Сетевой экран Kaspersky IoT Secure Gateway 1000

В этом документе содержится информация о работе и способах настройки сетевого экрана Kaspersky IoT Secure Gateway 1000 и приложения Kaspersky IoT Secure Gateway Network Protector.

Этот документ описывает особенности работы сетевого экрана Kaspersky IoT Secure Gateway 1000 в следующих сценариях:

- Настройка правил сетевого экрана Kaspersky IoT Secure Gateway 1000 для типа сетевого устройства сетевой роутер при использовании трансляции (проброса) портов.
- Настройка правил сетевого экрана Kaspersky IoT Secure Gateway 1000 для типа сетевого устройства сетевой роутер с использованием маршрутизации информационных потоков.
- Настройка правил сетевого экрана Kaspersky IoT Secure Gateway 1000 для типа сетевого устройства однонаправленный шлюз и пропуска трафика из внутренней сети во внешнюю.

kaspersky

kaspersky cyber immunity

Оглавление

Глоссарий

HTTP (HyperText Transfer Protocol) – протокол прикладного уровня для передачи данных.

Kaspersky IoT Secure Gateway 1000 – аппаратно-программный комплекс на базе кибериммунной 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.

MQTT (Message Queuing Telemetry Transport) – упрощенный сетевой протокол, работающий поверх TCP/IP, ориентированный на обмен сообщениями между устройствами по принципу издатель-подписчик.

NAT (Network Address Translation) – функциональность преобразования сетевых адресов и трансляции портов.

PPP (Point-to-Point Protocol) – двухточечный протокол канального уровня.

SSH (Secure Shell) – сетевой протокол прикладного уровня, позволяющий производить защищенное удаленное управление.

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.

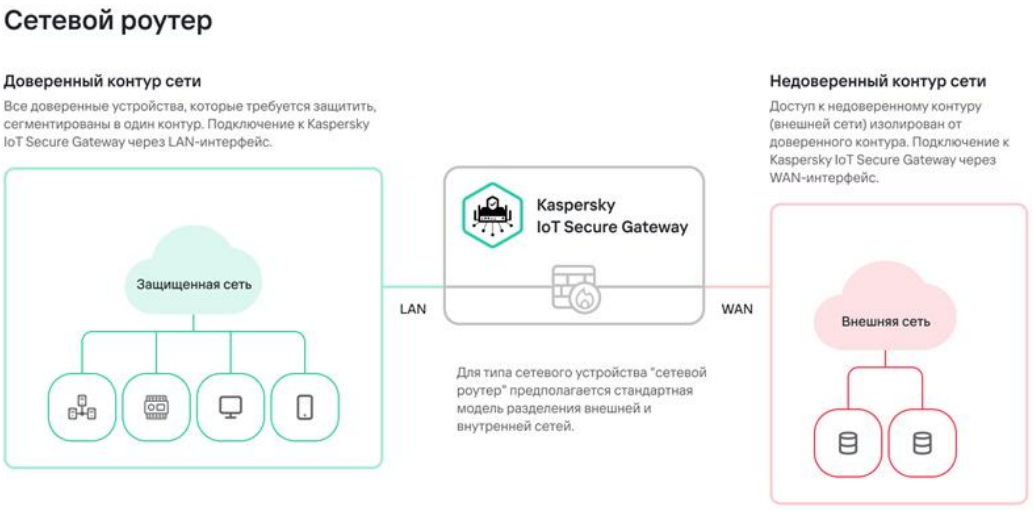
Сетевой экран – технология, разделяющая внешнюю и внутреннюю сети и ограничивающая движение трафика на основании правил.

Типы сетевого устройства Kaspersky IoT Secure Gateway 1000

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

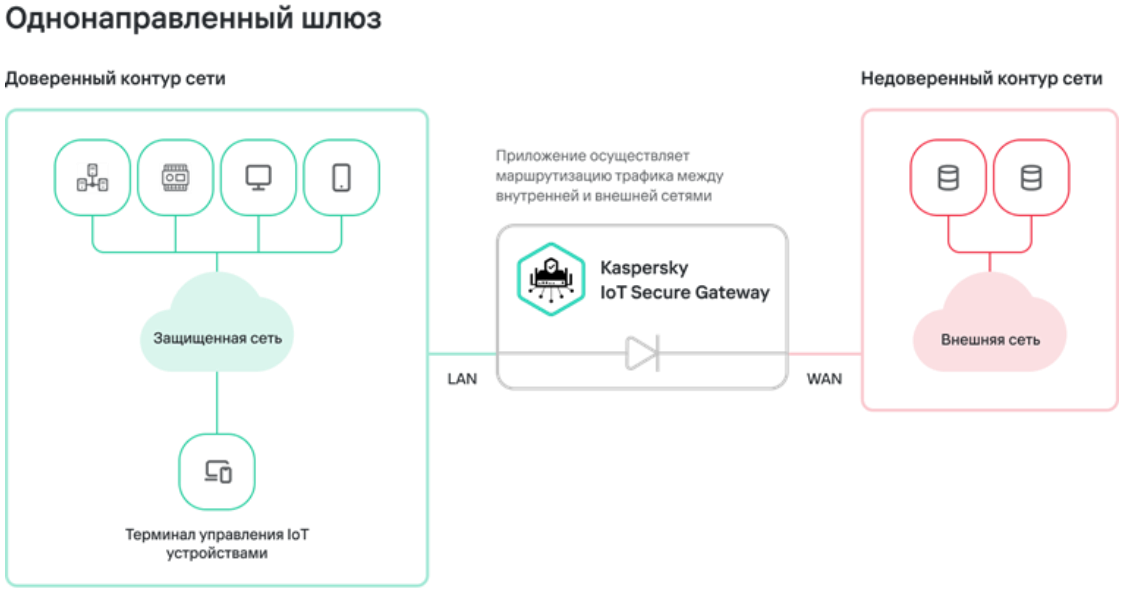
Kaspersky IoT Secure Gateway 1000 может работать в качестве следующих типов сетевого устройства:

- 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.
  При работе Kaspersky IoT Secure Gateway 1000 в качестве сетевого роутера обнаружение атак и блокировка хостов для внутренней сети производится так же, как для внешней сети. Если включена функциональность NAT, блокируются только атаки от хостов во внешней сети, так как после применения NAT сетевой пакет приходит с подмененным IP-адресом и портом. Если источник вредоносного трафика будет определен со стороны внешней сети, то такой адрес добавится в список запрещенных IP-адресов.



  Блокировка IP-адреса в Kaspersky IoT Secure Gateway 1000 также может срабатывать на IP-адреса хостов из внутренней сети, но в этом случае в качестве источника атаки указывается IP-адрес WAN-интерфейса. Этот адрес WAN-интерфейса не попадает в список запрещенных IP-адресов, так как он содержится в списке разрешающих служебных правил (System Rules).

- 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.



Сетевой экран и обнаружение угроз

Сетевой экран Kaspersky IoT Secure Gateway 1000 предназначен для фильтрации трафика на основе правил. По умолчанию сетевой экран Kaspersky IoT Secure Gateway 1000 запрещает любые соединения из внешней сети, если они не инициированы из внутренней сети. Чтобы настроить безопасный обмен данными между внутренней и внешней сетями и исключить нежелательный или избыточный трафик на устройстве, системному администратору нужно добавить соответствующие разрешения или запреты для сетевого экрана через приложение Kaspersky IoT Secure Gateway Network Protector.

Приложение Kaspersky IoT Secure Gateway Network Protector позволяет обнаруживать базовые сетевые атаки на Kaspersky IoT Secure Gateway 1000 и смежные хосты. Обнаруженные угрозы блокируются с помощью сетевого экрана с помощью динамического создания правил фильтрации.

Принцип работы сетевого экрана Kaspersky IoT Secure Gateway 1000

Сетевой экран Kaspersky IoT Secure Gateway 1000 осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с правилами фильтрации.

