Настройка отправки журналов с устройства Cisco Secure Firewall ASA

В данной статье описано, как настроить отправку журналов с Cisco Identity Services Engine (ISE).

Общие сведения

Для эффективного мониторинга и диагностики рекомендуется настроить отправку Syslog-сообщений на один или несколько внешних получателей:

- внешние Syslog-серверы;
- внутренний буфер журналов;
- ASDM;
- SNMP-станции управления;
- консольный порт;
- адреса электронной почты;
- сессии Telnet/SSH.

Если интерфейс, через который вы настраиваете отправку журналов, имеет включенный режим **management-only**, то dataplane-журналы (с ID 302015, 302014, 106023, 304001) не будут доставлены на сервер syslog. Убедитесь, что у интерфейса отключен режим **management-only**.

Настройка отправки журналов на внешний Syslog-сервер

Выполните следующие шаги:

Шаг 1. Укажите адрес Syslog-сервера:

logging host <имя_интерфейса> <IP_адрес_сервера> [tcp[/порт] | udp[/порт]] [format emblem]

Пример:

ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020

Параметры:

- **<имя_интерфейса>:** интерфейс, через который доступен Syslog-сервер;
- **<IP_адрес_сервера>:** IPv4 или IPv6-адрес сервера;
- **Протокол по умолчанию:** UDP;
- **Поддерживаемые порты:** от 1025 до 65535;
- **UDP-порт по умолчанию:** 514;
- **TCP-порт по умолчанию:** 1470.

При использовании **TCP** и недоступности Syslog-сервера новые соединения через ASA блокируются в целях безопасности. Чтобы этого избежать, см. шаг 3.

Шаг 2. Установите уровень важности журналов и укажите, какие сообщения отправлять на сервер:

logging trap {<уровень_важности> | <список_сообщений>}

Пример:

ciscoasa(config)# logging trap errors

Параметры:

- **уровень важности:** от 0 (emergency) до 7 (debugging). Если указан уровень **N**, отправляются все сообщения с уровнем **≤ N** (например, **logging trap** отправит уровни 0–3).

Можно также указать пользовательский список сообщений.

Шаг 3. (Опционально) Разрешите новые соединения при недоступности TCP-сервера. Если используется TCP и необходимо разрешить трафик даже при падении Syslog-сервера:

logging permit-hostdown

Пример:

ciscoasa(config)# logging permit-hostdown

Эта команда отключает блокировку новых соединений при недоступности TCP-сервера Syslog или переполнении очереди журналов.

Шаг 4. (Опционально) Измените facility-код. По умолчанию используется facility **20**. Для UNIX-систем часто требуется другой код:

logging facility <число>

Пример:

ciscoasa(config)# logging facility 21

Настройка защищенной отправки журналов (SSL/TLS)

Выполните следующие шаги:

Шаг 1. Для шифрования журналов по TCP используйте ключевое слово **secure**:

logging host <интерфейс> <IP> tcp/<порт> secure [reference-identity <имя>]

Пример:

ciscoasa(config)# logging host inside 10.0.0.1 tcp/1500 secure reference-identity syslogServer

Защищенная отправка работает только по TCP.

Параметр **reference-identity** включает проверку сертификата по RFC 6125. Объект **identity** должен быть предварительно настроен.

Отправка журналов в формате EMBLEM

Для настройки выполните следующие шаги:

Шаг 1. Формат **EMBLEM** поддерживается только по UDP:

- на Syslog-сервере:

  logging host <интерфейс> <IP> udp[/порт] format emblem

  Пример:

  ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
  ciscoasa(config)# logging host interface_1 2001::1 udp format emblem

- на другие получатели (Telnet/SSH и др.):

  logging emblem

  Пример:

  ciscoasa(config)# logging emblem

Дополнительные замечания

Учтите, что:

- можно настроить несколько Syslog-серверов с помощью нескольких команд **logging host**;
- при использовании нескольких серверов рекомендуется ограничить уровень логирования значением **warnings** или выше, чтобы избежать перегрузки;
- отправка журналов по TCP не поддерживается на standby-устройствах в отказоустойчивых конфигурациях.

Заключение

После выполнения этих шагов устройство ASA будет корректно отправлять системные журналы на указанные внешние или внутренние получатели.

ID статьи: 1613
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 Cisco Secure Firewall ASA
https://docs.axel.pro/entry/1613/