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)*

6 000+

Распознаваемых приложений с помощью собственного DPI

9 000+

Поддерживаемых сигнатур IDPS

до 100 000

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

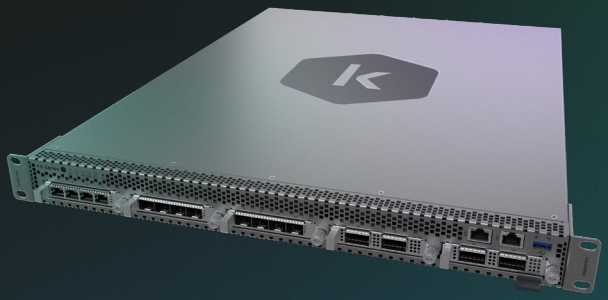
Внешний вид моделей

KX-100-KA1

KX-100-KB1

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 15 Гбит/с
Производительность в режиме Threat Prevention (L4 FW + Application Control + IDPS + AV + WC + DNS Sec)*	До 2 Гбит/с	До 2 Гбит/с	До 12 Гбит/с
Производительность в режиме Threat Prevention + SSL Inspection*	До 1.5 Гбит/с	До 1.5 Гбит/с	До 8 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 40 Гбит/с	До 140 Гбит/с
Производительность в режиме Threat Prevention (L4 FW + Application Control + IDPS + AV + WC + DNS Sec)*	До 30 Гбит/с	До 60 Гбит/с
Производительность в режиме Threat Prevention + SSL Inspection*	До 20 Гбит/с	До 33 Гбит/с
Скорость установления новых сессий в секунду (CPS) в режиме L4 FW + Application Control*	До 800 000	До 1 300 000
Максимальное количество одновременно установленных сессий (CC) в режиме L4 FW + Application Control*	До 40 000 000	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 4 Гбит/с
Производительность в режиме Threat Prevention (L4 FW + Application Control + IDPS + AV + WC + DNS Sec)*	До 2.5 Гбит/с
Производительность в режиме Threat Prevention + SSL Inspection*	До 2 Гбит/с
Скорость установления новых сессий в секунду (CPS) в режиме L4 FW + Application Control*	До 79 000
Максимальное количество одновременно установленных сессий (CC) в режиме L4 FW + Application Control*	До 512 000
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

Централизованная система управления (Kaspersky Security Center (KSC) + Kaspersky Unified Monitoring and Analysis Platform (KUMA))

Комплексное управления продуктами экосистемы Kaspersky для XDR-сценария через централизованную консоль управления Open Single Management Platform (OSMP)

Аналитические панели мониторинга и отчеты по результатам работы решения в OSMP или KUMA

Возможность предварительного просмотра внесенных в политику изменений перед ее применением

Централизованное управление сетевой конфигурацией при помощи шаблонов

Мониторинг состояния решения в режиме реального времени

Экспорт событий в SIEM-системы через Syslog	Zabbix-шаблон для мониторинга NGFW
Ролевая модель доступа (RBAC)	Командная строка (CLI)
Поддержка виртуальных контекстов (VSS)	Подключение через SSH
Поддержка обновления ПО NGFW	Интеграция по LDAP (MS AD)
SNMPv2, SNMPv2c, SNMPv3	Многофакторная аутентификация TOTP (RFC 6238)
SNMP trap	Языки интерфейса — русский, английский

Сетевые функции

Статическая маршрутизация IPv4	Поддержка VRF
BGPv4	Поддержка DNS-клиента
OSPFv2	Поддержка DHCP-клиента
BFD	Поддержка NTP-клиента
Поддержка агрегированных интерфейсов (LACP)	Policy-Based Routing (PBR)
Поддержка L2 (bridge) интерфейсов	Поддержка Multi-WAN на базе IP SLA
Поддержка L3-интерфейсов	DHCP Relay
Поддержка VLAN (802.1q) и саб-интерфейсов	

Site-to-Site VPN

Policy-Based IPSec

Route/GRE-Based IPSec

IKEv2

Алгоритмы шифрования

- AES-CBC-128	- AES-CBC-256	- AES-GCM-192
- AES-CBC-192	- AES-GCM-128	- AES-GCM-256

NAT Traversal

Трансляция сетевых адресов

Source NAT

Destination NAT

Статический NAT

Динамический NAT

PAT

NAT oversubscription

Отказоустойчивость

Поддержка отказоустойчивого кластера active-passive на базе собственного протокола KHCP (Kaspersky High-availability Cluster Protocol)

Синхронизация сессий

Синхронизация маршрутной информации (RIB)

Синхронизация ARP-таблиц

Мониторинг интерфейсов в кластере

Поддержка виртуальных MAC и IP-адресов

GARP

Режимы автоматического и ручного переключения на резервный узел кластера

Режим автоматического переключения на резервный канал связи в случае нарушения параметров IP SLA (задержка, потери, доступность)

Поддержка отказоустойчивости системы управления

Выделенный control plane

Межсетевой экран

Поддержка Stateful Packet Inspection

Поддержка использования зон

Поддержка фильтрации трафика по:

- IP-адресам (host, подсеть, диапазон)
- Зонам
- Пользователям и группам пользователей
- FQDN
- GeoIP
- Сервисам (L3/L4 протокол + порт)
- Приложениям и категориям приложений

Распознавание при помощи DPI более 6 000 приложений

Интеграция с внешними каталогами пользователей (MS AD)

Поддержка групп объектов и вложенных групп

Логирование начала и конца сессии

Время жизни и/или расписание работы для правил

Использование групповых профилей модулей безопасности в правилах

Функции безопасности

- Антивирусная проверка по протоколам: HTTP(S), SMTP(S), POP3(S) и IMAP(S)
- Антивирусная проверка архивов с любыми расширениями
- Проверка репутации URL-адресов (malware, phishing, c&c, adware и т.п.)
- Инспектирование SSL/TLS-трафика с поддержкой TLS 1.1, 1.2 и 1.3
- Система обнаружения и предотвращения вторжений (IDPS) с поддержкой более 9 000 собственных сигнатур
- Возможность исключений в SSL/TLS-инспекции по веб-категориям и конкретным доменам
- Отправка расшифрованного трафика на анализ всеми модулями безопасности
- Отображение страниц блокировок и предупреждения при попытке доступа на веб-ресурс
- Поддержка проверки DNS-трафика (DNS Security) по репутационным базам
- Возможность настройки периода и источника обновления локальных баз NGFW
- Нативная интеграция с Threat Intelligence для обогащения баз модулей антивируса и веб-фильтрации
- Менеджер сессий для просмотра и контроля установленных сессий
- Возможность настройки таймаутов сессий для устройств и VSS
- Потоковый антивирус
- AI-powered антивирус
- Возможность блокировки Partial Content
- Интеграция с песочницей KATA по API
- ICAP клиент
- Возможность указания минимальной версии TLS
- Валидация сертификата сервера
- Категоризация и контроль веб-трафика по SNI или URL
- Более 90 предустановленных веб-категорий
- Поддержка пользовательских веб-категорий
- Возможность исключения сигнатур IDPS
- Захват трафика при сработках сигнатур IDPS
- IDPS проверка по неклассифицированным сессиям
- Поддержка исключений для веб-фильтрации
- Поддержка работы правил фильтрации по расписанию
- Поддержка DNS-redirect
- Защита от IP Spoofing
- Защита от сетевого сканирования

Поддержка гипервизоров

- KVM
- VMware ESXi

Интеграция с продуктами от Лаборатории Касперского

- Kaspersky Symphony XDR (посредством плейбуков)
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Anti Targeted Attack (по API для проверки файлов с помощью Sandbox)

Почему Kaspersky NGFW

Полностью российский продукт, соответствующий стратегии движения к импортонезависимости (сертификация ФСТЭК России)

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

Исследование сложных угроз и расследование финансово мотивированных киберпреступлений

Центр исследования угроз

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

Центр исследования технологий искусственного интеллекта

Обнаружение угроз с помощью ИИ / усиление ИБ решений алгоритмами ИИ

Центр исследования безопасности промышленных систем*

Анализ угроз в индустриальных инфраструктурах

● Исследование угроз ● Расследование инцидентов

* В рамках разработки решения для промышленных инфраструктур, с 2027 года

Kaspersky NGFW

Узнать больше

www.kaspersky.ru

#kaspersky
#активируйбудущее