На версию ближе к SASE: выход Kaspersky SD-WAN 2.1

Вебинар для клиентов
12 октября 11.00 (МСК)

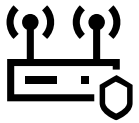
kaspersky

Кому и зачем нужен Kaspersky SD-WAN

Максим Каминский, менеджер по развитию бизнеса SD-WAN/SASE

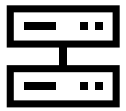
Коротко о SD-WAN

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

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

Проблемы корпоративных сетей

Проблемы традиционных сетей

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

Kaspersky SD-WAN

Комплексное решение для построения надежной и безопасной корпоративной сети

Зачем Kaspersky SD-WAN бизнесу?

Быстрое подключение новых офисов и точек продаж, используя существующие каналы 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

Пример решения задач ритейла с помощью Kaspersky SD-WAN

Сеть магазинов электроники

Задачи/проблемы

Требуется расширение MPLS каналов для эффективной работы приложений

Увеличение пропускной способности каналов – дорогая и не самая простая процедура

Одновременно необходимо снизить операционные затраты на каналы связи

Для специфического трафика магазинов необходимо настраивать отдельные SLA

Необходимо упростить управление инфраструктурой

Решение

Умные механизмы Kaspersky SD-WAN обеспечивают эффективную работу приложений даже с нестабильными каналами связи

Решение позволяет оптимизировать использование существующих каналов связи

Решение позволяет гибко управлять трафиком и гарантировать соблюдение SLA

Единая консоль управления позволяет централизованно изменять как сетевые настройки, так и политики безопасности

Результат

Оптимизировано использование каналов и увеличена производительность приложений

Затраты на каналы связи оптимизированы на 37%

Возможно подключение десятков точек продаж в течение 24 часов с учетом наличия CPE

ИТ команда переориентирована на приоритетные задачи

Пример решения задач промышленных компаний с помощью Kaspersky SD-WAN

Сеть заправок

Задачи/проблемы

Требуется возможность быстро подключать новые заправочные станции, в том числе находящиеся на удалении от населенных пунктов

Необходима бесперебойная связь с сетью аппаратов для оплаты топлива и товаров из магазина

Требуется организовать разделение основного трафика и трафика гостевой сети Wi-Fi для посетителей заправок

Решение

Решение позволяет использовать любые доступные каналы связи и их комбинации, а технология Zero-Touch Provisioning обеспечивает быстрое подключение точек

При сбое CPE можно перезапустить удаленно из консоли или заменить силами работников заправки при наличии подменного фонда

Интеграция с KICS for Networks позволяет передавать копию трафика промышленной сети, чтобы организовать систему централизованного мониторинга и защиты

Ряд умных механизмов гарантирует бесперебойную связь даже в условиях нестабильных подключений

Механизмы решения помогают отделить трафик одного типа от другого и обеспечить безопасное разделение сети

Результат

Решение помогло подключить заправки на отдаленных от населенных пунктов шоссе и оптимизировать расходы на каналы связи на 21%

Заправочная сеть оснащена подменным фондом CPE, чтобы гарантировать работу приложений и терминалов оплаты даже в экстремальных ситуациях

Построена единая система мониторинга и защиты

Сеть сегментирована, внутренний трафик безопасно изолирован, трафик Wi-Fi сетей контролируется в том числе с помощью технологии DPI

Пример решения задач компаний финансовой сферы с помощью Kaspersky SD-WAN

Крупный банк

Задачи/проблемы

Клиенты отдаленных региональных отделений испытывают проблемы из-за потери банкоматами связи с сетью

Отсутствие профильных ИТ-специалистов в небольших региональных отделениях

Необходимо снизить затраты на подключение новых филиалов и банкоматов

Необходимо обеспечить стабильную работу как основного клиентского приложения, так и сервисов для сотрудников

Решение

Целый ряд механизмов Kaspersky SD-WAN гарантирует доставку критически важного трафика даже через нестабильные каналы связи

Технология Zero-Touch Provisioning сильно упрощает подключение нового офиса или банкомата, предварительная настройка оборудования перед первым подключением не требуется

Управление всеми устройствами осуществляется из единой консоли

Интеллектуальные механизмы маршрутизации гарантируют необходимый SLA для критически важных бизнес-приложений.

Результат

Обеспечена бесперебойная работа банкоматов, клиентского приложения и сервисов для сотрудников

Устройствами в филиалах управляет один администратор из центрального офиса

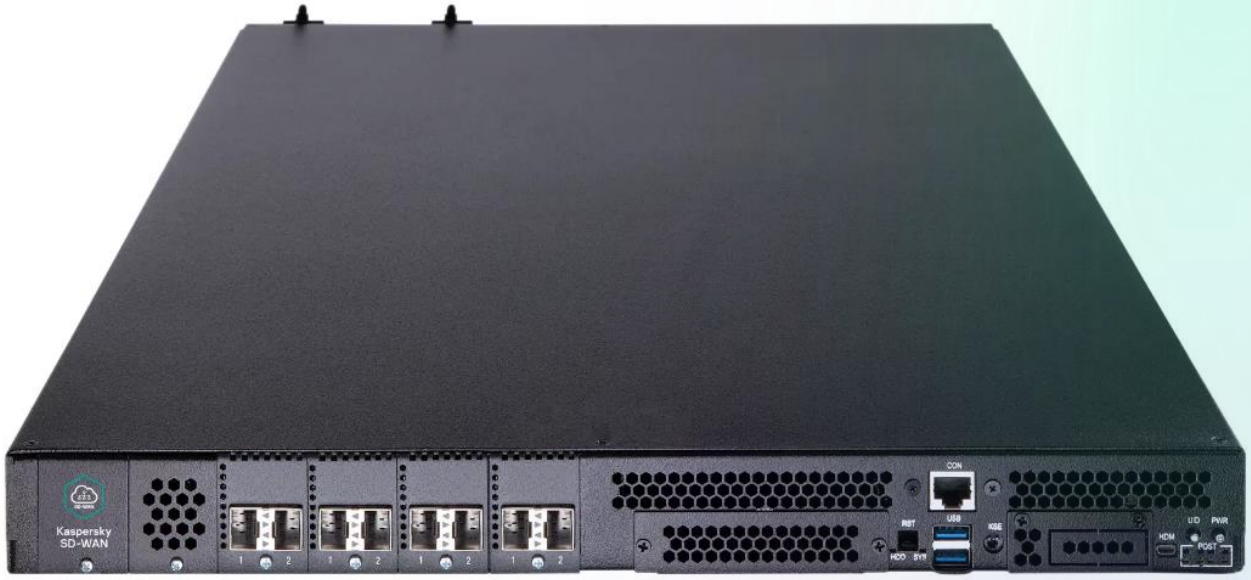
Для подключения новых офисов используются существующие каналы связи, в том числе беспроводные

Затраты на каналы связи оптимизированы на 23%

Ключевые нововведения Kaspersky SD-WAN 2.1

Дмитрий Головко, менеджер по продукту Kaspersky SD-WAN

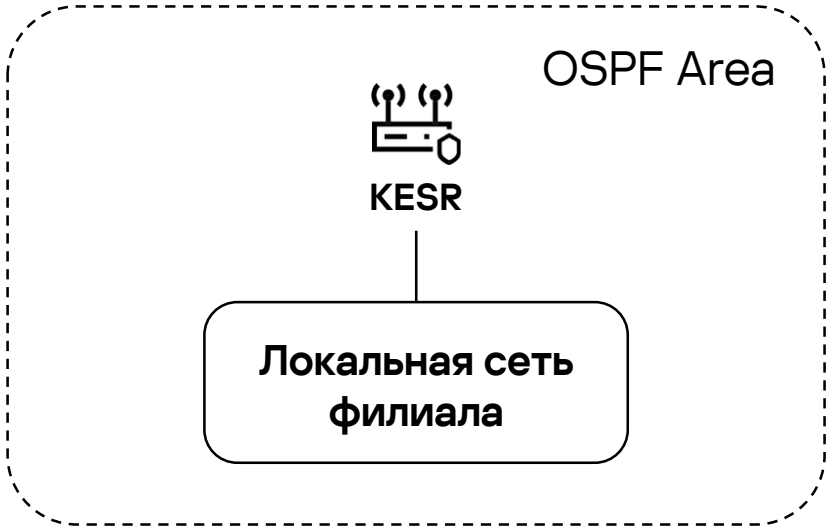
Поддержка высокопроизводительных платформ (10Gbps Full-Duplex)