Сетевой экран проверяет только входящие соединения со стороны внутренней и внешней сетей и не проверяет исходящие соединения. Системный администратор может создавать правила только для входящих соединений.

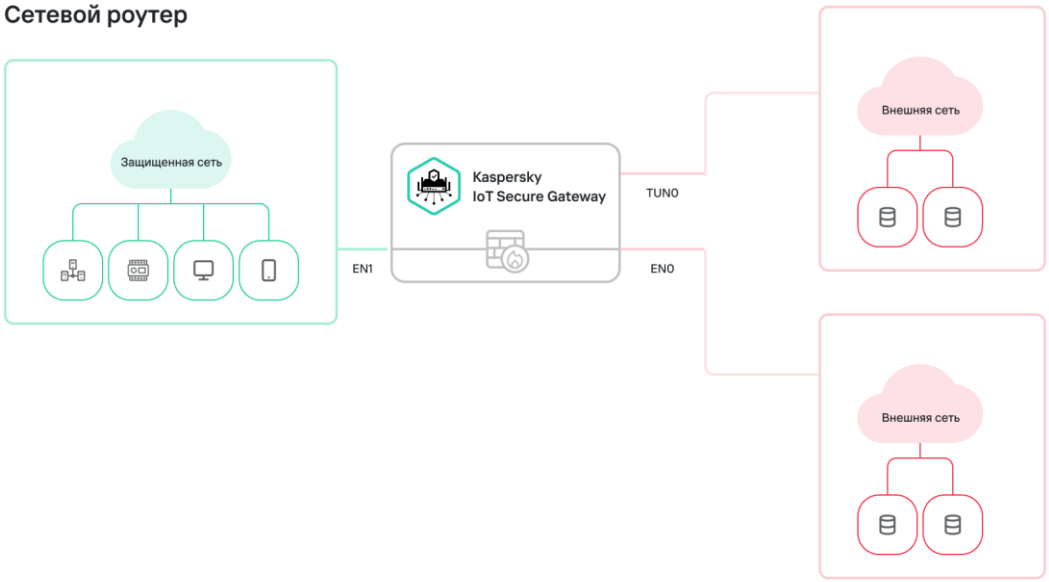
Сетевой экран проверяет пакеты с отслеживанием состояния соединения.
Это позволяет принимать входящий трафик для уже установленных соединений без необходимости создавать дополнительные разрешающие правила для ответных пакетов.

Сетевые сегменты сетевого экрана Kaspersky IoT Secure Gateway 1000

Сетевой экран Kaspersky IoT Secure Gateway 1000 работает со следующими сетевыми сегментами, между которыми настраиваются правила сетевого экрана:

- Зона внешней сети (WAN) использует интерфейс беспроводного модема tun0 и проводной Ethernet-адаптер en0.
- Зона внутренней сети (LAN) использует проводной Ethernet-адаптер en1.

Подключения из внешней сети происходят со стороны WAN-интерфейса (en0 или модема tun0), а из внутренней сети – со стороны LAN-интерфейса (en1). На рисунке ниже приведена схема расположения зон безопасности относительно сетевого экрана в Kaspersky IoT Secure Gateway 1000.



Правила сетевого экрана для внутренней и внешней сетей необходимо настраивать отдельно.

Формирование и порядок применения правил сетевого экрана

Правила сетевого экрана Kaspersky IoT Secure Gateway 1000 формируются в виде списка и применяются к каждому входящему сетевому пакету по одному в порядке, определенном в этом списке. При обнаружении первого совпадения Kaspersky IoT Secure Gateway 1000 применяет к пакету действие из совпавшего правила. Дальнейшая проверка для данного пакета прекращается, все нижестоящие правила игнорируется.

Список правил сетевого экрана различается в зависимости от типа сетевого устройства, выбранного в Kaspersky IoT Secure Gateway 1000.

Порядок применения правил сетевого экрана для типа устройства сетевой роутер

Для Kaspersky IoT Secure Gateway 1000 как сетевого роутера правила сетевого экрана применяются к входящим пакетам из внутреннего и внешнего сегментов сети в следующем порядке:

1. **Диагностические правила** разрешают все потоки, необходимые для самодиагностики Kaspersky IoT Secure Gateway 1000.
2. **Служебные правила** разрешают все потоки, необходимые для прохождения трафика по протоколам ICPM и CARP, трафика веб-интерфейса Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center Web Console.
   Полный список служебных правил см. в таблице ниже.
3. **Фильтрующие правила** блокируют все пакеты, в которых встречается определенный в правиле протокол.
   Вы можете самостоятельно выбрать протоколы, трафик по которым вы хотите заблокировать, через веб-интерфейс Kaspersky IoT Secure Gateway 1000 или веб-плагин для Kaspersky Security Center Web Console.
4. **Аварийные правила** блокируют все информационные потоки, если активен режим аварийной поддержки.
5. **Список разрешенных IP-адресов** разрешает прохождение трафика от хостов, определенных в приложении Kaspersky IoT Secure Gateway Network Protector. Если приложение Kaspersky IoT Secure Gateway Network Protector обнаруживает атаку от хоста в этом списке, хост игнорируется.
   Вы можете самостоятельно создавать и изменять правила в списке разрешенных IP-адресов в параметрах приложения Kaspersky IoT Secure Gateway Network Protector.
6. **Список запрещенных IP-адресов** запрещает прохождение трафика от хостов, определенных в приложении Kaspersky IoT Secure Gateway Network Protector. Список правил формируется автоматически приложением Kaspersky IoT Secure Gateway Network Protector. После перезагрузки устройства список сбрасывается.
7. **Правила адресной трансляции (NAPT)** разрешают входящие соединения для проброса портов.
   Вы можете самостоятельно создавать и изменять правила адресной трансляции через веб-плагин для Kaspersky Security Center Web Console.
8. **Пользовательские правила** запрещают или разрешают соединения во внутренней и внешней сети.
   Вы можете самостоятельно создавать и изменять эти правила. Эта категория также включает правила, созданные Kaspersky Industrial CyberSecurity. Порядок применения правил внутри этого списка для анализа трафика задается пользователем. Подробную информация о создании пользовательских правил сетевого экрана см. в разделе Создание правил сетевого экрана в справке Kaspersky IoT Secure Gateway 1000.
9. **Служебные правила** разрешают все потоки, необходимые для прохождения трафика для Syslog, MQTT, DHCP, DNS.
   Полный список служебных правил см. в таблице ниже.
10. **Запрещающие правила** запрещают все остальные информационные потоки.

Порядок применения правил сетевого экрана для типа устройства однонаправленный шлюз

Для Kaspersky IoT Secure Gateway 1000 как однонаправленного шлюза правила сетевого экрана применяются к входящим пакетам из внешнего сегмента сети в следующем порядке:

1. **Диагностические правила** разрешают все потоки, необходимые для самодиагностики Kaspersky IoT Secure Gateway 1000.
2. **Правила исходящего трафика** разрешают все исходящие информационные потоки.
3. **Служебные правила** разрешают все потоки, необходимые для прохождения трафика по протоколу ICPM.
   Полный список служебных правил см. в таблице ниже.
4. **Правила приложения VPN** разрешают все информационные потоки, инициированные приложением VPN.
5. **Запрещающие правила** запрещают все остальные входящие информационные потоки.

