

Table of Contents

Table of Contents	1
Политики сети	2
Общие сведения	3
Межсетевой экран	4
NAT и маршрутизация	7
Балансировка нагрузки	14
Пропускная способность	16

Product: DCFW

Version: 8.x

Раздел **Настройки → Политики сети** содержит параметры ключевых механизмов управления трафиком UserGate NGFW.

В этом разделе вы можете:

- Управлять прохождением трафика с помощью [правил межсетевого экрана](#). При настройке условий фильтрации могут использоваться зоны, адреса источника и назначения, пользователи и группы пользователей, а также сервисы.
- Выполнять трансляцию IP-адресов и портов сетевых пакетов с помощью [правил NAT и маршрутизации](#) для решения задач защиты внутренней сети, публикации внутренних ресурсов в интернете и объединения сетей.
- Распределять входящий трафик между публикуемыми ресурсами с помощью [правил балансировки нагрузки](#).
- Контролировать использование пропускной способности пользователями, узлами, сервисами и приложениями с помощью [правил управления пропускной способностью](#).

Информация о срабатывании правил регистрируется в журнале трафика (**Журналы и отчеты → Журнал трафика**) при включенном журналировании в свойствах правил.

Межсетевой экран

Product: DCFW
Version: 8.x
Technology: Firewall

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

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. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете менять порядок правил в списке, перетаскивая их мышью или используя кнопки «Выше», «Ниже», «Наверх» и «Вниз» на панели инструментов.

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

ПримечаниеЕсли не создано ни одного правила, любой транзитный трафик через UserGate DCFW запрещен.

В параметрах разрешающих правил межсетевого экрана могут быть добавлены [профили COB](#) и/или [профили приложений](#) (L7), содержащие определенные наборы сигнатур. После того, как трафик попадает в первое разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей COB и/или L7. При срабатывании сигнатур к трафику применяется действие, настроенное в правиле, и производится соответствующая запись в журналах (в **Журнале трафика** - для приложений и в **Журнале COB** - для COB), если в профилях была включена опция **Журналирование**.

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

Чтобы создать правило межсетевого экрана:

Перейдите в раздел **Настройки → Политики сети → Межсетевой экран**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Описание	Произвольное описание правила
Действие	Действие правила: - Запретить — блокировать трафик; - Разрешить — разрешить трафик
Профиль приложений	Профиль приложений, созданный заранее в разделе Настройки → Библиотеки → Профили приложений . Профиль приложений включает в себя набор сигнатур приложений, предназначенный для использования в правилах межсетевого экрана для анализа трафика на 7 уровне модели OSI. Подробнее о создании и настройке профилей приложений — в разделе « Профили приложений » Важно! Профиль приложений является дополнительным параметром для активации механизма анализа трафика на 7 уровне модели OSI. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.
Профиль COB	Профиль COB, созданный заранее в разделе Настройки → Библиотеки → Профили COB . Профиль COB включает в себя набор сигнатур, предназначенный для обнаружения вторжений и защиты определенных сервисов. Подробнее о создании и настройке профилей COB — в разделе « Профили COB » Важно! Профиль COB является дополнительным параметром для активации правила COB. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.

Параметр	Описание
Отбросить и	Параметр доступен 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 указать сервис (вкладка «Сервис»), использующий протокол TCP. • Посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Журналировать каждый пакет — в журнал трафика будет записываться информация о каждом передаваемом сетевом пакете. Для этого режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • Нет — в этом случае информация не будет записываться
Применить правило к	Указать, к каким пакетам будет применяться правило: • Все пакеты. • Только фрагментированные пакеты. • Только нефрагментированные пакеты
Вставить	Указать расположение правила в списке
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. 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
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. 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

Параметр	Описание
Сервис	Тип сервиса, например, HTTP или HTTPS. ПримечаниеЕсли в одном правиле межсетевого экрана одновременно указаны сервис с шаблоном Any (например, Any TCP) и сервисы с детализированными портами (например, TCP src 22), при обработке трафика будут учитываться только детализированные сервисы. Остальные порты, охватываемые сервисом Any, в рамках этого правила не обрабатываются.
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.

Product: DCFW
Version: 8.x

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, DNAT, Порт-форвардинга, Policy-based routing и Network mapping. UserGate DCFW поддерживает NAT/DNAT для сложных протоколов, которые могут использовать динамические порты для своей работы. Поддерживаются протоколы FTP, PPTP, SIP, H323.