KESR-M5

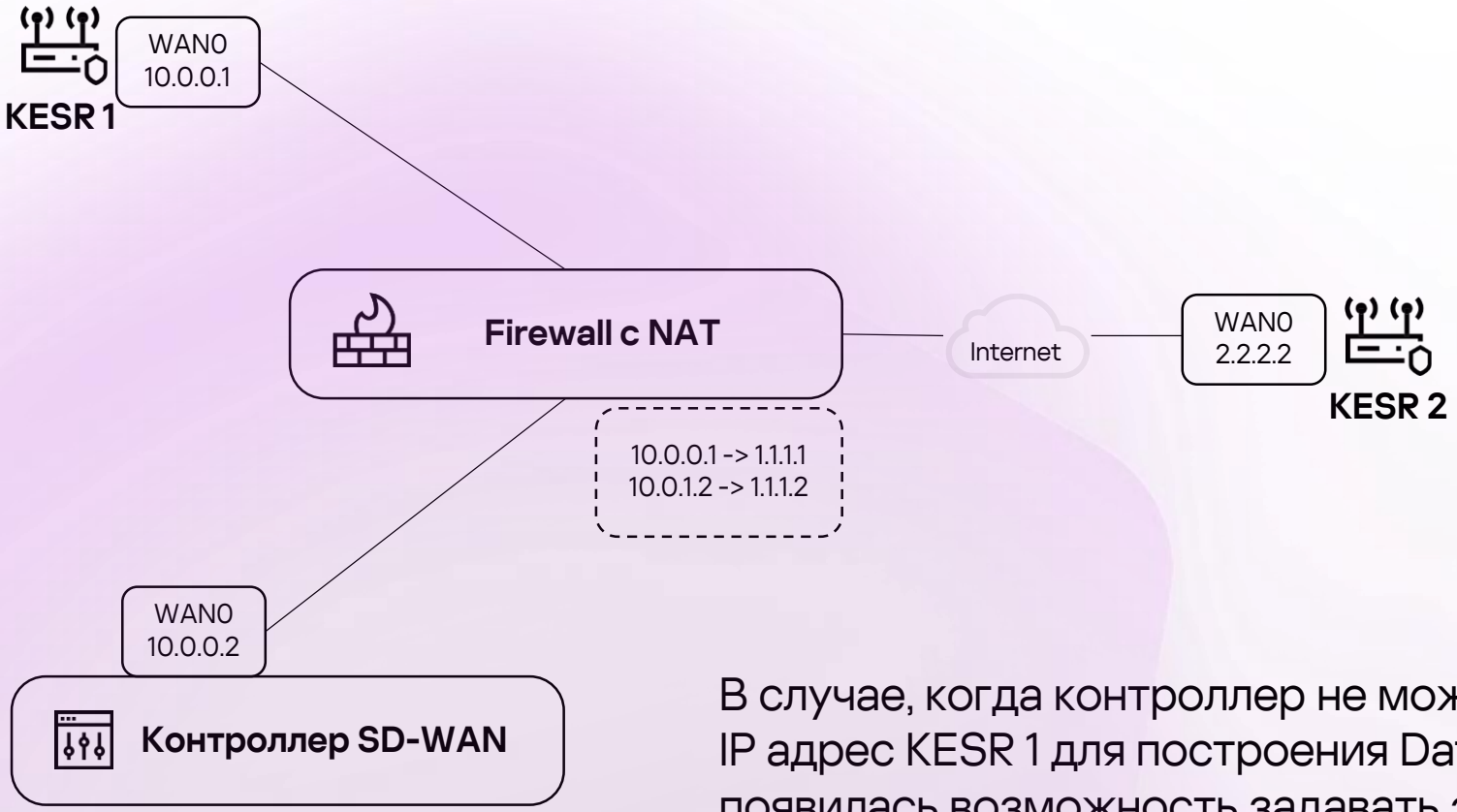
Возможность использования в качестве SD-WAN шлюзов или CPE устройств в HQ или в филиалах с большим количеством трафика.

Поддержка OSPF



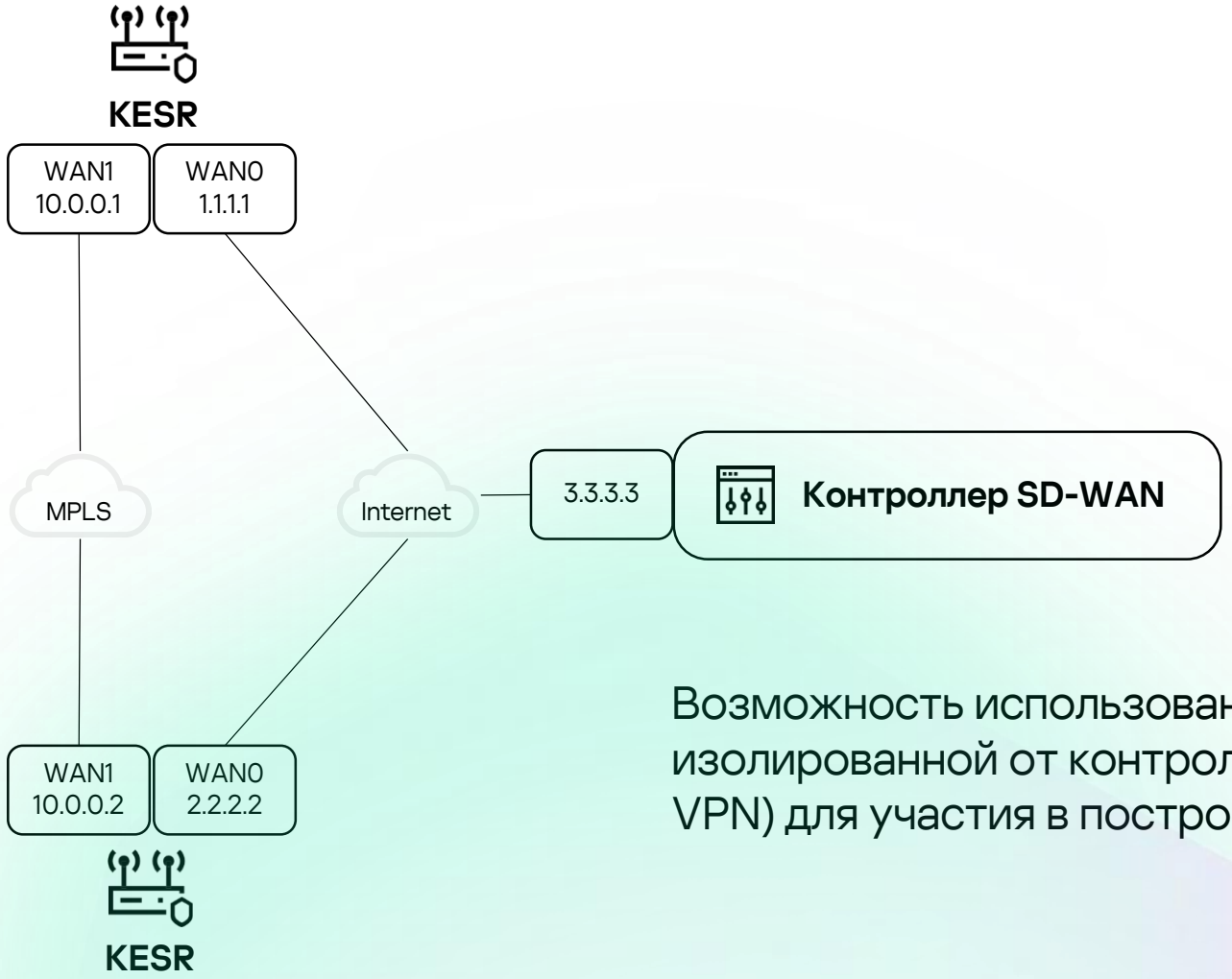
Полноценная поддержка протокола OSPF для организации связности филиалов по одному из самых популярных протоколов динамической маршрутизации с высокой скоростью сходимости сети.