Для Kaspersky IoT Secure Gateway 1000 как однонаправленного шлюза правила сетевого экрана применяются к входящим пакетам из внутреннего сегмента сети в следующем порядке:

1. **Диагностические правила** разрешают все потоки, необходимые для самодиагностики Kaspersky IoT Secure Gateway 1000.
2. **Правила исходящего трафика** разрешают все исходящие информационные потоки.
3. **Служебные правила** разрешают все потоки, необходимые для прохождения трафика по протоколам ICPM и CARP, трафика веб-интерфейса Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center Web Console.
   Полный список служебных правил см. в таблице ниже.
4. **Фильтрующие правила** блокируют все пакеты, в которых встречается определенный в правиле протокол.
   Вы можете самостоятельно выбрать протоколы, трафик по которым вы хотите заблокировать.
5. **Аварийные правила** блокируют все информационные потоки, если активен режим аварийной поддержки.
6. **Список разрешенных IP-адресов** разрешает прохождение трафика от хостов, определенных в приложении Kaspersky IoT Secure Gateway Network Protector. Если приложение Kaspersky IoT Secure Gateway Network Protector обнаруживает атаку от хоста в этом списке, хост игнорируется.
   Вы можете самостоятельно создавать и изменять правила в списке разрешенных IP-адресов в параметрам приложения Kaspersky IoT Secure Gateway Network Protector.
7. **Список запрещенных IP-адресов** запрещает прохождение трафика от хостов, определенных в приложении Kaspersky IoT Secure Gateway Network Protector. Список правил формируется автоматически приложением Kaspersky IoT Secure Gateway Network Protector. После перезагрузки устройства список сбрасывается.
8. **Пользовательские правила** запрещают или разрешают соединения во внутренней сети. Вы можете самостоятельно создавать и изменять эти правила. Эта категория также включает правила, созданные Kaspersky Industrial CyberSecurity. Порядок применения правил внутри этого списка для анализа трафика задается пользователем. Подробную информация о создании пользовательских правил сетевого экрана см. в разделе Создание правил сетевого экрана в справке Kaspersky IoT Secure Gateway 1000.
9. **Служебные правила** разрешают все потоки, необходимые для прохождения трафика для Syslog, DHCP.

Полный список служебных правил см. в таблице ниже.

10. **Запрещающие правила** запрещают все остальные входящие информационные потоки.

Служебные правила сетевого экрана

Служебные правила сетевого экрана применяются к трафику в следующих направлениях:

- input – соединение инициирует внешняя сторона;
- output – соединение инициирует Kaspersky IoT Secure Gateway 1000.

В таблице ниже представлены служебные правила сетевого экрана Kaspersky IoT Secure Gateway 1000 и порядок, в котором они применяются.

Порядок	Протокол	Краткое описание	Действие	Сеть	IP-адрес:номер порта источника	IP-адрес:номер порта назначения	Направление трафика
1	Служебный протокол	Протокол для связи с Сервером администрирования Kaspersky Security Center	Разрешить	Внешняя	any:any	<IP-адрес Kaspersky Security Center>:13294	output
2	Служебный протокол	Протокол для связи с Сервером администрирования Kaspersky Security Center	Разрешить	Внутренняя	any:any	<IP-адрес Kaspersky Security Center>:13294	output
3	UDP	Протокол для передачи сообщений на Syslog-сервер	Разрешить	Внешняя	any:any	<IP-адрес Syslog-сервера>:514	output
4	TCP	Протокол для передачи сообщений на Syslog-сервер	Разрешить	Внешняя	any:any	<IP-адрес Syslog-сервера>:514	output
5	TCP/TLS	Протокол для передачи сообщений на Syslog-сервер	Разрешить	Внешняя	any:any	<IP-адрес Syslog-сервера>:<порт Syslog-сервера>	output

6	MQTT	Протокол для приема MQTT-сообщений от устройств во внутренней сети	Разре-шить	Внутрен-няя	any:any	<IP-адрес Kaspersky IoT Secure Gateway 1000>:1883	input
7	MQTT	Протокол для приема MQTT-сообщений от устройств во внутренней сети	Разре-шить	Внутрен-няя	any:any	<IP-адрес Kaspersky IoT Secure Gateway 1000>:1883	input
8	MQTT	Протокол для пересылки MQTT-сообщений в облако	Разре-шить	Внешняя	<IP-адрес Kaspersky IoT Secure Gateway 1000>:any	<IP-адрес облачного MQTT-брокера>:8883	output
9	MQTT	Протокол для пересылки MQTT-сообщений в облако	Разреш ить	Внутрен-няя	<IP-адрес Kaspersky IoT Secure Gateway 1000>:any	<IP-адрес облачного MQTT-брокера>:8883	output
10	HTTPS	Протокол для работы веб-интерфейса Kaspersky IoT Secure Gateway 1000	Разре-шить	Внутрен-няя	any:any	<IP-адрес Kaspersky IoT Secure Gateway 1000>:443	input
11	DNS	Протокол для получения DNS-ответов	Разр-ешить	Внешняя	any:53	any:any	input
12	DNS	Протокол для отправки DNS-запросов	Разре-шить	Внешняя	<IP-адрес Kaspersky IoT Secure Gateway 1000>:any	any:53	output
13	DNS	Протокол для отправки DNS-запросов	Разре-шить	Внутрен-няя	any:any	any:53	output

14	DHCP	Протокол для приема запросов на выдачу IP-адресов по DHCP для устройств во внутренней сети	Разре-шить	Внутрен-няя	any:68	<IP-адрес Kaspersky IoT Secure Gateway 1000>:67	input
15	DHCP	Протокол для получения ответа на запрос IP-адреса по DHCP для интерфейса Kaspersky IoT Secure Gateway 1000 во внешней сети	Разре-шить	Внешняя	any:67	any:68	input
16	DHCP	Протокол для отправки ответа на запрос IP-адреса по DHCP для устройств во внутренней сети	Разре-шить	Внутрен-няя	<IP-адрес Kaspersky IoT Secure Gateway 1000>:67	any:68	output
17	DHCP	Протокол для отправки запроса на получение IP-адреса по DHCP для интерфейса Kaspersky IoT Secure Gateway 1000 во внешней сети	Разре-шить	Внешняя	any:68	any:67	output
18	CARP	Протокол для взаимодейст-вия по протоколу CARP	Разре-шить	Внутрен-няя	any:any	any:any	input или output

Предположения безопасности Kaspersky IoT Secure Gateway 1000

К предположениям безопасности Kaspersky IoT Secure Gateway 1000 относятся следующие предположения:

- 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.
- 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.
- 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 киберимунного режима. Для возврата в киберимунный режим требуется полная переустановка Kaspersky IoT Secure Gateway 1000 и повторная первоначальная настройка.

Приложение Kaspersky IoT Secure Gateway Network Protector

Приложение Kaspersky IoT Secure Gateway Network Protector позволяет анализировать трафик, проходящий через Kaspersky IoT Secure Gateway 1000, и обнаруживать базовые сетевые атаки. Чтобы начать работу приложения, вам нужно включить его и настроить. Подробнее о работе с приложением Kaspersky IoT Secure Gateway Network Protector см. в разделе Управление приложением Kaspersky IoT Secure Gateway Network Protector в справке Kaspersky IoT Secure Gateway 1000.

Приложение анализирует каждый входящий пакет трафика на соответствие правилам (сигнатурам), заданным в параметрах приложения. При первом обнаружении угрозы происходит следующее:

1. Формируется событие об обнаружении угрозы, содержащее информацию о хосте и описание угрозы, и записывается в журнале аудита. Если соответствующие параметры включены, событие также передается в Kaspersky Security Center, Syslog-сервер, MQTT-брокер.
2. Создается запрещающее правило в списке запрещенных IP-адресов сетевого экрана. Для разблокировки устройства вы можете удалить его из списка через интерфейс Kaspersky IoT Secure Gateway 1000.

Если обнаруженная угроза исходит от хоста, находящегося списке разрешенных IP-адресов, эта угроза игнорируется. Если вы используете специфичные сценарии обнаружения атак, вы можете добавить хост в список разрешенных IP-адресов через интерфейс Kaspersky IoT Secure Gateway 1000, чтобы исключить ложные срабатывания.

