

# Kaspersky SD-WAN

Комплексное решение  
для построения надежной  
и безопасной  
корпоративной сети



# Оглавление по темам

# Оглавление

01



01 Коротко о SD-WAN

02 Особенности корпоративных сетей

03 Решение Kaspersky SD-WAN

04 Возможности решения

05 Политика лицензирования

06 Kaspersky SD-WAN в концепции SASE

# Технология SD-WAN

SD-WAN — это решение для построения распределенных сетей, которое состоит из:



Специальных  
маршрутизаторов  
(SD-WAN CPE)

Устанавливаются  
на объектах компании  
(например, в филиалах)



Интеллектуальной  
системы  
управления

Устанавливается в ЦОД или  
головном офисе

## SD-WAN обеспечивает

Быстрое подключение  
новых объектов

Надежность сетевых  
подключений

Упрощенную  
миграцию в облако

Упрощенное  
управление сетью

Поддержку различных  
каналов связи  
и их комбинаций

Централизацию  
политик  
безопасности  
и сетевых настроек

Безопасную работу распределенных команд

# Рынок SD-WAN

SD-WAN заменяет традиционный подход к построению сети и стандартные маршрутизаторы

Основные драйверы

Стоимость

Доступность

Безопасность

Производительность

Облачные приложения

40%

крупных компаний  
внедрят решения  
SD-WAN и облачные  
SWG к 2025 году

20%

CAGR рынка SD-WAN  
в ближайшие 3 года

# Цифры говорят больше слов

40%

Компаний с распределенной сетью испытывают проблемы с сетью не меньше двух раз в месяц

82%

Компаний тратят больше одного часа для восстановления сетевой связности

69%

Компаний задействуют HQ команды для IT и ИБ поддержки на местах

12%

Из них тратят больше одного рабочего дня



01 Коротко о SD-WAN

02 Особенности корпоративных сетей

03 Решение Kaspersky SD-WAN

04 Возможности решения

05 Политика лицензирования

06 Kaspersky SD-WAN в концепции SASE

# Успех современного бизнеса – это гибкость

Сегодня для успешных компаний важно быстро адаптироваться к новым условиям.

Гибкий формат работы и достижение целей с помощью географически распределенных команд – современная реальность.

Скорость развития бизнеса, удобство работы сотрудников и надежность процессов тесно связаны и важны как никогда ранее.



# Проблемы традиционных сетей

9

## Недовольные клиенты и сотрудники

Задержки сетевых  
подключений

Плохое качество работы  
приложений

Длительное устранение  
проблем

## «Дыры» в сетевой безопасности

Отсутствие единой политики  
безопасности

Незащищенные домашние  
офисы

Большое количество  
разрозненных средств защиты

## Затраты на поддержку и обслуживание

85% изменений в сети  
настраивается вручную

Долго

Дорого

Не оптимально

# Автоматизация и технологии



## Автоматизация

Активно расти без автоматизации и обеспечения безопасности корпоративной сети стало невозможно



## Технологии

Программно-определяемые технологии помогут решить проблемы традиционных сетей и позволят вам сосредоточиться на бизнес-целях



# Оглавление

# 03



- 01 Коротко о SD-WAN
- 02 Особенности корпоративных сетей
- 03 Решение Kaspersky SD-WAN
- 04 Возможности решения
- 05 Политика лицензирования
- 06 Kaspersky SD-WAN в концепции SASE

Комплексное решение  
для построения надежной  
и безопасной корпоративной сети

# Зачем Kaspersky SD-WAN бизнесу?



**Быстрое подключение  
новых офисов и точек продаж**  
с использованием существующих  
каналов связи



**Управление  
и мониторинг всей сети**  
через единый веб-интерфейс



**Простая  
интеграция**  
решений сетевой  
безопасности  
и облачных сервисов



**Обеспечение  
гарантированного качества**  
передачи данных критических  
приложений



**Контроль используемых  
приложений в сети**  
и централизованная политика  
безопасности



**Использование  
отечественных  
аппаратных платформ,**  
входящих в реестр ТОРП  
Минпромторга России

# Технологическая концепция Kaspersky SD-WAN

Единое управление



Гибкая архитектура

Возможности

- Автоматизация
- Мониторинг
- Аналитика

Свойства

- Открытая
- Программируемая
- Масштабируемая

Развертывание

- On-premise
- Cloud
- Multi-tenant

Широкий набор возможностей



Простота  
и надежность  
технологий



Встроенное  
шифрование  
трафика



Легкая  
интеграция  
средств защиты



Интеллектуальное  
управление  
трафиком



Оптимизация  
для голоса  
и видео



Готовность  
к интеграции  
облачных  
сервисов

Любые каналы связи

Ethernet

MPLS

Спутник

L2TP

4G / LTE

Быстрое подключение



Филиалы и точки продаж

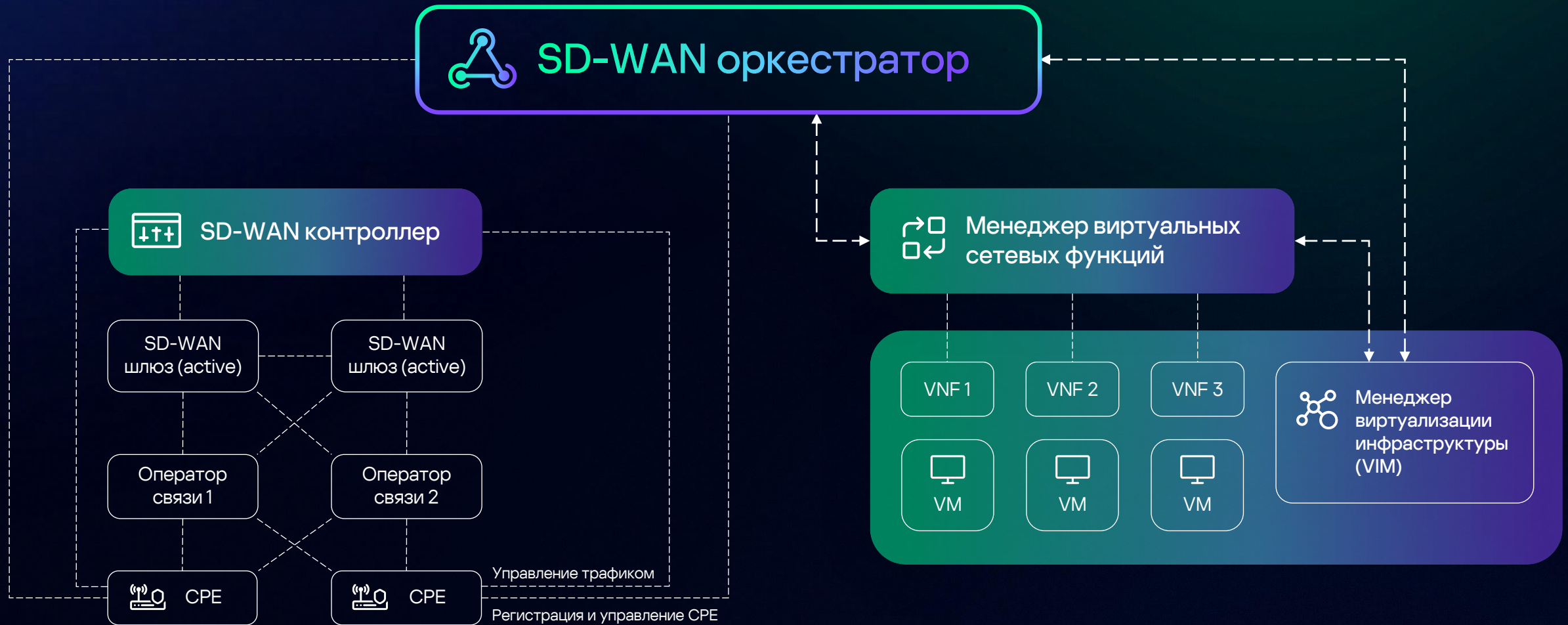


ЦОД

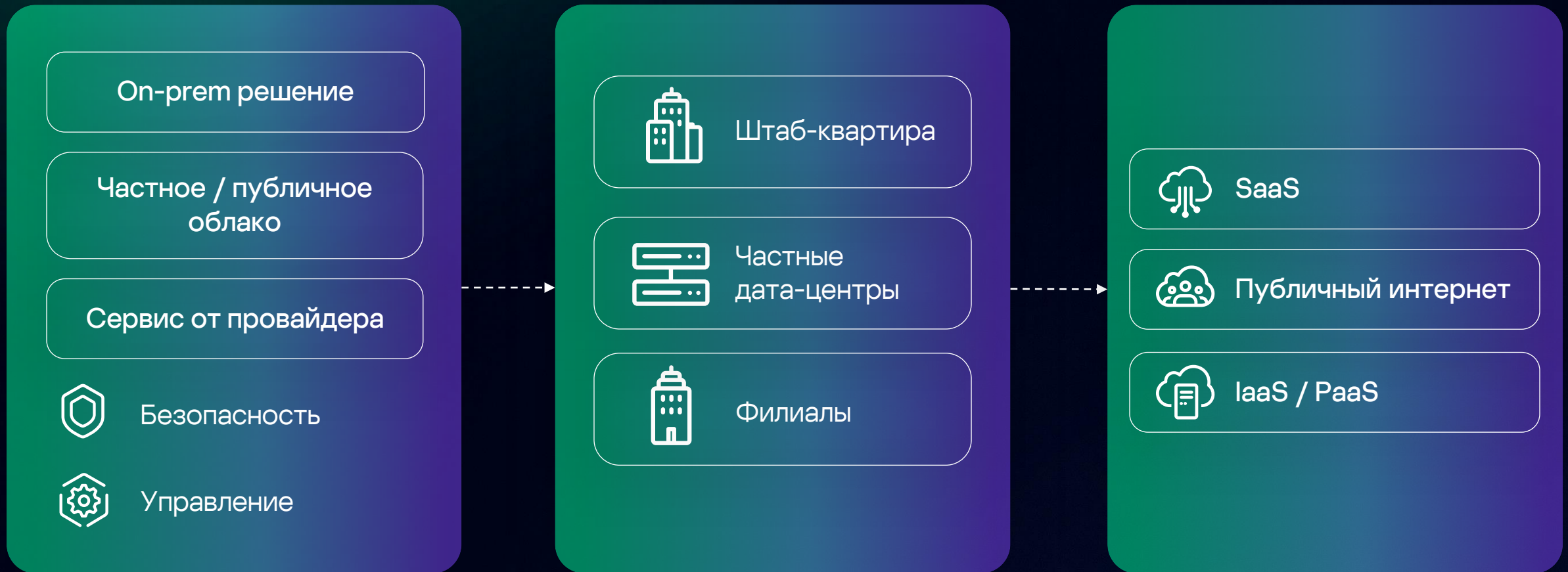


Облака

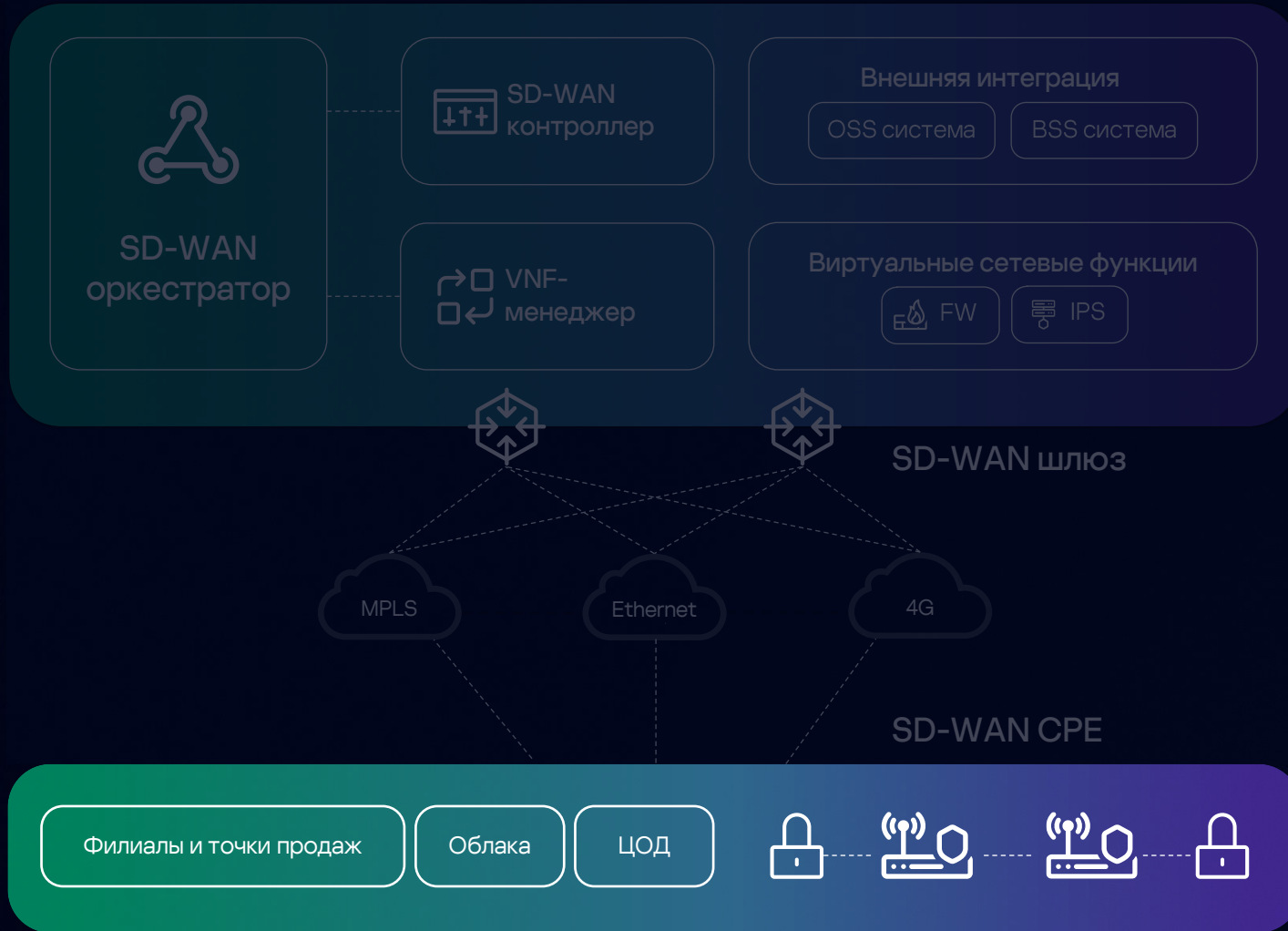
# Архитектура Kaspersky SD-WAN



# Гибкая архитектура – различные сценарии развертывания



# Передача данных



## SD-WAN CPE

Оперативное подключение удаленных площадок к корпоративной сети

Физическое или виртуальное оборудование

Защищенная передача данных и встроенное шифрование

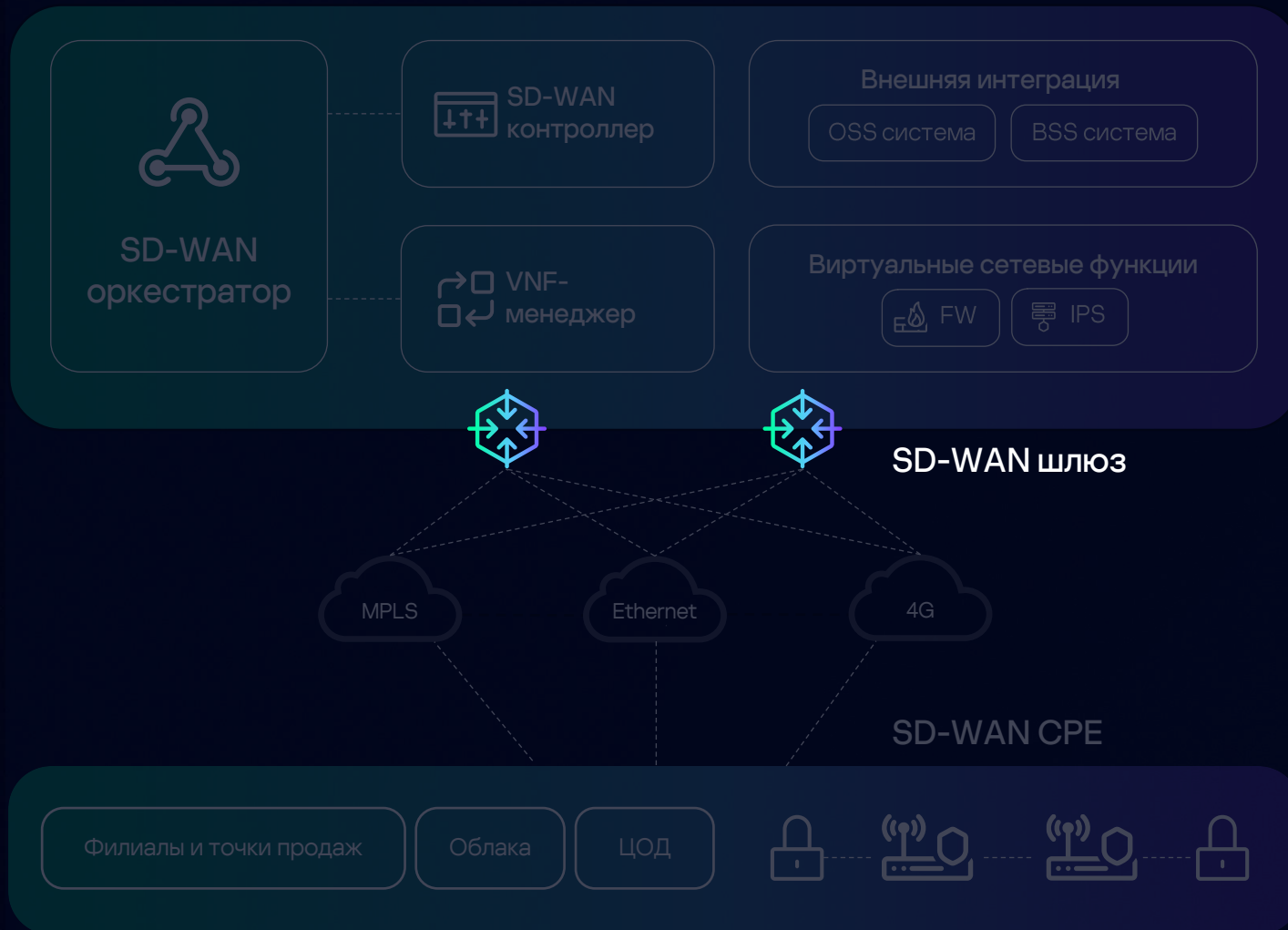
Соблюдение политик маршрутизации и безопасности

Сбор и экспорт информации для систем мониторинга

Поддержка быстрого развертывания Zero Touch Provisioning

Проводное и беспроводное подключение пользователей

# Передача данных



## SD-WAN шлюз

Гибкие возможности организации сетевой связности

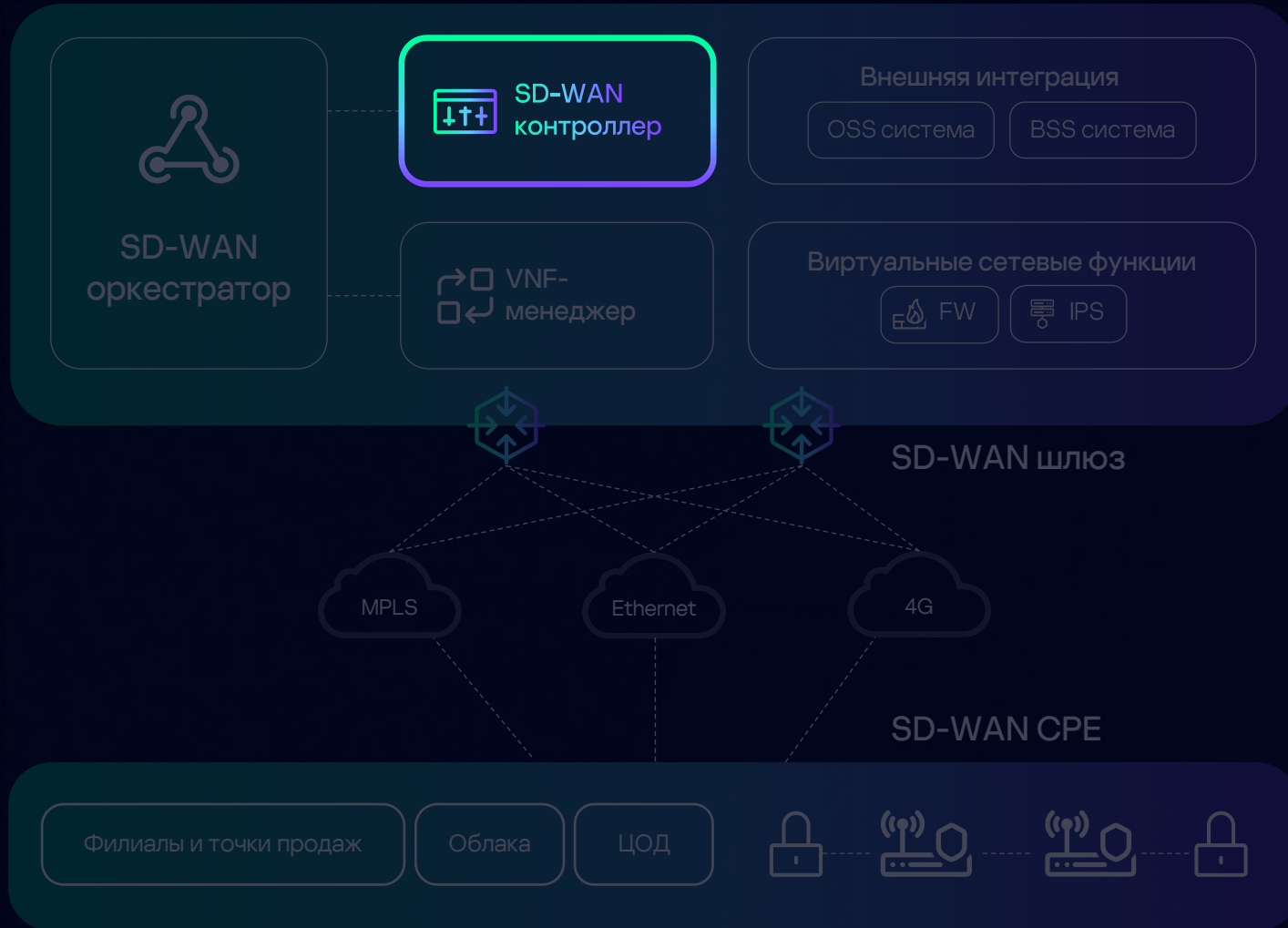
Физическое или виртуальное оборудование

Установка в центрах обработки данных, центральных офисах, частных и публичных облаках