Поддержка дополнительных сценариев CPE->CPE соединений в случае расположения SD-WAN шлюза за NAT



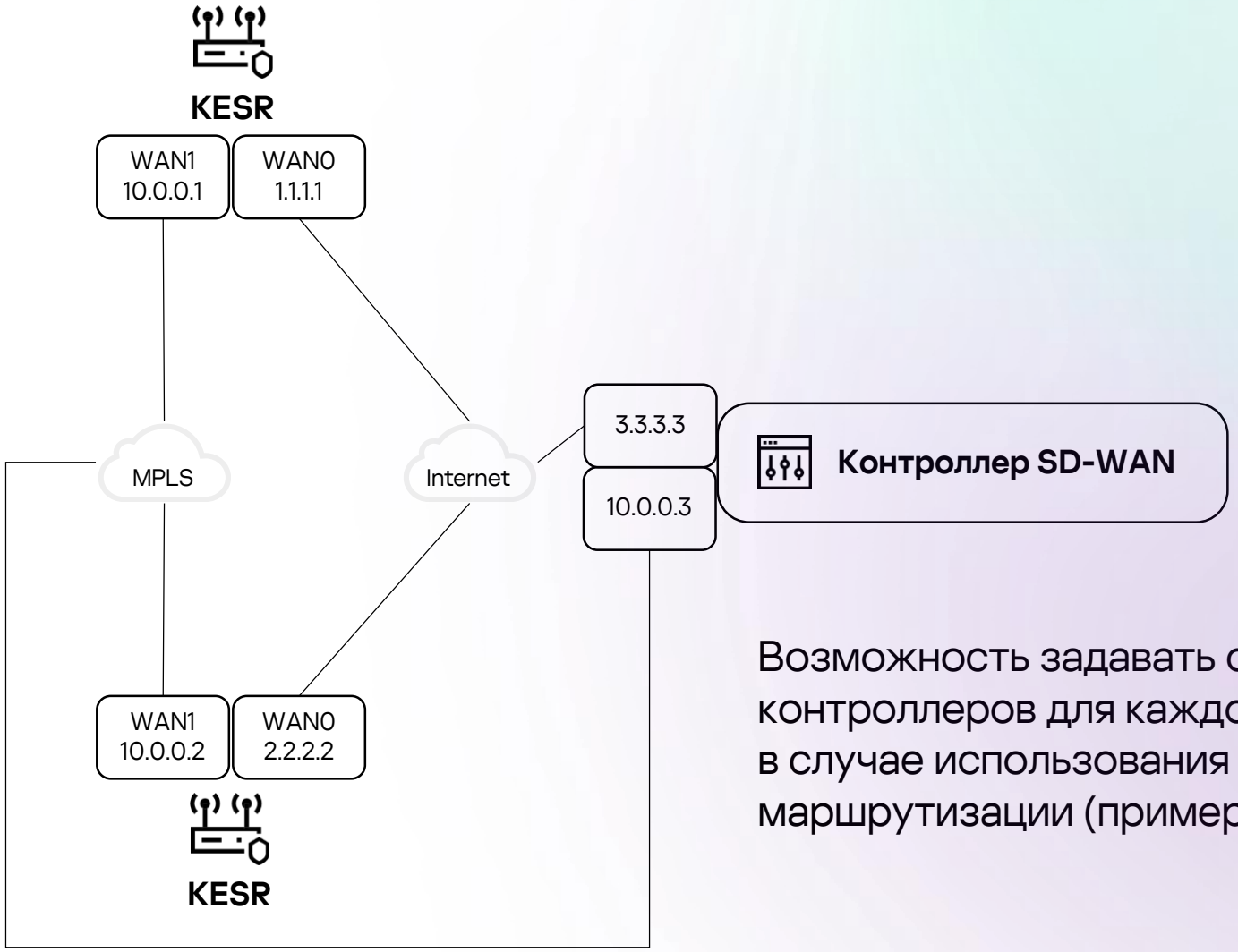
В случае, когда контроллер не может узнать реальный публичный IP адрес KESR 1 для построения Data Plane туннелей с KESR 2, появилась возможность задавать этот IP адрес (и в случае с PAT – UDP порт) в настройках WAN интерфейса KESR через графический интерфейс оркестратора.

