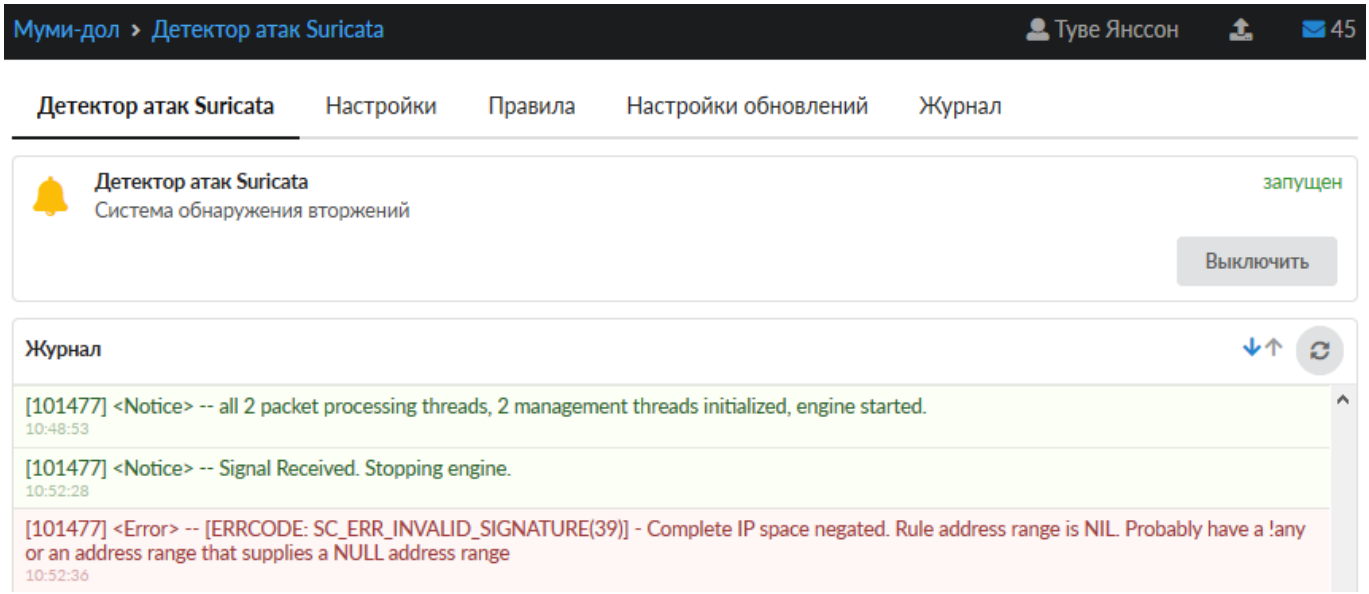
Детектор атак Suricata

Модуль «Детектор атак» расположен в Меню «Защита». Данный модуль предназначен для запуска, настройки и конфигурирования используемого в «ИКС» open source IPS/IDS системы – Suricata. Данная система была разработана Open Information Security Foundation в 2009 году. Intrusion Prevention System (IPS, система предотвращения вторжений) — это система сетевой безопасности, обнаруживающая вторжения или нарушения безопасности. IPS отслеживает сетевой трафик в реальном времени и применяет различные меры – сброс соединения, логирование выявленных сигнатур или пропускает его. Также IPS может выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами. Система Suricata поддерживает многозадачность, как следствие обладает высокой производительностью, позволяющая обрабатывать трафик до 10Gbit на обычном оборудовании, и многое другое, в том числе полная поддержка формата правил Snort.

Для работы детектора атак в режиме IPS используется фреймворк Netmap.
Netmap позволяет работать с сетевыми картам в **двух режимах**:
1. Режим эмулирования
2. Нативный режим
Нативный режим является предпочтительным и возможен при условии поддержки его сетевыми адаптерами. Данный режим позволяет обрабатывать трафик с минимальными потерями в скорости. Он включается автоматически, если в поле «Интерфейсы» в настройках детектора атак указаны исключительно адаптеры из следующего списка: cxgbe, em, igb, lem, ixgbe, ixl, re, vtnet.
Если в поле «Интерфейсы» указан хотя бы один интерфейс не из этого списка, Netmap будет работать в режиме эмулирования, основным недостатком которого будет потеря скорости обработки пакетов и вероятное значительное уменьшение скорости интернет-канала.

