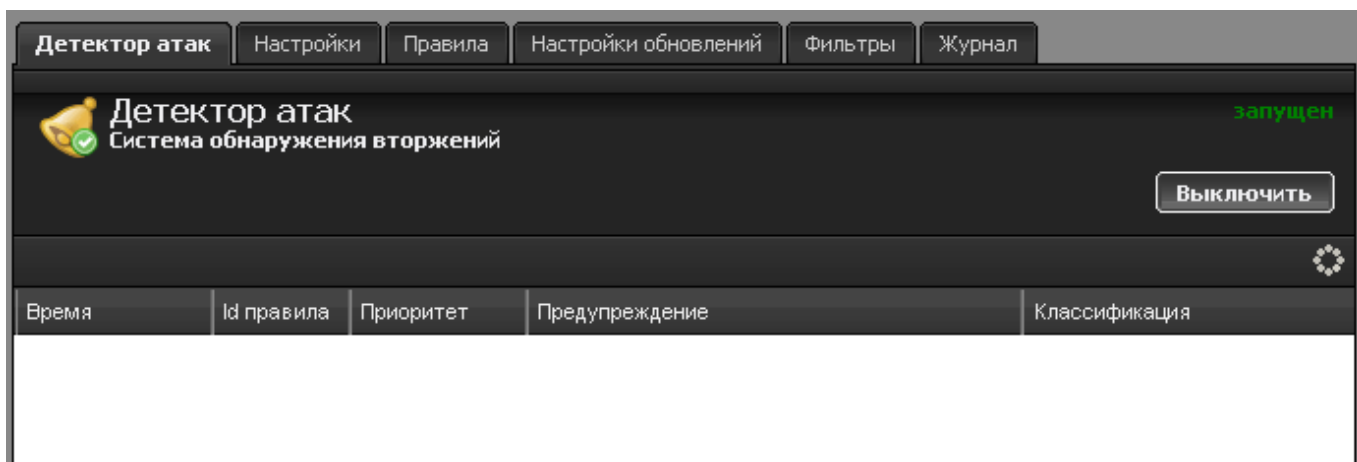


Детектор атак

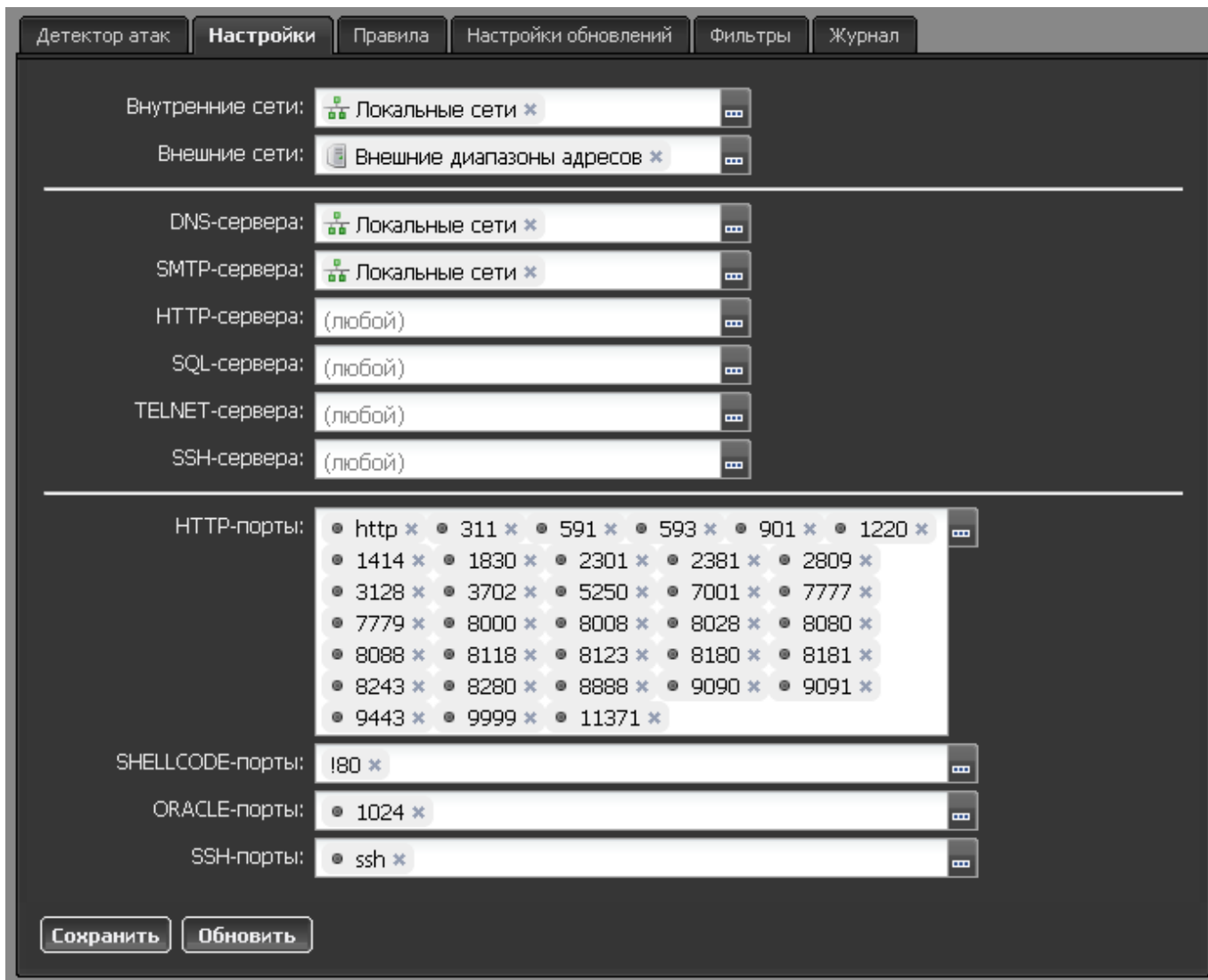
Общие положения

Детектор атак - программное средство для выявления некоторых видов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения. Функция