События срабатывания правил NAT, DNAT, порт-форвардинга, Policy-based routing и Network mapping отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

ПримечаниеGeoIP не может использоваться в качестве адреса источника трафика в правилах NAT и в качестве адреса назначения трафика в правилах NAT, DNAT и порт-форвардинг.

Правила NAT

Как правило, для предоставления пользователям доступа в интернет необходимо создать хотя бы одно правило NAT из зоны **Trusted** в зону **Untrusted**.

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).

Чтобы создать правило NAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать NAT .
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, то система будет использовать произвольный адрес из списка доступных IP-адресов, назначенных интерфейсам зоны назначения. Допускается указание диапазона IP-адресов, например: 192.168.10.10-192.168.10.20 В этом случае DCFW будет использовать все указанные адреса при Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана.
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. Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. Важно! Флажок Инвертировать не влияет на работу при использовании MAC-адресов. Важно! Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.

Параметр	Описание
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW 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.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. 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.

ПримечаниеПравило NAT без указанной зоны источника обрабатывает весь трафик, включая локальный (исходящий от самого устройства). Попадание трафика служебных протоколов (в частности, VRRP) под действие NAT может привести к сбоям в работе кластера отказоустойчивости. Рекомендуется явно указывать зону источника в правилах NAT, чтобы исключить обработку локального трафика.

ПримечаниеРекомендуется создавать общие правила NAT, например, правило NAT из локальной сети (обычно зона Trusted) в интернет (обычно зона Untrusted), а разграничение доступа по пользователям, сервисам, приложениям осуществлять с помощью правил межсетевого экрана.

Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет.

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/Низе, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

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

Чтобы создать правило DNAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать DNAT .
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника. Если SNAT IP не указан, то адрес источника будет заменён на адрес интерфейса DCFW, с которого отправлен пакет. Допускается указание диапазона IP-адресов, например: 192.168.10.10-192.168.10.20 Важно! Для замены адреса источника на указанный адрес необходимо во вкладке DNAT активировать Флажок Включить SNAT.

Параметр	Описание
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. Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. Важно! Флажок Инвертировать не влияет на работу при использовании MAC-адресов. 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	Один из внешних IP-адресов DCFW, доступный из сети интернет, куда адресован трафик внешних клиентов. Важно! Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Сервис	Тип сервиса, который необходимо опубликовать, например, HTTP. Если не указан сервис, то будут опубликованы все сервисы. Важно! Нельзя опубликовать сервисы, которые используют следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет.
Включить SNAT	При включении данной опции DCFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. 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.

Правила порт-форвардинга

Правила порт-форвардинга работают аналогично правилам DNAT за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис. Чтобы создать правило порт-форвардинга, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Примечание Правила 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/Низе, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

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

Параметр	Описание
Включено	Включает или отключает правило.

Параметр	Описание
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать Порт-форвардинг .
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. • Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. Важно! Флажок Инвертировать не влияет на работу при использовании MAC-адресов. 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 URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW 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.
Порт-форвардинг	Переопределения портов публикуемых сервисов: • Оригинальный порт назначения — номер TCP/UDP-порта, на который пользователи шлют запросы. Важно! Нельзя использовать следующие порты, поскольку они используются внутренними сервисами DCFW: 2200, 8001, 4369, 9000-9100. • Новый порт назначения — номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернете.
Включить SNAT	При включении данной опции DCFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. 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.

Policy-based routing

Правила policy-based routing обычно используются для указания определенного маршрута в интернет для определенных хостов и/или сервисов. Например, в организации используются 2 провайдера и необходимо весь HTTP-трафик пересылать через провайдера 1, а весь остальной — через провайдера 2. Для этого необходимо указать в качестве шлюза по умолчанию в интернет-шлюз провайдера 2 и настроить правило policy-based routing для HTTPS-трафика через шлюз провайдера 1.

ПримечаниеПравила PBR не заменяют и не влияют на работу правил NAT. Для трансляции адресов, после правила PBR необходимо поставить соответствующее правило NAT.

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).

Чтобы создать правило policy-based routing, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать Policy-based routing .
Шлюз	Выбор одного из существующих шлюзов. Вы можете добавить шлюз в разделе Сеть → Шлюзы . Важно! Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.
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. • Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. Важно! Флажок Инвертировать не влияет на работу при использовании MAC-адресов. 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.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any , Unknown , Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства .

Параметр	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW 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.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. 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.

Network mapping

Правила Network mapping позволяют подменить адрес сети источника или назначения. Как правило, это необходимо, если имеется несколько сетей с одинаковой адресацией, например, 192.168.1.0/24, и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес хоста без изменений, например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 хост 192.168.1.1 будет изменен на 192.168.2.1.

