Построение безопасной инфраструктуры для встраивания Kaspersky IoT Secure Gateway 1000

В этом документе приведены рекомендации по построению инфраструктуры предприятия таким образом, чтобы гарантировать безопасную работу Kaspersky IoT Secure Gateway 1000

kaspersky

kaspersky cyber immunity

Оглавление

1. Глоссарий

Kaspersky IoT Secure Gateway 1000 – аппаратно-программный комплекс на базе операционной системы KasperskyOS, предназначенный для защиты IoT-устройств.

Kaspersky Security Center – программа для централизованного решения основных задач по управлению и обслуживанию системы защиты сети предприятия.

Аппаратная платформа – конечное устройство, на которое устанавливается образ системы.

Внешняя сеть (англ. WAN) – внешний сегмент сети относительно Kaspersky IoT Secure Gateway 1000.

Внутренняя сеть (англ. LAN) – внутренний сегмент сети относительно Kaspersky IoT Secure Gateway 1000.

Данные и информация – любая информация в электронном виде, например, файлы приложений и данные в базах данных.

Демилитаризованная зона – сегмент сети, находящийся внутри доверенного сегмента и полностью изолированный от взаимодействия с другими объектами в доверенном сегменте.

Кибериммунная система – система, декларированные активы которой защищены от нежелательных событий при любых условиях, даже под атакой, при условии заданных ограничений. Необходимым условием кибериммунной системы является определение целей безопасности и предположений безопасности (условий, в которых будет эксплуатироваться система).

Образ приложения – набор исполняемых файлов и библиотек, из которых состоит приложение.

Объект – физический или виртуальный информационный ресурс. Например, файл, каталог, том, виртуальная машина или сетевой узел (устройство, маршрутизатор, компьютер).

Операция – действие, которое субъект выполняет над объектами. Например, чтение, запись, изменение, удаление, выполнение.

Предположения безопасности – дополнительные ограничения, накладываемые на условия эксплуатации системы, облегчающие или усложняющие выполнение целей безопасности.

Приложение – компонент, устанавливаемый поверх образа системы и запускаемый средствами Kaspersky IoT Secure Gateway 1000. Может быть разработано АО "Лаборатория Касперского" или поставляться партнером. Приложение взаимодействует с Kaspersky IoT Secure Gateway 1000 и другими приложениями посредством API, предоставляемого Kaspersky IoT Secure Gateway 1000.

Пакет приложения – набор всех файлов, из которых состоит приложение.

Ресурс – информационный ресурс, который может быть физическим (канал связи, порт, раздел диска, процессорное время) или логическим (файлы, данные, приложения, сетевые сервисы).

Система контроля – система которая решает, какие операции субъект может или не может выполнять над объектом.

Система предотвращения вторжений – система, которая обнаруживает вторжения нарушения безопасности и автоматически от них защищает.

Событие аудита – событие безопасности (например, перезагрузка, обновление версии системы, события информационной безопасности).

Субъект – сущность, которая потребляет информационные ресурсы. Например, пользователи, группы пользователей или прикладные процессы, потребляющие ресурсы от имени пользователей.

Цели безопасности – это требования, предъявляемые к кибериммунной информационной системе, выполнение которых обеспечивает безопасное функционирование в любых возможных сценариях ее использования с учетом предположений безопасности.

2. Цели безопасности Kaspersky IoT Secure Gateway 1000

Перечень целей безопасности Kaspersky IoT Secure Gateway 1000.

- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность и аутентичность) обновление версии системы и приложений, в том числе через не доверенные каналы связи.
- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность и аутентичность) хранение параметров и конфигураций системы, полученных от доверенного источника. Доверенными источниками информации являются:
- сервер администрирования Kaspersky Security Center;
- администратор, авторизованный посредством сертификата при установке безопасного канала между компьютером администратора и Kaspersky IoT Secure Gateway 1000.
- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность) хранение событий аудита и их передачу на Сервер администрирования Kaspersky Security Center безопасным (целостность и аутентичность) образом.
- Kaspersky IoT Secure Gateway 1000 обеспечивает компонентам безопасный (целостность и конфиденциальность) канал связи с удаленным сервером (через TLS-терминатор).
- Kaspersky IoT Secure Gateway 1000 обеспечивает целостность и аутентичность пакетов приложений при динамической установке в процессе своей работы.
- Kaspersky IoT Secure Gateway 1000 обеспечивает целостность и аутентичность образов приложений перед запуском.
- Kaspersky IoT Secure Gateway 1000 обеспечивает возможность наделения динамически запускаемых приложений привилегиями в процессе своей работы.
- Kaspersky IoT Secure Gateway 1000 обеспечивает применение политик безопасности Kaspersky Security System к любому взаимодействию между приложениями и Kaspersky IoT Secure Gateway 1000.
- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность и конфиденциальность) персональное хранилище данных для каждого приложения. Доступ к этому хранилищу имеет только приложение, данные которого в нем хранятся.
- Kaspersky IoT Secure Gateway 1000 гарантирует взаимодействие приложений с внешними системами только посредством безопасного (целостность и конфиденциальность) канала связи (через TLS-терминатор).
- При работе в режиме однонаправленного шлюза Kaspersky IoT Secure Gateway 1000 обеспечивает однонаправленную передачу данных от приложений, взаимодействующих с внутренней сетью, с приложениями, взаимодействующими с внешней сетью, без возможности воздействия на внутренние ресурсы со стороны внешней сети.

3. Предположения безопасности Kaspersky IoT Secure Gateway 1000

Перечень предположений безопасности Kaspersky IoT Secure Gateway 1000.

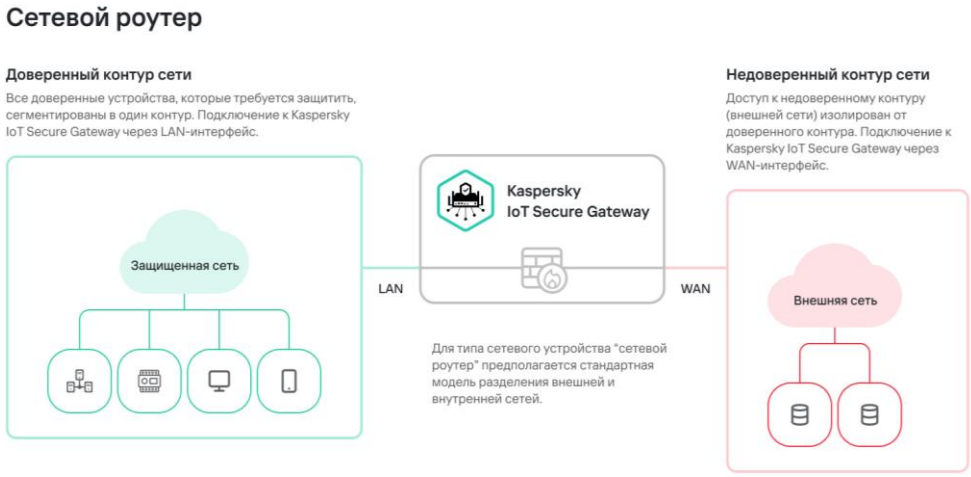
- Не рассматриваются угрозы, связанные с уязвимостью аппаратной платформы. Предполагается, что аппаратная платформа является доверенной.
- Устройство, на котором установлен Kaspersky IoT Secure Gateway 1000, работает в окружении, гарантирующем отсутствие физического доступа со стороны злоумышленника, в том числе для подключения напрямую к устройству. Не рассматриваются угрозы, связанные с соответствующими уязвимостями.
- Предполагается средний (базовый повышенный) уровень угроз со стороны внешней сети.
- Предполагается низкий (базовый) уровень угроз со стороны внутренней сети.
- Подробную информацию об оценке уровня угроз безопасности информации вы можете получить на сайте Федеральной службы по техническому и экспортному контролю России.
- Первоначальная настройка решения должна производиться в условиях, когда отсутствует угроза подмены Сервера администрирования Kaspersky Security Center (то есть доверенным администратором в контролируемой зоне).
- При работе в режиме однонаправленного шлюза:
    - Не гарантируется целостность данных, передаваемых во внутренней сети от устройств к шлюзу.
    - Не обеспечивается защита безопасности устройств, подключенных к шлюзу, от атак из внутренней сети.
    - Аппаратная платформа должна иметь отдельные физические порты для подключения к внутренней и внешней сети.
- Доступность Kaspersky IoT Secure Gateway 1000 не является целью безопасности.
- Не гарантируется выполнение целей безопасности при установке приложений VPN или службы отладки Kaspersky Debug Service (KDS). При установке одного из этих приложений устройство перезагружается и выходит из кибериммунного режима. Для возврата в кибериммунный режим требуется полная переустановка Kaspersky IoT Secure Gateway 1000 и повторная первоначальная настройка.

