



Комплексное решение
для построения надежной
и безопасной корпоративной
сети

Kaspersky SD-WAN

kaspersky активируй
будущее

Введение



SASE

Пограничный сервис безопасного доступа. Сетевая модель, которая объединяет средства защиты и сетевые технологии. Модель призвана обеспечить надежность и гибкость сети, а также защитить корпоративные сетевые ресурсы в условиях современных тенденций развития удаленных подключений и облачных сервисов.

Решение Kaspersky SD-WAN позволяет построить отказоустойчивую, территориально распределенную филиальную сеть с централизованным управлением, а также обеспечить непрерывность бизнес-процессов. Решение является основой для построения экосистемы сетевой безопасности и позволяет путем интеграции средств защиты реализовать подход SASE — Secure Access Service Edge.

Kaspersky SD-WAN — решение с фокусом на бизнесе



Использование любых доступных каналов связи, включая MPLS VPN, Ethernet, LTE, и их комбинаций для подключения филиалов организации к корпоративной сети и облачным сервисам



Интегрированные сервисы безопасности и мониторинг всех компонентов решения в реальном времени, а также состояния туннелей и приложений на основе DPI-анализа



Подключение филиалов к корпоративной сети с помощью технологии Zero Touch Provisioning без предварительной настройки устройств и дополнительных командировок сотрудников



Централизованное управление с помощью единого веб-интерфейса или API для оперативного внесения изменений в параметры решения и мониторинга сети SD-WAN любого масштаба



Интеллектуальное управление трафиком и максимальное качество сетевого обслуживания для критически важных бизнес-приложений



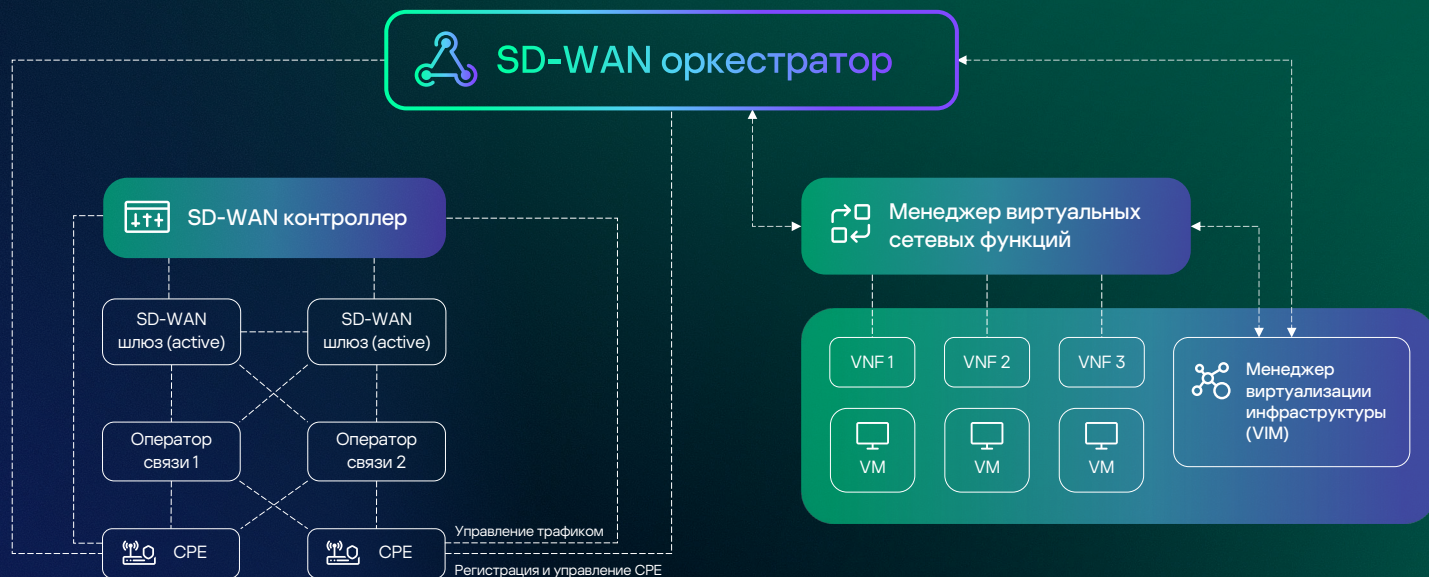
Встроенный менеджер виртуальных сетевых функций (VNF) для легкого внедрения средств защиты Kaspersky и сторонних производителей