детектора атак в Интернет Контроль Сервере реализуется с помощью свободной сетевой системы обнаружения вторжений с открытым исходным кодом Snort.



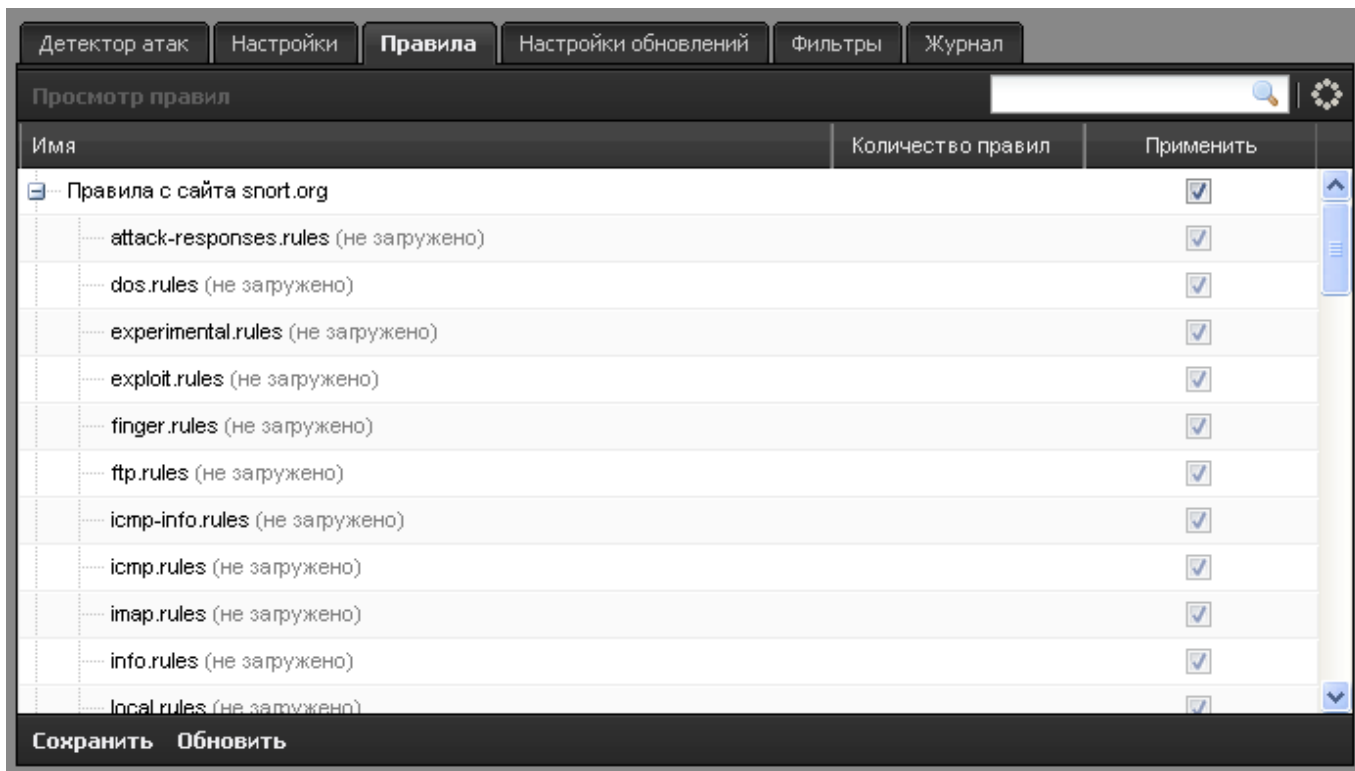
При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Настройки



