EzWAN

Техническое описание · 2026

Архитектура и принципы работы EzWAN

Защищённая распределённая сеть с интуитивно понятным управлением



EzWAN объединяет сети филиалов, ЦОД и облаков через существующие IP-каналы. Контроллер управляет связностью; Edge и Relay передают данные. Документ объясняет архитектуру, модель

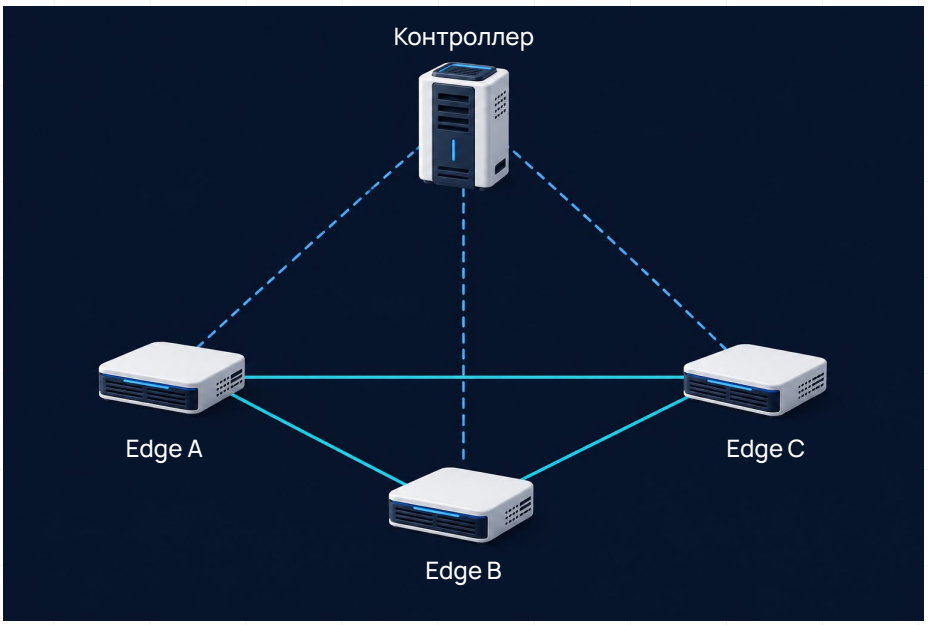
Control Plane · Data Plane

Разделение управления и передачи данных

Централизованный Контроллер отвечает за распространение конфигураций и синхронизацию сведений о топологии сети.

Автономные Edge-узлы бесшовно объеденяют филиалы с помощью защищенного транспорта.

Транзитные Relay-серверы обеспечивают обход NAT с помощью "проксирования" соединений между филиалами без расшифровывания трафика и потери скорости, если прямое P2P-соединение между площадками невозможно или невозможно выполнить NAT Hole Punching



Пунктир — служебные связи. Сплошные линии — передача данных между Edge.

Control Plane

Контроллер

API, конфигурация и топология. Выпуск и обновление сертификатов. Сбор телеметрии и логов.

Data Plane

Edge

Ethernet- и IP-трафик. Защищённые соединения.

