Глобальная экспертиза
и передовые технологии
для защиты от сетевых
угроз и контроля активности
приложений

Kaspersky NGFW KX-Series

kaspersky активируй будущее

Kaspersky NGFW

Межсетевой экран нового поколения на основе глобальной экспертизы и передовых технологий. Продукт защищает корпоративную сеть компаний от широкого спектра киберугроз, контролирует активность приложений и сервисов, позволяет эффективно управлять трафиком и оптимизирует производительность инфраструктуры.

95%

Показатель обнаружения и предотвращения сетевых угроз с помощью IDPS (Detection Rate)*

5 000+

Распознаваемых приложений с помощью собственного DPI

7 000+

Поддерживаемых сигнатур IDPS

20 000+

Поддерживаемых правил Firewall

AI-powered антивирус

На базе оптимизированных технологий Kaspersky Endpoint Security

Кластер active-passive

На базе собственного протокола Kaspersky High-availability Cluster Protocol

Threat Intelligence

Автоматическое обогащение решения уникальными данными об угрозах со всего мира

Комплексная защита

Интеграция с решениями класса XDR, Sandbox и SIEM «Лаборатории Касперского», а также SIEM-системами сторонних производителей

Показатель ТОП-3

Надежные и признанные технологии

Подробнее

Линейка аппаратных платформ KX-Series

Линейка KX (Kaspersky Extension) — семейство сетевых аппаратных платформ, разработанных специально для решения Kaspersky NGFW. Эти устройства обеспечивают высокую производительность, надежную защиту от киберугроз и масштабируемость для различных сценариев использования.

Аппаратные платформы KX-Series предназначены для максимального раскрытия потенциала решения Kaspersky NGFW и подходят для работы даже в сложных сетевых инфраструктурах.

Особенности KX-Series

До 200 Гбит/с

Производительность в режиме L4 FW + Application Control**

1 Rack Unit

Удобное исполнение и экономия места в серверной стойке

Архитектура x86

Высокая производительность без использования внешних ускорителей

SFP+ и QSFP28

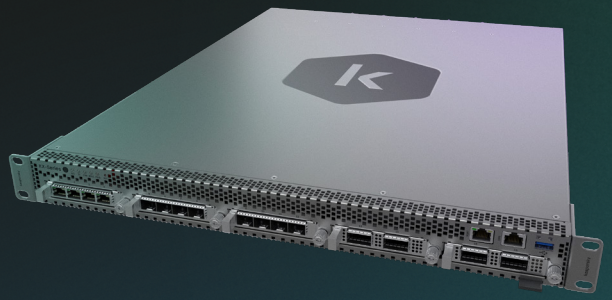
Высокоскоростные порты для обеспечения связности и упрощения дизайна высоконагруженной сети

Внешний вид модели

KX-100

Внешний вид моделей

KX-400
KX-1000
KX-3500



* Тестирование проводилось с помощью IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

** Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Параметры аппаратных платформ

	KX-100-KA1	KX-100-KB1	KX-400
Производительность в режиме L4 FW + Application Control*	До 10 Гбит/с	До 10 Гбит/с	До 40 Гбит/с
Производительность в режиме NGFW (L4 FW + Application Control + IDPS)*	До 3 Гбит/с	До 3 Гбит/с	До 10 Гбит/с
Производительность в режиме Threat Prevention (L4 FW + Application Control + IDPS + AV + WC + DNS Sec)*	До 1.2 Гбит/с	До 1.2 Гбит/с	До 7 Гбит/с
Производительность в режиме Threat Prevention + SSL Inspection*	До 1.1 Гбит/с	До 1.1 Гбит/с	До 6 Гбит/с
Скорость установления новых сессий в секунду (CPS) в режиме L4 FW + Application Control*	До 64 000	До 64 000	До 370 000
Максимальное количество одновременно установленных сессий (CC) в режиме L4 FW + Application Control*	До 3 000 000	До 3 000 000	До 25 000 000
Процессор	Intel Atom	Intel Atom	Intel Xeon Gen4
Интерфейсы	• 6 × 10/100/1000 Ethernet RJ45 • 2 × SFP+	• 14 × 10/100/1000 Ethernet RJ45 • 2 × SFP+	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28
Питание	Два блока питания 220В	Два блока питания 220В (hot-swap)	Два блока питания 220В (hot-swap)
Энергопотребление	< 350 Вт	< 350 Вт	< 700 Вт
Размеры (ш × г × в)	285 x 240 x 48 мм	438 x 336 x 44 мм	439 x 630 x 43 мм
Вес	5 кг	8 кг	10 кг
Охлаждение	Пассивное	Активное	Активное, 5 вентиляторов (hot-swap)
Направление воздушного потока	—	От передней панели к задней (Front to back)	От передней панели к задней (Front to back)
Крепление	Настольное размещение	Размещение в серверной стойке 19"	Размещение в серверной стойке 19"

