Kaspersky IoT Secure Gateway 3.0

kaspersky aprotech Kaspersky IoT company

Kaspersky IoT Secure Gateway 3.0 поддерживает два режима работы:

однонаправленный шлюз (диод данных)

роутер/межсетевой экран

Ниже описаны основные возможности Kaspersky IoT Secure Gateway 3.0 при работе в каждом из режимов, а также общие для обоих режимов возможности.

Основные характеристики Kaspersky IoT Secure Gateway 3.0 при работе в качестве однонаправленного шлюза

Однонаправленный транспорт данных

Ethernet, 3G/LTE. Шлюз обеспечивает однонаправленную передачу данных через Ethernet и сети 3G/LTE, что позволяет надежно передавать данные с промышленного оборудования на облачные платформы. Такая конфигурация повышает безопасность системы, предотвращая обратные потоки данных и киберугрозы.

Сетевые функции

- **DHCP-сервер.** Встроенный DHCP-сервер автоматизирует процесс назначения IP-адресов и других сетевых параметров, упрощая управление сетью и снижая вероятность конфигурационных ошибок.

Подключение к облачным сервисам с помощью сторонних приложений. Шлюз позволяет подключаться к различным облачным сервисам, обеспечивая гибкость и масштабируемость при передаче данных с промышленного оборудования на облачные платформы для дальнейшей обработки и анализа.

Безопасность

- **Шифрованный канал TLS.** Шлюз обеспечивает шифрование данных при передаче через сеть с использованием протокола TLS, что гарантирует защиту информации от перехвата и несанкционированного доступа.

VPN-клиент. Устройство поддерживает установку сторонних VPN-клиентов, которые обеспечивают защищенное соединение с удаленными сетями и серверами, повышая уровень безопасности данных при передаче через интернет.

— приложение доступно в Kaspersky Appicenter

Основные характеристики Kaspersky IoT Secure Gateway 3.0

при работе в качестве роутера/межсетевого экрана

Двунаправленный транспорт данных

Ethernet, 3G/LTE. Шлюз обеспечивает двунаправленную передачу данных через Ethernet и сети 3G/LTE, что позволяет гибко подключаться к различным сетям и адаптироваться к меняющимся условиям связи. Это делает устройство идеальным для использования в промышленности и других областях, требующих надежной и быстрой передачи данных.

Сетевые функции

- **Маршрутизация.** Шлюз поддерживает функции маршрутизации, позволяя эффективно управлять сетевыми потоками и обеспечивать надежную передачу данных между различными сегментами сети. Это способствует улучшению сетевой производительности и управляемости.
- **NAT и Port Forwarding.** Поддержка NAT и переадресации портов позволяет скрывать внутренние IP-адреса и управлять доступом к сетевым ресурсам. Эти функции улучшают безопасность сети и обеспечивают гибкость в управлении сетевыми подключениями.
- **Кластеризация VRRP.** Поддержка кластеризации с помощью VRRP (Virtual Router Redundancy Protocol) обеспечивает высокую доступность и отказоустойчивость сети, позволяя минимизировать время простоя и потери данных.
- **DHCP-сервер.** Встроенный DHCP-сервер автоматизирует процесс назначения IP-адресов и других сетевых параметров, что упрощает управление сетью и снижает вероятность конфигурационных ошибок.
- **MQTT-брокер.** Поддержка MQTT-брокера позволяет эффективно управлять публикацией и подпиской на данные в IoT-сетях, обеспечивая быструю и надежную передачу сообщений между устройствами.