По умолчанию в следующих случаях запрещен весь трафик:

- при запуске Kaspersky IoT Secure Gateway 1000 до момента завершения самодиагностики и инициализации;
- если приложение Kaspersky IoT Secure Gateway Network Protector установлено, но выключено или не прошло самодиагностику.

Это необходимо для исключения несанкционированного сетевого взаимодействия и выполнения целей безопасности.

Улучшение качества обнаружения угроз

Мы не рекомендуем добавлять для сетевого экрана разрешающие правила формата `allow any:any→any:any` для интерфейсов LAN и WAN. Такие правила могут снизить уровень защищенности зон безопасности, так как они разрешают потенциально вредоносные сетевые взаимодействия. Также при использовании таких правил может возрасти количество сетевых соединений, за которыми необходимо следить. Использование точных правил для сетевого экрана снижает нагрузку на приложение Kaspersky IoT Secure Gateway Network Protector и может уменьшить количество ложных срабатываний.

Примеры использования сетевого экрана в различных сценариях работы Kaspersky IoT Secure Gateway 1000

Подготовка к разграничению доступа

Перед настройкой правил сетевого экрана выполните следующие действия:

1. Войдите в учетную запись Kaspersky IoT Secure Gateway 1000, используя веб-интерфейс, и выполните действия быстрого старта для администратора.
2. Настройте параметры подключения к Серверу администрирования Kaspersky Security Center.

После этого вы можете настроить правила сетевого экрана в интерфейсе веб-плагина для Kaspersky Security Center Web Console.

Использование сетевого экрана при включенном маскарадинге в Kaspersky IoT Secure Gateway 1000 как типа сетевого устройства сетевой роутер

Если включена функция маскарадинга, Kaspersky IoT Secure Gateway 1000 осуществляет работу механизма SNAT (Source Network Address Translation), при котором при пересылке пакета заменяется адрес источника. Исходный IP-адрес источника, расположенного во внутренней сети, преобразуется в IP-адрес WAN-интерфейса Kaspersky IoT Secure Gateway 1000 с заменой порта источника. При этом для ответных пакетов производится обратное преобразование IP-адреса и порта назначения. Механизм SNAT не позволяет внешним источникам напрямую обращаться к хостам во внутренней сети, то есть хост из внешней сети не может инициализировать соединения к хостам внутренней сети.

Во внешней сети Kaspersky IoT Secure Gateway 1000 расположены интерфейсы tun0 и en0. Интерфейс en0 является проводным, а интерфейс tun0 является интерфейсом модема. При включении маскарадинга NAT работает для обоих соединений. Трафик будет передаваться согласно таблице маршрутизации для каждого соединения:

- Устройства, подключенные к интерфейсу Kaspersky IoT Secure Gateway 1000 с помощью модема tun0 и Ethernet-адаптера en0, находятся во внешней сети.
  На рисунке в разделе *Типы сетевого устройства Kaspersky IoT Secure Gateway* 1000 этой статьи внешняя сеть обозначена красным цветом.
- Устройства, подключенные к интерфейсу Kaspersky IoT Secure Gateway 1000 с помощью Ethernet-адаптера en1, находятся во внутренней сети.
  На рисунке в разделе *Типы сетевого устройства Kaspersky IoT Secure Gateway* 1000 этой статьи сегмент безопасности обозначен зеленым цветом.

Вам необходимо настроить параметры WAN-интерфейса таким образом, чтобы обеспечить доступ к DNS-серверу, Серверу администрирования Kaspersky Security Center и MQTT-брокеру в облаке. DNS-сервер должен иметь возможность разрешать имя Kaspersky Security Center, указанное в сертификате, который был добавлен через веб-интерфейс Kaspersky IoT Secure Gateway 1000. Если сертификат для подключения к Kaspersky Security Center выписан на IP-адрес, то DNS-сервер настраивать не обязательно. Подробную информацию о добавлении сертификата Kaspersky Security Center см. в разделе Настройка параметров подключения к Kaspersky Security Center в справке Kaspersky IoT Secure Gateway 1000.

Разрешение доступа из внутренней сети к хосту во внешней сети, если маскарадинг включен

Если функция маскарадинга включена в Kaspersky IoT Secure Gateway 1000, чтобы разграничить доступ из внутренней сети, необходимо добавить разрешающее пользовательское правило только для внутренней сети. Создавать разрешающее правило для внешней сети не нужно, так как при прохождении пакета через Kaspersky IoT Secure Gateway 1000 происходит подмена IP-адреса источника соединения. Во внешнюю сеть пакет попадает с замененными IP-адресом и портом. Для ответного пакета подставляются IP-адрес и порт источника соединения.

Например, рассмотрим сценарий, в котором для клиента во внутренней сети необходимо настроить доступ к серверу во внешней сети по протоколу HTTP. Клиент во внутренней сети имеет IP-адрес 192.168.1.10, а сервер во внешней сети имеет IP-адрес 192.168.77.20:8000.

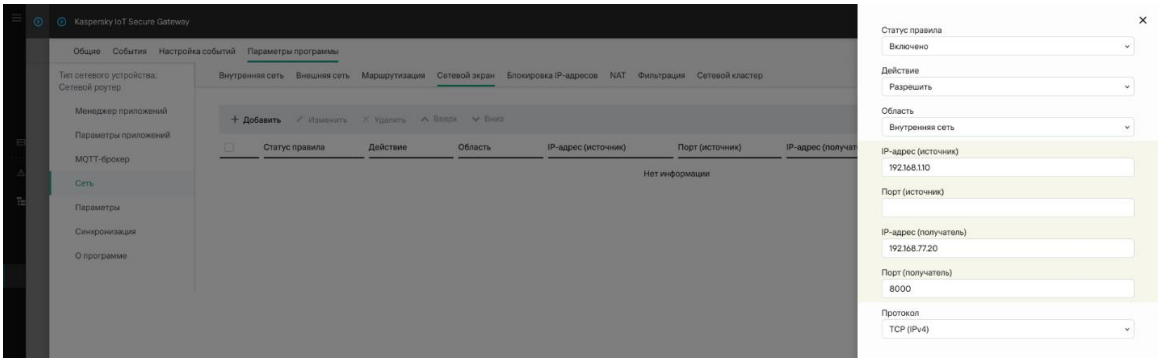
В этом случае необходимо создать правило сетевого экрана со следующими параметрами:

Действие	Сеть	Протокол L4	IP-адрес:номер порта источника	IP-адрес:номер порта назначения
Разрешить	Внутренняя	TCP	192.168.1.10:any	192.168.77.20:8000

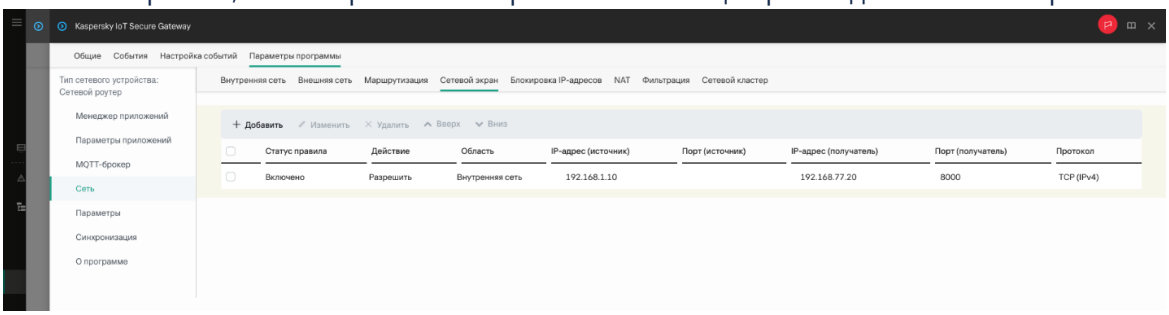
Чтобы разрешить доступ из внутренней сети к серверу во внешней сети с помощью сетевого экрана Kaspersky IoT Secure Gateway 1000:

1. Создайте правило сетевого экрана с параметрами, указанными в таблице выше, через веб-плагин Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center Web Console, по инструкции в разделе Создание правил сетевого экрана в справке Kaspersky IoT Secure Gateway 1000.