Data Plane

Relay

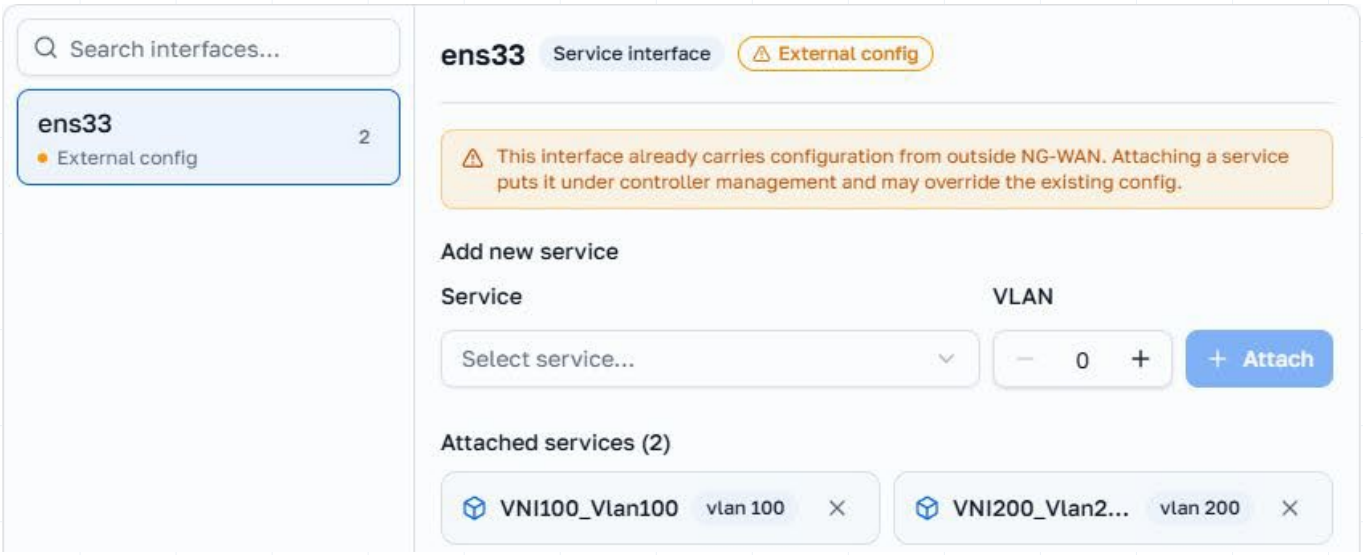
Транзит между Edge без доступа к содержимому данных. Размещается вместе с контроллером или отдельно.

Service · Interface attachment

Один Service — разные локальные VLAN

Service — логический L2-сегмент. Инженер назначает его на интерфейсы выбранных Edge. Локальное значение номера подсети (Vlan) задаётся для каждого подключения и может различаться между площадками.

Площадка	Локальный VLAN	Service
Офис · Edge A	100	Voice
ЦОД · Edge B	333	Voice
Филиал · Edge C	900	Voice



Manage Interfaces: выбор Service, локального VLAN и список назначений интерфейса.

Назначение на интерфейс

После запуска Edge устройства и установления сессии до контроллера, контроллер получает список всех локальных сетевых интерфейсов Edge. Инженер в разделе настроек (Managed interfaces) выбирает интерфейс Edge устройства и настраивает соответствие сервиса локальной подсети (Vlan) данного филиала.

External config

Передача интерфейса для управления контроллеру может изменить его текущие настройки. В случае изменения настроек, система показывает предупреждение, но старается сохранить все текущие настройки интерфейсов, включая маршруты и IP адресацию.

Доступность пути · NAT

Прямое соединение и передача через Relay

При доступном прямом соединении Edge передают данные друг другу. Когда внешняя сеть препятствует такой связи, включая NAT с обеих сторон, Edge устройства запускают механизмы NAT Hole Punching и пытаются построить прямое соединение. Если данный процесс неуспешен, используется промежуточный узел, Relay, гарантированно передающий трафик между Edge устройствами.

01 Прямой путь



02 Через промежуточный узел



Сквозная защита

Relay состыковывает защищённые сессии и передаёт трафик без расшифровки. Содержимое данных доступно конечным Edge.

Behind NAT

Признак задаётся при регистрации Edge. Само наличие NAT не означает, что прямой путь обязательно недоступен: выбор зависит от условий соединения.

Прямой путь и транзит через Relay относятся к Data Plane.

Organisation · Network · Site · Edge · Service

Ключевые объекты управления

Ключевые элементы управления

01 Организация (Organisation)

Верхний уровень иерархии для администрирования сетевых ресурсов компании и разграничения прав доступа.

02 Сеть (Network)

Изолированная оверлейная среда с собственной топологией, набором сервисов и центром сертификации (CA).

03 Площадка (Site)

Точка присутствия (офис, ЦОД или облако). Географический адрес и координаты служат для наглядного отображения на карте.

04 Edge и Сервис (Edge / Service)

Edge выступает шлюзом подключения к транспорту, а Service объединяет ресурсы площадок, на которых он настроен, в единый коммутируемый или маршрутизируемый сегмент.