Агрегация защищенных туннелей от SD-WAN CPE

Отказоустойчивое развертывание

# Централизованные политики безопасности и маршрутизации



## SD-WAN контроллер

Централизованное управление сетевыми устройствами, каналами связи и трафиком

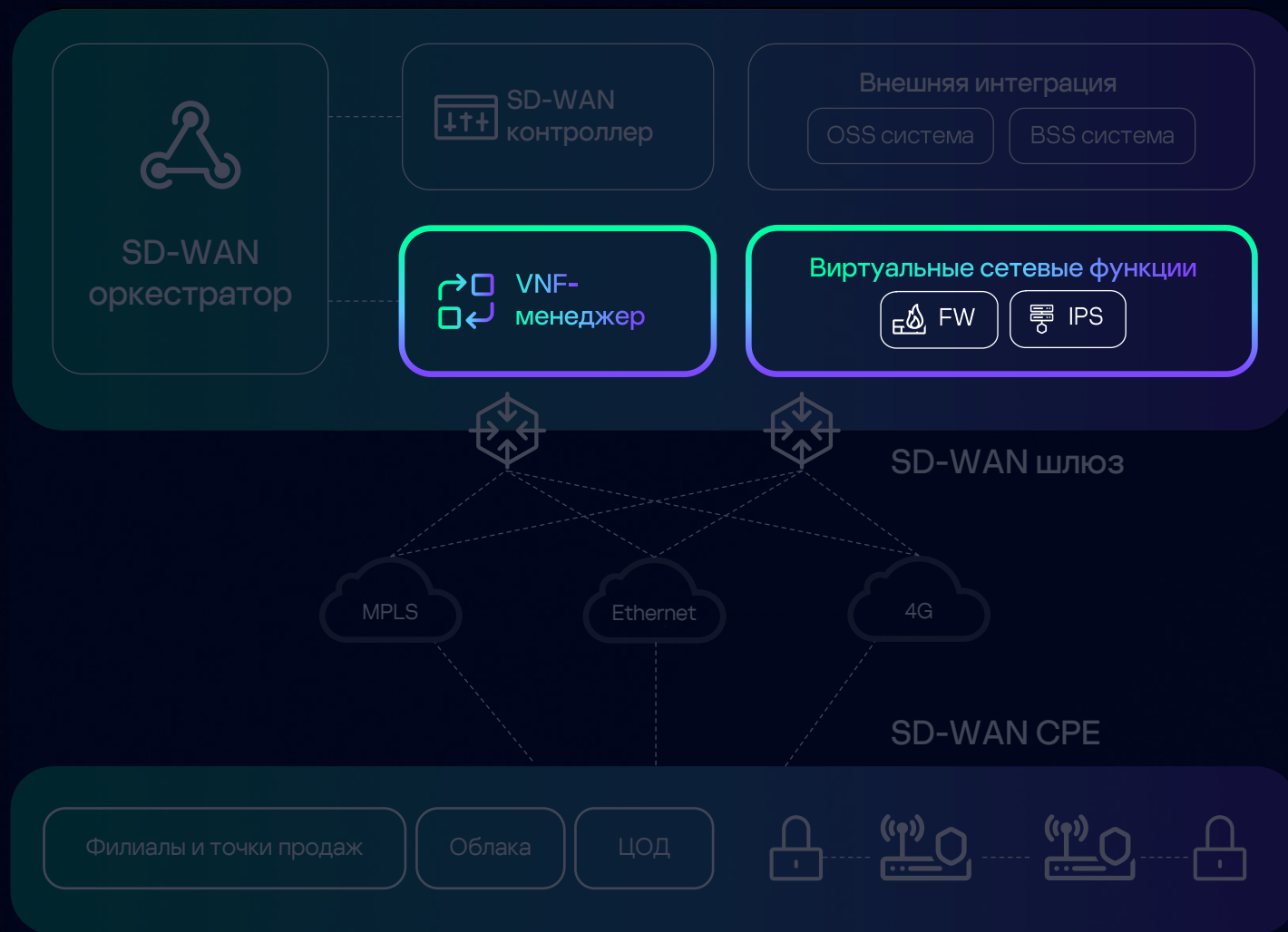
Виртуальная машина

Отказоустойчивое развертывание

Управление SD-WAN CPE:  
настройка маршрутизации,  
обработки трафика, политик  
безопасности

Основной интерфейс  
взаимодействия между SD-WAN  
CPE и плоскостью управления

# Виртуализация сетевых функций



## VNF-менеджер

Полный контроль  
жизненного цикла  
сетевых функций

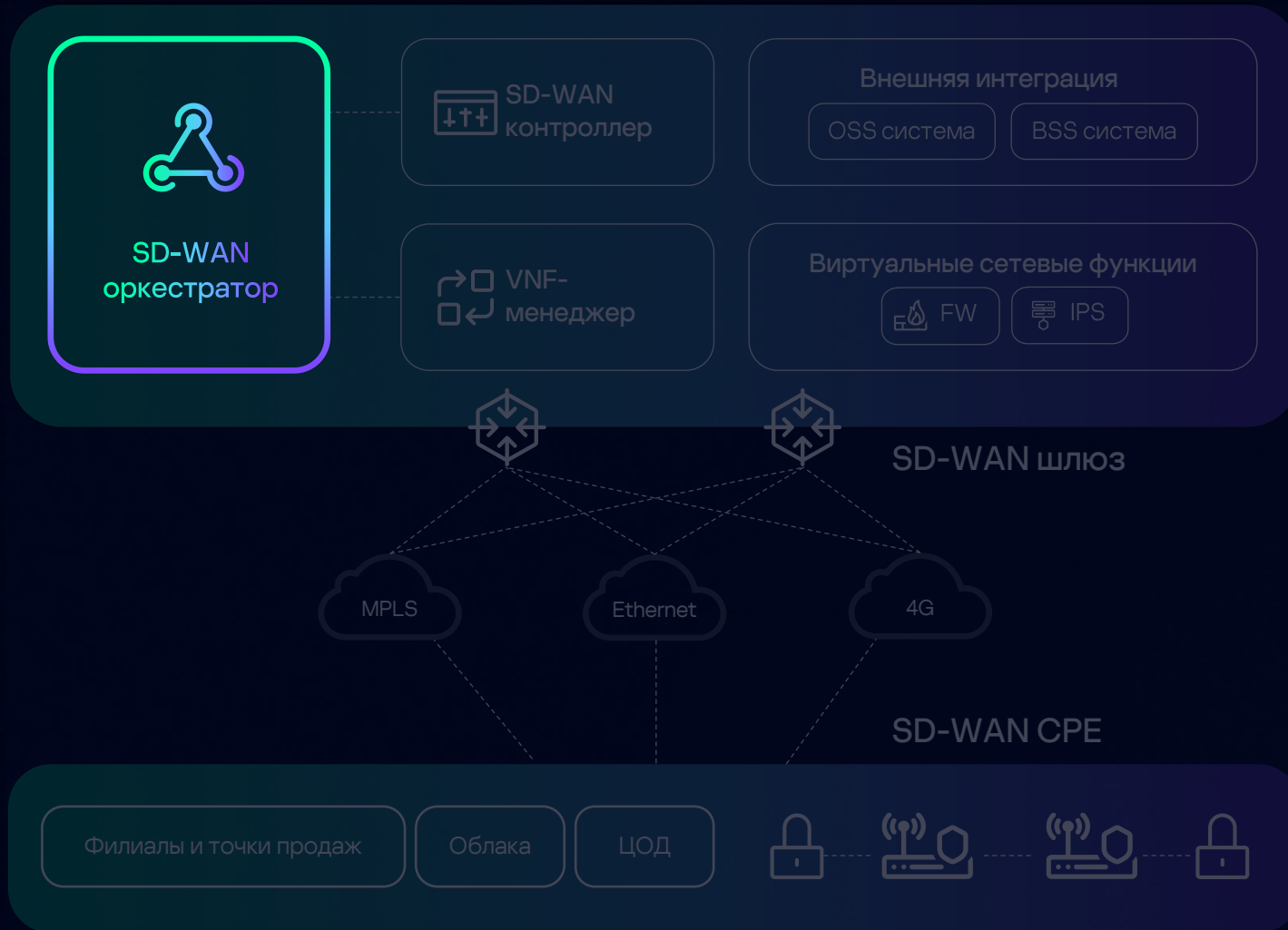
Виртуальная машина

Отказоустойчивое  
развертывание

Управление сетевыми функциями

Контроль инсталляции,  
активации, масштабирования,  
обновления и терминирования  
виртуальных сетевых функций

# Единая панель управления и оркестрации



## SD-WAN оркестратор

Единое окно взаимодействия со всеми компонентами решения

Виртуальная машина

Отказоустойчивое развертывание

Управление контроллерами и виртуализацией

Единый графический и API-интерфейсы для взаимодействия со всеми компонентами решения

Сбор, хранение и визуализация информации о состоянии сети SD-WAN

Запуск шаблонов сервисных цепочек, обеспечение виртуализации и контроля ресурсов, управление лицензиями

# Преимущества SD-WAN



## Быстро

Подключение филиалов благодаря технологии Zero Touch Provisioning не требует настройки устройств и происходит автоматически