4. Типы сетевого устройства Kaspersky IoT Secure Gateway 1000

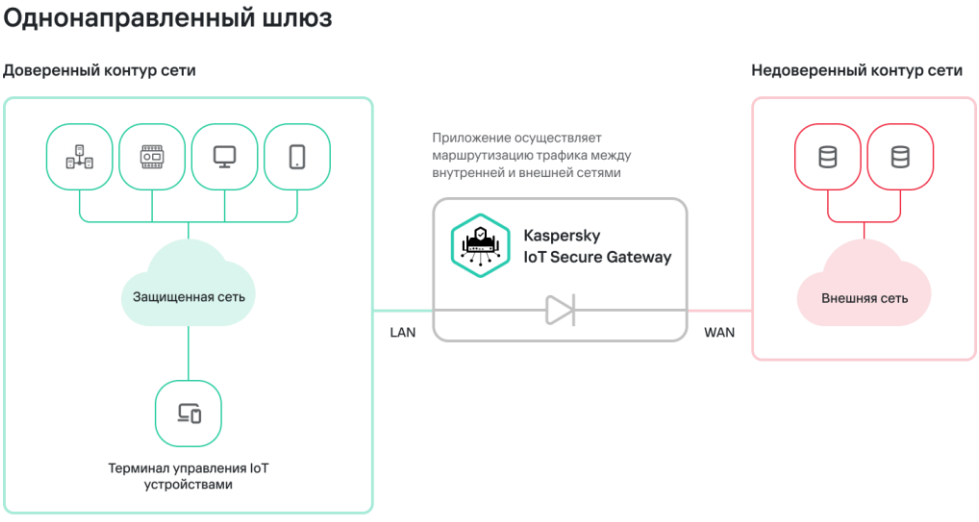
Архитектура сети и сценарии использования Kaspersky IoT Secure Gateway 1000 зависят от выбранного типа сетевого устройства Kaspersky IoT Secure Gateway 1000.

Kaspersky IoT Secure Gateway 1000 может работать в качестве следующих типов сетевого устройства:

- Kaspersky IoT Secure Gateway 1000 как сетевой роутер обеспечивает маршрутизацию трафика в двух направлениях (см. рис. ниже).
  Если вам требуется обмен данными в двух направлениях, включая управление устройствами из внешней сети, используйте Kaspersky IoT Secure Gateway 1000 как сетевой роутер.



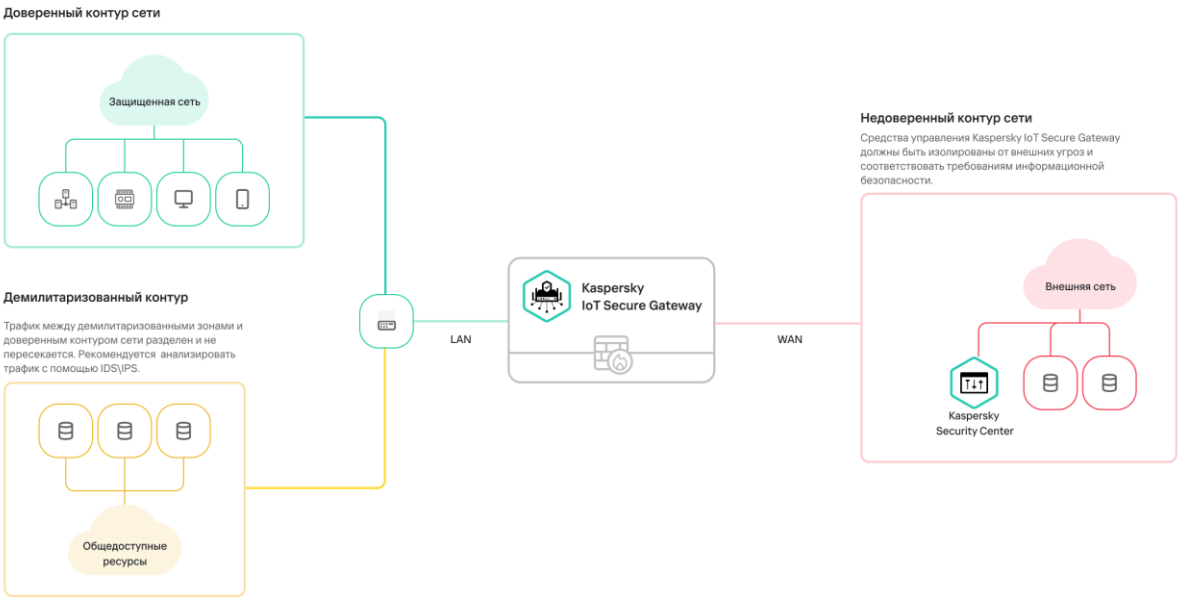
- Kaspersky IoT Secure Gateway 1000 как однонаправленный шлюз обеспечивает передачу трафика только из внутренней сети во внешнюю сеть (см. рис. ниже).
  Однонаправленный шлюз не позволяет передавать данные и управляемые сигналы из внешней сети во внутреннюю. Если вы используете Kaspersky IoT Secure Gateway 1000 как однонаправленный шлюз, вы не сможете управлять устройствами из внешней сети.