   Параметры разрешающего правила для TCP:8000 будет выглядеть следующим образом:



2. Нажмите на кнопку **OK**, чтобы создать правило.
   Панель закроется, новое правило отобразится в таблице правил для сетевого экрана:



3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, и закройте окно с параметрами Kaspersky IoT Secure Gateway 1000.

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center правило будет применено, и клиент во внутренней сети сможет подключиться к серверу во внешней сети. Вы можете узнать время синхронизации в разделе **Устройства → Управляемые устройства** в столбце **Последнее подключение к Серверу администрирования**.

Разрешение доступа из внутренней сети к хосту во внешней сети, если маскарадинг выключен

Если функция маскарадинга выключена в Kaspersky IoT Secure Gateway 1000, необходимо создать разрешающее правило сетевого экрана и настроить маршрутизацию на сервере, чтобы он мог ответить на пакеты, пришедшие из внутренней сети.

Например, рассмотрим сценарий, в котором клиент во внутренней сети имеет IP-адрес 192.168.1.10, а сервер во внешней сети имеет IP-адрес 192.168.77.20:8000.

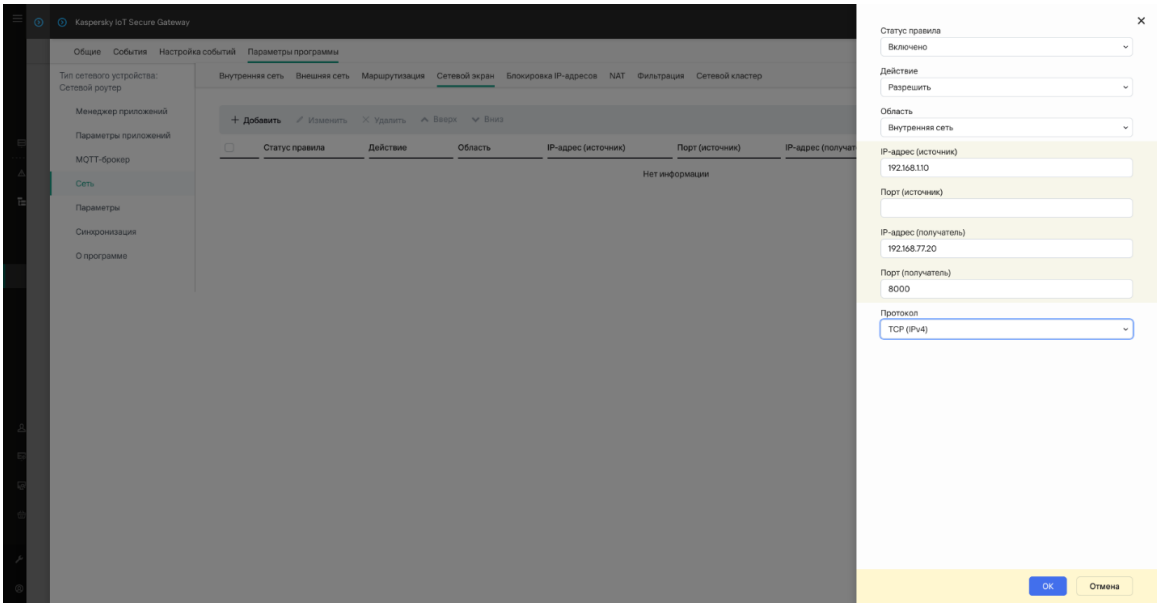
В этом случае необходимо создать правило сетевого экрана со следующими параметрами:

Действие	**Сеть**	**Протокол L4**	**IP-адрес:номер порта источника**	**IP-адрес:номер порта назначения**
Разрешить	Внутренняя	TCP	192.168.1.10:any	192.168.77.20:8000

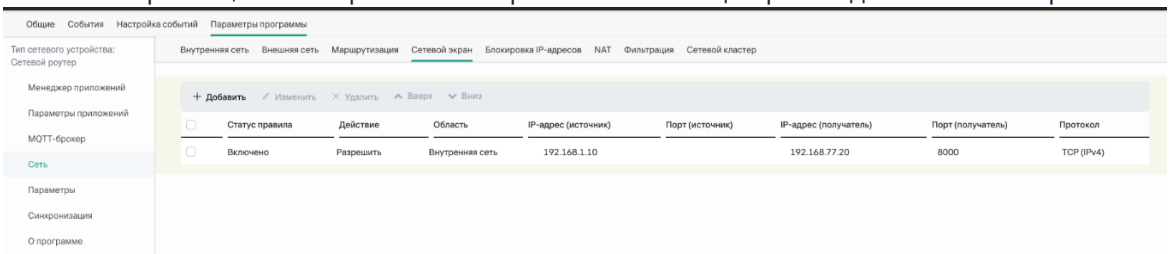
Чтобы разрешить доступ из внутренней сети к серверу во внешней сети с помощью сетевого экрана Kaspersky IoT Secure Gateway 1000:

1. Создайте правило сетевого экрана с параметрами, указанными в таблице выше, через веб-плагин Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center Web Console, по инструкции в разделе Создание правил сетевого экрана в справке Kaspersky IoT Secure Gateway 1000.

   Параметры разрешающего правила для TCP:8000 будут выглядеть следующим образом:



2. Нажмите на кнопку **OK**, чтобы создать правило.
   Панель закроется, новое правило отобразится в таблице правил для сетевого экрана:



3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, и закройте окно с параметрами Kaspersky IoT Secure Gateway 1000.

   После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center правило будет применено. Вы можете узнать время синхронизации в разделе **Устройства → Управляемые устройства** в столбце **Последнее подключение к Серверу администрирования**.

4. На стороне сервера во внешней сети создайте маршрут для хоста 192.168.1.0/24 через 192.168.77.10.

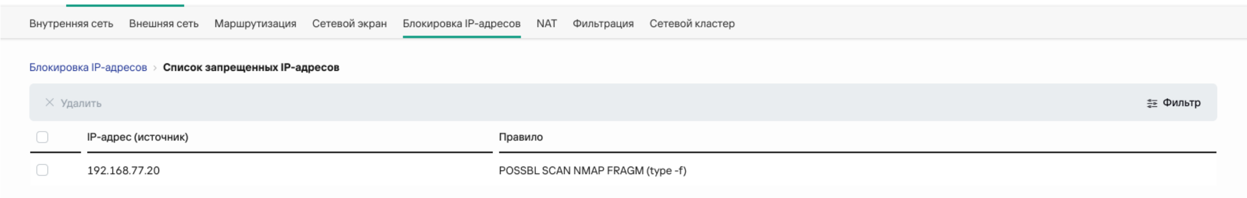
После этого клиент во внутренней сети сможет подключиться к серверу во внешней сети.

Блокировка хоста после обнаружения угрозы приложением Kaspersky IoT Secure Gateway Network Protector

Во время штатной работы клиент во внутренней сети может получать доступ к серверу во внешней сети по порту 8000.

Если приложение Kaspersky IoT Secure Gateway Network Protector обнаружит вредоносный трафик, IP-адрес хоста (например, 192.168.77.20), с которого исходит трафик, будет добавлен в список запрещенных IP-адресов и заблокирован. После этого в веб-интерфейсе Kaspersky IoT Secure Gateway появится событие об обнаружении угрозы и блокировке хоста 192.168.77.20 (см. рис. ниже).

