

Table of Contents

Table of Contents	1
Журналы	2
Описание	3
Журнал событий	4
Журнал веб-доступа	5
Журнал WebSocket	6
Журнал трафика	7
Журнал технологий	8
Экспорт журналов	9
Поиск и фильтрация данных	12
Описание форматов журналов	14

Описание

Version: 7.7.x

Product: WAF

UserGate WAF журналирует все события, происходящие во время его работы, и записывает их в следующие журналы:

- **Журнал событий** — события, связанные с изменением параметров устройства, например, авторизацией администраторов или обновлением библиотек.
- **Журнал веб-доступа** — подробные сведения о веб-запросах, обработанных UserGate WAF.
- **Журнал WebSocket** — сведения об установленных и заблокированных WebSocket-соединениях.
- **Журнал трафика** — подробные сведения о срабатываниях правил межсетевого экрана. Для регистрации срабатываний правила необходимо включить журналирование в свойствах этого правила.
- **Журнал технологий** — события, связанные с обнаружением технологий в трафике.

В разделе **Журналы и отчеты → Журналы** вы можете управлять данными журналов: просматривать эти данные, фильтровать их, скачивать в CSV-файл, а также экспортировать на внешние серверы.

Примечание При настроенной интеграции с UserGate Log Analyzer или UserGate SIEM журналы UserGate WAF хранятся и обрабатываются в базе данных внешнего сервера.

UserGate WAF автоматически освобождает дисковое пространство путем ротации журналов. По мере заполнения выделенного объема диска старые записи перезаписываются новыми (кроме журнала событий). Уведомления об этом фиксируются в журнале событий, записи которого не ротируются.

Журнал событий

Version: 7.7.x

Product: WAF

Журнал событий отображает события, связанные с изменением настроек WAF, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал веб-доступа

Version: 7.7.x

Product: WAF

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL в настройках которых включено журналирование. Отображается следующая информация:

- Узел, на котором произошло событие.
- Время события.
- Содержание события.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Useragent браузера.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Version: 7.7.x

Product: WAF

Если для сервера reverse-прокси настроены правила, фильтрующие WebSocket-соединения, вы можете отслеживать события, связанные с установленными или заблокированными WebSocket-соединениями. Результаты фильтрации WebSocket-соединений отображаются на странице **Журнал WebSocket**. Запись событий в журнал ведется для правил публикации, в которых разрешено журналирование этих событий.

Чтобы разрешить запись событий в журнал WebSocket:

1. В разделе **Настройки** → **Политика безопасности** → **WebSocket-профили** выберите WebSocket-профиль или настройте новый. Подробнее — в разделе «[Защита WebSocket-соединений](#)».
2. В окне **Свойства WebSocket-профиля** на вкладке **Общие** установите флажок **Включить журналирование** и сохраните изменения.
3. Убедитесь, что WebSocket-профиль с включенным журналированием подключен в правиле reverse-прокси.

На странице **Журнал WebSocket** можно настроить сортировку и отображение данных с помощью меню, которое вызывается из заголовка любого столбца. Вы также можете просмотреть подробную информацию о событии, дважды нажав на нужную запись.

Для поиска событий записи могут быть отфильтрованы по различным критериям, например по зоне источника, действию или дате.

С помощью кнопки **Экспортировать в CSV** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Журнал трафика

Version: 7.7.x

Product: WAF

Журнал трафика отображает события срабатывания правил межсетевого экрана, в настройках которых включено журналирование. Отображается следующая информация:

- Узел, на котором произошло событие.
- Время события.
- Содержание события.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.
- Байт отправлено/получено.
- Пакетов отправлено/получено.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Version: 7.7.x

Product: WAF

Documentation: 

Если в правиле публикации включено обнаружение технологий, UserGate WAF определяет технологии, используемые веб-сервисом, по анализируемому трафику. Подробнее — в разделе «[Включение обнаружения технологий](#)».

Вы можете просматривать результаты обнаружения технологий в разделе **Журнал технологий**. В журнале отображаются результаты обнаружения для всех правил публикации, в которых включена эта функция.

На странице **Журнал технологий** можно настроить сортировку и отображение данных с помощью меню, которое вызывается из заголовка любого столбца. Вы также можете просмотреть подробную информацию о событии, дважды нажав на нужную запись.

Для поиска событий записи могут быть отфильтрованы по различным критериям, например по серверу публикации или WAF-профилю.

С помощью кнопки **Экспортировать** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Экспорт журналов

Version: 7.7.x
Product: WAF

Функция экспортирования журналов позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate WAF поддерживает выгрузку следующих журналов:

- журнал событий;
- журнал веб-доступа;
- журнал WebSocket;
- журнал трафика;
- атаки.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

Параметр	Описание
Название правила	Название правила экспорта журналов
Описание	Опциональное поле для описания правила
Параметры разового экспорта	Выбор диапазона экспорта журналов. Опция доступна в версии ПО 7.2.0 и выше
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий; • Журнал веб-доступа; • Журнал трафика; • Журнал WebSocket (доступно начиная с версии ПО 7.4.1); • Атаки. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight); • CEF Compact; • JSON — JSON format; • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов — в разделе «Описание форматов журналов»
Тип сервера	SSH (SFTP), FTP, Syslog
Адрес сервера	IP-адрес или доменное имя сервера
Транспорт	Только для типа серверов Syslog — TCP или UDP
Порт	Порт сервера, на который следует отправлять данные

Параметр	Описание
Протокол	Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: в системе возникли ошибки. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные сообщения
Объект	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Сообщения пользовательские; • Системный сервис; • Безопасность/авторизация; • Аудит; • Тревога; • Local 0; • Local 1; • Local 2; • Local 3; • Local 4; • Local 5; • Local 6; • Local 7
Имя хоста	Только для типа серверов Syslog. Уникальное имя узла, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN)
Название приложения	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog

Параметр	Описание
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно; • Еженедельно; • Ежемесячно; • Каждые ... часов; • Каждые ... минут; • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки. Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.

Documentation: 
Version: 7.7.x
Product: WAF

Объем данных, регистрируемых в журналах, как правило, значителен, поэтому в стандартном режиме просмотра отображается лишь часть доступных полей. Для быстрого доступа к необходимой информации в UserGate WAF предусмотрены средства поиска и фильтрации журналов. Поиск может выполняться как в простом, так и в расширенном режиме.

В режиме простого поиска фильтрация записей осуществляется с помощью графического интерфейса. Настройка условий поиска выполняется в удобной форме и не требует знания специальных команд или синтаксиса.

Для создания более сложных условий отбора предназначен режим расширенного поиска, использующий специализированный язык запросов. В этом режиме доступны поля журналов, которые не отображаются и не могут использоваться в стандартном режиме поиска. Запросы формируются с использованием имен полей, их значений, ключевых слов и логических операторов. Значения, содержащие пробелы, необходимо заключать в одинарные (' ') или двойные (" ") кавычки. Для значений без пробелов кавычки не требуются. Для объединения и группировки нескольких условий в запросе можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Ключевые поля	Значение
AND или and	Логическое «И», требует выполнение всех условий, заданных в запросе
OR или or	Логическое «ИЛИ», требует выполнение одного из условий запроса

Операторы определяют условия фильтра и могут быть следующими:

Оператор	Значение
=	Равно — требует полного совпадения значения поля с указанным значением. Пример: ip = 172.16.31.1. Будут отображены все записи журнала, в которых поле ip будет точно соответствовать значению 172.16.31.1
!=	Не равно — значение поля не должно совпадать с указанным значением. Пример: ip != 172.16.31. Будут отображены все записи журнала, в которых поле ip не будет равно значению 172.16.31.1
<=	Меньше либо равно — значение поля должно быть меньше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date <= '2019-03-28T20:59:59' AND statusCode = 303
>=	Больше либо равно — значение поля должно быть больше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date >= "2019-03-13T21:00:00" AND statusCode = 200
<	Меньше — значение поля должно быть меньше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date < '2019-03-28T20:59:59' AND statusCode = 404
>	Больше — значение поля должно быть больше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: (statusCode > 200 AND statusCode < 300) OR (statusCode = 404)
IN	Позволяет указать в запросе несколько значений поля. Список значений необходимо заключать в круглые скобки. Пример: category IN (botnets, compromised, 'illegal software', 'phishing and fraud',' reputation high risk', 'unknown category')

Оператор	Значение
NOT IN	Позволяет указать в запросе несколько значений поля. Будут отображены записи, в которых значение поля не совпадает ни с одним из указанных. Список значений необходимо заключать в круглые скобки. Пример: category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category')
~	Содержит — позволяет указать подстроку, которая должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра. Пример: browser ~ "Mozilla/5.0". Оператор применяется только к полям, содержащим строковые значения
!~	Не содержит — позволяет указать подстроку, которая не должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра. Пример: browser !~ "Mozilla/5.0". Оператор применяется только к полям, содержащим строковые значения
MATCH	Поиск по полю с помощью регулярного выражения. Будут показаны только те записи, в которых значение поля соответствует заданному шаблону. Пример: details MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details найдется слово «NAT»
NOT MATCH	Поиск записей, в которых значение поля не совпадает с заданным регулярным выражением. Будут показаны только те записи, в которых значение поля не соответствует заданному шаблону. Пример: details NOT MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details не найдется слово «NAT»

При формировании запроса в режиме расширенного поиска UserGate WAF предлагает варианты названий полей, допустимых операторов и возможных значений. Это упрощает создание сложных поисковых выражений и снижает вероятность ошибок при вводе. Набор доступных полей и перечень допустимых значений зависят от типа просматриваемого журнала.

При переходе из режима простого поиска в режим расширенного поиска UserGate WAF автоматически преобразует заданные параметры фильтрации в строку запроса, соответствующую условиям, указанным в базовом режиме. Вы можете продолжить формирование строки поиска с использованием расширенных возможностей языка запросов без необходимости повторного ввода критериев отбора.

Экспорт журналов в формате CEF

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	events
	Origin	Модуль, в котором произошло событие	admin_console
	Severity	Важность события	Может принимать значения: 1 — информационные; 4 — предупреждения; 7 — ошибки; 10 — критичные
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Тип события	login_successful
	src	IPv4-адрес источника	192.168.117.254
	cat	Компонент, в котором произошло событие	console_auth
	cs1Label	Поле используется для указания деталей события	Attributes
	cs1	Детали события в формате JSON	{"name":"MIME_BUILTIN_COMPOSITE","module":"nlist_import"}

Формат журнала веб-доступа

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF

Тип поля	Название поля	Описание	Пример значения
	Device Version	Версия продукта	7
	Source	Название журнала	webaccess
	Name	Тип источника	log
	Threat Level	Уровень угрозы категории URL	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта	{"id":39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня	TCP.
	app	Протокол прикладного уровня и его версия	HTTP/1.1
	suser	Имя пользователя	username
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.)	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40

Тип поля	Название поля	Описание	Пример значения
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Default Allow
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Trusted
	cs3Label	Поле используется для указания страны источника	Source Country
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Untrusted
	cs5Label	Поле используется для указания страны назначения	Destination Country
	cs5	Название страны назначения	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает, было ли содержимое расшифровано	Decrypted
	cs6	Статус расшифрования: расшифровано или нет	true, false
	flexString1Label	Поле используется для указания типа контента	Media type
	flexString1	Тип контента	text/html
	flexString2Label	Поле используется для указания категории запрашиваемого URL-адреса	URL Categories
	flexString2	Категория URL	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник	1

Тип поля	Название поля	Описание	Пример значения
	cn3Label	Поле используется для указания исходного ответа сервера	Response
	cn3	Код ответа HTTP	302

Формат журнала веб-доступа **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовков	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Название журнала	webaccess
	Name	Тип источника	log
	Threat Level	Уровень угрозы категории URL	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена
	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта	{"id":39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня	TCP.
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.)	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Default Allow
	cs2Label	Поле используется для указания зоны источника	SrcZone
	cs2	Название зоны источника	Trusted
	cs3Label	Поле используется для указания зоны назначения	DstZone
	cs3	Название зоны назначения	Untrusted
	flexString1Label	Поле используется для указания категории запрашиваемого URL-адреса	URLCats
	flexString1	Категория URL	Computers & Technology
	cn1Label	Поле используется для указания исходного ответа сервера	Response
	cn1	Код ответа HTTP	302

ПримечаниеОбщее правило для компактного формата — значения некоторых полей обрезаются по длине до 80 символов. Например, список url, имя правила, имя зоны.