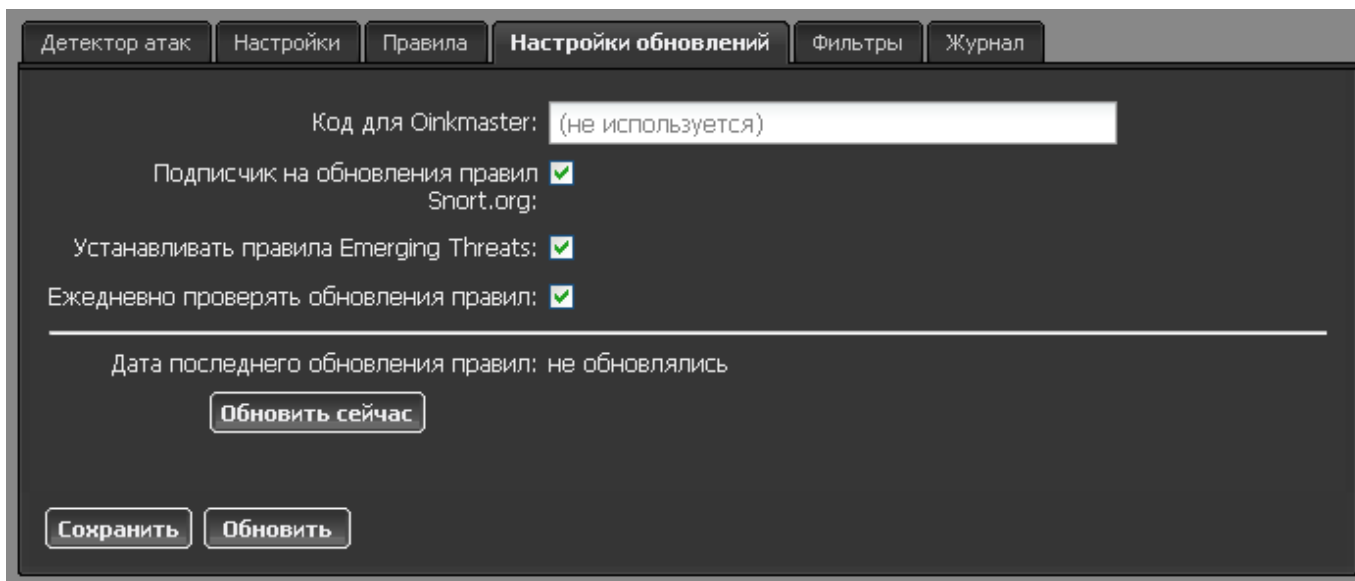
Во вкладке настроек можно редактировать параметры работы детектора атак. Здесь можно указать внутренние, внешние сети, диапазоны адресов различных серверов, а также используемые порты. Всем этим переменным присвоены значения по умолчанию, с которыми детектор атак может корректно запуститься. По умолчанию, анализируется трафик на внешних интерфейсах.

Правила



Детектору атак можно подключать правила, с помощью которых он будет анализировать трафик. Все правила разбиты на три категории: правила с сайта snort.org, прекомпилированные правила с сайта snort.org и правила Emerging Threats. На данной вкладке можно посмотреть наличие и содержимое того или иного файла с правилами, а также включить или выключить его действие (с помощью флажков справа). В правом верхнем углу располагается поиск по названию или по количеству правил в файле.