Поддержка дополнительных сценариев работы KESR с одновременным использованием Internet и MPLS каналов



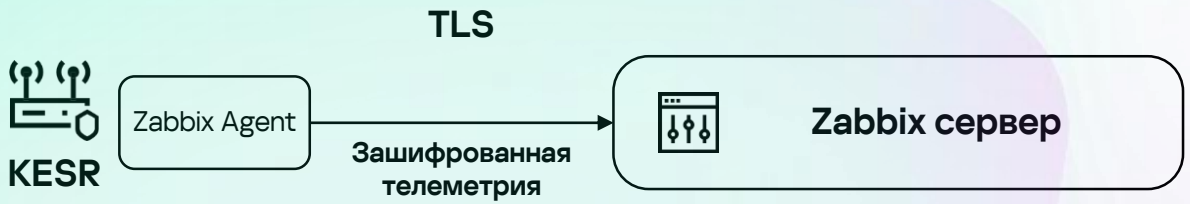
Возможность использования WAN интерфейсов изолированной от контроллера сети (пример – L2 VPN) для участия в построении SD-WAN фабрики.

Поддержка настройки IP адресов контроллера на WAN интерфейсах CPE



Возможность задавать специфические IP адреса контроллеров для каждого WAN интерфейса KESR, в случае использования изолированных доменов маршрутизации (пример – Internet и MPLS).

Шифрование данных мониторинга при их отправке вне SD-WAN туннеля



Добавление поддержки TLS в Zabbix агентах на KESR позволяет пересылать трафик телеметрии на Zabbix сервер в зашифрованном виде, в том числе вне туннелей.

Планы на Kaspersky SD-WAN 2.2

Q1 2024 **2.2**

SD-WAN 2.2*

- **Централизованное управление правилами Firewall (L7) и NAT на CPE.**
- **Поддержка DIA.**
- **Централизованное управление Netflow.**
- **ISO образ для развертывания решения.**
- Поддержка PIM.
- Поддержка 2FA при доступе на оркестратор.
- OVF шаблон vCPE для упрощения ZTP на VMware.
- Поддержка цепочки сертификатов для ZTP.
- Расширение количества диагностических инструментов для CPE в оркестраторе.
- Поддержка Zabbix 6.0.
- Возможность настройки Fragmentation Check IP в GUI.
- Отправка событий на e-mail соответствующих тенантов.

* [Возможны изменения]