Формат журнала WebSocket (версия 7.4.1 и выше)

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	NGFW
	Device Version	Версия продукта	7
	Source	Тип журнала	websocket

Тип поля	Название поля	Описание	Пример значения
	Origin	Источник события	log
	Severity	Уровень опасности	Не используется. Поле передается с пустыми данными
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1759728622455
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@havntohanmin
	act	Действие, предпринятое модулем анализа websocket-трафика на устройстве	pass или deny
	reason	Информация о причине возникновения события	{"request": "GET /ws HTTP/1.1\r\nConnection: upgrade\r\nUpgrade: websocket\r\nContent-Length: 0\r\nsec-websocket-version: 13\r\nsec-websocket-key: +V9uPwL0ZfDTjmwMvnVUZA==\r\nHost: w.com \r\n\r\n", "response": "HTTP/1.1 101 Switching Protocols\r\naccess-control-allow-origin: *\r\nX-Request-ID: d8814097-a68c-4120-8912-23a11b8e88da\r\nConnection: Upgrade\r\nDate: Mon, 06 Oct 2025 05:35:52 GMT\r\nsec-websocket-accept: mn0nG2s62J2pY5E8ssleD2gnGRQ=\r\nServer: Cowboy\r\nUpgrade: websocket\r\nx-test-srv: pft-serve\r\n\r\n\r\n", "websocket_profile_name": "test", "websocket_profile_guid": "9e939b74-5620-46de-ad4b-7df4a90bd3fb"}
	proto	Используемый протокол 4-го уровня	TCP или SSL
	app	Используемый протокол прикладного уровня и его версия	HTTP/1.1
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	requestMethod	Метод HTTP-запроса	GET
	request	URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.w.com

Тип поля	Название поля	Описание	Пример значения
	requestContext	URL-адрес источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	cs1Label	Поле используется для указания срабатывания правила reverse-прокси	Rule
	cs1	Название правила reverse-прокси, срабатывание которого вызвало событие	Test rule
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Management
	cs3Label	Поле используется для указания страны источника	Source Country
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Management
	cs5Label	Поле используется для указания страны назначения	Destination Country
	cs5	Название страны назначения	RU (отображается двухбуквенный код страны)
	flexString1Label	Поле используется для указания типа контента	Media type

Тип поля	Название поля	Описание	Пример значения
	flexString1	Тип контента	application/json
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник	1
	cn3Label	Поле используется для указания кода HTTP-ответа	Response
	cn3	Код HTTP-ответа	101

Формат журнала WebSocket **CEF Compact**

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	websocket
	Origin	Источник события	log
	Severity	Уровень опасности	Не используется. Поле передается с пустыми данными
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1759728622455

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@havntohanmin
	act	Действие, предпринятое модулем анализа websocket-трафика на устройстве	pass или deny
	reason	Информация о причине возникновения события	{"request":"GET /ws HTTP/1.1\r\nConnection: upgrade\r\nUpgrade: websocket\r\nContent-Length: 0\r\nsec-websocket-version: 13\r\nsec-websocket-key: +V9uPwL0ZfDTjmwMvnVUZA==\r\nHost: w.com \r\n\r\n","response":"HTTP/1.1 101 Switching Protocols\r\naccess-control-allow-origin: *\r\nX-Request-ID: d8814097-a68c-4120-8912-23a11b8e88da\r\nConnection: Upgrade\r\nDate: Mon, 06 Oct 2025 05:35:52 GMT\r\nsec-websocket-accept: mn0nG2s62J2pY5E8sleD2gnGRQ=\r\nServer: Cowboy\r\nUpgrade: websocket\r\nx-test-srv: pft-serve\r\n\r\n\r\n","websocket_profile_name":"test","websocket_profile_guid":"9e939b74-5620-46de-ad4b-7df4a90bd3fb"}
	proto	Используемый протокол 4-го уровня	TCP или SSL
	app	Используемый протокол прикладного уровня и его версия	HTTP/1.1
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	requestMethod	Метод HTTP-запроса	GET
	request	URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.w.com
	requestContext	URL-адрес источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0

Тип поля	Название поля	Описание	Пример значения
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	cs1Label	Поле используется для указания срабатывания правила reverse-прокси	Rule
	cs1	Название правила reverse-прокси, срабатывание которого вызвало событие	Test rule
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Management
	cs3Label	Поле используется для указания страны источника	Source Country
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7