Обновления



Существует 2 компании, которые занимаются разработкой правил для системы предотвращения вторжений Snort. Первая - Sourcefire. Чтобы скачать разработанные ими правила, необходимо:

- Зарегистрироваться на сайте Snort.org (при необходимости стать подписчиком на

- обновления правил),
- Получить Oinkcode для скачивания правил,
- Ввести код в поле «Код для Oinkmaster»,
- Отметить следующий за этим полем флажок в том случае, если вы действительно стали подписчиком на обновления правил,
- Сохранить;

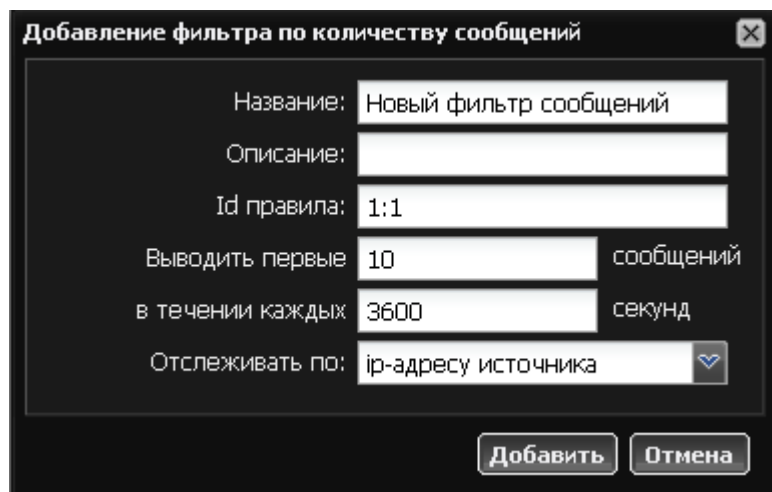
Правила можно скачать при условии наличия одно лишь кода. Обратите внимание на отличия прав подписчика от обычного зарегистрированного пользователя. После удачного скачивания правил от данного разработчика, они будут отображаться во вкладке «Правила» без пометки (не загружено).

Второе сообщество называется Emerging Threats. Для того, чтобы скачать правила от этого разработчика, достаточно поставить галку «Устанавливать правила Emerging Threats» и сохранить изменения.

Ещё один параметр, который можно настроить в этом разделе - это возможность ежедневно проверять обновления правил, которые были загружены. По умолчанию, установлено значение «истина», при необходимости его можно изменить.

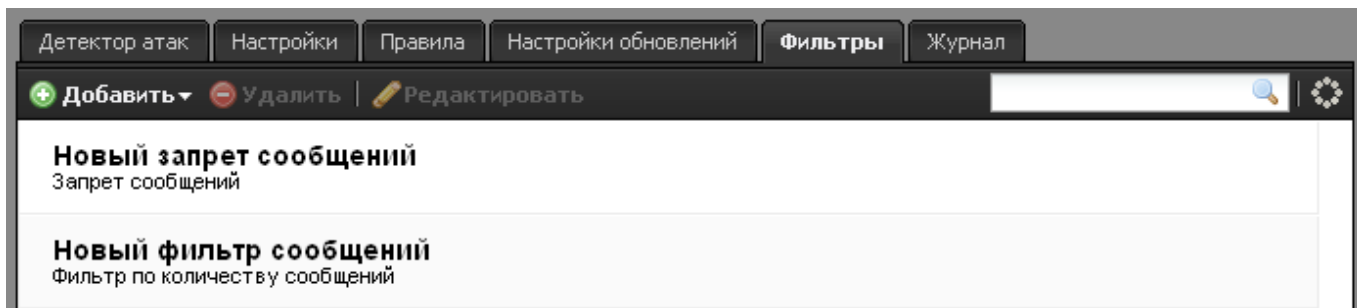
После того, как всё настроено, можно нажимать кнопку «Обновить сейчас».

Фильтры



Для того, чтобы настроить ограничения в выводе предупреждений детектором атак, необходимо перейти на вкладку «Фильтры». Здесь можно добавить следующие ограничения:

- фильтр по количеству сообщений,
- фильтр сообщений по частоте появления,
- фильтр смешанного типа,
- запрет на сообщения определённого типа;



При настройке необходимо помнить, что поле «Id правила» в различных фильтрах должно быть различным.

Журнал

В закладке «Журнал» находится сводка всех системных сообщений от FTP-сервера. Журнал разделен на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее.

Во вкладке журнал можно наблюдать работу сервиса. С течением времени там будут отображаться сообщения о различных событиях, замеченных детектором атак. У каждого такого события есть приоритет, и вы сможете фильтровать сообщения на этой вкладке по этому параметру. Выбрав одно из значений в выпадающем списке, можно увидеть все сообщения о событиях, приоритет которых выше или равен установленному. По умолчанию показываются все сообщения.

Журнал может быть очищен с помощью функции отчистки системных логов, которая находится в модуле «Система»→«Удаление данных».

В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать в журнале нужные вам записи.

Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, выберите нужную дату, используя календарь в левом верхнем углу модуля.

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

Permanent link:
<https://doc.a-real.ru/doku.php?id=en:snort>

Last update: **2020/01/27 16:28**

