

Table of Contents

Table of Contents	1
Политики сети	2
Межсетевой экран	3
Балансировка нагрузки	5

Межсетевой экран

Product: WAF
Version: 7.x
Technology: Firewall

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate WAF. В качестве условий правила могут выступать зоны и IP-адреса источника/назначения.

События срабатывания правил межсетевого экрана отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила, то любой транзитный трафик через WAF запрещен.

Чтобы создать правило межсетевого экрана, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Межсетевой экран** и указать необходимые параметры.

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Запретить : блокирует трафик. Разрешить : разрешает трафик.
Отбросить и	Настройка данного параметра доступна для правил, блокирующих трафик (выбрано действие Запретить). Параметр может принимать одно из следующих значений: • Не выбран. • Посылать ICMP host unreachable: блокировка трафика с отправкой ICMP-сообщения. • Посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указание сервиса (вкладка Сервис), использующего протокол TCP. • Посылать TCP reset в обе стороны: блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • Нет. В этом случае информация не будет записываться.
Применить правило к	Применимость правила: • Все пакеты. • Только фрагментированные пакеты. • Только нефрагментированные пакеты.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки имен доменов источника трафика. Важно! Строки с символом "*" в списках имен доменов не работают (игнорируются). Каждые 5 минут WAF производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни WAF автоматически обновляет значение IP-адреса. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки имен доменов назначения трафика. Важно! Строки с символом "*" в списках имен доменов не работают (игнорируются). Каждые 5 минут WAF производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни WAF автоматически обновляет значение IP-адреса. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Время	Интервалы времени, когда правило активно.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Балансировка нагрузки

Product: WAF
Version: 7.x

WAF позволяет осуществлять балансировку нагрузки на серверы, публикуемые через reverse-прокси.

Балансировщик распределяет запросы, поступающие на IP-адрес виртуального сервера, на IP-адреса реальных серверов. Чтобы настроить балансировку, необходимо в разделе **Политики сети → Балансировка нагрузки** создать правила балансировки.

Балансировщик серверов reverse-прокси позволяет распределить нагрузку на внутренние серверы или ферму серверов, публикуемую с помощью правил reverse-прокси. Данный балансировщик затем может быть использован в правилах reverse-прокси. Для создания балансировщика reverse-прокси необходимо в разделе **Политики сети → Балансировка нагрузки** нажать кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
Серверы reverse-прокси	Выбрать reverse-прокси серверы, на которые будет распределяться нагрузка. Более подробно о публикации с помощью reverse-прокси читайте в разделе Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси .