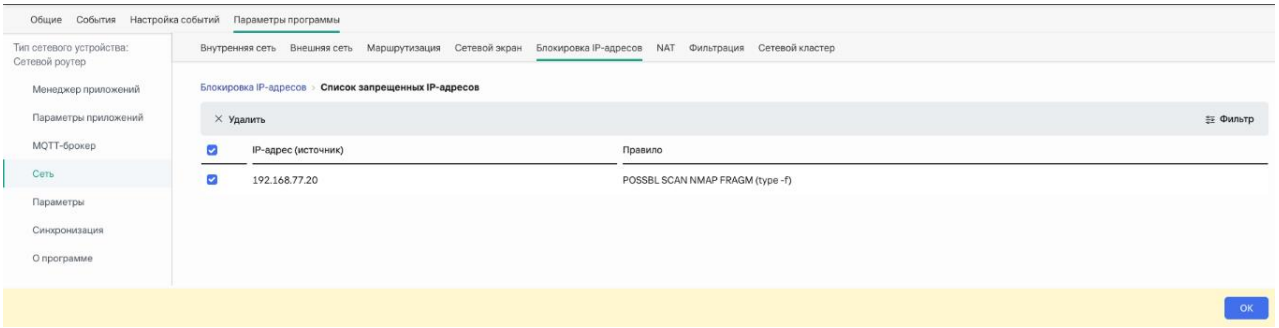
В списке запрещенных IP-адресов в разделе **Сеть → Блокировка IP-адресов** появится хост с IP-адресом источника атаки (см. рис. ниже).



В результате сетевой экран заблокирует сетевые соединения между сервером во внешней сети и хостом с IP-адресом 192.168.77.20.

При необходимости вы можете разблокировать устройство, попавшее в список запрещенных IP-адресов, одним из следующих способов:

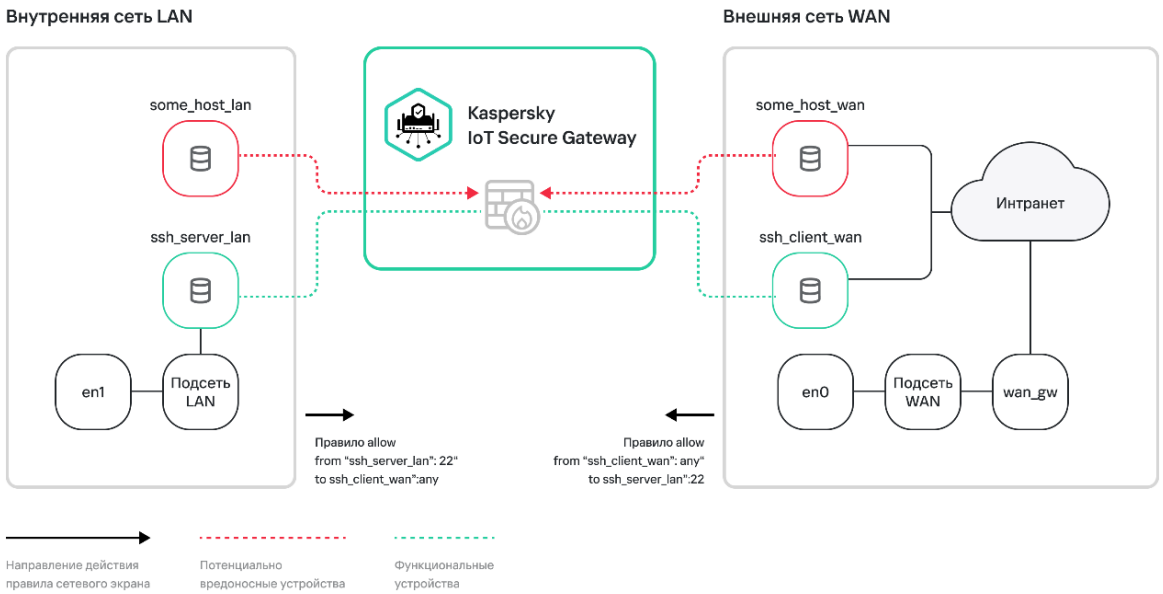
- Подождите 60 минут.
  По истечении 60 минут после блокировки IP-адрес заблокированного устройства будет автоматически удален из списка запрещенных IP-адресов.
- Удалите IP-адрес хоста из списка запрещенных IP-адресов вручную (см. рис. ниже).
  Подробную информацию см. в разделе Удаление IP-адреса из списка запрещенных IP-адресов в справке Kaspersky IoT Secure Gateway 1000.
-



Использование сетевого экрана при использовании маршрутизации пакетов в Kaspersky IoT Secure Gateway 1000 как типа сетевого устройства сетевой роутер

В этом разделе приведен пример разграничения доступа клиента во внешней сети к серверу во внутренней сети по протоколу SSH (см. рис. ниже). Сценарий разграничения доступа состоит из следующих этапов:

1. Настройка маршрутизации и проверка сетевой доступности.
2. Добавление правил сетевого экрана для внутренней и внешней сети.

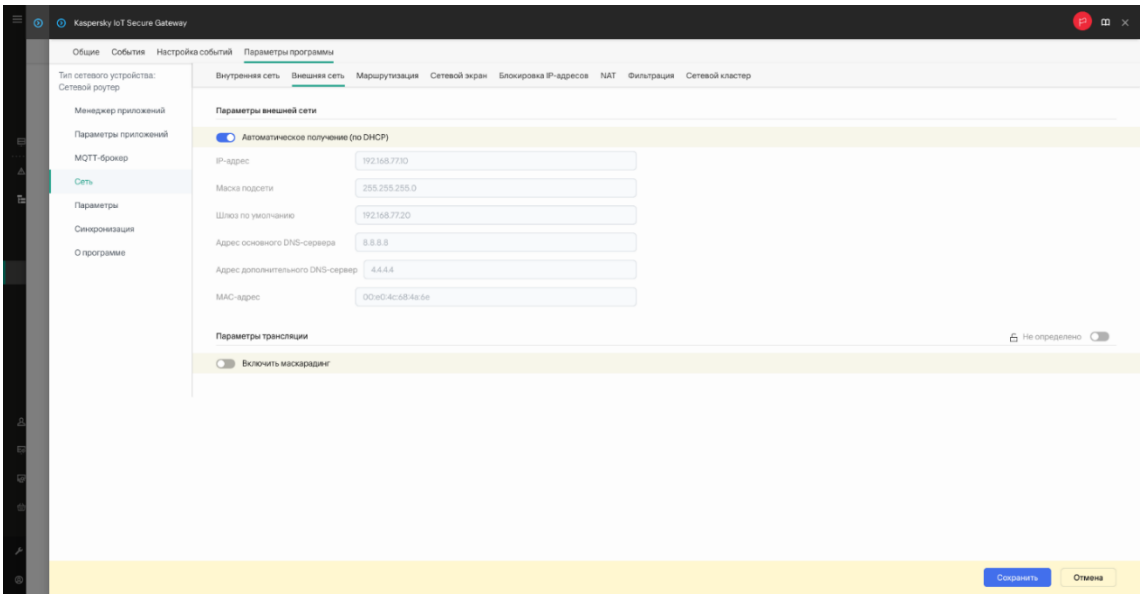


Подробнее о настройке доступа из внешней сети к внутренней сети см. в разделе Сценарий: Настройка доступа из внешней сети к устройствам внутренней сети в справке Kaspersky IoT Secure Gateway 1000.

Настройка маршрутизации

Для настройки маршрутизации в Kaspersky IoT Secure Gateway 1000 из внешней сети во внутреннюю, вам нужно выполнить следующие действия через веб-плагин Kaspersky IoT Secure Gateway 1000 для Kaspersky Security Center Web Console:

1. Выключите маскарадинг.
   Для этого перейдите в раздел **Параметры программы** → **Сеть** → **Внешняя сеть** и в блоке **Параметры трансляции** установите переключатель **Включить маскарадинг** в положение выключено (см. рис. ниже).
   Подробнее о функциональности маскарадинга см. в разделе Настройка маскарадинга через Web Console в справке Kaspersky IoT Secure Gateway 1000.