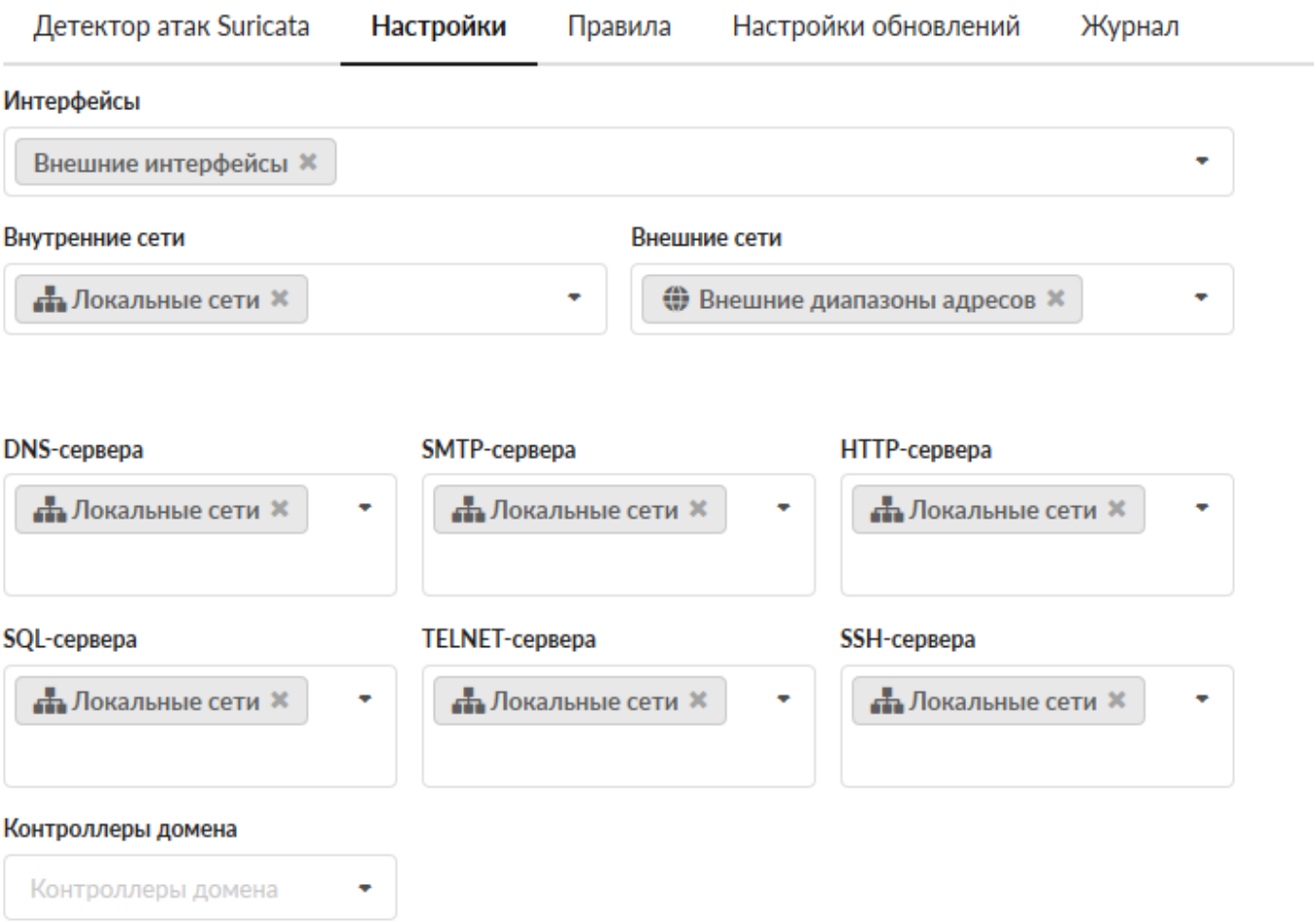
При открытии модуля в основном окне отобразятся вкладки «Детектор атак Suricata», «Настройки», «Правила», «Настройки обновлений» и «Журнал», при этом вкладка «Детектор атак Suricata» будет активна.