5. Требования к инфраструктуре

Для обеспечения безопасности сети предприятия необходимо создать доверенный контур сети, который удовлетворяет следующим условиям:

- Все субъекты и объекты внутри доверенного контура сети предприятия являются контролируемыми.
- Все объекты внутри доверенного контура изолированы от внешних угроз.
- Маршрутизация трафика внутри доверенного контура сети является контролируемой. Это означает, что все потоки данных между устройствами в защищенном сегменте сети маршрутизируются, бесконтрольные и избыточные маршруты отсутствуют.
- Весь трафик в доверенном контуре сети изолирован от внешней сети в обход Kaspersky IoT Secure Gateway 1000.
- Устройства в рамках доверенного контура должны быть доверенными и контролируемыми администратором контура.
- Администратор безопасного контура должен обеспечить контроль трафика. Администратор должен понимать предназначение трафика. Должны быть установлены соответствующие ограничения для запрещённого трафика или запрещенных хостов.
- Общедоступные ресурсы, к которым требуется доступ из не доверенного контура сети, сегментированы в отдельные демилитаризованные зоны.
- Для сегментирования сети используются управляемые коммутаторы, за которыми вы сможете организовать контролируемые демилитаризованные зоны.
- В демилитаризованных зонах используются инструменты отслеживания и контроля угроз.
- Если для доступа к Kaspersky IoT Secure Gateway 1000 или к доверенному контуру используются защищенные тоннели, необходимо, чтобы такие тоннели соответствовали тем же условиям безопасности, что и доверенный контур.



6. Требования к средствам управления Kaspersky IoT Secure Gateway 1000

Для обеспечения безопасности сети предприятия средства, которые используются для управления Kaspersky IoT Secure Gateway 1000, должны удовлетворять следующим условиям:

- Устройства, с которых производятся настройка и управление Kaspersky IoT Secure Gateway 1000, являются контролируемыми и защищены от неконтролируемого управления и внешних угроз.
- Устройства, с которых производятся настройка и управление Kaspersky IoT Secure Gateway 1000, должно быть доверенным и соответствовать требованиям ИБ.
- Рекомендуется ограничивать доступ устройств с которых запрещено управление Kaspersky IoT Secure Gateway 1000 в доверенном контуре.

7. Уровни угроз в Kaspersky IoT Secure Gateway 1000

В цели безопасности Kaspersky IoT Secure Gateway 1000 входит защита от следующих уровней угроз:

- Угрозы со стороны внешней сети имеют средний (базовый повышенный) уровень. Предполагается, что внешний сегмент сети изолирован от внутреннего, а объекты внутренней сети защищены от внешних угроз, если доступ к ним не разрешен в явном виде или не был инициирован из внутренней сети.
- Угрозы со стороны внутренней сети имеют низкий (базовый) уровень. Предполагается, что устройства защищены только от внешнего воздействия, и безопасность внутри контура внутренней сети не обеспечивается.

