Комплексное решение
для построения надежной
и безопасной корпоративной
сети

Kaspersky SD-WAN

kaspersky активируй будущее

Введение

Сегодня непрерывность бизнес-процессов большинства компаний напрямую зависит от надежности их сети и бесперебойного доступа к веб-ресурсам. Большое количество филиалов, распределенные команды, размещение ресурсов компании в облаке и удаленная работа сотрудников – все это усложняет сетевую инфраструктуру, управление ею и обеспечение ее безопасности. В этих условиях необходим гибкий подход, который соответствует меняющимся потребностям бизнеса.

Проблемы клиентов при использовании WAN-сетей

- Долгое подключение новых офисов и трудоемкое масштабирование
- Управление сложной инфраструктурой, нехватка квалифицированных специалистов
- ИТ- и ИБ-инциденты, связанные с человеческими ошибками при выполнении рутинных операций
- Недостаточная пропускная способность соединений и высокая общая стоимость эксплуатации сети
- Неудовлетворительное качество работы приложений, проблемы при организации голосовых и видеоконференций
- Сложность поддержания целостности политик безопасности

Какие проблемы решает Kaspersky SD-WAN

Kaspersky SD-WAN успешно решает проблемы, встречающиеся в классических WAN-сетях, и предоставляет удобное управление сетевым оборудованием, обеспечивает необходимое качество работы приложений, оптимизирует подключение к облакам, повышает уровень безопасности и скорость внедрения новых сервисов, а также сокращает расходы на инфраструктуру.

Решение Kaspersky SD-WAN позволяет не только управлять транспортной сетевой инфраструктурой, но также интегрировать инструменты безопасности и аналитики благодаря менеджеру виртуальных сетевых функций и сервисному оркестратору в своем составе. Такая архитектура позволяет без труда построить экосистему сетевой безопасности, реализовав подход SASE – Secure Access Service Edge.

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 рамках SASE сетевые сервисы и сервисы безопасности предоставляются одним провайдером.

Простая масштабируемость

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

Централизованная безопасность

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

Оптимизация расходов

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

Легкое управление

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

Ключевые особенности решения

Надежная сеть для всех офисов

Любые каналы связи

Доступ ко всем ресурсам компании (офисам, частным и публичным облакам и центрам обработки данных) можно организовать с помощью различных каналов связи: 4G, MPLS, Ethernet и PPPoE.

Быстрое подключение офисов

Для подключения филиалов используются универсальные сетевые устройства (CPE) с технологией Zero Touch Provisioning, которая обеспечивает простое развертывание новых телекоммуникационных устройств без необходимости предварительной настройки.

Бесперебойная передача данных

Решение позволяет настраивать динамические туннели между CPE, приоритизировать трафик приложений и управлять им, оптимизировать передачу данных и оркестрировать сетевые функции.

Единая консоль управления

Управление всей сетью

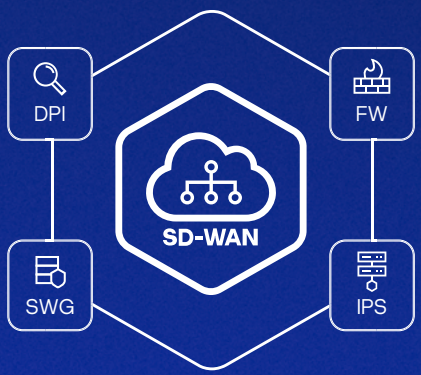
Управление осуществляется через единый веб-интерфейс: вы можете настраивать CPE и резервирование каналов связи, создавать правила фильтрации трафика и задавать параметры SLA для сервисов.

Построение и визуализация инфраструктуры

С помощью удобного графического конструктора вы можете продумывать и визуализировать инфраструктуру сети, добавляя в режиме drag & drop необходимые сетевые функции и объединяя их в сервисные цепочки, которые сразу становятся доступными для запуска.

