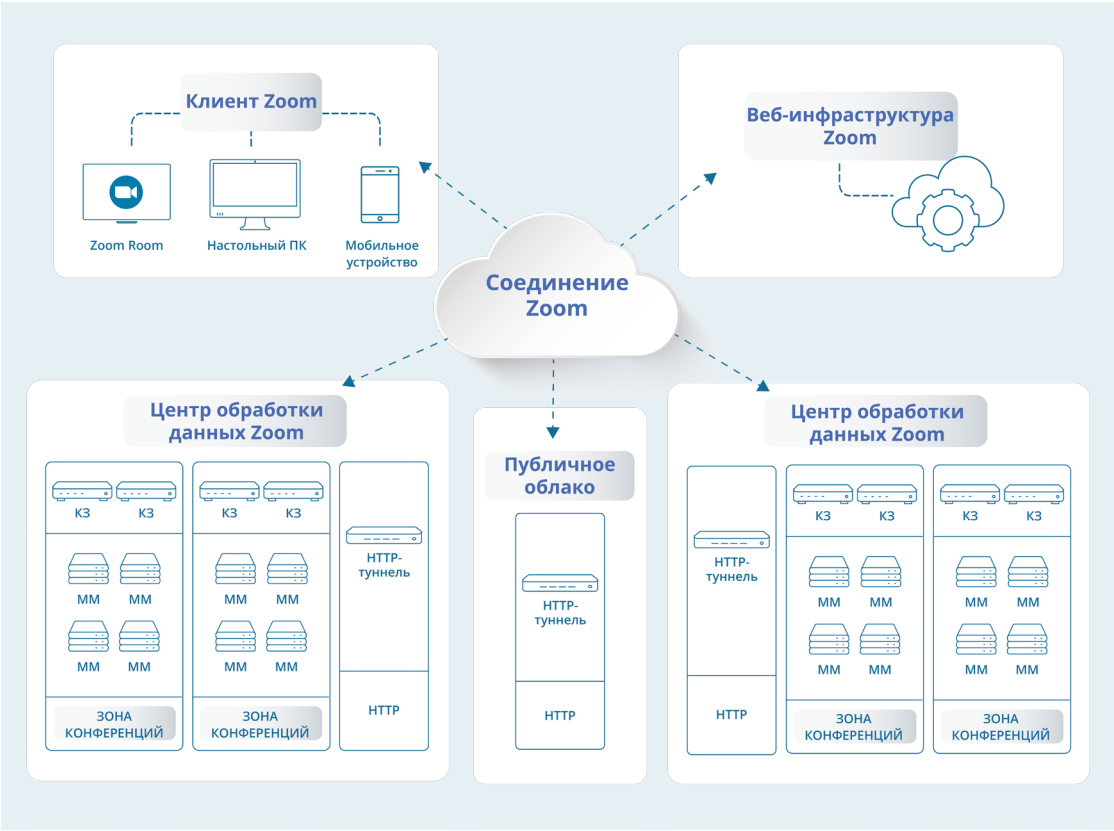
Обзор

Компания Zoom является лидером в области современных средств видеосвязи для предприятий. Одним из продуктов компании является простая и надежная облачная платформа для видео- и аудиоконференцсвязи, чатов и вебинаров, которую можно использовать на различных мобильных и стационарных устройствах, телефонах и конференц-системах. Одно из основных отличий, обусловленных удобством и надежностью облачной платформы, — это процесс подключения Zoom. Процесс подключения Zoom устроен таким образом, что при каждой попытке доступа на платформу система подбирает оптимальный маршрут подключения к географически распределенной инфраструктуре Zoom, обладающей высокой доступностью. В настоящем техническом документе подробно рассматривается этот процесс и стоящие за ним технологии.

Ключевые понятия и компоненты

Прежде чем мы перейдем к рассмотрению процесса, крайне важно познакомиться с ключевыми компонентами, которые используются в процессе подключения, и их ролью в архитектуре Zoom.



Клиент Zoom

Клиент Zoom — это основной способ доступа в облако Zoom, доступный пользователю. Хотя клиент доступен для различных операционных систем (macOS, Windows, Linux, Android, iOS, Chrome OS) и в различных контекстных сценариях использования (мобильные устройства, настольные компьютеры, конференц-системы Zoom Rooms), его схема взаимодействия с облаком Zoom остается неизменной во всех конфигурациях.

Веб-инфраструктура Zoom
Веб-инфраструктура — это интернет-приложение с высокой доступностью, которое не только отвечает за размещение веб-сайта zoom.us, ежедневно посещаемого множеством пользователей, но также помогает обрабатывать запросы приложений с помощью обширных ресурсов API, используемых внешними разработчиками и различными компонентами инфраструктуры Zoom.

Зона конференций Zoom
Зона конференций Zoom — это логическая ассоциация серверов, обычно сгруппированных физически по местоположению и использующихся для размещения сеанса Zoom. Зона конференций Zoom и связанные с ней серверы могут находиться в одном из международных центров обработки данных Zoom или же могут располагаться в сети организации, если Zoom работает в локальном режиме. Основные компоненты зоны конференций — мультимедийные маршрутизаторы и контроллеры зон.