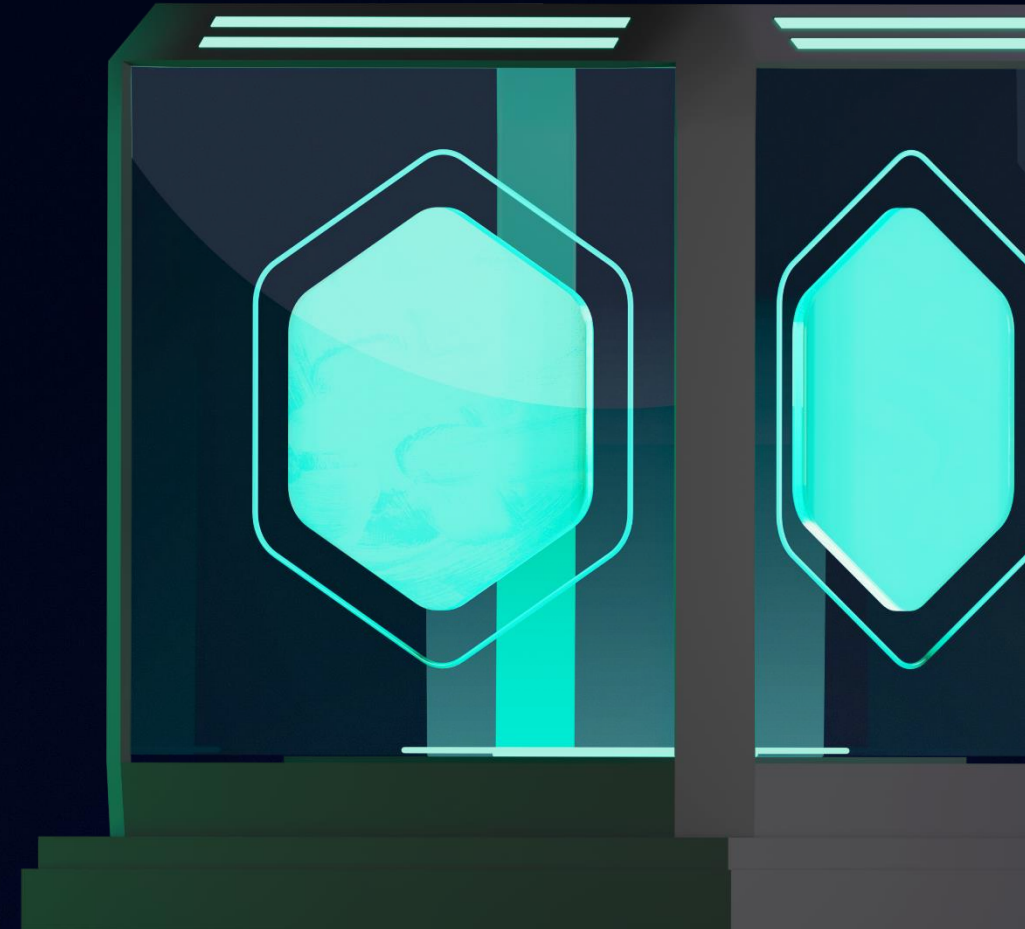
## Просто

Единый интерфейс управления, контроля маршрутизации и настройки политик безопасности для сети любого масштаба



## Удобно

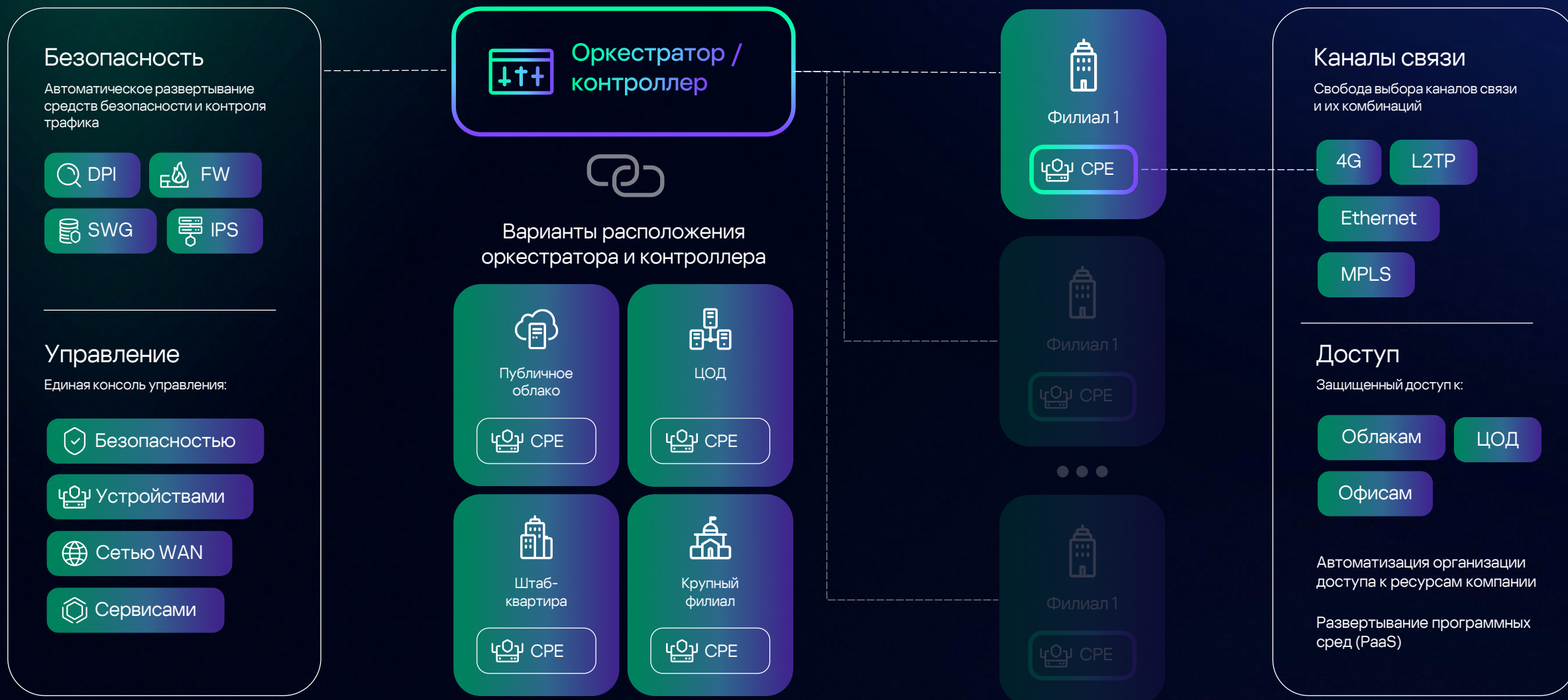
Встроенные интеллектуальные механизмы обработки трафика и качества обслуживания для оптимизации работы приложений без дополнительных затрат



# Пример внедрения Kaspersky SD-WAN



# Просто о Kaspersky SD-WAN



# Подключение Kaspersky SD-WAN – это быстро

1

Разверните центральные компоненты решения в ЦОД или головном офисе

2

Доставьте CPE на объект (например, в филиал)

3

Подключите CPE к электросети и любым каналам связи для доступа к контроллеру

4

Решение готово к использованию. Настройки применятся автоматически

# Что такое Kaspersky SD-WAN сегодня



## Простая масштабируемость

Адаптируйте сеть к постоянно меняющимся потребностям бизнеса, легко подключая новые офисы и сетевые устройства



## Легкое управление

Управляйте всей филиальной сетью из единой консоли, изменяя настройки доступа и политики безопасности в любое время



## Оптимизация расходов

Сократите расходы на построение и обслуживание сети, используя любые доступные каналы связи и их комбинации



## Централизованная безопасность

Легко подключайте виртуализированные средства защиты и контроля трафика в режиме автоматического развертывания



## Важное преимущество

Kaspersky SD-WAN позволяет легко интегрировать средства защиты «Лаборатории Касперского» и других производителей

# Классические WAN сети и SD-WAN

## Классические WAN сети

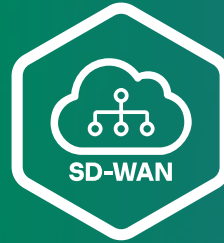
Долгое подключение новых офисов

Необходимы дорогие MPLS каналы

Каждое сетевое устройство управляется отдельно

Необходимы специалисты в каждом филиале

Бреши в безопасности



## Kaspersky SD-WAN

Быстрое подключение объектов благодаря Zero Touch Provisioning

Надежные соединения даже на нестабильных каналах связи

Централизованное управление всей сетью

Достаточно одного специалиста для управления

Единые политики безопасности

Простая интеграция средств защиты и сетевых сервисов

# Комплементарные продукты и решения



## Kaspersky Security для интернет-шлюзов

Защищает инфраструктуру организации от угроз из интернета



## Kaspersky Unified Monitoring and Analysis Platform

SIEM-система, которая повышает прозрачность инфраструктуры и усиливает эффективность мер защиты



## Kaspersky Anti Targeted Attack

XDR-платформа нативного типа: современная защита от сложных кибератак



## Kaspersky Industrial CyberSecurity

Специализированная промышленная XDR-платформа для комплексной защиты предприятий различных индустрий



## Kaspersky Managed Detection and Response

Непрерывный поиск, обнаружение и устранение угроз, направленных на ваше предприятие



## Kaspersky Services

Широкий набор сервисов, которые повышают уровень безопасности компаний



## Kaspersky Professional Services

Получите максимум преимуществ от продуктов «Лаборатории Касперского»

# Оглавление

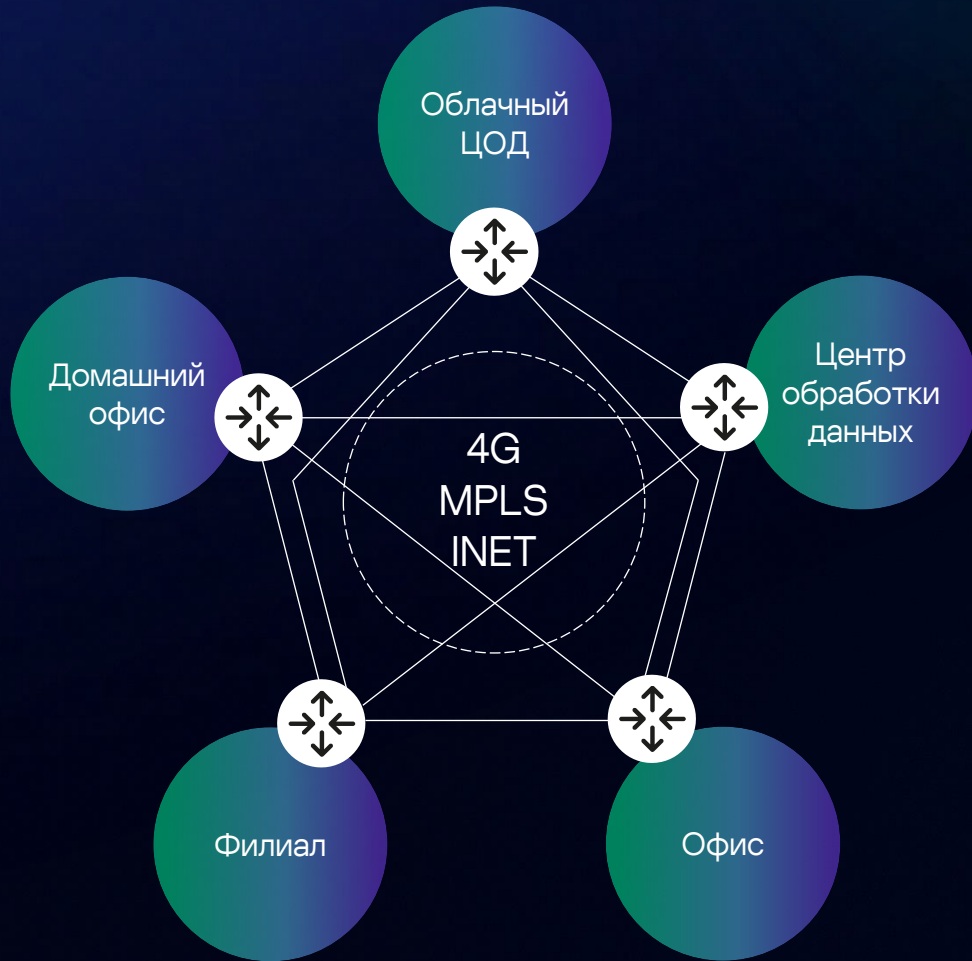
# 04



- 01 Коротко о SD-WAN
- 02 Особенности корпоративных сетей
- 03 Решение Kaspersky SD-WAN
- 04 Возможности решения
- 05 Политика лицензирования
- 06 Kaspersky SD-WAN в концепции SASE

# Идентификация используемых приложений и единая политика безопасности

# Идентификация трафика приложений: встроенный DPI



## Идентификация трафика в реальном времени



Telegram

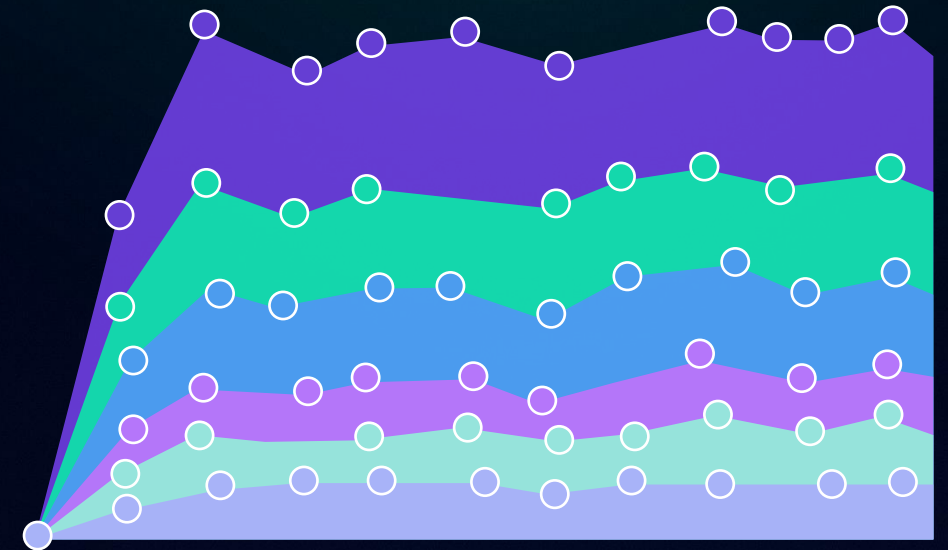
Google

Steam

Xiaomi

Outlook

Youtube



Улучшение качества  
голосовых и видео звонков  
без дополнительных вложений  
в расширение каналов связи

# Маршрутизация на основе качества каналов связи

## Преимущества

Возможность выбора предпочтительного канала для каждого конкретного приложения

Контроль задержки, джиттера и уровня потерь для каждого канала связи в реальном времени

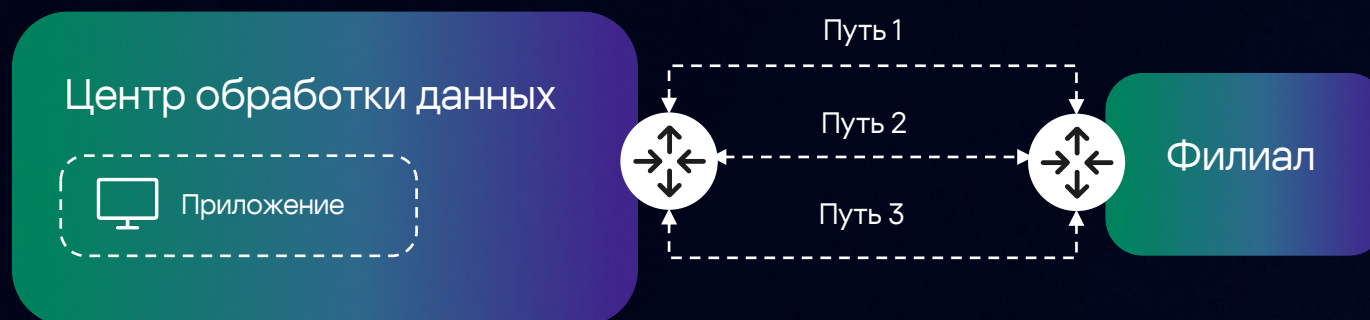
Политики на основе SLA могут использоваться для выбора оптимального маршрута критически важных приложений и динамического переключения маршрута в случае, если эти SLA не выполнены

Поддержка соединений в режиме active / active

Балансировка трафика между каналами

## Контроль качества канала для приложения

задержка <150 ms, потери <2%

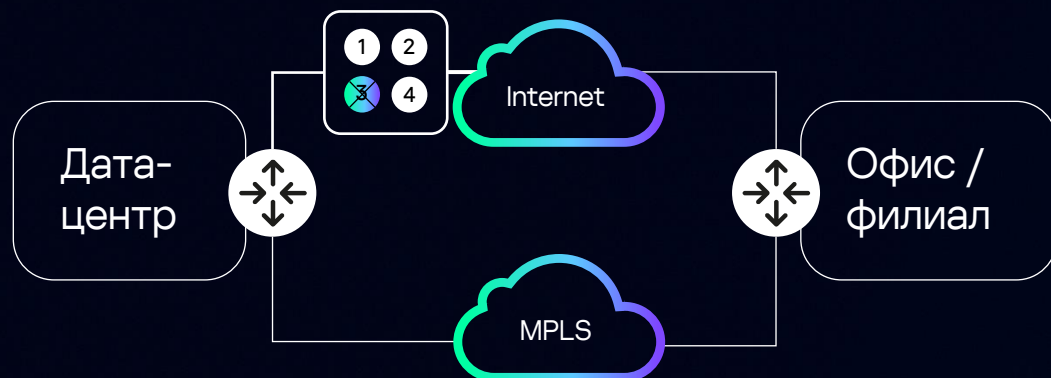


| Путь 1   | Путь 2  | Путь 3  |
|----------|---------|---------|
| Internet | MPLS    | 4G LTE  |
| 1 ms     | 2 ms    | 3 ms    |
| 0% loss  | 3% loss | 1% loss |