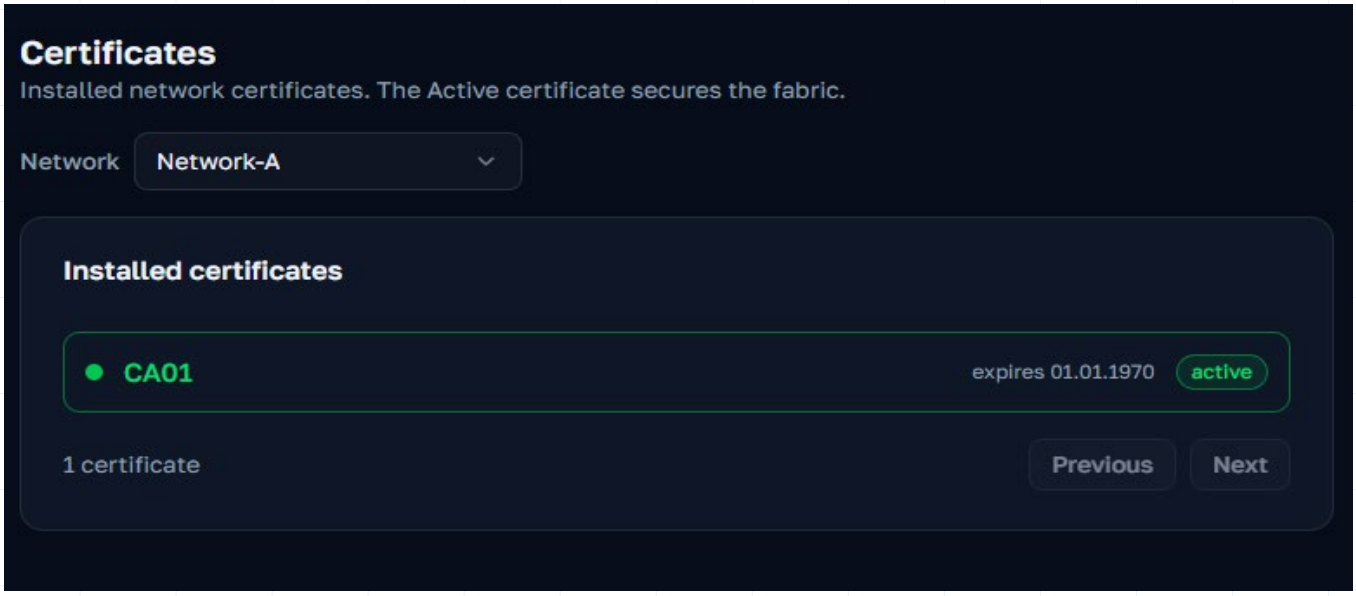
Network CA · Init token · TLS

Сертификаты сети и подключение Edge

Безопасность оверлейной сети строится на собственном центре сертификации (Network CA), который отвечает за аутентификацию всех устройств:

Управление доверием (Network CA)

Для каждой сети можно сгенерировать новый центр сертификации внутри платформы или импортировать существующий ключ и сертификат (в формате PEM). Назначение нового активного CA автоматически обновляет сертификат сети.



Ручное добавление Network CA

Инициализация Edge

Контроллер централизованно выпускает и своевременно обновляет уникальные сертификаты для каждого устройства Edge, обеспечивая их автоматический ввод в эксплуатацию.

Дальнейшая работа

Агент получает индивидуальный сертификат и конфигурацию, взаимодействует с контроллером по TLS и сообщает параметры узла.

Во время первого запуска Edge устройства, в зависимости от его типа (контейнер, аппаратный сервер или докер контейнер) может использовать Init Token для первоначальной настройки и автоматического выпуска сертификата на Edge устройство. Система автоматически управляет сертификатами без ручной работы

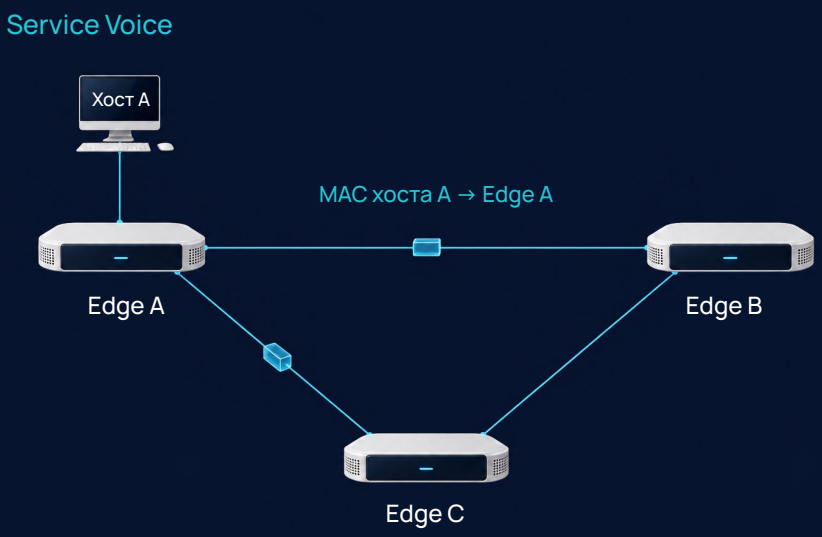
MAC-маршруты · BGP EVPN · Route Reflector