Информативные дашборды

Информативные дашборды позволяют оценить состояние всей инфраструктуры SD-WAN в любой момент времени: CPE, виртуализированных функций и используемых физических ресурсов.



Унифицированная безопасность

Единая политика безопасности

Решение обеспечивает безопасность всех подразделений компании за счет использования шифрованных VPN-соединений, а также позволяет централизованно управлять конфигурациями устройств, политиками безопасности и правилами обработки трафика, гарантируя их целостность для всей сети.

Легкое подключение средств защиты

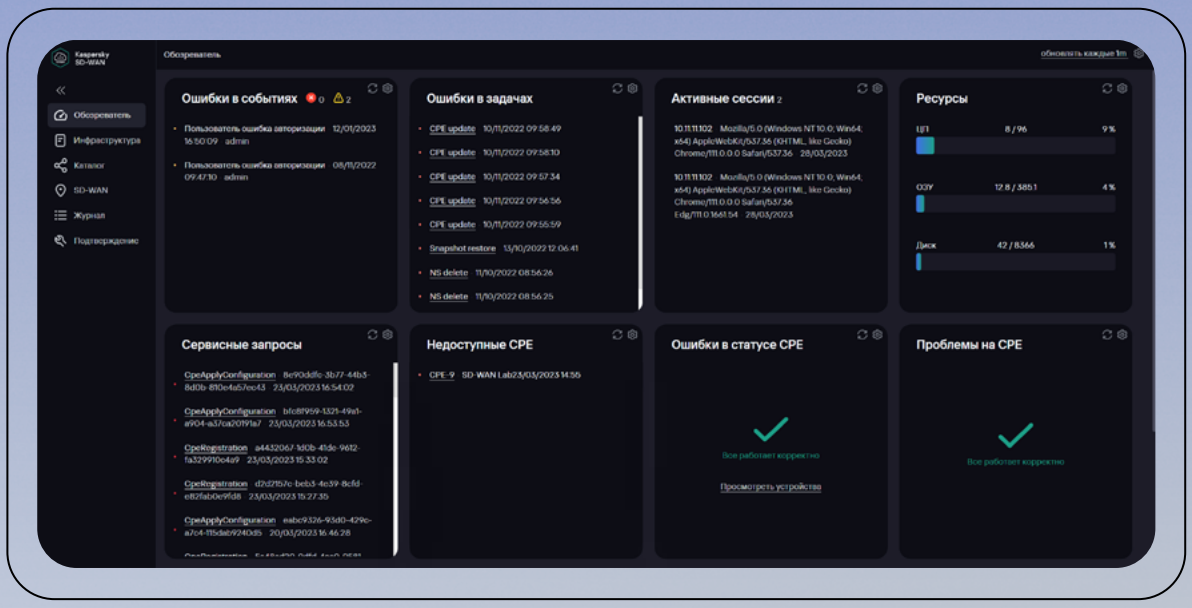
Виртуализация сетевых функций позволяет автоматически развертывать средства защиты и контроля трафика, включая межсетевые экраны, шлюзы сетевой безопасности и системы предотвращения вторжений.

Гибкая архитектура

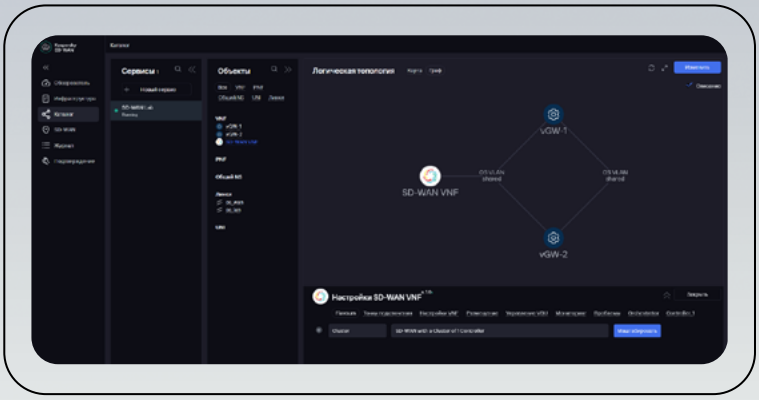
Гибкая архитектура решения позволяет легко интегрировать средства защиты самых разных вендоров благодаря менеджеру виртуальных сетевых функций и сервисному оркестратору в своем составе.