# Специализированные механизмы работы для каналов плохого качества

# Механизмы работы для каналов низкого качества

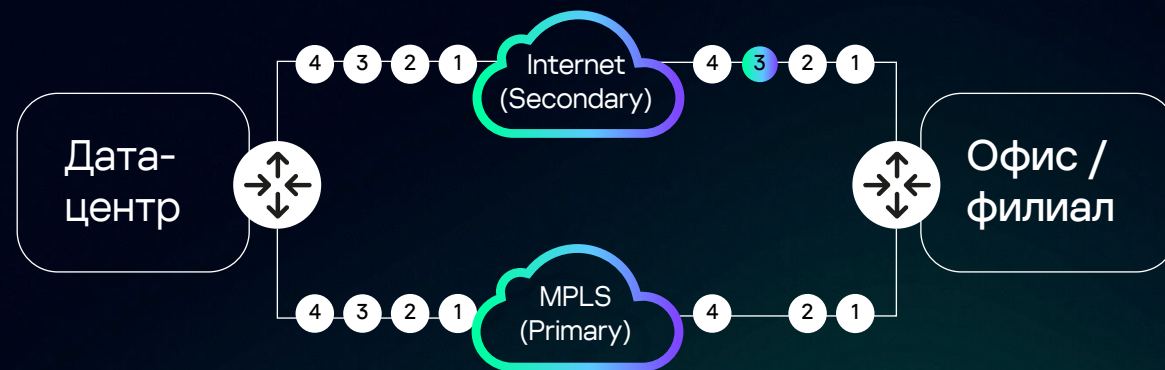
## Механизм поточной коррекции ошибок (Forward Error Correction)



Может использоваться для гарантии передачи критически важного трафика по ненадежным каналам связи, в которых наблюдаются потери пакетов. Благодаря специальному алгоритму, FEC позволяет восстанавливать потерянные пакеты. Механизм FEC предусматривает кодирование группы пакетов таким образом, чтобы принимающее СРЕ-устройство могло восстановить потерянный пакет на основе других пакетов группы.

Такой подход позволяет сохранить производительность без повторной передачи данных, что особенно критично для трафика приложений, которые передают данные в реальном времени.

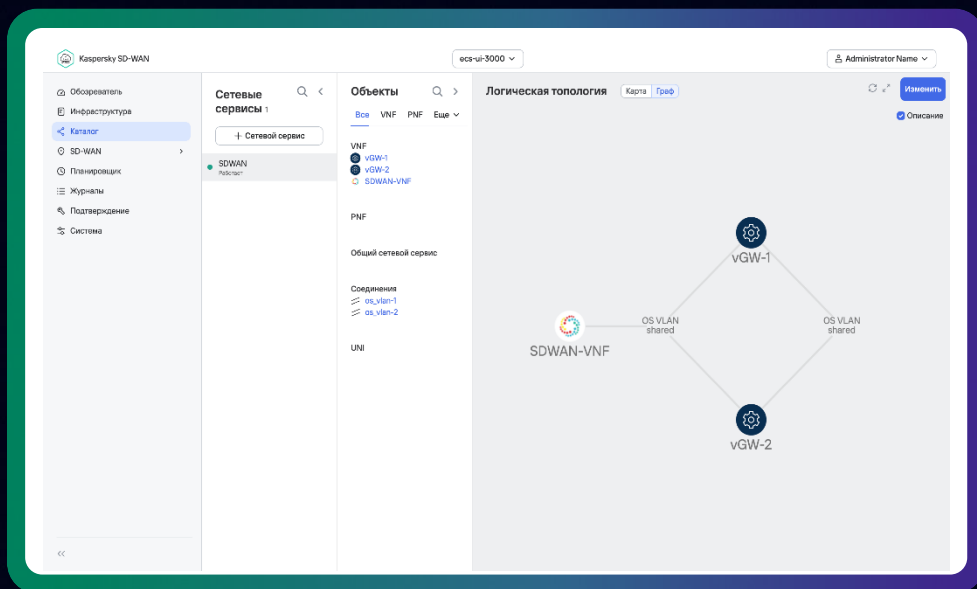
## Дублирование пакетов (Packet Duplication)



Может использоваться для отправки одних и тех же пакетов данных по нескольким каналам связи для повышения надежности приложений. Если некоторые пакеты потока теряются в одном канале, то принимающее СРЕ-устройство использует дублированные пакеты из другого канала для восстановления потерянных пакетов.

Построение сервисных  
цепочек — простая настройка  
обработки трафика любой  
сложности

# Построение цепочек сетевых сервисов и оркестрация виртуализированных функций



Традиционные сетевые устройства  
виртуализируются и становятся  
доступны как программные функции

## Виртуализация аппаратных решений

IPS

SWG

Router

DPI

FW



## Виртуализированные сетевые функции

IPS

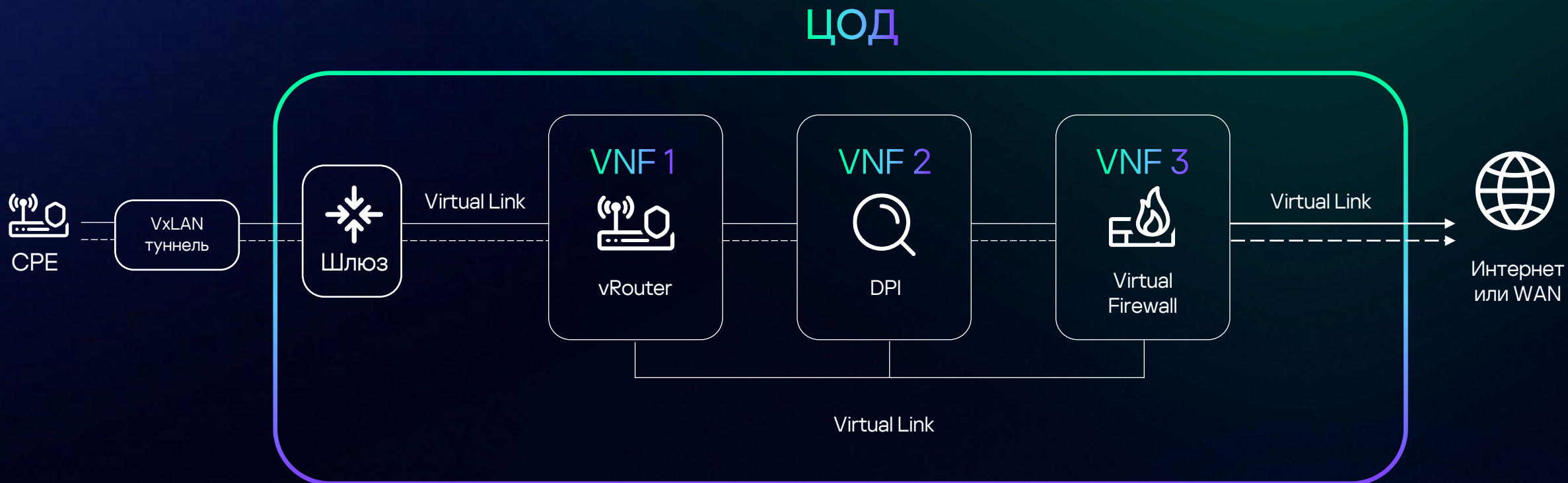
SWG

Router

DPI

FW

# Сценарии применения. Цепочка сервисов в ЦОД



Гибкая логика обработки трафика: любое количество проверок и графическое представление сервисной цепочки

# Оглавление

# 05



- 01 Коротко о SD-WAN
- 02 Особенности корпоративных сетей
- 03 Решение Kaspersky SD-WAN
- 04 Возможности решения
- 05 Политика лицензирования**
- 06 Kaspersky SD-WAN в концепции SASE

# Уровни и возможности Kaspersky SD-WAN

## Возможности

|                                                                                                                 |                                                                                                    | Standard | Advanced |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------|----------|
|  Подключение и управление      | Поддержка CPE производительностью до 10 Гбит/с                                                     | •        | •        |
|                                                                                                                 | Управление из частного/публичного облака или локально                                              | •        | •        |
|                                                                                                                 | Интеграция управления платформой с Open Single Management Platform (OSMP)                          | •        | •        |
|                                                                                                                 | Организация связности CPE с контроллером через LAN и WAN порты                                     | •        | •        |
|                                                                                                                 | Поддержка топологий Hub-and-Spoke, Full Mesh, Partial Mesh                                         | •        | •        |
|                                                                                                                 | SLA-политики для приложений                                                                        | •        | •        |
|                                                                                                                 | Динамическая маршрутизация (BGP, OSPF)                                                             | •        | •        |
|                                                                                                                 | Поддержка VRF Lite                                                                                 | •        | •        |
|                                                                                                                 | Встроенный DPI                                                                                     | •        | •        |
|                                                                                                                 | Stateful firewall                                                                                  | •        | •        |
|  Сервисы SD-WAN                | NAT (PAT, SNAT, DNAT)                                                                              | •        | •        |
|                                                                                                                 | Zero Touch Provisioning                                                                            | •        | •        |
|                                                                                                                 | Контроль качества каналов в реальном времени                                                       | •        | •        |
|                                                                                                                 | Мониторинг состояния туннеля (Connectivity Fault Management)                                       | •        | •        |
|                                                                                                                 | Поддержка Openflow                                                                                 | •        | •        |
|                                                                                                                 | Оптимизация каналов (поддержка FEC и дубликации пакетов)                                           | •        | •        |
|                                                                                                                 | Policy-Based Routing (PBR) с централизованным управлением                                          | •        | •        |
|                                                                                                                 | Поддержка сервисов P2P, P2M, L2/L3 VPN                                                             | •        | •        |
|                                                                                                                 | Поддержка встроенного высокоскоростного шифрования                                                 | •        | •        |
|                                                                                                                 | Поддержка ГОСТ-шифрования (получена сертификация ФСБ о соответствии требованиям к СКЗИ класса KC2) | •        | •        |
|  Виртуальные сетевые функции | Поддержка интеграции комплементарных продуктов Kaspersky                                           | •        | •        |
|                                                                                                                 | Реализация ETSI MANO                                                                               |          | •        |
|                                                                                                                 | Поддержка VNF сторонних производителей                                                             |          | •        |
|                                                                                                                 | Управление жизненным циклом сервисных цепочек                                                      |          | •        |
|  Сервисы                     | Поддержка Multicast                                                                                |          | •        |
|                                                                                                                 | Поддержка PIM                                                                                      |          | •        |
|                                                                                                                 | Поддержка Multi-Tenancy                                                                            |          | •        |

# Лицензирование и возможности устройств Kaspersky SD-WAN Edge Service Router

Лицензирование осуществляется по CPE в зависимости от необходимой пропускной способности.

Широкая линейка Kaspersky SD-WAN Edge Service Router (KESR) представлена маршрутизаторами производительностью от 50 Мбит/с до 10 Гбит/с.

## Модели отличаются комплектующими и возможностями



Поддержка LTE модулей



Поддержка VNF



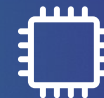
Производительность до 10 Гбит/с



До 2-х SIM-карт в режиме active / active



Поддержка SFP / SFP+ 10 Гбит/с



До двух CPU

# Модельный ряд Kaspersky SD-WAN Edge Service Router

## Производительность\*

KESR  
Model 1-R

До 50 Мбит/с

KESR  
Model 2-K

До 350 Мбит/с

KESR  
Model 3-K

До 600 Мбит/с

KESR  
Model 4-K

До 1,2 Гбит/с

KESR  
Model 5-K

До 10 Гбит/с

## С поддержкой ГОСТ-шифрования

KESR  
Model 1-N

До 200 Мбит/с

KESR  
Model 2-N

До 600 Мбит/с

KESR  
Model 3-N

До 3 Гбит/с

\* В режиме шифрования с включенным анализом DPI для пакетов IMIX. Реальная производительность зависит от условий использования

# Оглавление

# 06



- 01 Коротко о SD-WAN
- 02 Особенности корпоративных сетей
- 03 Решение Kaspersky SD-WAN
- 04 Возможности решения
- 05 Политика лицензирования
- 06 Kaspersky SD-WAN в концепции SASE

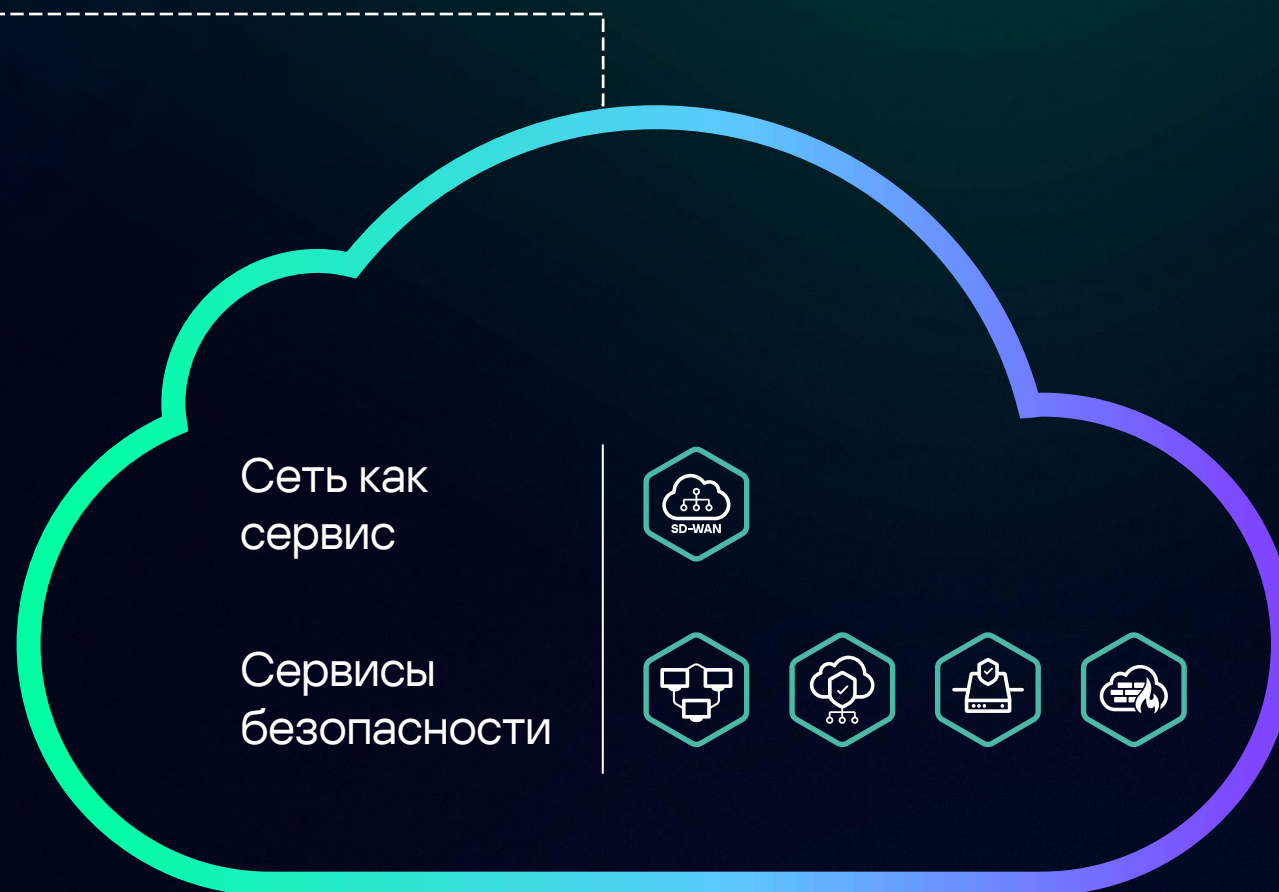
# SD-WAN – важнейшая часть архитектуры SASE

# SASE

Secure Access  
Service Edge

## Пограничный сервис безопасного доступа

- Концепция SASE предполагает переход от использования разрозненных средств защиты к унифицированной безопасности из частного или публичного облака.
- Где бы ни находились пользователи, как бы они ни подключались, ваша сеть абсолютно защищена.
- Технология SD-WAN – транспортная основа сетевой безопасности будущего.



# SASE – часть архитектуры XDR



# Безопасная разработка — основа решения Kaspersky SD-WAN

Решение SD-WAN, как и другие решения «Лаборатории Касперского», разработано в соответствии с методологией SSDLC (Secure Software Development Lifecycle).

Kaspersky Threat Research (Центр исследования угроз) — один из пяти центров экспертизы «Лаборатории Касперского», специалисты которого занимаются снижением рисков, связанных с уязвимостями в решениях «Лаборатории Касперского».



[Узнать больше](#)

# Спасибо!

Лаборатория Касперского  
Ленинградское шоссе, д.39А, стр.2  
Россия, Москва, 125212  
Tel: +7 (495) 797-8700  
[kaspersky.ru](https://kaspersky.ru)



kaspersky