Тип поля	Название поля	Описание	Пример значения
	Source	Тип журнала	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие	firewall
	Threat Level	Уровень угрозы приложения	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	accept
	proto	Используемый протокол 4-го уровня	TCP или UDP
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	smac	MAC-адрес источника	00:50:56:80:28:08
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	dmac	MAC-адрес назначения	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT)	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT)	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила	Rule

Тип поля	Название поля	Описание	Пример значения
	cs1	Название правила, срабатывание которого вызвало событие	Allow trusted to untrusted
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Trusted
	cs3Label	Поле используется для указания страны источника	Source Country
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Untrusted
	cs5Label	Поле используется для указания страны назначения	Destination Country
	cs5	Название страны назначения	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник	1

Формат журнала трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие	firewall

Тип поля	Название поля	Описание	Пример значения
	Threat Level	Уровень угрозы приложения	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	accept
	proto	Используемый протокол 4-го уровня	TCP или UDP
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	smac	MAC-адрес источника	00:50:56:80:28:08
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	dmac	MAC-адрес назначения	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT)	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT)	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Allow trusted to untrusted

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для индикации зоны источника	SrcZone
	cs2	Название зоны источника	Trusted
	cs3Label	Поле используется для индикации зоны назначения	DstZone
	cs3	Название зоны назначения	Untrusted

Формат журнала атак

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Название журнала	waf
	Name	Тип источника	log
	Threat Level	Уровень угрозы категории URL	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); принимает значение Unknown, если категория не определена
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	deny
	proto	Используемый протокол 4-го уровня	TCP.
	app	Протокол прикладного уровня и его версия	HTTP/1.1
	suser	Имя пользователя	Unknown
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	dst	IPv4-адрес назначения трафика	194.226.127.130

Тип поля	Название поля	Описание	Пример значения
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т. п.)	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Default Allow
	cs2Label	Поле используется для указания идентификатора правила	Rule Id
	cs2	Идентификатор правила	200016017
	cs3Label	Поле используется для указания зоны источника	Source Zone
	cs3	Название зоны источника	Trusted
	cs4Label	Поле используется для указания страны источника	Source Country
	cs4	Название страны источника	RU (отображается двухбуквенный код страны)
	cs5Label	Поле используется для указания зоны назначения	Destination Zone
	cs5	Название зоны назначения	Untrusted
	cs6Label	Поле используется для указания страны назначения	Destination Country
	cs6	Название страны назначения	RU (отображается двухбуквенный код страны)
	cs7Label	Поле используется для указания профиля ответа	Response Profile

Тип поля	Название поля	Описание	Пример значения
	cs7	Название профиля ответа	Unknown
	cs8Label	Поле используется для указания названия исключения	Exception Name
	cs8	Название исключения	exampleExceptionName
	cs9Label	Поле используется для указания идентификатора исключения	Exception Id
	cs9	Идентификатор исключения	522d6f5b-af87-4473-91e3-780d8874056d
	cs10Label	Поле используется для указания названия пакета экспертизы	Package Name
	cs10	Название пакета экспертизы	Owasp top 10
	cs11Label	Поле используется для указания версии пакета экспертизы	Package Version
	cs11	Версия пакета экспертизы	395
	cs12Label	Поле используется для указания идентификатора WAF-профиля	WAF Profile Id
	cs12	Идентификатор WAF-профиля	234f96b4-c011-4b6d-96ae-260b2a82895c
	cs13Label	Поле используется для указания реального IP-адреса источника	Real Ip
	cs13	Реальный IP-адрес источника	172.25.0.1
	cs14Label	Поле используется для указания названия страны реального IP-адреса источника	Real Country
	cs14	Название страны реального IP-адреса источника	RU (отображается двухбуквенный код стран)
	flexString1Label	Поле используется для указания типа контента	Media type
	flexString1	Тип контента	text/html
	flexString2Label	Поле используется для указания категории запрашиваемого URL-адреса	URL Categories
	flexString2	Категория URL	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3

Тип поля	Название поля	Описание	Пример значения
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник	1
	cn3Label	Поле используется для указания исходного ответа сервера	Response
	cn3	Код ответа HTTP	302
	cn4Label	Поле используется для указания уровня угрозы	Threat Level
	cn4	Уровень угрозы	1
	cn5Label	Поле используется для указания времени обновления пакета	Package Update Time
	cn5	Время обновления пакета экспертизы в миллисекундах с 1 января 1970 года	1773237844774955

Формат журнала атак CEF Compact

Тип поля	Название поля	Описание	Пример значения
CEF-заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	waf
	Name	Тип источника	log
	Threat Level	Уровень угрозы категории URL	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); принимает значение Unknown, если категория не определена
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	deny
	proto	Используемый протокол 4-го уровня	TCP.