Распространение Control Plane информации

Изучение адресов: При появлении трафика Edge автоматически фиксирует MAC-адреса локальных устройств.

Распространение MAC адресов: Control Plane распространяет выученные MAC-адреса только тем Edge, которые входят в данный сервис через контроллер.

Маршрутизация: На основе полученных таблиц Edge сразу определяет целевой узел для отправки пакетов через защищенный транспорт.



Точечная адресация и изоляция трафика

Привязка MAC -> Edge

Каждая запись строго связывает MAC-адрес устройства с конкретным шлюзом Edge, за которым оно находится. Именно эту информацию удаленные узлы используют для точной отправки Ethernet-кадров.

Строгая изоляция сервисов

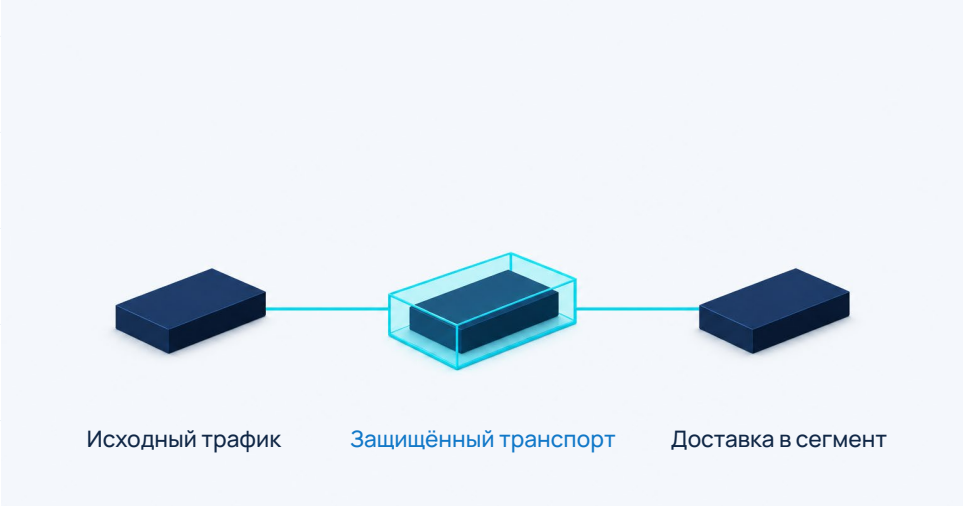
Данные об адресах распространяются только между Edge, входящими в один сегмент. Таблицы маршрутизации разных сервисов полностью изолированы друг от друга.

L2 · L3 · Защищённый транспорт

Инкапсуляция трафика и целостность адресации

Платформа обеспечивает изоляцию и передачу данных без вмешательства в существующую инфраструктуру:

- Универсальный транзит: Edge инкапсулируют локальные Ethernet-кадры и IP-пакеты в защищенные оверлейные сессии, передаваемые по любым внешним каналам связи.
- Прозрачность для приложений: Корпоративная схема адресации сохраняется в неизменном виде — конечным сервисам и оборудованию не требуется перенастройка при работе через EzWAN.



Локальный трафик поступает на Edge, проходит защищённый транспорт и доставляется получателю.

