Настройка отправки журналов с устройства Check Point Security Gateway

В данной статье описано, как настроить отправку журналов с устройства Check Point Security Gateway.

Общие сведения

Syslog (System Logging Protocol) — это стандартный протокол, используемый для передачи системных сообщений и журналов на специализированный сервер (Syslog-сервер).
Большинство сетевых устройств, включая маршрутизаторы и коммутаторы, поддерживают этот протокол.

Check Point поддерживает два стандарта Syslog:

- **RFC 3164** (устаревший, также называется BSD-протоколом);
- **RFC 5424** (новый).

- Протокол Syslog не шифрует данные. Убедитесь, что Security Gateway и Syslog-сервер находятся в защищенной сети и максимально близко друг к другу.
- Не поддерживаются: журналы по IPv6 и журналы Software Blade.

По умолчанию журналы Security Gateway отправляются на Security Management Server. Однако можно настроить прямую отправку журналов на внешний Syslog-сервер.

Создание объектов Syslog-сервера в SmartConsole

Выполните следующие шаги:

Шаг 1. Подключитесь к **Security Management Server** через **SmartConsole**.

Шаг 2. В левой панели навигации выберите **Gateways & Servers**.

Шаг 3. В **Object Explorer** создайте хост-объект для Syslog-сервера:

1. Нажмите **New → Host**.
2. Заполните поля:
   - **Name** — уникальное имя (например, Syslog_Server_01);
   - **IPv4 address** — IP-адрес Syslog-сервера;
   - **IPv6 address** — опционально (требует включенной поддержки IPv6 на Gateway).
3. Нажмите **OK**.

Шаг 4. Создайте объект Syslog-сервера:

1. В **Object Explorer** выберите **New → Server → More → Syslog** .
2. Заполните поля:
   - **Name** — уникальное имя (например, Syslog_SVC_01);
   - **Host** — выберите ранее созданный хост или создайте новый;
   - **Port** — порт Syslog-сервера (по умолчанию **514**);
   - **Version** — выберите один из вариантов:
     - **BSD Protocol** (RFC 3164);
     - **Syslog Protocol** (RFC 5424).
3. Нажмите **OK**.

Все Syslog-серверы, назначенные одному Gateway/Cluster, **должны использовать один и тот же протокол** (либо все BSD, либо все RFC 5424).
Резервные (backup) Syslog-серверы не поддерживаются.

Назначение Syslog-сервера Security Gateway

Шаг 1. В SmartConsole дважды нажмите по объекту нужного **Security Gateway** или **Cluster**.

Шаг 2. В левом дереве выберите **Logs**.

Шаг 3. В таблице **Send logs and alerts to these log servers** нажмите зеленый значок **+**.

Шаг 4. Выберите ранее созданный(е) объект(ы) **Syslog Server**.

Шаг 5. Нажмите **OK**.

Шаг 6. Установите политику (**Install Policy**) на Gateway/Cluster.

Для кластеров: настройки должны быть одинаковыми на всех членах кластера.

Включение функции Syslog in Kernel (опционально)

Функция **Syslog in Kernel** позволяет отправлять журналы напрямую из ядра, минуя пользовательское пространство. По умолчанию она отключена (fwsyslog_enable = 0).

Шаг 1. Проверка текущего состояния:

fw ctl get int fwsyslog_enable

- 0 — отключено (по умолчанию);
- 1 — включено.

Шаг 2. Включение функции:

- Временное (до перезагрузки):

  fw ctl set int fwsyslog_enable 1

  После этого **обязательно установите политику** в SmartConsole.

- Постоянное (сохраняется после перезагрузки):
  1. Перейдите в Expert Mode на Gateway.
  2. Отредактируйте файл **vi $FWDIR/boot/modules/fwkern.conf**.
  3. Добавьте строку:

     fwsyslog_enable=1

  4. Сохраните файл и перезагрузите устройство.

Шаг 3. Если необходимо отключение функции:

- Временное:

  fw ctl set int fwsyslog_enable 0

- Постоянное:
  1. Откройте файл $FWDIR/boot/modules/fwkern.conf.
  2. Либо измените значение на 0, либо удалите строку fwsyslog_enable=1.
  3. Сохраните и перезагрузите устройство.

Мониторинг количества отправленных журналов (для CoreXL)

Если используется архитектура **CoreXL**, можно проверить количество журналов, отправленных каждым экземпляром:

Для одного экземпляра

Для проверки количества журналов отправленных одним экземпляром, выполните:

Шаг 1. Выполните в терминале:

fw -i <номер_экземпляра> ctl get fwsyslog_nlogs_counter

Пример:

```
fw -i 0 ctl get fwsyslog_nlogs_counter
# Вывод: fwsyslog_nlogs_counter = 21
```

Для всех экземпляров одновременно

Для проверки количества журналов отправленных каждым экземпляром, выполните:

Шаг 1. Откройте **два терминала** к Gateway.

Шаг 2. В первом запустите:

fw ctl zdebug | grep logs

Шаг 3. Во втором выполните:

fw ctl set int fwsyslog_print_counter 1

Шаг 4. В первом терминале вы увидите счетчики по каждому экземпляру и общий итог:

```
;[cpu_2];[fw4_0];Number of logs sent from instance 0 is 43;
;[cpu_2];[fw4_0];Number of logs sent from instance 1 is 39;
;[cpu_2];[fw4_0];Total logs sent from kernel (all instances) = 132;
```

Шаг 5. Остановите вывод в первом терминале: **Ctrl+C**.

Заключение

После выполнения всех шагов Security Gateway будет отправлять журналы безопасности на указанный Syslog-сервер в выбранном формате (RFC 3164 или RFC 5424). Убедитесь, что ваш Syslog-сервер настроен на прием сообщений на указанном порту и может корректно обрабатывать выбранный формат.

ID статьи: 1619
Последнее обновление: 14 апр., 2026
Обновлено от: Михалева А.
Ревизия: 1
База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.6.0 -> Логикор. Руководство разработчика -> Подключение источников событий в Логикор -> Настройка источников -> Настройка отправки журналов с устройства Check Point Security Gateway
https://docs.axel.pro/entry/1619/