Тип поля	Название поля	Описание	Пример значения
	app	Протокол прикладного уровня и его версия	HTTP/1.1
	suser	Имя пользователя	Unknown
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т. п.)	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Default Allow
	cs2Label	Поле используется для указания идентификатора правила	Rule Id
	cs2	Идентификатор правила	200016017
	cs3Label	Поле используется для указания зоны источника	Source Zone
	cs3	Название зоны источника	Trusted
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Untrusted
	cs5Label	Поле используется для указания профиля ответа	Response Profile

Тип поля	Название поля	Описание	Пример значения
	cs5	Название профиля ответа	Unknown
	cn1Label	Поле используется для указания исходного ответа сервера	Response
	cn1	Код ответа HTTP	302
	cn2Label	Поле используется для указания уровня угрозы	Threat Level
	cn2	Уровень угрозы	1
	flexString1Label	Поле используется для указания категории запрашиваемого URL-адреса	URLCats
	flexString1	Категория URL	Computers & Technology

Экспорт журналов в формате JSON

Описание журнала событий

Название поля	Описание	Пример значения
timestamp	Время получения события в формате уууу-мм-ддThh:mm:ssZ	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
ip_address	IPv4-адрес источника события	192.168.174.134
attributes	Детали события в формате JSON	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}}
event_type	Тип события	logexport_rule_updated
event_severity	Важность события	info (информационные), warning (предупреждения), error (ошибки), critical (критичные)
event_origin	Модуль, в котором произошло событие	core
event_component	Компонент, в котором произошло событие	console_auth

Описание журнала веб-доступа

Название поля	Описание	Пример значения
timestamp	Время получения события в формате уууу-мм-ддThh:mm:ssZ	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)

Название поля		Описание	Пример значения
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
reasons		Причина, по которой было создано событие, например причина блокировки сайта.	"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]
proto		Используемый протокол 4-го уровня	TCP
host		Имя хоста	www.google.com
action		Действие, принятое устройством в соответствии с настроенными политиками	block
bytes_sent		Количество байтов, переданных в направлении источник — назначение	52
bytes_rcv		Количество пакетов, переданных в направлении назначение — источник	100
packets_sent		Количество пакетов, переданных в направлении источник — назначение	2
packets_rcv		Количество байтов, переданных в направлении назначение — источник	5
request_method		Метод, используемый для доступа к URL-адресу (POST, GET и т.п.)	GET
url		Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com
media_type		Тип контента	application/json
status_code		Код ответа HTTP	302
http_referer		URL источника запроса (реферер HTTP)	https://www.google.com/
decrypted		Поле указывает, было ли содержимое расшифровано	true, false
useragent		Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
request_id		Идентификатор запроса	12e4d951-a4a6-4338-a5bb-81a7f4130d93
application	id	Идентификатор приложения	20
	name	Название приложения	Youtube
	threat_level	Уровень угрозы приложения	0
	app_protocol	Протокол прикладного уровня и его версия	HTTPV1.1"
url_categories	id	Идентификатор категории, к которой относится URL	39

Название поля		Описание	Пример значения
	threat_level	Уровень угрозы категории URL	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий
	name	Название категории, к которой относится URL	Social Networking
source	zone	guid	d0038912-0d8a-4583-a525-e63950b1da47
		name	Trusted
	country	Страна источника трафика	RU (отображается двухбуквенный код страны)
	ip	IPv4-адрес источника	10.10.10.10
	port	Порт источника	Может принимать значения от 0 до 65535
	mac	MAC-адрес источника	01:23:45:67:89:AB
real_ip	country	Название страны реального IP-адреса источника	RU (отображается двухбуквенный код страны)
	ip	Реальный IP-адрес источника	172.25.0.1
destination	zone	guid	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Untrusted
	country	Страна назначения	RU (отображается двухбуквенный код страны)
	ip	IPv4-адрес назначения	192.168.174.134
	port	Порт назначения	Может принимать значения от 0 до 65535
	mac	MAC-адрес назначения	01:23:45:67:89:AB
rule	guid	Уникальный идентификатор правила, срабатывание которого вызвало создание события	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name	Название правила	Default allow
	type	Тип сработавшего правила	
user		Имя пользователя	null