Уровень	Передаваемый трафик	Что сохраняется
L2	Ethernet-кадры в пределах Service	MAC-адреса и принадлежность сегменту
L3	IP-трафик между подсетями площадок	Корпоративная IP-адресация

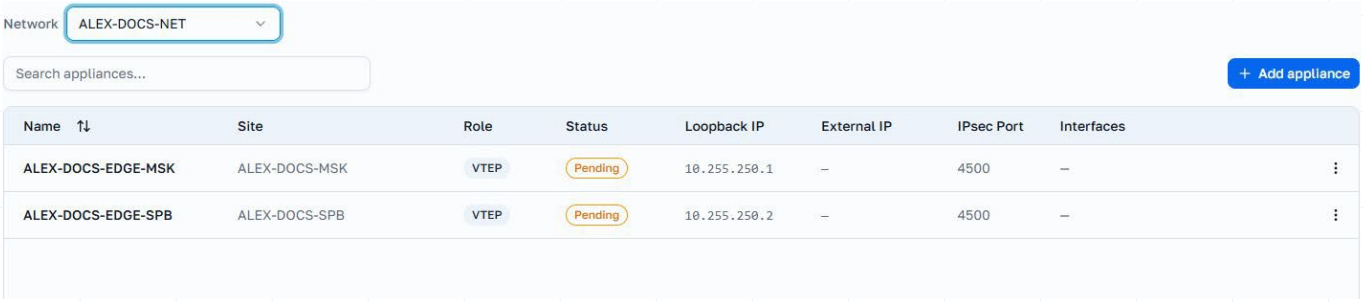
L3-связность

Подсети площадок объединяются поверх общего защищённого контура. Адреса внутренних устройств не заменяются адресами внешнего транспорта.

Прозрачная работа с MTU: Внутри сетевого сегмента можно использовать стандартный размер кадра. EzWAN берёт на себя фрагментацию и сборку пакетов, делая этот процесс полностью невидимым для конечного оборудования.

Appliances · Dashboard · Телеметрия

Все этапы регистрации Edge устройства и соответствующие состояния отслеживаются контроллером



Средства контроля и разбора инцидентов

Состояние узла: Проверка принадлежности Edge к конкретной сети и площадке, а также текущего статуса активности. Доступность устройства по служебному каналу непрерывно контролируется протоколом Keepalive.

Сервисная связность: Валидация привязки обнаруженных интерфейсов к назначенным сервисам и контрольное тестирование передачи данных между участниками сегмента.

Анализ телеметрии: Расследование сетевых событий на основе системных параметров, эксплуатационных метрик и логов Edge.

Координаты Site нужны для отображения Edge устройств в соответствующих филиалах на географической карте.

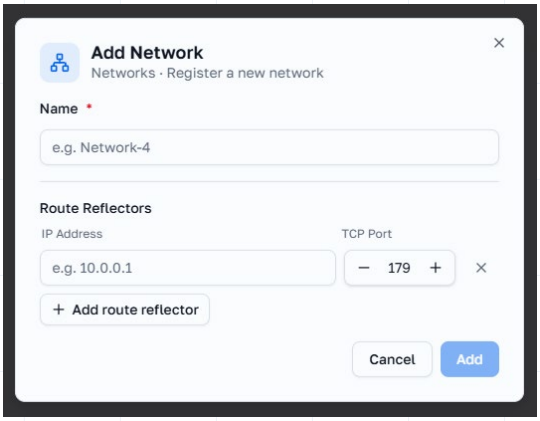
Отдельный компонент Data Plane

Relay: размещение и регистрация

Relay может работать на одном узле с контроллером или отдельно. На контроллере он регистрируется как Appliance с ролью RELAY.

По умолчанию Relay оставляется в составе контроллера





Форма регистрации Relay. Для Edge используется роль

Управление

Контроллер хранит конфигурацию и сведения об узлах. Совместное размещение компонентов не меняет разделение их функций.

Передача данных

Relay пересылает защищённый трафик между Edge при недоступности прямой связи и не получает доступа к содержимому.

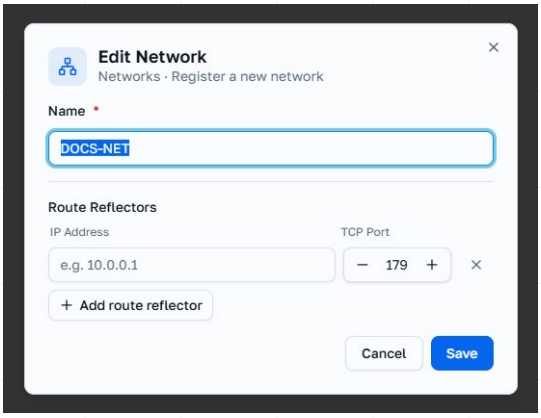
Network и CA → Site и регистрация узлов → запуск агента → Service на интерфейсах → проверка связи

Настройка · Рабочая область и сертификаты

Создание сети и привязка CA

- Авторизуйтесь в консоли контроллера и выберите нужную Организацию.
- В разделе Networks создайте оверлейную сеть.
- Перейдите в раздел PKI и выберите созданную сеть для настройки инфраструктуры ключей.