Узнать подробнее о методике тестирования производительности

Подробнее

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

	KX-1000	KX-3500
Производительность в режиме L4 FW + Application Control*	До 100 Гбит/с	До 200 Гбит/с
Производительность в режиме NGFW (L4 FW + Application Control + IDPS)*	До 20 Гбит/с	До 50 Гбит/с
Производительность в режиме Threat Prevention (L4 FW + Application Control + IDPS + AV + WC + DNS Sec)*	До 15 Гбит/с	До 35 Гбит/с
Производительность в режиме Threat Prevention + SSL Inspection*	До 10 Гбит/с	До 25 Гбит/с
Скорость установления новых сессий в секунду (CPS) в режиме L4 FW + Application Control*	До 449 000	До 1 500 000
Максимальное количество одновременно установленных сессий (CC) в режиме L4 FW + Application Control*	До 48 000 000	До 100 000 000
Процессор	Intel Xeon Gen5	Intel Xeon Gen5
Интерфейсы	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28
Питание	Два блока питания 220В (hot-swap)	Два блока питания 220В (hot-swap)
Энергопотребление	< 700 Вт	< 700 Вт
Размеры (ш × г × в)	439 x 630 x 43 мм	439 x 630 x 43 мм
Вес	10 кг	10 кг
Охлаждение	Активное, 5 вентиляторов (hot-swap)	Активное, 5 вентиляторов (hot-swap)
Направление воздушного потока	От передней панели к задней (Front to back)	От передней панели к задней (Front to back)
Крепление	Размещение в серверной стойке 19"	Размещение в серверной стойке 19"

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Виртуальные платформы

В рамках линейки KX-Series доступны также виртуальные исполнения — vKX. Они предназначены для развертывания Kaspersky NGFW на собственных ресурсах заказчика без необходимости использования аппаратных платформ. В данный момент доступно виртуальное исполнение Kaspersky NGFW vKX-8.

vKX-8

Параметры	Значения
Производительность в режиме L4 FW + Application Control*	До 5 Гбит/с
Производительность в режиме NGFW (L4 FW + Application Control + IDPS)*	До 2.5 Гбит/с
Производительность в режиме Threat Prevention (L4 FW + Application Control + IDPS + AV + WC + DNS Sec)*	До 1.6 Гбит/с
Производительность в режиме Threat Prevention + SSL Inspection*	До 1.6 Гбит/с
Скорость установления новых сессий в секунду (CPS) в режиме L4 FW + Application Control*	До 11 000
Максимальное количество одновременно установленных сессий (CC) в режиме L4 FW + Application Control*	До 64 000
Гипервизоры	KVM или VMware ESXi
Количество ядер	8
Интерфейсы	10 шт.
Оперативная память	16 ГБ
Хранилище	128 ГБ
Требования к процессору	Broadwell или выше
Требования к ОС	Ubuntu 22.04 или выше
Формат поставки	• QCOW2 + XML файл • OVA

Узнать подробнее о методике тестирования производительности

Подробнее

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Возможности продукта

Функции управления и мониторинга

Централизованное управление Kaspersky NGFW и мониторинг состояния решения через централизованную консоль управления Open Single Management Platform (OSMP)	●
Ролевая модель доступа (RBAC) для разграничения возможных действий пользователя при работе с политиками и настройками в OSMP	●
Отправка системных событий и событий безопасности, сформированных Kaspersky NGFW, в консоль OSMP и сторонние SIEM-системы	●
Аналитические панели мониторинга и отчеты по результатам работы решения в OSMP	●
Импорт и экспорт политик безопасности решения в OSMP	●
Централизованное управление сетевой конфигурацией при помощи шаблонов	●
Создание и настройка зон в OSMP	●
Поддержка обновления ПО NGFW	●
Возможность настройки периода и источника обновления локальных баз NGFW	●
Zabbix-шаблон для мониторинга NGFW	●