Детектор атак



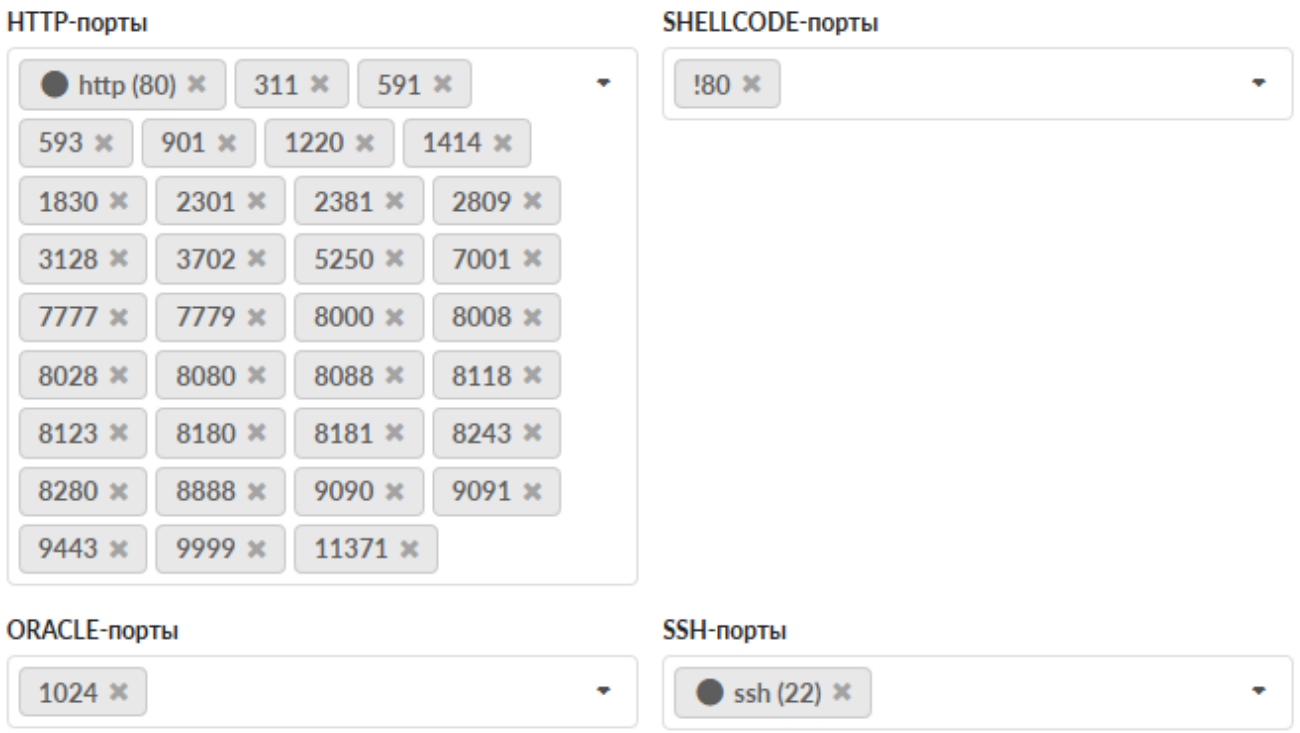
Вкладка «Детектор атак Suricata». На данной вкладке отображается состояние службы «Детектор атак Suricata» с возможностью «Выключить» (или «Включить» если служба выключена), а также последние события журнала за текущую дату.