Описание журнала WebSocket (версия 7.4.1 и выше)

--

Название поля	Описание	Пример значения
timestamp	Время получения события в формате yyyy-mm-ddThh:mm:ssZ	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии	00000006-0a00-010c-c404-ac196d411f90
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@havntohanmin
reasons	Информация о причине возникновения события	{ "request": "GET /ws HTTP/1.1\r\nConnection: upgrade\r\nUpgrade: websocket\r\nContent-Length: 0\r\nsec-websocket-version: 13\r\nsec-websocket-key: +V9uPwL0ZfDTjmwMvnVUZA==\r\nHost: w.com\r\n\r\n", "response": "HTTP/1.1 101 Switching Protocols\r\naccess-control-allow-origin: *\r\nX-Request-ID: d8814097-a68c-4120-8912-23a11b8e88da\r\nConnection: Upgrade\r\nDate: Mon, 06 Oct 2025 05:35:52 GMT\r\nsec-websocket-accept: mn0nG2s62J2pY5E8ssleD2gnGRQ=\r\nServer: Cowboy\r\nUpgrade: websocket\r\nx-test-srv: pft-serve\r\n\r\n", "websocket_profile_name": "test", "websocket_profile_guid": "9e939b74-5620-46de-ad4b-7df4a90bd3fb" }
proto	Используемый протокол 4-го уровня	TCP или SSL
host	Имя хоста	w.com
action	Действие, предпринятое модулем анализа websocket-трафика на устройстве	pass или deny
bytes_sent	Количество байтов, переданных в направлении источник — назначение	100
bytes_recv	Количество байтов, переданных в направлении назначение — источник	6
packets_recv	Количество пакетов, переданных в направлении назначение — источник	1
packets_sent	Количество пакетов, переданных в направлении источник — назначение	1
request_method	Метод HTTP-запроса	GET
url	URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.w.com
media_type	Тип контента	application/json
status_code	Код HTTP-ответа	101
http_referer	URL-адрес источника запроса (реферер HTTP)	https://www.google.com/
decrypted	Поле указывает, было ли содержимое расшифровано	true, false
useragent	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0

Название поля			Описание	Пример значения
request_id			Идентификатор запроса	
application	id		Идентификатор приложения	Не используется. Поле передается с пустыми данными
	name		Название приложения	Не используется. Поле передается с пустыми данными
	threat_level		Уровень угрозы приложения	Не используется. Поле передается с пустыми данными
	app_protocol		Протокол прикладного уровня	HTTP/1.1
source	zone	guid	Уникальный идентификатор зоны источника трафика	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика	Management
	country		Название страны источника	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика	10.10.10.10
	port		Порт источника	Может принимать значения от 0 до 65535
	mac		MAC-адрес источника	Может отсутствовать
real_ip	country		Название страны реального IP-адреса источника	RU (отображается двухбуквенный код страны)
	ip		Реальный IP-адрес источника	172.25.0.1
destination	zone	guid	Уникальный идентификатор зоны назначения трафика	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика	Management
	country		Название страны назначения	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535
	mac		MAC-адрес назначения	Может отсутствовать
rule	guid		Уникальный идентификатор правила reverse-прокси, срабатывание которого создало событие	59e38e06-533a-4771-9664-031c3e8b2e1f

Название поля	Тип правила	Описание	Не используется.
			Пример значения
			Поле передается с пустыми данными
	name	Название правила reverse-прокси, срабатывание которого вызвало событие	test rule