Соответствие требованиям

Решение поддерживает ГОСТ-шифрование, входит в реестр российского ПО и работает на отечественных аппаратных платформах

Архитектура решения



Основные компоненты

Гибкая архитектура Kaspersky SD-WAN обеспечивает весь жизненный цикл решения: централизованную оркестрацию, автоматизированную настройку, а также мониторинг и диагностику.

SD-WAN orchestrator

Программный компонент, управляющий SD-WAN контроллерами и менеджером виртуализации инфраструктуры. SD-WAN orchestrator предоставляет единый графический и API-интерфейсы для взаимодействия со всеми компонентами решения, осуществляет сбор, хранение и визуализацию информации о состоянии SD-WAN сети, запускает шаблоны и задает параметры сервисных цепочек, обеспечивает виртуализацию и контроль ресурсов, а также управление лицензиями

SD-WAN controller

Программный компонент управления SD-WAN CPE. SD-WAN controller обеспечивает управление трафиком, обмен маршрутной информацией, настройку политик безопасности и параметров защиты каналов связи

Менеджер виртуализации инфраструктуры (VIM)

Стороннее программное обеспечение, отвечающее за конфигурацию и управление виртуальной инфраструктурой. В составе Kaspersky SD-WAN по умолчанию используется VIM OpenStack

Менеджер виртуальных сетевых функций (VNF-менеджер)

Программный компонент управления жизненным циклом виртуальных сетевых функций. VNF-менеджер контролирует установку, активацию, масштабирование, обновление и завершение виртуальных сетевых функций

SD-WAN шлюз

Сетевое оборудование, развернутое в центре обработки данных (ЦОД) или центральном офисе, которое осуществляет агрегацию SD-WAN туннелей. Рекомендованным дизайном является установка SD-WAN шлюзов в отказоустойчивой паре

CPE

Телекоммуникационное оборудование, устанавливаемое в филиалах для подключения каналов связи и организации туннелей до SD-WAN шлюза

Технические характеристики и возможности

Возможности

Технические характеристики

Варианты развертывания решения

- На площадке заказчика (On-premises)
- Частное/публичное облако

Управление сетевыми функциями и оркестрация платформы предоставления сетевых услуг

- Реализация ETSI MANO
- Интеграция управления платформой с Open Single Management Platform (OSMP)
- Поддержка VNF (продуктов Kaspersky или сторонних производителей)
- Service-chain lifecycle management
- Active-Active Multimaster

Типы CPE

- Программно-аппаратные комплексы
- Виртуальные CPE

Управление

- Централизованное управление версиями ПО для CPE и центральных компонентов решения
- Out-of-Band управление CPE (не через клиентские туннели)

Функции SD-Branch

- Сегментация LAN
- Локальные сервисы (DHCP и др.)
- Статическое резервирование для DHCP
- Локальный доступ в интернет

Поддерживаемые каналы связи

- 4G
- MPLS
- Ethernet
- PPPoE

Поддерживаемые топологии сети

- Full mesh
- Partial mesh
- Hub-and-Spoke

Zero Touch Provisioning

- DHCP
- Static
- С поддержкой двухфакторной аутентификации
- URL Auth

VPN/Overlay

- L2 Point-to-Point
- Point-to-Multipoint
- Multipoint-to-Multipoint
- L3 VPN

Отказоустойчивость и резервирование

- Кластеризация центральных компонентов
- Дублирование SD-WAN шлюзов (active/active)
- Дублирование CPE (VRRP)

Сегментация LAN

Полноценная поддержка стандарта 802.1q на LAN-портах CPE (Access, Trunk, Q-in-Q)