Настройки



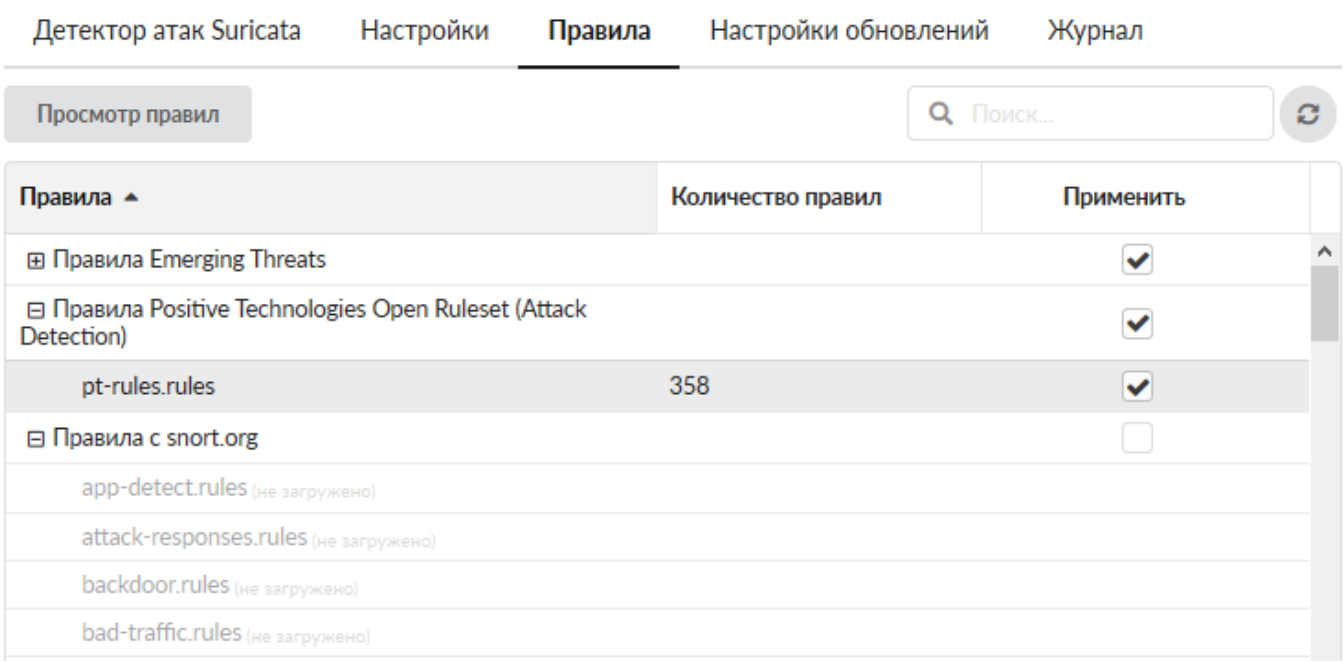
Вкладка «Настройки». Данная вкладка предназначена для настройки работы детектора

атак. Для корректного применения базы сигнатур модуля, необходимо указать расположение объектов (сетей, серверов и портов), подверженных проверке. Здесь можно указать внутренние и внешние сети, диапазоны адресов различных серверов, а также используемые порты. Всем этим переменным присвоены значения по умолчанию, с которыми детектор атак может корректно запуститься. Для изменения конфигурации по умолчанию необходимо открыть выпадающий список в соответствующей ячейки и выбрать необходимые значения из известных «ИКС» портов или диапазона адресов, заданных Пользователем «ИКС». Либо в соответствующей ячейки в ручную указать необходимое значение. Для ячеек «сети» и «сервера» допустимыми являются следующие значения: доменное имя (host.ru); ip-адрес (192.168.1.1); ip-адрес/префикс (192.168.1.1/24); ip-адрес:маска (192.168.1.1:255.255.255.0); диапазон ip-адресов (192.168.1.1 - 192.168.1.254); пользователь; группа; локальная, внутренняя, VPN, OpenVPN, WiFi сети; и другие объекты, которыми оперирует «ИКС».