Все последующие сертификаты устройств и параметры конфигураций будут формироваться строго в контексте выбранной сети.



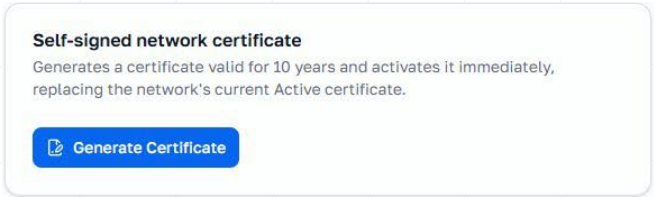
Edit Network: имя сети и параметры Route Reflectors.

01 · Network

Задайте имя сети. При необходимости укажите адрес и TCP-порт Route Reflector. В показанной реализации он размещён вместе с контроллером.

02 · Генерация CA

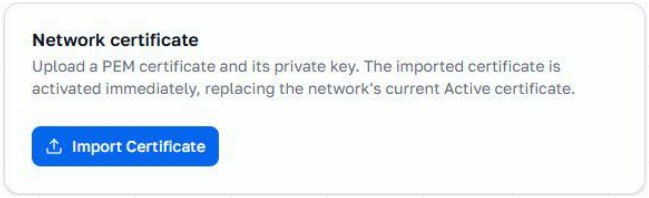
В PKI → Generate Certificates выберите Network и создайте её сертификат.



Generate Certificates

Или импорт CA

В PKI → Import Certificates выберите Network и загрузите certificate PEM вместе с private key PEM.



Import Certificates

Генерация и импорт активируют новый сертификат, заменяя текущий активный сертификат Network. Перед применением проверьте выбранную сеть.

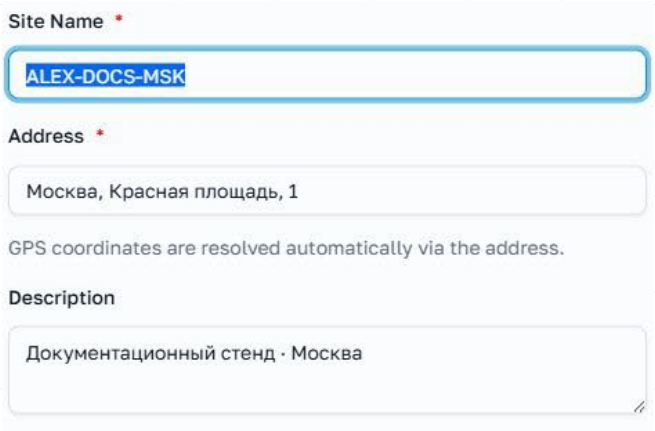
Настройка · Site, Appliance и init token

Регистрация Edge

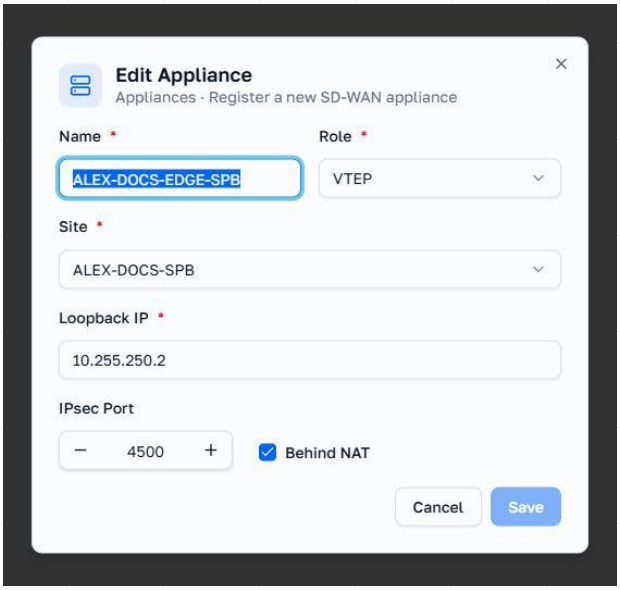
Создайте площадку в Sites. Затем в Appliances выберите Network и зарегистрируйте Edge. Для подключения реального устройства воспользуйтесь рекомендациями системы для установки и настройки Edge устройства

01 · Площадка

Укажите имя и адрес Site. Координаты определяют положение на карте.