Маршрутизаторы KESR: обзор линейки моделей под любые задачи

Сергей Гаврилов, Старший инженер предпродажной поддержки

Маршрутизаторы KESR: что нужно знать

Срочная лицензия

Зависит от пропускной способности

Доступна техническая поддержка Premium или Premium Plus

Маршрутизатор KESR

- Виртуальный
- Аппаратный

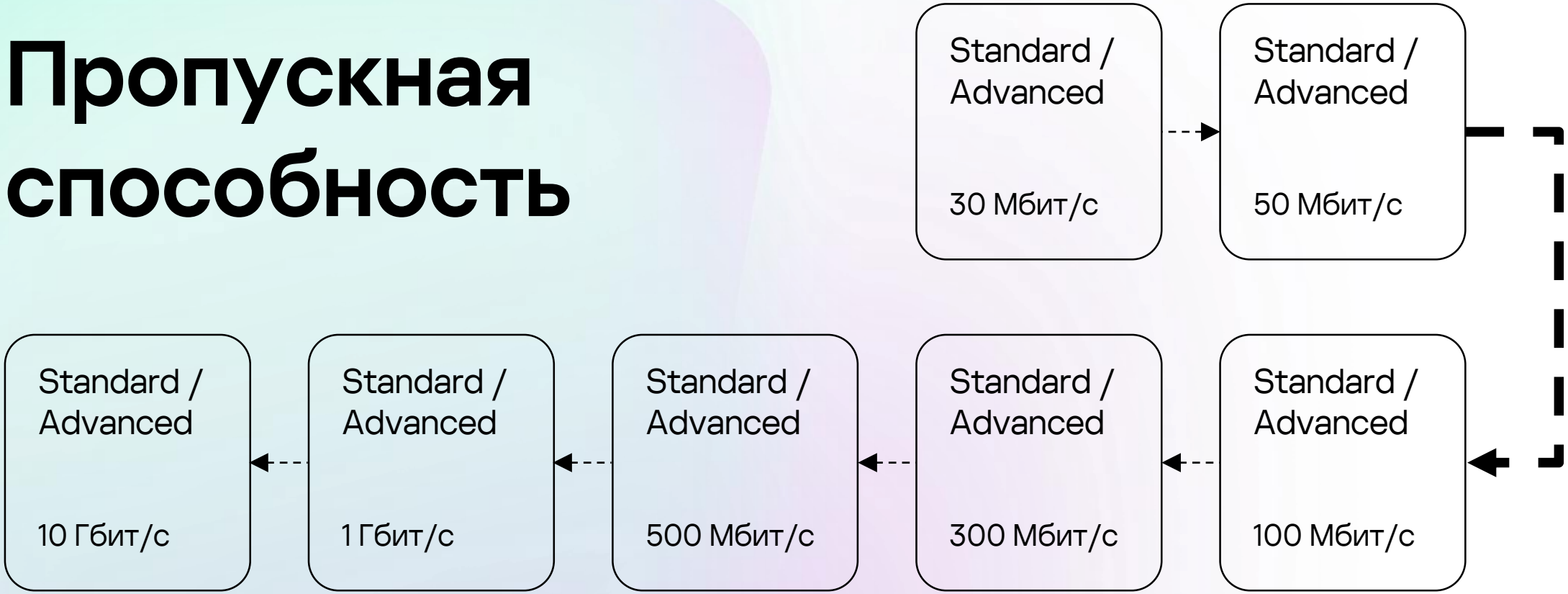
Дополнительные возможности

Доступны сертификаты на замену оборудования в случае выхода из строя

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	●	●
	Поддержка топологий Hub-and-Spoke, Full Mesh, Partial Mesh	●	●
	SLA политики для приложений	●	●
	Динамическая маршрутизация (BGP)	●	●
	Встроенный DPI	●	●
Сервисы SD-WAN	Zero Touch Provisioning	●	●
	Контроль качества каналов в реальном времени	●	●
	Оптимизация каналов (поддержка FEC и дупликации пакетов)	●	●
	Поддержка сервисов P2P, P2M, L2/L3 VPN	●	●
	Поддержка встроенного высокоскоростного шифрования	●	●
Виртуальные сетевые функции	Поддержка интеграции комплиментарных продуктов Kaspersky	●	●
	Реализация ETSI MANO		●
	Поддержка VNF сторонних производителей		●
	Управление жизненным циклом сервисных цепочек		●
	Поддержка uCPE		●
Сервисы	Поддержка Multicast		●
	Поддержка Multi-Tenancy		●

Пропускная способность



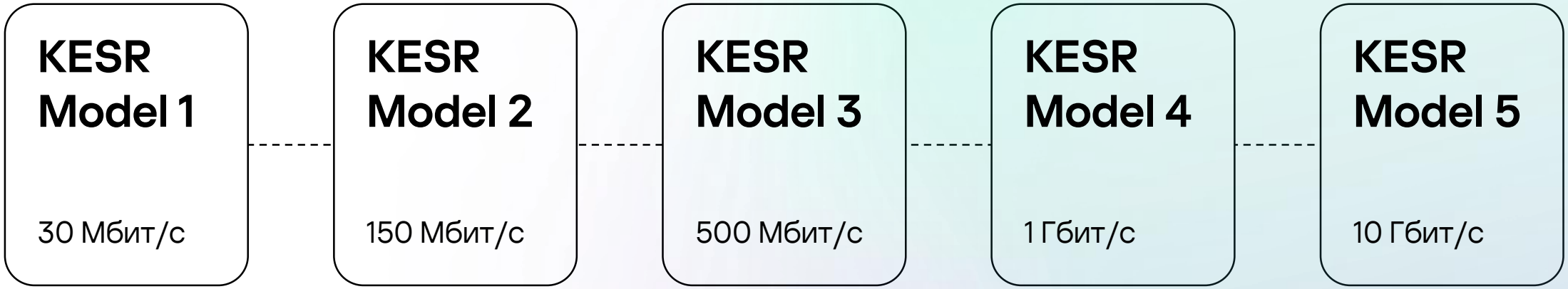
Время реакции на инциденты

Уровень критичности	Premium	Premium Plus
Критический	2 часа *	30 минут *
Высокий	6 рабочих часов	2 часа *
Средний	8 рабочих часов	6 рабочих часов
Низкий	10 рабочих часов	8 рабочих часов

Инциденты обрабатываются в формате 24/7.
Во вне рабочее время требуется дополнительный звонок в тех. поддержку

Рабочими часами считаются будни с 10:00 по 18:30 (время Московское)

