Использование базовых сигнатур в приложении Kaspersky IoT Secure Gateway Network Protector

kaspersky

kaspersky cyber immunity

Сертифицированное устройство Kaspersky IoT Secure Gateway 1000 в конфигурации межсетевого экрана поставляется с предустановленным приложением Kaspersky IoT Secure Gateway Network Protector.

Приложение Kaspersky IoT Secure Gateway Network Protector использует правила анализа трафика для детектирования входящих угроз. Для выполнения целей безопасности весь трафик, проходящий через устройство под управлением Kaspersky IoT Secure Gateway 1000, блокируется, если не обнаружены правила анализа трафика.

Чтобы использовать функциональность сертифицированного устройства Kaspersky IoT Secure Gateway 1000 в качестве межсетевого экрана, вам необходимо настроить конфигурацию приложения Kaspersky IoT Secure Gateway Network Protector. Без настроенных параметров конфигурации Kaspersky IoT Secure Gateway 1000 перейдет в аварийный режим для обеспечения безопасного состояния и выполнения целей безопасности.

Для настройки конфигурации приложения Kaspersky IoT Secure Gateway Network Protector требуется добавить не менее одного правила анализа трафика. Если вам не нужно использовать анализ трафика, но важно использовать сертифицированную функциональность устройства, вы можете воспользоваться базовыми правилами анализа трафика. Базовые правила анализа трафика не детектируют угрозы, но позволяют в полном объеме использовать функциональность межсетевого экрана.

Вы можете добавить базовые сигнатуры, воспользовавшись любым инструментом управления Kaspersky IoT Secure Gateway 1000: через веб-плагин, установленный в Kaspersky Security Center Web Console, или локальный веб-интерфейс.

Добавление базовых сигнатур через Kaspersky Security Center Web Console

Чтобы добавить базовую сигнатуру в приложение Kaspersky IoT Secure Gateway Network Protector через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства → Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.
   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений → Приложения**.
   Отобразится таблица установленных приложений.
7. Остановите приложение Kaspersky IoT Secure Gateway Network Protector, если оно запущено:
   a. Установите флажок напротив приложения Kaspersky IoT Secure Gateway Network Protector.
   b. Нажмите на кнопку **Запустить/Остановить** в верхней части таблицы.

   Пока приложение Kaspersky IoT Secure Gateway Network Protector остановлено, транзитный трафик на устройстве будет заблокирован для обеспечения безопасности подключенных устройств.

8. Нажмите на название приложения Kaspersky IoT Secure Gateway Network Protector. Справа откроется панель **Kaspersky IoT Secure Gateway Network Protector application management**.
9. В поле **Rules for filtering commands in industrial protocols** укажите следующую сигнатуру:

```
alert tcp 169.254.254.255 any -> any any (msg:"Stub rule for IP4LL address"; sid: 424559; rev: 1; )
```

10. Нажмите на кнопку **Сохранить** в нижней части панели, чтобы сохранить изменения.
11. Запустите приложение Kaspersky IoT Secure Gateway Network Protector:
    a. Установите флажок напротив приложения Kaspersky IoT Secure Gateway Network Protector.
    b. Нажмите на кнопку **Запустить/Остановить** в верхней части таблицы.

Приложение Kaspersky IoT Secure Gateway Network Protector будет запущено с настроенной конфигурацией с использованием базовой сигнатуры.

Добавление базовых сигнатур через локальный веб-интерфейс Kaspersky IoT Secure Gateway 1000

Чтобы добавить базовую сигнатуру в приложение Kaspersky IoT Secure Gateway Network Protector через локальный веб-интерфейс Kaspersky IoT Secure Gateway 1000:

1. Остановите приложение Kaspersky IoT Secure Gateway Network Protector, если оно запущено:
    a. В меню в левой части экрана веб-интерфейса перейдите на вкладку **Приложения** → **Установленные приложения**.
    Отобразится таблица всех приложений, которые установлены в Kaspersky IoT Secure Gateway 1000.
    b. В строке приложения Kaspersky IoT Secure Gateway Network Protector в столбце **Управление** нажмите на кнопку **Остановить**.
    Пока приложение Kaspersky IoT Secure Gateway Network Protector остановлено, транзитный трафик на устройстве будет заблокирован для обеспечения безопасности подключенных устройств.В меню в левой части экрана веб-интерфейса выберите раздел **Параметры** → **Конфигурация**.
2. В меню в левой части экрана веб-интерфейса выберите раздел **Параметры** → **Конфигурация**.
3. В поле конфигурации в блоке `netprotector` добавьте следующий параметр, содержащий базовую сигнатуру:

```
"APP_CONFIGURATION": {

  "industrial_commands_rules": "YWxlcnQgdGNwIDE2OS4yNTQuMjU0LjI1NSBhbnkgLT4gYW55IGFueSAobXNnOiJTdHViIHJ1bGUgZm9yIElQNExMIGFkZHJlc3MiOyBzaWQ6IDQyNDU1OTsgcmV2OiAxOyAp"

}
```

Нажмите на кнопку **Сохранить**, чтобы применить параметры конфигурации.

4. Запустите приложение Kaspersky IoT Secure Gateway Network Protector:
    a. В меню в левой части экрана перейдите на вкладку **Приложения → Установленные приложения**.
    b. В строке приложения Kaspersky IoT Secure Gateway Network Protector в столбце **Управление** нажмите на кнопку **Запустить**.

Приложение Kaspersky IoT Secure Gateway Network Protector будет запущено с настроенной конфигурацией с использованием базовой сигнатуры.

ВАЖНО
IP-адрес 169.254.254.255, используемый в базовой сигнатуре, взят из диапазона адресов IPv4 Link-Local по спецификации (https://www.rfc-editor.org/rfc/rfc3927#section-2).

Этот адрес может быть назначен Kaspersky IoT Secure Gateway 1000, но только если получение IP-адреса происходит по DHCP и Kaspersky IoT Secure Gateway 1000 не смог получить от DHCP-сервера корректный IP-адрес.

Это не влияет на функциональность устройства Kaspersky IoT Secure Gateway 1000. Администратору необходимо самостоятельно исправить ситуацию с получением корректного IP-адреса.