

Table of Contents

Table of Contents	1
Атаки	2
Просмотр обнаруженных атак	3

Product: WAF
Version: 7.x
Technology: WAF

UserGate WAF, работающий в режиме reverse-прокси, анализирует HTTP- и HTTPS-трафик на прикладном уровне, чтобы защитить веб-приложения от атак. Под атаками понимаются несанкционированные воздействия на информационную инфраструктуру организации, способные нарушить ее работу или создать угрозу безопасности обрабатываемой в ней информации. Продукт обнаруживает атаки и другие угрозы безопасности с помощью [правил в WAF-профилях](#).

При срабатывании правила UserGate WAF записывает информацию об обнаружении атаки или другого события ИБ. В веб-интерфейсе продукта администраторы могут просматривать информацию о срабатываниях правил и использовать ее для дальнейшего анализа. Список срабатываний правил отображается в разделе **Атаки**.

В таблице атак вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Вы можете фильтровать данные в таблице с помощью специальных запросов [на языке фильтрации продукта](#). Для ввода запросов используется строка фильтрации. По нажатию на значение параметра срабатывания в строку фильтрации добавляется запрос с этим параметром (например, name = "(PSM) alert"). Действие доступно только для тех параметров, значения которых в таблице отображаются в виде ссылок.

Кроме того, вы можете сохранять примененные фильтры по кнопке **Сохранить как**. Список сохраненных фильтров доступен по кнопке **Популярные фильтры**. Также для дальнейшего анализа вы можете скачать отфильтрованные данные таблицы в виде CSV-файла по кнопке **Экспортировать в CSV**.

ПримечаниеВы можете отправлять сведения об атаках на серверы SSH (SFTP), FTP и Syslog. Подробнее — в разделе « [Экспорт журналов](#) ».

Для каждого срабатывания в списке отображается следующая информация.

Параметр	Описание
Время	Время срабатывания правила
Уровень угрозы	Уровень опасности угрозы согласно срабатыванию правила
WAF-профиль	WAF-профиль, к которому относится сработавшее правило. Параметр доступен начиная с версии 7.4.1
WAF-слой	WAF-слой, к которому относится сработавшее правило. Параметр доступен начиная с версии 7.4.1
ID правила	Идентификатор сработавшего правила
Название	Название сработавшего правила
IP источника	IP-адрес источника HTTP-запроса
IP назначения	IP-адрес назначения HTTP-запроса
Реальный IP	Реальный IP-адрес источника HTTP-запроса
Действие	Действие, выполненное в результате срабатывания правила
HTTP метод	Метод HTTP-запроса
HTTP версия	Версия HTTP-протокола
HTTP хост	Адрес узла, которому направлен HTTP-запрос
Код ответа HTTP	Код HTTP-ответа
URI	URI в HTTP-запросе
Useragent	Информация о клиенте в HTTP-запросе
Реферер	Ссылка на предыдущую страницу в HTTP-запросе
Профиль ответа	Название профиля ответа, который возвращается клиенту, если его HTTP-запрос был заблокирован WAF-правилом. Параметр доступен начиная с версии 7.5.0

Параметр	Описание
Идентификатор запроса	Уникальный идентификатор HTTP-запроса

Вы можете просматривать подробную информацию о срабатывании в его карточке. Действие доступно по нажатию на строку срабатывания в таблице.