Пропускная способность



Пример устройства KESR Model 1 - 30 Мбит/с

KESR-M1-R-5G-2L-W

Процессор
Mediatek MT7621a

Интерфейсы
5 × 10/100/1000 (Auto MDI/MDIX) IEEE 802.3/802.3u/802.ab
2 × LTE Cat.4, 2 × Nano SIM Card, Supports SIM/USIM
2 × встроенных интерфейса mPCIe для модулей 4G
1 × USB 2.0 type-A (USB-порт не используется одновременно со вторым LTEмодулем)
1 × Standard TF card interface

Оперативная память
256 MB

Питание
Внешний адаптер 12В 2.5А

Пример устройства KESR Model 2 - 150 Мбит/с

KESR-M2-K-5G-1L-W

KESR-M2-K-5G-1S

Процессор
Intel Apollo Lake

Интерфейсы
Вариант исполнения 1
5 × 10/100/1000 Ethernet RJ45
1 × LTE
1 × Wi-Fi
Вариант исполнения 2
5 × 10/100/1000 Ethernet RJ45
1 × SFP

Оперативная память:
8 GB

Питание
Внешний блок питания 220 В
Резервирование питания

Пример устройства KESR Model 3 - 500 Мбит/с

KESR-M3-K-4G-4S

Процессор
Intel Xeon-D 1500 (Broadwell)

Интерфейсы
4 × 10/100/1000 Ethernet RJ45
4 × SFP

Оперативная память
32 GB

Питание
Блок питания 220 В
Резервирование питания

Управление сетевыми функциями
Поддержка VNF (продуктов Kaspersky или сторонних производителей)

Примеры устройств KESR Model 4 - 1 Гбит/с

KESR-M4-K-2X-1CPU

KESR-M4-K-8G-4X-1CPU

Процессор
Intel Xeon Scalable

Интерфейсы:
Вариант исполнения 1
2 × SFP+
Вариант исполнения 2
8 × 10/100/1000 Ethernet RJ45
4 × SFP+

Оперативная память
64 GB

Питание
Блок питания 220 В
Резервирование питания

Управление сетевыми функциями
Поддержка VNF (продуктов Kaspersky или сторонних производителей)

Примеры устройств KESR Model 5 - 10 Гбит/с

KESR-M5-K-8X-2CPU

KESR-M5-K-8G-4X-2CPU

Процессор
2 × Intel Xeon Scalable

Интерфейсы
Вариант исполнения 1
8 × SFP+
Вариант исполнения 2
8 × 10/100/1000 Ethernet RJ45
4 × SFP+

Оперативная память
64 GB

Питание
Блок питания 220 В
Резервирование питания

Управление сетевыми функциями
Поддержка VNF (продуктов Kaspersky или сторонних производителей)

Продажа лицензий на ПАК

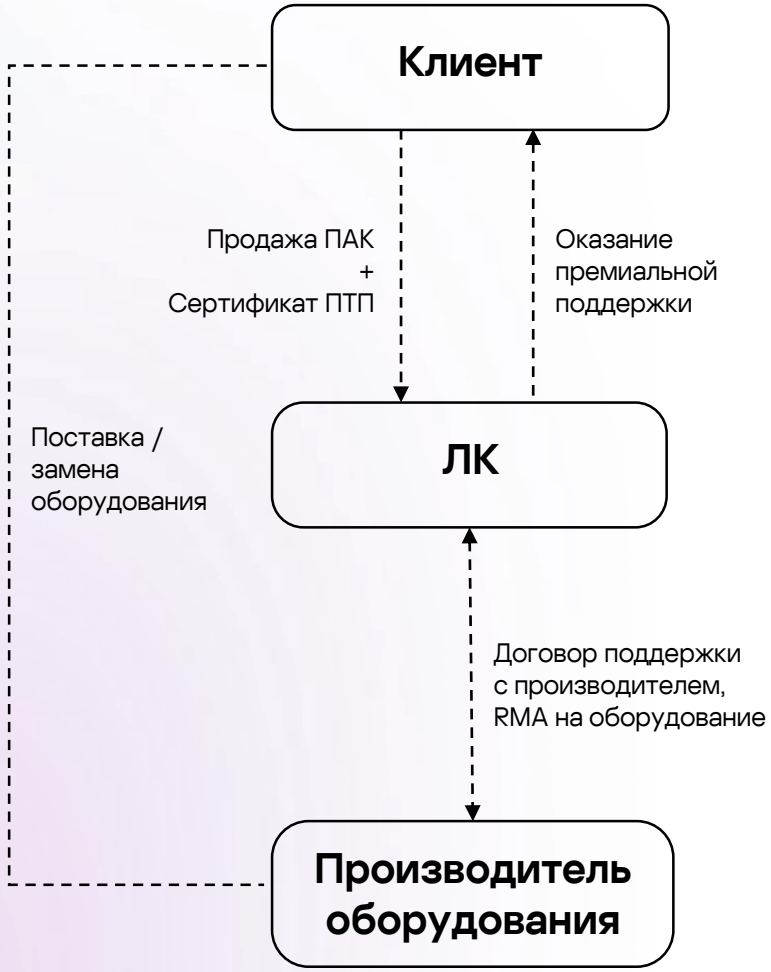
Base

+ сертификат(ы) на ПТП

Сертификат 1

Сертификат 2

Сертификат 3



SLA на премиальную поддержку для программно-аппаратного комплекса

Уровень критичности	Время реакции	Время отправки оборудования
Критический	30 минут *	Следующий календарный день
Высокий	4 часа *	
Средний	6 рабочих часов	
Низкий	8 рабочих часов	