02 · Параметры Edge



Имя, роль VTEP, Site, loopback IP, IPsec Port и признак Behind NAT.

Поля Site и Edge показаны на формах редактирования созданных тестовых

03 · Запуск Edge

Контроллер показывает init token однократно. Передайте его установщику или агенту на сервере либо VM будущего Edge, используя инструкцию из пакета поставки.

04 · Подключение

Агент регистрируется, получает индивидуальный сертификат и конфигурацию. Проверьте состояние Edge и появление переданных им интерфейсов в Edges.

Созданная запись Edge остаётся Pending до подключения Edge. Init token используется на стороне Edge; сертификат CA импортируется отдельно через PKI.

Настройка · Service, интерфейс и локальный VLAN

Назначение Service на интерфейсы Edge

В Services выберите Network и создайте сегмент. После подключения Edge откройте Manage Interfaces нужного Edge: назначение Service связывает локальный интерфейс с общим L2-сегментом.

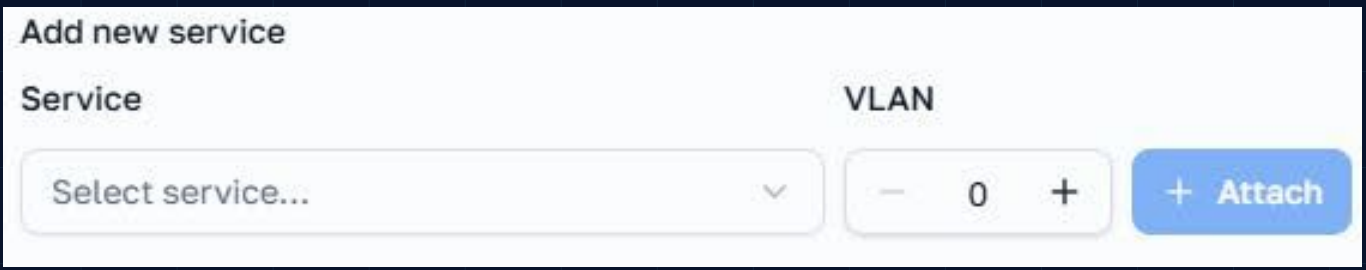
01 · Создать сегмент

Задайте имя и описание Service. Например, отдельные сервисы для телефонии и видеонаблюдения.

Name ↑↓	Description
ALEX-DOCS-VOICE	Корпоративная телефония между площадками
ALEX-DOCS-CCTV	Видеонаблюдение между площадками

02 · Подключить интерфейс

Выберите интерфейс, Service и локальный VLAN, затем нажмите Attach. Повторите на нужных Edge; номера VLAN могут различаться.



Manage Interfaces: Service и VLAN задаются для выбранного интерфейса Edge.

External config: подключение Service передаёт интерфейс под управление контроллера и может изменить его действующую конфигурацию.

03 · Проверить результат

Сверьте состояние Edge, интерфейсы и назначения Service. Проверьте передачу трафика между участниками сегмента.

Network и CA → Site и Edge → Service и интерфейсы → проверка

EzWAN: Архитектурная гармония вашей сети

Платформа создает гибкую виртуальную сеть поверх существующей IP-инфраструктуры, избавляя от необходимости выбирать между удобством управления и надежностью:

- Управляемость без компромиссов: Контроллер обеспечивает сквозную синхронизацию настроек и актуальную картину сети из одной точки — от локальных офисов до облачных ресурсов.
- Нативная устойчивость: Edge-устройства строят кратчайшие маршруты, а при необходимости подключают транзитные узлы, сохраняя доступность сервисов при любых колебаниях каналов.
- Единый технологический фундамент: Сочетайте прозрачные L2-сегменты и передачу IP-трафика между площадками, дата-центрами и публичными облаками без привлечения сторонних инструментов.
- Операторская независимость: Объединяйте каналы разных провайдеров и облачные подключения в устойчивый и экономически выгодный транспорт.

Контакты

info@ezwan.ru

+7 (495) 477-88-85

https://ezwan.example

Открыть сайт