Описание журнала трафика

Название поля		Описание	Пример значения
timestamp		Время получения события в формате уууу-мм-ддThh:mm:ssZ	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
proto		Используемый протокол 4-го уровня	TCP или UDP
action		Действие, принятое устройством в соответствии с настроенными политиками	accept
bytes_sent		Количество байтов, переданных в направлении источник — назначение	100
bytes_recv		Количество байтов, переданных в направлении назначение — источник	6
packets_recv		Количество пакетов, переданных в направлении назначение — источник	1
packets_sent		Количество пакетов, переданных в направлении источник — назначение	1
json_data		Дополнительные данные	null
application	id	Идентификатор приложения	195
	threat_level	Уровень угрозы приложения	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий
	app_protocol	Протокол прикладного уровня	HTTP
	name	Название приложения	Youtube

Название поля			Описание	Пример значения
source	zone	guid	Уникальный идентификатор зоны источника трафика	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика	Trusted
	country		Название страны источника	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика	10.10.10.10
	port		Порт источника	Может принимать значения от 0 до 65535
destination	zone	guid	Уникальный идентификатор зоны назначения трафика	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика	Untrusted
	country		Название страны назначения	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535
nat	source	ip	Адрес источника после переназначения (если настроены правила NAT)	192.168.117.85 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
	destination	ip	Адрес назначения после переназначения (если настроены правила NAT)	64.233.164.198 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила	firewall
	name		Название правила, срабатывание которого вызвало событие	Allow trusted to untrusted

Описание журнала атак

Название поля		Описание	Пример значения
timestamp		Время получения события в формате уууу-мм-ддThh:mm:ssZ	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica

Название поля	Описание	Пример значения
proto	Используемый протокол 4-го уровня	TCP
host	Имя хоста	www.google.com
action	Действие, принятое устройством в соответствии с настроенными политиками	block
rule_id	Идентификатор правила	200016017
waf_profile_name	Название WAF-профиля	wafProfileName
waf_profile_id	Идентификатор WAF-профиля	522d6f5b-af87-4473-91e3-780d8874056d
waf_layer_name	Название WAF-слоя	Detection Evasion
response_profile_name	Название профиля ответа	Unknown
threat_level	Уровень угрозы атаки	Может принимать значения: • 0 — нулевой; • 1 — низкий; • 2 — средний; • 3 — высокий
package_name	Название пакета экспертизы	Owasp top 10
package_version	Версия пакета экспертизы	340
package_update_time	Время обновления пакета экспертизы: миллисекунды с 1 января 1970 года	1773237844774955
exception_name	Название исключения	name
exception_id	Идентификатор исключения	b4ce2bfa-b090-4318-a4b2-676c5ff62051
bytes_sent	Количество байтов, переданных в направлении источник — назначение	52
bytes_recv	Количество пакетов, переданных в направлении назначение — источник	100
packets_sent	Количество пакетов, переданных в направлении источник — назначение	2
packets_recv	Количество байтов, переданных в направлении назначение — источник	5
request_method	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.)	GET
url	Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com

Название поля		Описание	Пример значения
media_type		Тип контента	application/json
status_code		Код ответа HTTP	302
http_referer		URL источника запроса (реферер HTTP)	https://www.google.com/
useragent		Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
request_id		Идентификатор запроса	931d66e1-7d3a-4870-9791-b05b5eb6c01a
application	id	Идентификатор приложения	20
	name	Название приложения	Youtube
	threat_level	Уровень угрозы приложения	0
	app_protocol	Протокол прикладного уровня и его версия	HTTPV1.1"
source	zone	guid	Уникальный идентификатор зоны источника трафика
		name	Название зоны источника
	country		Страна источника трафика
	ip		IPv4-адрес источника
	port		Порт источника
	mac		MAC-адрес источника
real_ip	country		Название страны реального IP-адреса источника
	ip		Реальный IP-адрес источника
destination	zone	guid	Уникальный идентификатор зоны назначения трафика
		name	Название зоны назначения трафика
	country		Страна назначения
	ip		IPv4-адрес назначения
	port		Порт назначения
	mac		MAC-адрес назначения
rule	guid		Уникальный идентификатор правила, срабатывание которого вызвало создание события

Название поля		Описание	Пример значения
	name	Название правила	Default allow
	type	Тип сработавшего правила	
user		Имя пользователя	null
url_categories	id	Идентификатор категории, к которой относится URL	39
		Уровень угрозы категории URL	Может принимать значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий
	name	Название категории, к которой относится URL	Social Networking

