Настройка отправки журналов с устройства Palo Alto Networks (PAN-OS)

В данной статье описано, как настроить отправку журналов с Palo Alto Networks (PAN-OS).

Общие сведения

Для централизованного сбора и анализа журналов с межсетевого экрана Palo Alto Networks необходимо:

1. Создать профиль Syslog-сервера.
2. Назначить его на нужные типы журналов.
3. (Опционально) настроить формат заголовка, TLS-шифрование и другие параметры.

Стандартная конфигурация Syslog не поддерживает сбор журналов в формате CEF (Common Event Format). Для CEF требуется ручная настройка.

Создание профиля Syslog-сервера

Шаг 1. Перейдите в веб-интерфейсе **Device → Server Profiles → Syslog → Add** .

Шаг 2. Укажите параметры профиля:

- **Name:** уникальное имя профиля;
- **Location:** если используются виртуальные системы (vsys), выберите vsys или Shared.

Шаг 3. Добавьте один или несколько Syslog-серверов (максимум 4):

- **Name:** имя сервера внутри профиля;
- **Syslog Server:** IP-адрес или FQDN сервера.

  Если указан FQDN и используется UDP, при невозможности разрешения имени будет использован предыдущий кэшированный IP-адрес.

- **Transport** — протокол:
  - UDP (по умолчанию);
  - TCP;
  - SSL (TLSv1.2) — только TLS 1.2.

Шаг 4. (Опционально) На вкладке **Custom Log Format** можно задать собственный формат сообщений (например, для CEF).

Шаг 5. Нажмите **OK**.

Настройка пересылки журналов трафика, угроз и WildFire

Шаг 1. Создайте профиль пересылки журналов:

1. Перейдите в раздел **Objects → Log Forwarding → Add** .
2. Укажите **Name** профиля.
3. Для каждого типа журнала (Traffic, Threat, WildFire Submission) и уровня серьезности/вердикта WildFire:
   - Выберите созданный **Syslog-профиль**.
   - Нажмите **OK**.

Шаг 2. Назначьте профиль правилам безопасности:

1. Перейдите в раздел **Policies → Security**.
2. Выберите правило или создайте новое.
3. На вкладке **Actions** укажите ваш **Log Forwarding Profile**.
4. Для журналов трафика отметьте:
   - **Log at Session Start** (при начале сессии);
   - **Log at Session End** (при завершении сессии).
5. Нажмите **OK**.

Настройка пересылки системных и конфигурационных журналов

Шаг 1. Перейдите в раздел **Device → Log Settings**;

Шаг 2. Настройте по категориям:

Тип журнала	Действие
System, Correlation	Нажмите по каждому уровню серьезности → выберите Syslog-профиль → OK
Config, HIP Match, Correlation	Отредактируйте раздел → выберите Syslog-профиль → OK

(Опционально) Настройка формата имени хоста в заголовке Syslog

Это глобальная настройка, влияющая на все Syslog-профили.

Шаг 1. Перейдите в раздел **Device → Setup → Management → Edit Logging and Reporting Settings** .

Шаг 2. На вкладке **Log Export and Reporting** выберите **Syslog HOSTNAME Format**:

- **FQDN (по умолчанию):** hostname.domain;
- **hostname:** только имя хоста;
- **ipv4-address:** IPv4-адрес интерфейса (обычно MGT);
- **ipv6-address:** IPv6-адрес интерфейса;
- **none:** без идентификатора (не рекомендуется).

Шаг 3. Нажмите **OK**.

(Опционально) Настройка TLS-шифрования с аутентификацией клиента

Требуется, если Syslog-сервер проверяет подлинность firewall через сертификат. Требования к сертификату:

- закрытый ключ должен храниться на самом firewall (не на HSM);
- Subject ≠ Issuer;
- сертификаты firewall и Syslog-сервера должны быть подписаны одним доверенным УЦ (или использовать self-signed сертификат, импортированный на обе стороны);
- цепочка сертификатов должна поддерживать OCSP или CRL (и быть валидной).

Создание сертификата

Для создания сертификата выполните следующие шаги:

Шаг 1. Перейдите в раздел **Device → Certificate Management → Certificates →**

- **Device Certificates (PAN-OS ≤ 11.2)**;
- **Custom Certificates (PAN-OS ≥ 12.1)**;
  → Generate.

Шаг 2. Заполните:

- **Name:** имя сертификата;
- **Common Name:** IP-адрес firewall (тот, с которого отправляются журналы);
- **Signed by:** доверенный УЦ или self-signed CA.

Шаг 3. Убедитесь, что **не отмечены** опции:

- Certificate Authority;
- External Authority (CSR).

Шаг 4. Нажмите **Generate**.

Шаг 5. После создания:

1. Кликните по имени сертификата → **Edit**.
2. Отметьте **Certificate for Secure Syslog**.
3. Нажмите **OK**.

Шаг 6. Выполните **Commit**.

(Опционально) Принудительное обновление соединения при смене FQDN

По умолчанию firewall сохраняет соединение даже при изменении IP-адреса FQDN. Чтобы соединение пересоздавалось при обновлении DNS-записи:

Шаг 1. Подключитесь к CLI firewall.

Шаг 2. Выполните команду:

```
admin> set syslogng fqdn-refresh yes
```

Завершение настройки

Выполните следующие шаги:

Шаг 1. Нажмите **Commit**, чтобы применить изменения.

Шаг 2. Проверьте поступление журналов на вашем Syslog-сервере.

При необходимости сверьтесь с документацией вашего SIEM или Syslog-коллектора (например, Splunk, QRadar, ELK).

Теперь ваш межсетевой экран Palo Alto Networks будет надежно передавать журналы на внешний сервер в нужном формате и с требуемым уровнем безопасности.

ID статьи: 1552
Последнее обновление: 31 мар., 2026
Обновлено от: Михалева А.
Ревизия: 8
База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.5.0 -> Логикор. Руководство разработчика -> Подключение источников событий в Логикор -> Настройка источников -> Настройка отправки журналов с устройства Palo Alto Networks (PAN-OS)
https://docs.axel.pro/entry/1552/