Маршрутизация	• Static • BGP • OSPF • BFD • PIM • NAT (PAT, SNAT, DNAT) • VRF Lite • Поддержка multicast service в SD-WAN сети • Поддержка Path MTU discovery
Балансировка и отказоустойчивость WAN	• Active/Standby • Active/Active • Bonding
Мониторинг качества каналов	• Оценка показателей SLA на основе активных проб в пользовательском трафике • Мониторинг состояния туннеля (Connectivity Fault Management) • BFD
Оптимизация и коррекция ошибок WAN	• FEC • Дублирование пакетов
Качество обслуживания (QoS)	• Многоуровневое качество обслуживания • 8 очередей на каждый виртуальный сервис • Поддержка DSCP • Оценка SLA (задержка, джиттер, потери) • Поддержка QoS remapping на WAN-интерфейсах CPE • Поддержка policing и shaping • Поддержка QoS при передаче транзитного трафика
Распознавание и маршрутизация трафика приложений на уровне L7	• Built-in DPI • Application aware routing • Application SLA
Безопасность	• Stateful firewall • Встроенное высокоскоростное шифрование • Настройка шифрования по каналам • Защита от SYN-flood атак • Фильтрация фрагментированных пакетов • Поддержка ГОСТ-шифрования (Получена сертификация ФСБ о соответствии требованиям к СКЗИ класса KC2) • Поддержка интеграции СКЗИ, сертифицированных ФСБ России
Мониторинг системы	• Мониторинг центральных компонентов, CPE, VNF • Зеркалирование трафика (TAP) • Netflow
Поддержка российских ОС	• Astra Linux SE 1.7 • РЕД ОС 7.3

Лицензирование

Решение Kaspersky SD-WAN представлено в двух вариантах:



**Kaspersky
SD-WAN**

Standard

Предлагает основные инструменты для организации сети и управления ею, поддерживает работу сервисов SD-WAN и интеграцию продуктов «Лаборатории Касперского» в виде виртуальных сетевых функций.



**Kaspersky
SD-WAN**

Advanced

Предоставляет расширенные возможности для работы с виртуальными сетевыми функциями, в том числе сторонних производителей, а также включает поддержку Multicast и Multi-Tenancy для сервисов.

Для каждого варианта решения лицензирование осуществляется по CPE в зависимости от необходимой пропускной способности и поддержки ГОСТ-шифрования. В качестве аппаратных платформ для CPE на выбор доступны устройства модельного ряда Kaspersky SD-WAN Edge Service Router (KESR) с различным набором интерфейсов и производительностью.

**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*

* Реальная производительность зависит от условий использования.

Основные параметры устройств KESR

Модель	Производительность	Ключевые характеристики	Продуктовая позиция
KESR Model 1-R	До 50 Мбит/с	• 4 × LAN • 1 × WAN • 2 × LTE (active/active)	KESR-M1-R-5G-2L-W
KESR Model 2-K	До 350 Мбит/с	• 5 × LAN • LTE	KESR-M2-K-5G-1L-W
		• 5 × LAN • 1 × SFP	KESR-M2-K-5G-1S
KESR Model 3-K	До 600 Мбит/с	• 4 × LAN • 4 × SFP	KESR-M3-K-4G-4S
KESR Model 4-K	До 1,2 Гбит/с	• 4 × LAN • 2 × SFP+ • 1 × CPU	KESR-M4-K-4G-2X-1CPU
		• 8 × LAN • 4 × SFP+ • 1 × CPU	KESR-M4-K-8G-4X-1CPU
KESR Model 5-K	До 10 Гбит/с	• 8 × LAN • 4 × SFP+ • 2 × CPU	KESR-M5-K-8G-4X-2CPU
		• 8 × SFP+ • 4 × LAN • 2 × CPU	KESR-M5-K-4G-8X-2CPU

С поддержкой ГОСТ-шифрования

Модель	Производительность	Ключевые характеристики	Продуктовая позиция
KESR Model 1-N	До 200 Мбит/с	• 4 × LAN • 2 × SFP+	KESR-M1-N-4G-2X
KESR Model 2-N	До 600 Мбит/с	• 4 × LAN • 4 × SFP+	KESR-M2-N-4G-4X
KESR Model 3-N	До 3 Гбит/с	• 8 × LAN • 4 × SFP+	KESR-M3-N-8G-4X

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](#)



Kaspersky SD-WAN

[Подробнее](#)

www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)