Удобный и информативный веб-интерфейс

Вся основная информация о состоянии решения и сети на главном экране

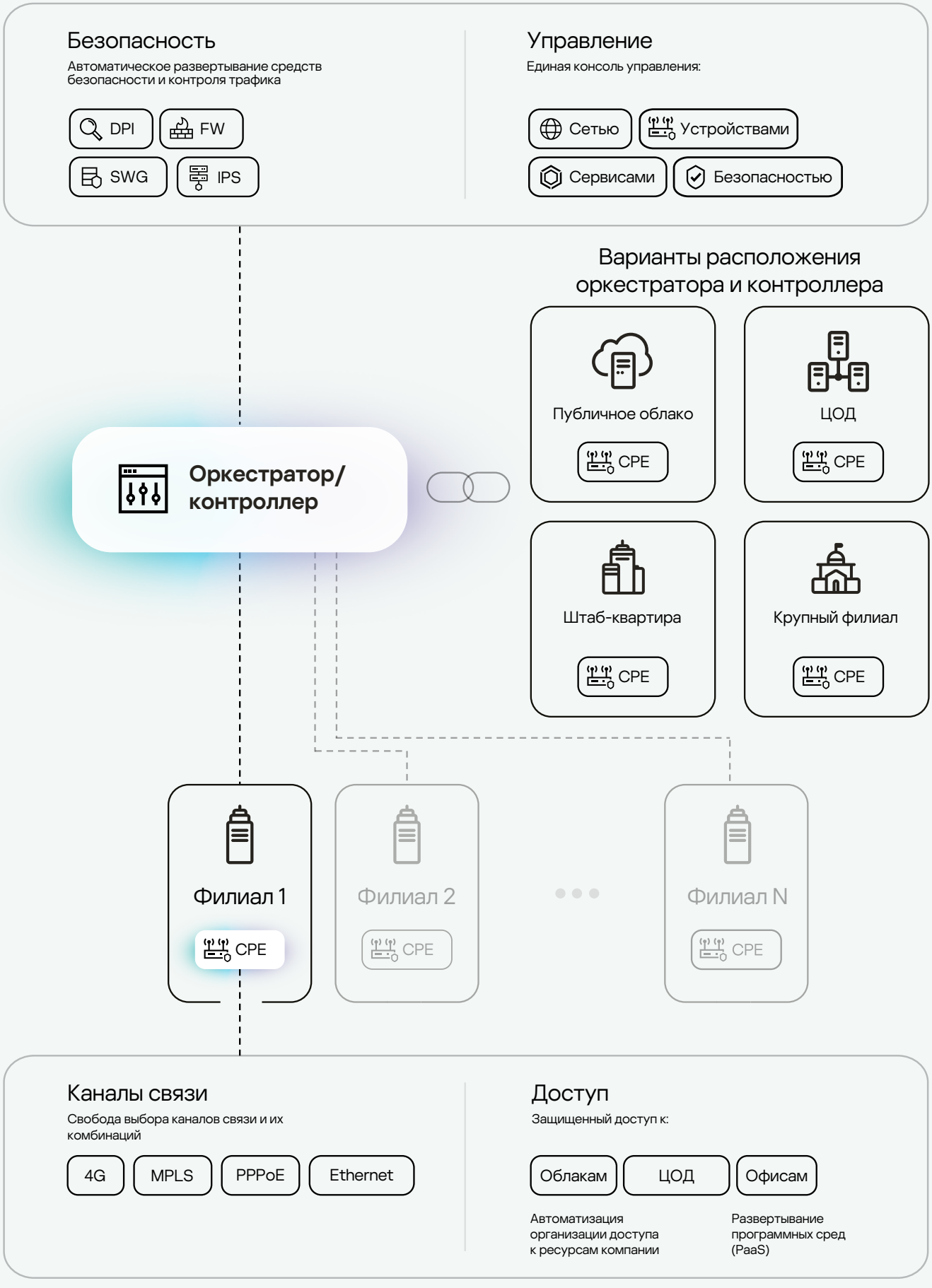


Графический конструктор сервисных цепочек с широкими возможностями управления объектами