* 24/7 при условии сопровождение заявки дополнительным звонком в службу технической поддержки

Фактическое время доставки зависит от места нахождения клиента и места нахождения сервисного центра, где подменное оборудования есть в наличии

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.

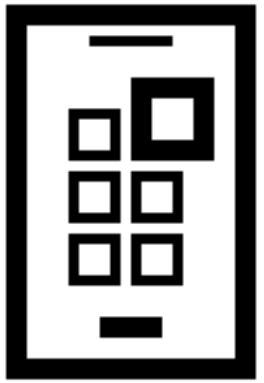
Раньше

Сейчас

Телефон

Навигатор

Компьютер



Смартфон

Раньше

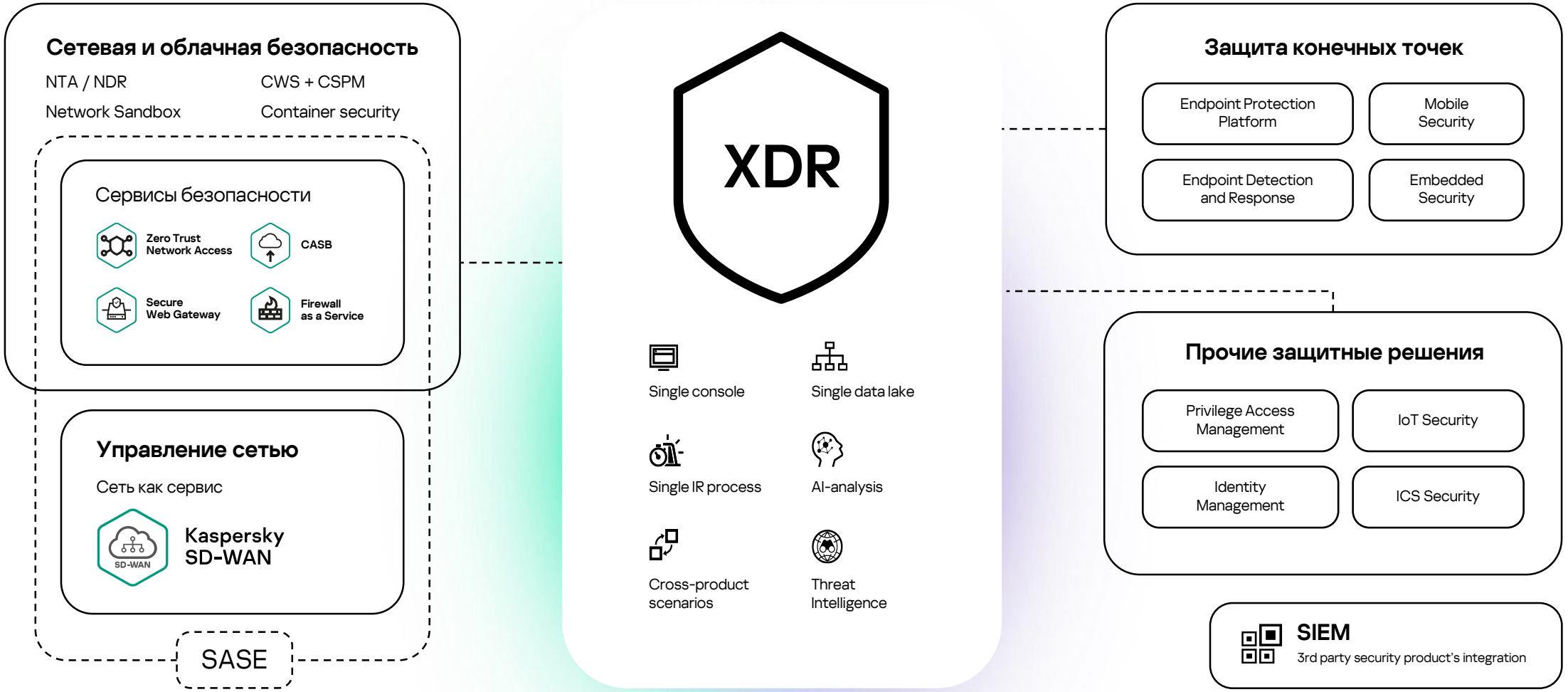
Сейчас

Средства защиты

Сеть

Управление и мониторинг

SD-WAN – важнейшая часть архитектуры SASE



Q&A

Спасибо!

kaspersky