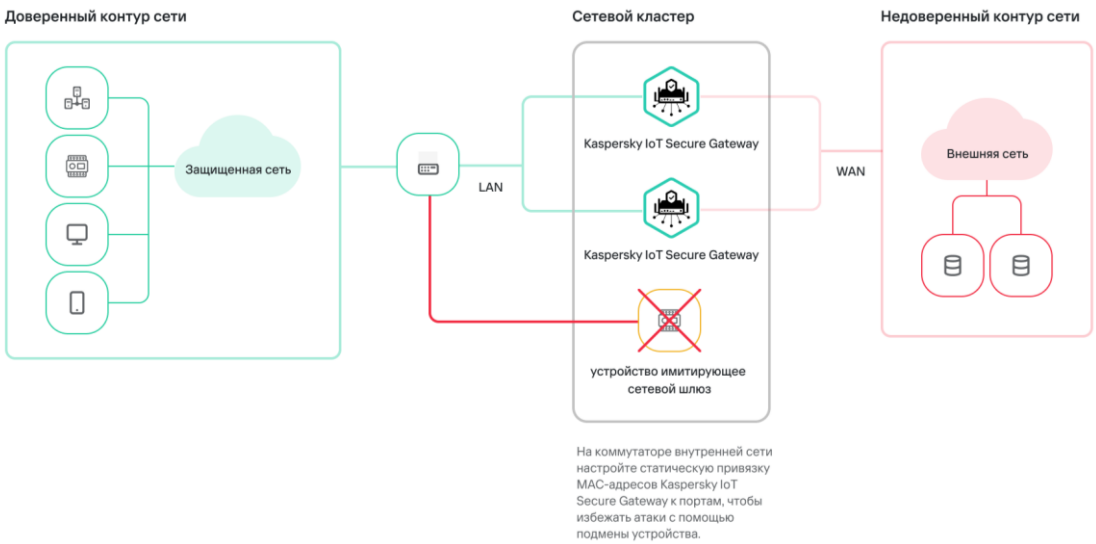
8. Митигация потенциальных рисков безопасности

Если злоумышленник проникнет в защищенный (доверенный) контур сети, безопасность сети предприятия может оказаться под угрозой.

Для митигации возможных рисков мы рекомендуем устанавливать следующие параметры на коммутаторах во внутреннем сегменте сети, защищенном Kaspersky IoT Secure Gateway 1000:

1. Если Kaspersky IoT Secure Gateway 1000 используется в качестве DHCP-сервера, но инфраструктура сети не гарантирует создание доверенного контура, вы можете защитить DHCP-сервер от подмены, настроив конфигурацию коммутаторов в защищенном контуре сети следующим образом (см. рис. ниже):
    a. перенаправлять весь трафик, связанный с выдачей IP-адресов DHCP сервером (UDP-порт 67), на MAC-адреса Kaspersky IoT Secure Gateway 1000;
    b. отбрасывать широковещательные запросы с пакетами, содержащими сообщение типа DHCP_OFFER, с MAC-адресов, не принадлежащих Kaspersky IoT Secure Gateway 1000 (UDP-порт 68);
    c. установить предельное количество запросов в единицу времени на MAC-адрес Kaspersky IoT Secure Gateway 1000 (UDP-порт 67) для получения IP-адреса.

2. Если несколько устройств под управлением Kaspersky IoT Secure Gateway 1000 работают в качестве отказоустойчивого кластера, но инфраструктура сети не гарантирует создание доверенного контура, вы можете защитить устройства в кластере от подмены. Для этого настройте конфигурацию коммутаторов в безопасном контуре сети таким образом чтобы MAC-адреса устройств Kaspersky IoT Secure Gateway 1000, были статично записаны в таблицах MAC-адресов на коммутаторе для исключения возможности их подмены (см. рис. ниже).



3. По умолчанию сетевой экран Kaspersky IoT Secure Gateway 1000 запрещает все соединения кроме тех, которые инициированы из доверенного сегмента сети.

   Это гарантирует безопасность сети от внешнего вторжения. Гарантия безопасности прекращается, если нарушены требования по обеспечению доверенности контура и в защищенном сегменте сети присутствуют внешние угрозы. Создавайте новые разрешающие правил сетевого экрана, только если они явно не нарушают доверенность и не создают уязвимости для угроз из внешних источников.

4. Если вы настроили правила адресной трансляции для переадресации портов в Kaspersky IoT Secure Gateway 1000, вам нужно обеспечить контроль такого соединения, чтобы соединения извне не нарушали доверенность защищаемого контура. В случае необходимости выделяйте такие соединения в отдельные демилитаризованные зоны, которые вы можете контролировать и изолировать с помощью управляемых коммутаторов.