Сетевые функции

Поддержка настройки статической маршрутизации IPv4 через CLI Kaspersky NGFW	●
Поддержка отказоустойчивого кластера active-passive с синхронизацией сессий на базе собственного протокола KHCP (Kaspersky High-availability Cluster Protocol)	●
Поддержка синхронизации маршрутной информации между нодами кластера (RIB)	●
Поддержка агрегированных интерфейсов	●
Поддержка L2-интерфейсов	●
Поддержка VLAN и саб-интерфейсов	●
Поддержка VRF	●
Поддержка DNS-клиента	●
Поддержка DHCP-клиента	●
Поддержка NTP-клиента	●
Поддержка SNMP	●
Поддержка виртуального исполнения Kaspersky NGFW на базе гипервизоров KVM и VMware ESXi	●
BFD	●
BGP	●
OSPF	●
Мониторинг интерфейсов в кластере	●
DHCP Relay	●
Возможность настройки таймаутов сессий	●

Функции безопасности

Возможность создания групповых политик безопасности	●
Автоматическое обновление локальных баз движков безопасности Kaspersky NGFW: антивируса, веб- контроля, защиты DNS-трафика и IDPS	●
Межсетевой экран с отслеживанием состояния сессий (Stateful Firewall)	●
Поддержка GeoIP-политик	●
Система обнаружения и предотвращения вторжений (IDPS) с поддержкой более 7 000 сигнатур	●
Глубокая проверка пакетов (DPI) с поддержкой контроля трафика более 5 000 приложений	●
Инспектирование SSL/TLS-трафика с поддержкой TLS 1.1, 1.2 и 1.3	●
Возможность создания исключений по веб-категориям и конкретным доменам в движке SSL/TLS-инспекции	●
Потоковый антивирус	●
Проверка репутации URL-адресов (malware, phishing, c&c, adware и т.п.)	●
Категоризация и контроль веб-трафика	●
Возможность создания пользовательских веб-категорий	●
Механизм добавления исключений в правила проверки веб-трафика	●
Менеджер для просмотра установленных через Kaspersky NGFW сессий с возможностью их сброса	●
Поддержка проверки DNS-трафика (DNS Security) по репутационным базам	●
Получение актуальных тактических данных об угрозах (Threat Intelligence) для проверки репутации URL-адресов и обогащения баз антивируса и веб-категоризатора	●
Нативная интеграция с Kaspersky Symphony XDR посредством плейбуков	●
Поддержка политик с использованием зон	●
Поддержка NAT	●
Поддержка работы правил фильтрации по расписанию	●
Интеграция по API с Kaspersky Anti Targeted Attack для проверки файлов с помощью Sandbox	●
AI-powered антивирус	●
Антивирусная проверка архивов с любыми расширениями	●
Поддержка ICAP-клиента для отправки файлов на проверку в сторонние системы	●
User-aware политики	●
Возможность использования FQDN в качестве destination в правилах межсетевого экрана	●
Поддержка действия Reset-both в правилах межсетевого экрана	●
Антивирусная проверка по почтовым протоколам	●
Использование зон в качестве квалификаторов в правилах SSL/TLS-инспекции	●

Почему Kaspersky NGFW

Полностью российский продукт, соответствующий стратегии движения к импортонезависимости

Полный контроль и эффективное управление сетевым трафиком и активностью приложений

Экосистемный подход к защите корпоративной инфраструктуры и централизованное управление

Собственная архитектура и механизмы безопасности, основанные на лидерских технологиях

Прозрачное лицензирование без дополнительных модулей и расширений

Глобальная экспертиза в борьбе с киберугрозами, разработке продуктов и поддержке клиентов

Подробнее

Уникальный опыт экспертов в основе решения

Глобальный центр исследований и анализа угроз

GREAT

Исследование сложных угроз и расследование финансово мотивированных киберпреступлений

Центр исследования угроз

Threat Research

Исследование угроз, создание детектирующей логики, контентная фильтрация, безопасная разработка

Центр исследования технологий искусственного интеллекта

AI Technology Research

Обнаружение угроз с помощью ИИ / усиление ИБ решений алгоритмами ИИ

Центр исследования безопасности промышленных систем*

ICS CERT

Анализ угроз в индустриальных инфраструктурах

● Исследование угроз ● Расследование инцидентов

* В рамках разработки решения для промышленных инфраструктур, с 2026 года

Kaspersky NGFW

Узнать больше

www.kaspersky.ru

#kaspersky
#активируйбудущее