Контроллер зоны Zoom
Контроллер зоны Zoom отвечает за управление и оркестрацию всех действий, происходящих в рамках определенной зоны конференций Zoom. Эти системы развернуты в конфигурациях с высокой доступностью и отслеживают нагрузку на все серверы в зоне, а также выступают в качестве посредников для новых подключений к зоне.

Мультимедийный маршрутизатор (MM)
Мультимедийный маршрутизатор отвечает за размещение конференций и вебинаров Zoom. Как следует из названия, эти серверы следят за тем, чтобы высококачественные голосовые данные, видеопотоки и содержимое были равномерно распределены между всеми участниками определенного сеанса.

HTTP-туннель Zoom
Сервис HTTP-туннелирования является ключевым аспектом стратегии сетевой отказоустойчивости Zoom. Эти серверы размещены в различных публичных облаках и центрах обработки данных Zoom и предлагают точку подключения для клиентов, которым не удалось подключиться к платформе Zoom по другим сетевым каналам. После установления туннеля между клиентом Zoom и HTTP-туннелем Zoom клиент может получить доступ к зоне конференций Zoom в различных центрах обработки данных.

Схема процесса подключения

Процесс подключения к сеансу Zoom можно разделить на четыре этапа, как описано ниже.

Поиск конференции
После получения запроса на присоединение к определенному сеансу клиент Zoom сначала обратится к веб-инфраструктуре Zoom для получения соответствующих метаданных, необходимых для доступа к конференции или вебинару. Используя HTTPS-соединение и порт 443, клиент Zoom произведет оценку текущей сетевой среды, в том числе, проверит наличие прокси-сервера. На другой стороне соединения веб-инфраструктура Zoom подготовит пакет данных, оптимизированных для данного клиента. Благодаря использованию технологии Geo-IP и прочих технологий доставки сервиса Zoom клиенту возвращается перечень оптимальных зон конференций Zoom и связанных с ними контроллеров зон Zoom в совокупности со сведениями о конференции, позволяющими перейти на следующий этап процесса подключения.

Выбор зоны конференции

При наличии списка зон конференций Zoom, способных обслужить клиента Zoom в данном сеансе, процесс подключения переходит на следующий этап. Для подбора наилучшего соединения из доступных клиент Zoom пытается подключиться к каждому контроллеру зоны Zoom в зонах конференций Zoom, полученных на предыдущем этапе, а затем выполняет проверку пропускной способности сети. За счет сравнения результатов клиент может убедиться в наличии сетевых маршрутов для каждой из зон конференций Zoom и выбрать наиболее быстрый из них. Инновационный протокол Zoom использует HTTPS. Попытка установления соединения осуществляется через SSL (порт 443).

Выбор MM

После подбора оптимальной зоны конференций Zoom на предыдущем этапе клиент запрашивает у контроллера зоны Zoom сведения о наиболее подходящем мультимедийном маршрутизаторе (MM). После его определения клиент Zoom обращается непосредственно к MM, чтобы установить канал управления сеансом. Это соединение использует протокол, разработанный компанией Zoom, и выполняет обмен данными через SSL и порт 443.

Маршрутизация медиаданных

При успешном подключении к оптимальному мультимедийному маршрутизатору для сеанса клиент Zoom осуществляет приоритизацию за счет создания соединений для каждого типа передаваемых медиаданных, например видео-, аудиопотоков и содержимого. Каждое из этих соединений для передачи медиаданных пытается использовать собственный протокол Zoom и подключается через UDP и порт 8801. Если такое соединение не удается установить, Zoom попробует подключиться через TCP и порт 8801, а затем через SSL (порт 443). Благодаря использованию различных соединений для передачи каждого типа медиаданных можно применить другие технологии оптимизации сети, например, маркировку DSCP, чтобы обеспечить быструю передачу наиболее важных медиаданных по сети.

Особые случаи

Вышеописанный процесс распространяется на большинство сценариев использования, однако существует несколько исключений, которые были внедрены для установления надежных сеансов связи даже в очень сложных сетях.

Прокси-серверы

На этапе поиска конференции в процессе подключения клиент Zoom может определить наличие прокси-сервера в составе маршрута сетевого подключения. При его обнаружении на этапах выбора зоны конференций и выбора MM в процессе подключения клиент Zoom немедленно использует прокси-сервер и попытается установить соответствующие соединения с контроллером зоны Zoom и мультимедийным маршрутизатором Zoom через SSL.

HTTP-туннель

При отсутствии ответа со стороны контроллера зоны в течение 5,5 секунд клиент Zoom попытается установить подключение через HTTP-туннель. Для создания нескольких маршрутов в целях успешного подключения эти серверы размещаются как в публичных облаках, так и в центрах обработки данных Zoom. Попытка установления соединения осуществляется через SSL (порт 443). Клиент Zoom пропингует несколько HTTP-туннелей и воспользуется первым из ответивших.

Веб-клиент

Если клиент Zoom не сможет подключиться с помощью одного из вышеперечисленных методов, он попросит пользователя подключиться к конференции с помощью веб-клиента Zoom в браузере без загрузки дополнительных плагинов или программ. Веб-клиент Zoom попытается установить соединение через SSL (порт 443).

Заключение

Все большее количество организаций разных размеров ежедневно отдает предпочтение сервисам Zoom. Zoom предлагает несколько маршрутов подключения, использующих различные протоколы в географически распределенной инфраструктуре, для обеспечения надежного соединения для всех пользователей.