2. На клиенте настройте маршруты из внешней сети во внутреннюю и укажите в качестве шлюза IP-адрес WAN-интерфейса Kaspersky IoT Secure Gateway 1000 (en0).

   Вы можете посмотреть актуальные IP-адреса и маршруты для Kaspersky IoT Secure Gateway 1000 в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 на странице диагностики неисправностей, расположенной по адресу <веб-адрес Kaspersky IoT Secure Gateway 1000>/troubleshooting.html.

   Если маршрутизация настроена верно, клиент во внешней сети сможет выполнить пинг до сервера во внутренней сети. Сетевой экран Kaspersky IoT Secure Gateway 1000 не блокирует ICMP-пакеты.

Перед подключением Kaspersky IoT Secure Gateway к маршрутизатору убедитесь, что внешняя сеть на маршрутизаторе отличается от внутренней сети, так как маршрутизаторы часто могут использовать подсеть 192.168.1.0/24, которая совпадает с LAN-интерфейсом Kaspersky IoT Secure Gateway 1000.

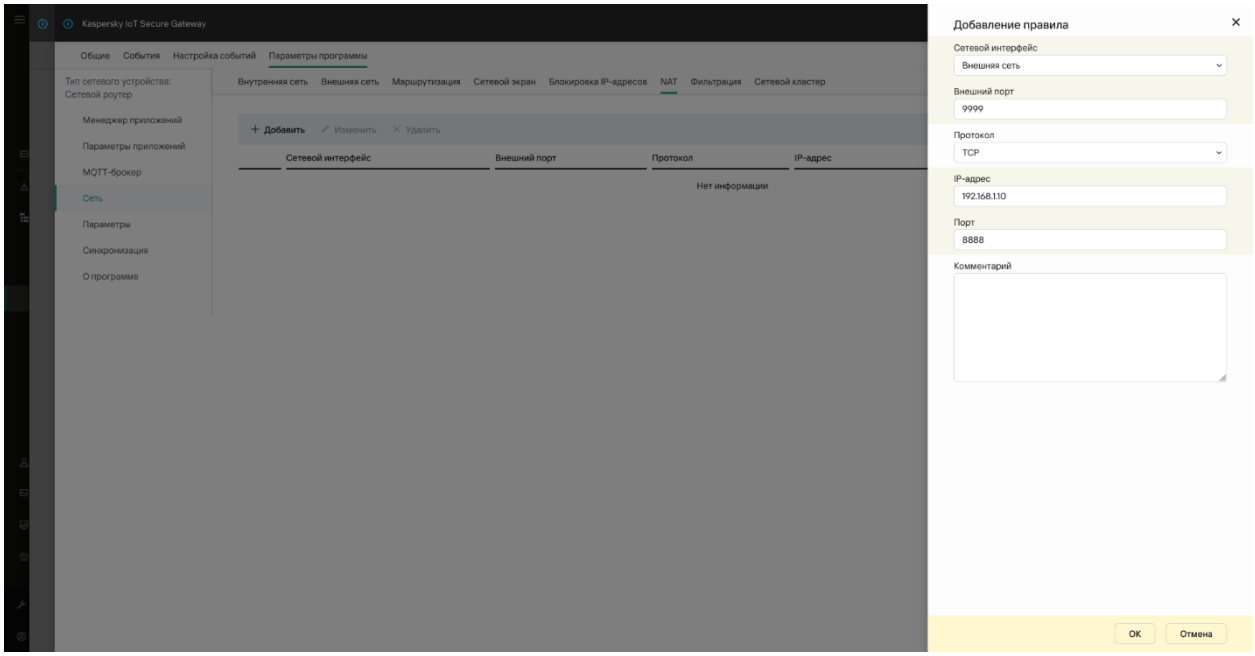
Разрешение доступа из внешней сети к хосту во внутренней сети, если маскарадинг включен

Если функция маскарадинга включена в Kaspersky IoT Secure Gateway 1000, для разрешения доступа из внешней сети к хосту во внутренней сети необходимо настроить проброс порта (NAPT). Дополнительных правил сетевого экрана или маршрутизации настраивать не нужно.

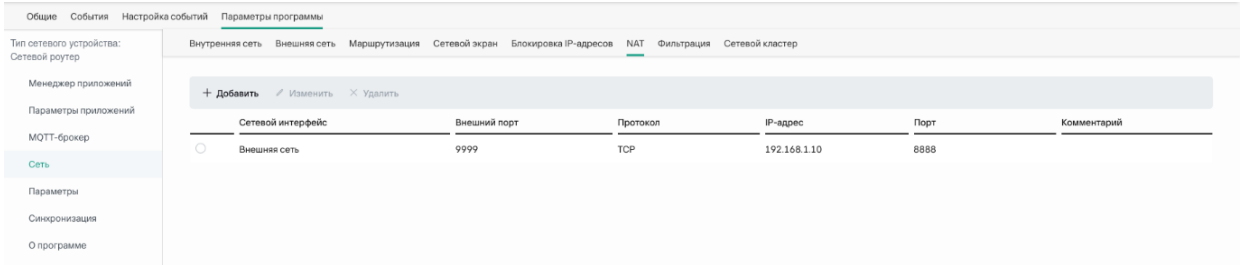
Например, рассмотрим сценарий, в котором клиент во внешней сети имеет IP-адрес 192.168.77.122, сервер во внутренней сети имеет IP-адрес 192.168.1.10:8888, а Kaspersky IoT Secure Gateway 1000 во внешней сети имеет IP-адрес 192.168.77.10.

Вам нужно настроить проброс порта (NAPT) в Kaspersky IoT Secure Gateway 1000 для IP-адреса 192.168.77.10:9999 таким образом, чтобы преобразовать его в IP-адрес 192.168.1.10:8888. После применения этих настроек все входящие пакеты на IP-адрес и порт 192.168.77.10:9999 будут переадресованы на 192.168.1.10:8888 через Kaspersky IoT Secure Gateway 1000.

Вы можете сделать это через веб-плагин Kaspersky Security Center Web Console, создав правило адресной трансляции.



Созданное правило адресной трансляции будет выглядеть следующим образом в таблице правил:



Подробнее о настройке правил адресной трансляции см. в разделе Настройка правил адресной трансляции через Web Console в справке Kaspersky IoT Secure Gateway 1000.

Разрешение доступа из внешней сети к хосту во внутренней сети, если маскарадинг выключен

Если функция маскарадинга выключена в Kaspersky IoT Secure Gateway 1000, для разрешения доступа из внешней сети к хосту во внутренней сети необходимо разрешающее правило сетевого экрана в Kaspersky IoT Secure Gateway 1000 и маршрутизацию на сервере.