Безопасность

- **Межсетевой экран (Default Deny).** Политика межсетевого экрана по умолчанию «Default Deny» обеспечивает высокий уровень безопасности, блокируя все неавторизованные подключения и предотвращая несанкционированный доступ.
- **Фильтрация (блокирование) трафика прикладных протоколов.** Функция глубокого анализа пакетов (DPI) позволяет фильтровать и блокировать трафик прикладных протоколов (FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3), улучшая контроль над сетевым трафиком и предотвращая потенциальные угрозы.
- **Дополнительные функции межсетевого экранирования.** Функции реализованы с помощью приложения Network Protector, доступного в Kaspersky Appicenter
  - **Межсетевой экран уровня промышленной сети:** Kaspersky IoT Secure Gateway 3.0 поддерживает контроль и фильтрацию промышленных протоколов (MQTT, Modbus, BACnet, DNP3, MMS, OMRON-FINS, ENIP/CIP, TriStation, S7comm), что обеспечивает защиту критически важных инфраструктур от киберугроз.
  - **IDS/IPS.** Модуль IDS/IPS обнаруживает и предотвращает сетевые вторжения, обеспечивая активную защиту сети от атак и обеспечивая безопасность данных.
- **Интеграция с SIEM.** Интеграция с системами управления информационной безопасностью (SIEM) обеспечивает централизованный мониторинг и анализ событий безопасности, повышая общую осведомленность о состоянии сети и ускоряя реакцию на инциденты.

— приложение доступно в Kaspersky Appicenter

Общие характеристики для обоих режимов работы

Kaspersky IoT Secure Gateway 3.0

Гибкое управление шлюзом

- **Централизованное управление через.** Для Kaspersky IoT Secure Gateway 3.0 доступно централизованное управление через Kaspersky Security Center (KSC), что позволяет легко и эффективно настраивать, мониторить и управлять устройствами из единого центра. Это упрощает администрирование и улучшает контроль над сетью.
- **Веб-интерфейс:** Удобный веб-интерфейс Kaspersky IoT Secure Gateway 3.0 обеспечивает прямой доступ к настройкам и управлению устройством из локальной сети с помощью веб-браузера. Доступ к веб-интерфейсу защищается с помощью сертификатов TLS.
- **Управление доступом на основе ролей (Пользователь и Администратор).** Шлюз поддерживает управление доступом на основе ролей, что позволяет разграничить права пользователей и администраторов. Это обеспечивает безопасный доступ к конфигурации и функциям устройства, предотвращая несанкционированные изменения.
- **Поддержка сторонних приложений.** Шлюз может использовать приложения сторонних разработчиков, которые доступны в платформе Kaspersky Appicenter. Например, возможна поддержка приложений для работы с протоколами OPC UA и Modbus TCP (для приема данных) и MQTT Publisher (для передачи данных в облачную платформу). Эти приложения обеспечивают эффективную и надежную конвертацию данных между протоколами, что упрощает интеграцию и взаимодействие между устройствами в сети IoT.
- **Управление сторонними приложениями.** Вне зависимости от подхода к управлению устройством функциональность Kaspersky Appicenter позволяет находить, устанавливать, обновлять и удалять приложения в любом интерфейсе.

Защита шлюза от кибератак

- **ОС типа «А» четвертого класса защиты.** Шлюз разработан на базе операционной системы KasperskyOS, которая сертифицирована как операционная система типа «А» четвертого класса защиты, что подтверждает его соответствие высоким стандартам информационной безопасности.
- **Кибериммунитет (Secure by Design).** Шлюз разработан с учетом принципов кибериммунитета, что означает встроенную защиту от кибератак и уязвимостей на этапе разработки. Это значительно снижает риск успешных атак и повышает надежность устройства.
- **Безопасная загрузка (Secure boot).** Функция безопасной загрузки (Secure boot) шлюза обеспечивает проверку подлинности и целостности программного обеспечения при запуске, предотвращая загрузку неавторизованных и потенциально вредоносных программ.
- **Безопасное обновление (Secure update).** Шлюз поддерживает безопасное обновление программного обеспечения, что позволяет надежно обновлять систему, минимизируя риск установки неподлинных или скомпрометированных обновлений. Это помогает поддерживать актуальность и безопасность устройства в течение всего срока его эксплуатации.