

# Web Application Firewall

Модуль «Web Application Firewall» (WAF) расположен в Меню «Защита». Данный модуль отслеживает и блокирует весь HTTP/HTTPS трафик входящий и исходящий от установленных Web-приложений на «ИКС» или в локальной сети. Путём анализа HTTP/HTTPS трафика WAF может предотвращать атаки, основанные на недостатках защиты Web-приложений, таких как: SQL инъекции, межсайтовый скриптинг (XSS), включение файлов, не правильная настройка безопасности.

The screenshot displays the WAF management interface. At the top, there is a navigation bar with the text "ИКС > Web Application Firewall" and a user profile icon labeled "Администратор" with a notification badge showing "17". Below this, a date range selector shows "13.09.2019 - 13.09.2019" with tabs for "Сегодня", "Неделя", "Месяц", and "Другой период". There are buttons for "Экспорт" (Export) and "Удалить логи" (Delete logs), and a search input field labeled "Поиск...". The main area contains a list of log entries, each showing the source IP (192.168.17.8), timestamp, HTTP method, path, status code, and user agent. The entries are as follows:

192.168.17.8	- [13/Sep/2019:12:36:57 +0300]	"GET /styles.css?ver=7.0.0 HTTP/2.0"	200	129812	"https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"	12:36:57
192.168.17.8	- [13/Sep/2019:12:36:57 +0300]	"GET /jquery-3.1.1.min.js?ver=7.0.0 HTTP/2.0"	200	30120	"https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"	12:36:57
192.168.17.8	- [13/Sep/2019:12:36:57 +0300]	"GET /script.min.js?ver=7.0.0 HTTP/2.0"	200	732	"https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"	12:36:57
192.168.17.8	- [13/Sep/2019:12:36:57 +0300]	"GET /sockjs-1.1.5.min.js?ver=7.0.0 HTTP/2.0"	200	17900	"https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"	12:36:57
192.168.17.8	- [13/Sep/2019:12:36:58 +0300]	"GET /script.js?ver=7.0.0 HTTP/2.0"	200	71304	"https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"	12:36:58

At the bottom of the log list, there is a pagination control showing "Стр 1 из 1" and a status message "Показаны записи 1 - 84 из 84".

В самом модуле отображается сводка 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) - 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**».

Для включения/выключения фильтрации трафика необходимо установить/снять соответствующий флажок при добавлении или редактировании «**Виртуального хоста**»/«**Виртуального хоста с перенаправлением**», расположенных в Меню «**Файловый сервер**» - «**Веб**» - вкладка «**Веб-ресурсы**». Стоит отметить, что **Веб-сервер** должен быть настроен и запущен.

From:

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

Permanent link:

<https://doc-old.a-real.ru/doku.php?id=ics70:waf&rev=1573397477>

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