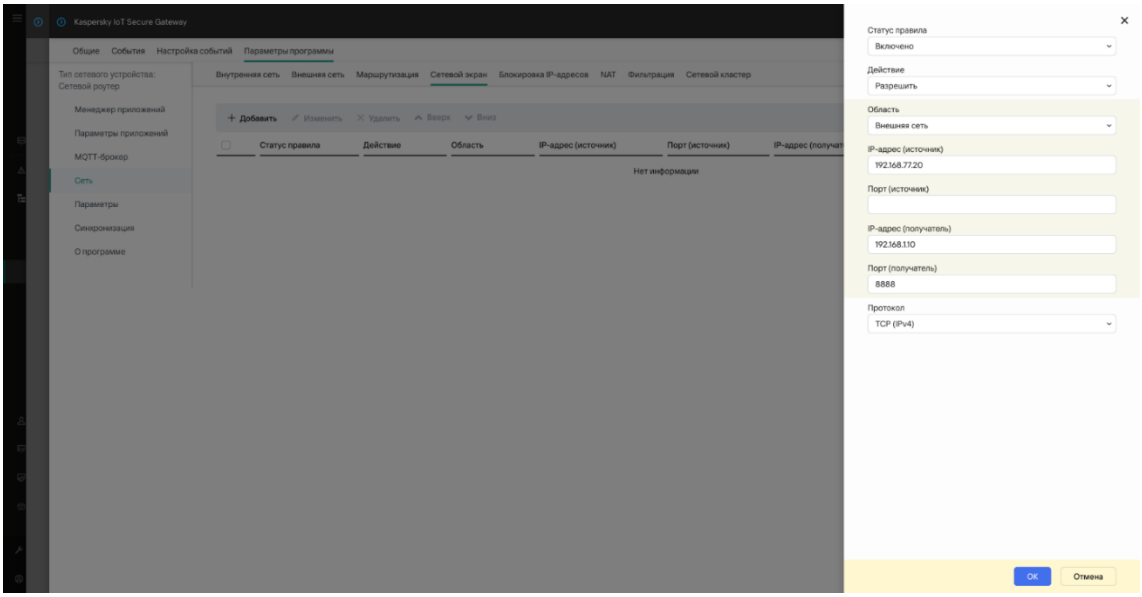
Например, рассмотрим сценарий, в котором клиент во внешней сети имеет IP-адрес 192.168.77.20, сервер во внутренней сети имеет IP-адрес 192.168.1.10:8888, а Kaspersky IoT Secure Gateway 1000 во внешней сети имеет IP-адрес 192.168.77.10.

Чтобы разрешить из внешней сети к хосту во внутренней сети:

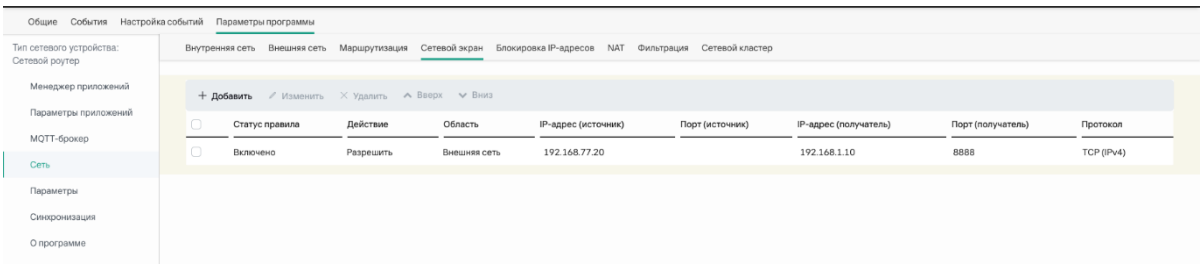
1. Настройте разрешающее правило сетевого экрана в Kaspersky IoT Secure Gateway 1000 для IP-адреса 192.168.77.20 таким образом, чтобы разрешить его доступ по адресу 192.168.1.10:8888. Вы можете сделать это, создав правило сетевого экрана через веб-плагин Kaspersky Security Center Web Console со следующими параметрами:

Действие	**Сеть**	**Протокол L4**	**IP-адрес:номер порта источника**	**IP-адрес:номер порта назначения**
Разрешить	Внешняя	TCP	192.168.77.20:any	192.168.1.10:8888

   При создании разрешающее правило будет выглядеть следующим образом:



   В результате в таблице правил появился следующее правило:



2. На стороне сервера во внешней сети создайте маршрут для хоста 192.168.1.0/24 через 192.168.77.10.

Ограничение доступа для хоста из внешней сети по конкретному порту

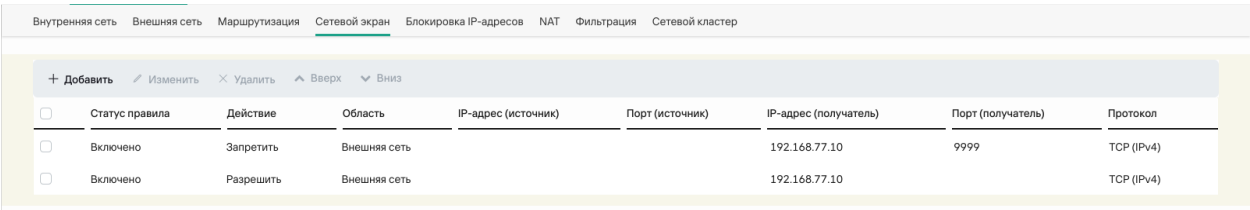
Если для хоста во внешней сети необходимо ограничить доступ во внутреннюю сеть по конкретному порту, вам нужно создать пользовательские правила сетевого экрана так, чтобы запретить доступ для необходимого порта во внешней сети и разрешить доступ для остальных портов.

В этом случае необходимо создать правила сетевого экрана со следующими параметрами:

Действие	**Сеть**	**Протокол L4**	**IP-адрес:номер порта источника**	**IP-адрес:номер порта назначения**
Запретить	Внешняя	TCP	any:any	192.168.77.10:9999
Разрешить	Внешняя	TCP	any:any	192.168.77.10:any

Вы можете создать правила сетевого экрана с параметрами, указанными в таблице выше, через веб-плагин Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center Web Console, по инструкции в разделе Создание правил сетевого экрана в справке Kaspersky IoT Secure Gateway 1000.

В результате таблица правил сетевого экрана будет выглядеть следующим образом:



Настройка Kaspersky IoT Secure Gateway 1000 как тип сетевого устройства однонаправленный шлюз

Если вы используете Kaspersky IoT Secure Gateway 1000 в качестве однонаправленного шлюза, устройство имеет следующие особенности функционирования:

- Устройство представляет собой программный однонаправленный шлюз.
- Сетевые стеки, относящиеся к сетевым интерфейсам внутренней и внешней сетей, разделены на уровне процессов.
- Передача данных между сетевыми интерфейсами возможна только через приложения, поддерживающие специальный интерфейс – Message Sender и Message Receiver.
- Передача данных возможна только в одном направлении – из внутренней сети во внешнюю.
- Приложение Kaspersky IoT Secure Gateway Network Protector подключено только ко внутренней сети.

Передача информационных пакетов осуществляется с помощью маршрутизациии между эндпоинтами приложений Message Sender и Message Receiver следующим образом:

1. Приложение Message Sender принимает входящие соединения из локальной сети по списку своих эндпоинтов и поддерживает эти соединения.
2. Приложение Message Sender отправляет полученные данные в виде сообщений на эндпоинты приложения Message Receiver в соответствии с таблицей маршрутов.
3. Для каждого полученного на эндпоинт сообщения приложение Message Receiver создает новое TLS-соединение на указанный IP-адрес во внешней сети, отправит полученные в сообщении данные и закроет соединение.

Чтобы настроить прохождение трафика до хоста во внешней сети:

1. Установите приложения Message Sender и Message Receiver на устройстве Kaspersky IoT Secure Gateway 1000 по инструкции в разделе Скачивание и установка приложений в справке Kaspersky IoT Secure Gateway 1000.
2. Настройте эндпоинты и маршрутизацию между приложениями Message Sender и Message Receiver.

   Подробную информацию о настройке параметров маршрутизации см. в разделе Маршрутизация приложений в справке Kaspersky IoT Secure Gateway 1000.

3. Добавьте разрешающее пользовательское правило сетевого для указанного в эндпоинте IP-адреса во внутренней сети по инструкции в разделе Создание правил сетевого экрана в справке Kaspersky IoT Secure Gateway 1000.

Выбор схемы использование сетевого экрана в зависимости от конфигурации Kaspersky IoT Secure Gateway 1000

Вы можете использовать схему (рис. ниже), чтобы определить схему настройки сетевого экрана для конфигурации Kaspersky IoT Secure Gateway 1000, которую вы настроили на устройстве.