Мониторинг использования виртуальных и серверных ресурсов по целому ряду параметров

Концептуальная архитектура решения



Уровни и возможности Kaspersky SD-WAN

Решение Kaspersky SD-WAN представлено в двух вариантах: Standard и Advanced.

	Возможности	Standard	Advanced
Подключение и управление	Поддержка CPE производительностью до 10 Гбит/с	●	●
	Управление из частного/публичного облака или локально	●	●
	Поддержка топологий Hub-and-Spoke, Full Mesh, Partial Mesh	●	●
	SLA политики для приложений	●	●
	Динамическая маршрутизация (BGP, OSPF)	●	●
	Поддержка VRF-Lite	●	●
	Встроенный DPI	●	●
	Stateful Firewall	●	●
	NAT (PAT, SNAT, DNAT)	●	●
Сервисы SD-WAN	Zero Touch Provisioning	●	●
	Контроль качества каналов в реальном времени	●	●
	Мониторинг состояния туннеля (Link State Control)	●	●
	Поддержка OpenFlow	●	●
	Оптимизация каналов (поддержка FEC и дупликации пакетов)	●	●
	Поддержка сервисов P2P, P2M, L2/L3 VPN	●	●
	Поддержка встроенного высокоскоростного шифрования	●	●
	Поддержка ГОСТ-шифрования (ПАК в процессе сертификации)	●	●
Виртуальные сетевые функции	Поддержка интеграции комплементарных продуктов Kaspersky	●	●
	Реализация ETSI MANO		●
	Поддержка VNF сторонних производителей		●
	Управление жизненным циклом сервисных цепочек		●
	Поддержка uCPE		●
Сервисы	Поддержка Multicast		●
	Поддержка PIM		●
	Поддержка Multi-Tenancy		●

Лицензирование

Лицензирование решения осуществляется по CPE в зависимости от необходимой пропускной способности. На выбор доступны устройства модельного ряда Kaspersky SD-WAN Edge Service Router (KESR), который представлен широким набором аппаратных платформ с различными интерфейсами.

KESR Model 1	KESR Model 2	KESR Model 3	KESR Model 4	KESR Model 5
50 Мбит/с	350 Мбит/с	600 Мбит/с	1.2 Гбит/с	10 Гбит/с

Соответствие требованиям законодательства

Решение и входящие в его состав аппаратные платформы внесены в реестр российского программного обеспечения

В рамках решения используется отечественное оборудование, входящее в реестр ТОРП Минпромторга России

Kaspersky SD-WAN поддерживает ГОСТ-шифрование (ПАК в процессе сертификации)

Комплексное решение для построения надежной и безопасной корпоративной сети

Основа сетевой безопасности будущего

Kaspersky SD-WAN является основой для построения экосистемы сетевой безопасности. Решение уже сейчас позволяет реализовать подход SASE – Secure Access Service Edge.

Команда «Лаборатории Касперского» имеет большой опыт в области кибербезопасности, а продукты компании по итогам более 700 независимых тестов оценены как наиболее эффективные защитные решения. Активно развивая направление сетевой безопасности, команда «Лаборатории Касперского» ставит своей целью увеличить уровень защищенности российских компаний с помощью экосистемы пограничных сервисов безопасного доступа (SASE).

Подключение Kaspersky SD-WAN — это быстро

1. Доставьте CPE в офис
2. Подключите CPE к сети
3. Оборудование готово к использованию

Kaspersky SD-WAN

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее