Kaspersky IoT Secure Gateway 1000. Характеристики продукта

Kaspersky IoT Secure Gateway 1000 помогает строить безопасные и функциональные системы интернета вещей. Основанный на операционной системе KasperskyOS, шлюз обладает кибериммунитетом — это значит, что он будет выполнять свои критичные функции даже в агрессивной среде.

KISG 1000 служит надежной точкой подключения IoT-устройств к облачным платформам, защищает инфраструктуру от кибератак и делает ее прозрачной. Шлюз безопасно собирает данные и отправляет их в облака через протокол MQTT поверх TLS.

Удобный централизованный мониторинг и администрирование всех событий KISG 1000 осуществляется через консоль **Kaspersky Security Center**. Вместе эти два продукта образуют комплексное решение **Kaspersky IoT Infrastructure Security**.

Подробнее на os.kaspersky.ru

Аппаратная платформа	Advantech UTX-3117
Процессор	Intel Pentium N4200, 1,1 ГГц, 2МБ L2 Cache
ОЗУ	4ГБ, DDR3L, 1600 МГц
Накопители	SATA II SSD (32 ГБ), 2xMiniPCIe, 1xM.2 B-key
Интерфейсы	2xGbE LAN
Габариты	128x152x37 мм
Диапазон рабочих температур	-20...+60 °C
Дополнительно	SIM-карта

Подключение	
Ethernet	Два гигабитных интерфейса для подключения к различным сегментам сети по витой паре (LAN и WAN)
Сотовый модем	Возможность использовать мобильную сеть передачи данных в качестве основного или резервного канала связи
Маршрутизация и NAT	Автоматически настраиваемая маршрутизация между интерфейсами KISG 1000. Возможность управлять работой NAT (маскарадинг)
DHCP-сервер	Автоматическое распространение сетевой конфигурации на IoT и другие устройства, расположенные в локальной сети
MQTT-брокер	MQTT-брокер на базе Mosquitto позволяет осуществлять централизованный сбор данных IoT-устройств (сенсоров и актуаторов, умных реле и т.д.)

kaspersky

KasperskyOS

OpenSSL/TLS	Поддержка распространенных механизмов криптографической защиты данных, передаваемых по протоколу MQTT (Syslog)
MQTT поверх TLS	Безопасное подключение и защищенная передача данных между шлюзом и облачной платформой
Интеграция с облачными сервисами	MS Azure, Amazon AWS, IBM Bluemix и т.д. Работа с любыми облачными системами по протоколу MQTT

Гибкое управление защитой и шлюзом

Веб-интерфейс	Удобная настройка и мониторинг IoT-сети, видимость и прозрачность благодаря WebGUI. Информативный дэшборд позволяет быстро получить все необходимые сведения
Централизованная система управления	Платформа Kaspersky Security Center позволяет работать с событиями, получаемыми со всех KISG 1000, развернутых в инфраструктуре организации. Также она позволяет отслеживать состояние шлюзов и управлять их конфигурацией

Защита IoT-шлюза от кибератак

Исходная безопасность (Secure by design)	Кибериммунная операционная система KasperskyOS исключает возможность компрометации устройства, а значит, делает невозможной утечку данных или проникновение в инфраструктуру предприятия
Безопасная загрузка (Secure boot)	Верификация целостности и подлинности прошивки шлюза с использованием криптографических методов перед загрузкой образа. Несанкционированно измененная или поврежденная прошивка не будет загружена
Безопасное обновление (Secure update)	Работая в комплексе с Безопасной загрузкой, технология позволяет обновлять прошивку только с использованием правильно подписанных и зашифрованных образов

Защита IoT-инфраструктуры

IDS/IPS и межсетевой экран (Firewall)	Межсетевой экран работает по принципу Default Deny. Администратор может быть уверен, что через шлюз будут проходить только разрешенные сетевые взаимодействия. Модуль IDS/IPS (обнаружение и предотвращение вторжений) уведомляет и блокирует зловредные активности, обнаруженные с помощью подготовленного специалистами «Лаборатории Касперского» набора сигнатур
Обнаружение и классификация IoT-устройств	Обнаруживает устройства, расположенные в локальной сети на основе их сетевой активности. В пользовательском интерфейсе можно увидеть все устройства сети, взаимодействующие с KISG 1000, а новые будут обнаружены в течение 60 секунд
Отчеты и уведомления (MQTT, SYSLOG, push-уведомления, Kaspersky Security Center)	Администратор может получать события безопасности KISG 1000 в единую систему управления безопасностью предприятия — Kaspersky Security Center, а также передавать события в сторонние системы (SIEM, облачные платформы и т.п.) по протоколам Syslog и MQTT. KISG 1000 поддерживает интеграцию с Google Firebase для передачи push-уведомлений на мобильные устройства

KasperskyOS

Kaspersky IoT Secure Gateway 1000

Подробнее на os.kaspersky.ru

www.kaspersky.ru