Для ячеек «порты» допустимыми являются следующие значения: номер порта (25, 110), диапазон портов (1000-2000), объекты порт заведенные на «ИКС». Для ячейки «SHELLCODE-порты» также допустимо исключение портов, например, !80. По умолчанию, анализируется трафик на внешних интерфейсах. Для анализа трафика локальной сети необходимо добавить в поле «Внешние сети» объект «Локальные сети».

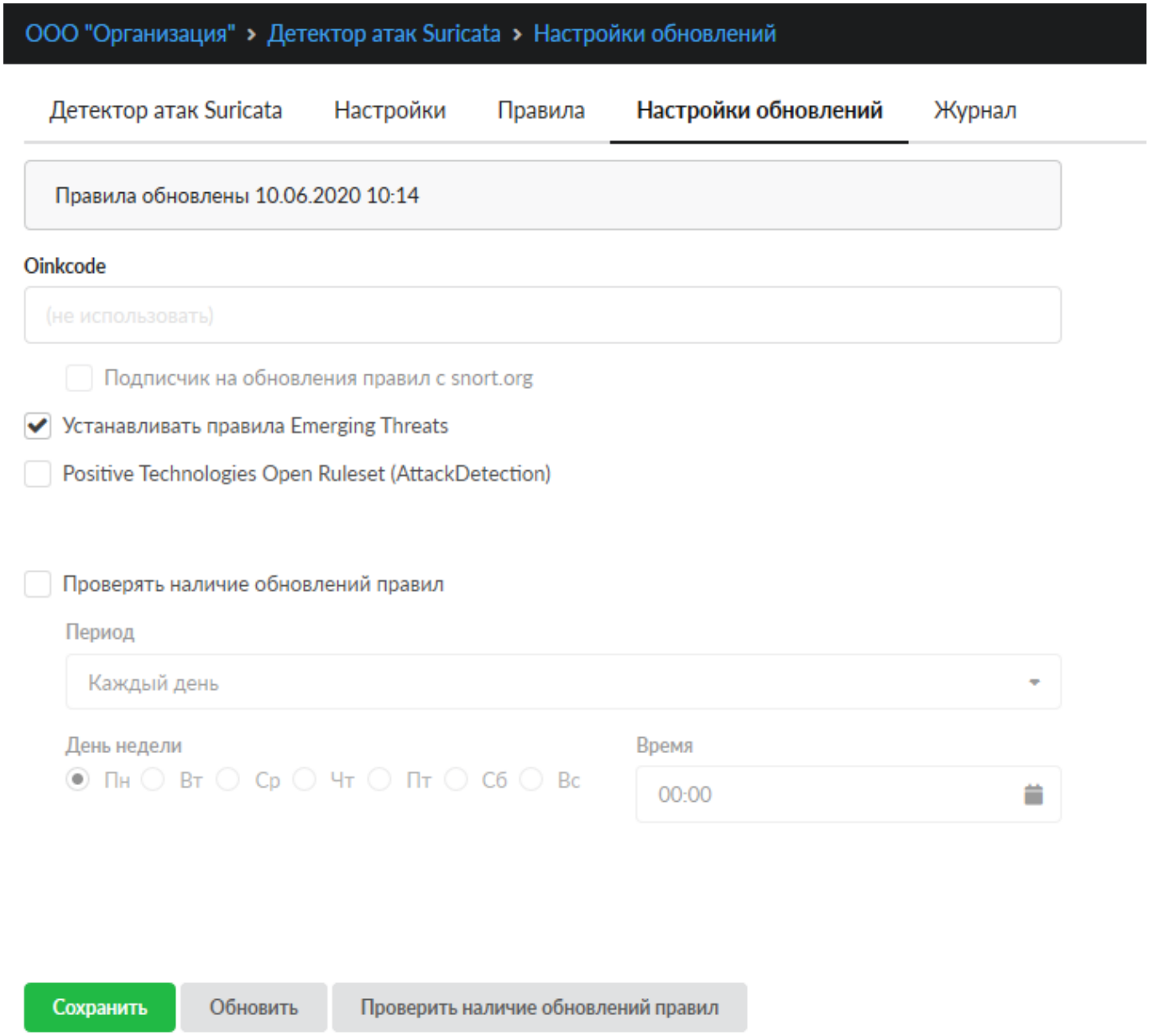
Правила



Вкладка «Правила». В данной вкладке отображаются возможные базы модуля детектора атак. Существует три базы правил: правила с сайта snort.org, прекомпилированные правила с сайта snort.org и правила Emerging Threats. Каждая база содержит в себе набор скачиваемых файлов, в каждом файле содержится набор правил, объединенных по цели защиты. Для работы набора правил из базы, необходимо чтобы данная база была скачена (см. описание вкладки «настройка обновлений»), если база не скачена, то напротив каждого файла будет надпись «не загружено». Если база была загружена, то возможно выбрать применение всей базы целиком, отметив флажок в столбце «применить». Если необходимо применить определенный файл или наоборот не применять его, то необходимо отметить флажком в столбце «применить» соответствующий файл. Напротив каждого файла показано какое количество правил тот содержит. В правом верхнем углу располагается поиск по названию файла или по id правила в файле.

Для просмотра правил и выбора действия необходимо кликнуть по имени файла, будет открыто новое диалоговое окно с таблицей. Таблица имеет следующие поля: id правила – номер правила; приоритет – значение угрозы; предупреждение – описание производимой атаки; классификация – к какому классу относится атака; действие – определяет, что необходимо сделать при обнаружении данной атаки (alert – запишет в собственный лог обнаружение и пропустит, drop – уничтожит пакет, allow - пропустит, reject – уничтожит пакет и уведомит отправителя о данном событии); включение/выключение соответствующего правила. Каждый столбец в таблице может быть отсортирован по содержимому.
Поиск работает по всем столбцам. К результатам поиска возможно применение группового действия. Также групповое действие возможно применить к правилам выделенным при помощи ctrl+левая кнопка мыши.

Настройки обновлений



Вкладка «Настройки обновлений». Данная вкладка предназначена для настройки процесса обновлений правил модуля. Существует 2 компании, которые активно занимаются разработкой правил для систем предотвращения вторжений – Sourcefire и Emerging Threats.
Для того чтобы скачать базы «Правила с snort.org» необходимо:

- Зарегистрироваться на сайте Snort.org (при необходимости стать подписчиком на обновления правил),
- Получить Oinkcode для скачивания правил, находится в личном кабинете на сайте snort.org,
- Ввести код в поле «Oinkcode»,
- Отметить следующий за этим полем флажок в том случае, если вы действительно стали подписчиком на обновления правил,
- Сохранить.

Правила можно скачать при условии наличия одного лишь кода. Обратите внимание на отличие прав подписчика от обычного зарегистрированного пользователя. После удачного скачивания правил от данного разработчика, они будут отображаться во вкладке «Правила» без пометки (не загружено).
Для того чтобы скачать базу «Правила Emerging Threats» и/или «Правила Positive Technologies

Open Ruleset (Attack Detection)» достаточно поставить флаги «Устанавливать правила Emerging Threats» и/или «Positive Technologies Open Ruleset (AttackDetection)» и сохранить изменения. Ещё один параметр, который возможно настроить на данной вкладке - это проверка наличия обновлений правил, которые были загружены. Если был установлен флаг «Проверять наличие обновлений правил», то в заданное время ИКС будет проверять наличие доступных обновлений. Если таковые есть, то произведет скачку новых правил. Также проверить наличие обновлений и скачать их, не в заданное время, возможно нажав на кнопку «Проверять наличие обновлений правил».

Журнал

Отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

From:
https://doc-old.a-real.ru/ - **Документация**

Permanent link:
https://doc-old.a-real.ru/doku.php?id=ics70:suricata&rev=1594895592

Last update: **2020/07/16 13:33**