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.

Чтобы создать правило **Network mapping**, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать Network mapping .
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. • Нет. В этом случае информация не будет записываться.

Параметр	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW автоматически обновляет значение IP-адреса. Важно! Флажок Инвертировать не влияет на работу при использовании MAC-адресов. 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 URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW 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.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Network mapping	Задаются параметры подмены сетей. Направление: • Входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле Новая IP-сеть/маска. • Исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле Новая IP-сеть/маска. • Новая IP-сеть/маска — адрес сети, на которую будет производится замена.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. 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: DCFW
Version: 8.x

DCFW позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена:

UserGate DCFW поддерживает балансировку трафика между различными сервисами. Балансировка может применяться в следующих сценариях:

- для внутренних серверов, опубликованных в интернете с использованием DNAT;
- внутренних серверов без публикации во внешней сети;

Балансировщик принимает запросы, направленные на IP-адрес виртуального сервера, и распределяет их между IP-адресами реальных серверов, применяя различные алгоритмы балансировки.

Для создания правила балансировки TCP/UDP перейдите в раздел **Настройки → Политики сети → Балансировка нагрузки**, нажмите **Добавить**, выберите **Балансировщик TCP/UDP** и укажите необходимые параметры.

Параметр	Описание
Включен	Включение или отключение правила балансировки
Название	Название правила балансировки
Описание	Описание правила балансировки
IP-адрес виртуального сервера	Выбор адреса из списка IP-адресов, назначенных на сетевые интерфейсы узла. При необходимости вы можете добавить дополнительные IP-адреса на желаемый интерфейс
Порт	Порт, для которого необходимо производить балансировку нагрузки
Протокол	Протокол, для которого необходимо производить балансировку нагрузки (TCP или UDP)
Метод балансировки	Выбор метода распределения трафика на реальные серверы: • Round robin — каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • Weighted round robin — работает аналогично методу round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. • Least connections — новое подключение передается на сервер, на котором в данный момент установлено наименьшее число соединений. • Weighted least connections — работает аналогично методу least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера
Реальные серверы	Добавление пула реальных серверов, на которые перенаправляется трафик. Для каждого из серверов необходимо указать: • IP-адрес сервера. • Порт сервера — порт, на который необходимо пересылать запросы пользователей. • Вес — параметр для неравномерного распределения трафика на реальные серверы для режимов балансировки weighted round robin и weighted least connections. Чем больше вес, тем больше будет нагрузка на сервер. • Режим: ◦ Шлюз — для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ Маскарадинг — для перенаправления трафика на виртуальный сервер используется DNAT. ◦ Маскарадинг с подменой IP-источника (SNAT) — аналогично маскарадингу, но при этом UserGate DCFW подменяет IP-адрес источника на свой Важно! Поскольку в режиме «Шлюз» балансировщик не изменяет заголовки пакетов, обратный трафик от реального сервера должен обеспечиваться средствами маршрутизации. То есть шлюз для обратного трафика должен отличаться от адреса UserGate DCFW.

Параметр	Описание
Аварийный режим	Аварийный режим используется, когда не доступен ни один из реальных серверов. Для активации аварийного режима необходимо включить его и указать: • IP-адрес сервера. • Порт сервера. Порт, на который пересылать запросы пользователей. • Режим. Может быть три варианта: ◦ Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ Максарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ Маскарадинг с подменой IP-источника (SNAT) : аналогично маскарадингу, но при этом UserGate DCFW подменяет IP-адрес источника на свой
Мониторинг	Механизм мониторинга выполняет проверку доступности реальных серверов. Недоступные серверы автоматически выводятся из пула балансировки нагрузки
Режим	Способ мониторинга реальных серверов: • ping — проверка доступности узла с помощью утилиты ping. • connect — проверка работоспособности узла с помощью установления TCP-соединения на определенный порт. • negotiate — проверка работоспособности узла с помощью отправки определенного HTTP- или DNS-запроса и сравнения полученного ответа с ожидаемым. Для настройки этого режима выберите тип сервиса (HTTP или DNS), заполните строки Запрос и Ожидаемый ответ. Например, для HTTP-запроса: ◦ Запрос: /robots.txt; ◦ Ожидаемый ответ: Disallow: /bin/. Строка запроса в этом примере указывает путь на реальных серверах, который будет использован в HTTP-запросе. Строка ожидаемого ответа содержит фрагмент возвращаемой веб-страницы
Интервал проверки	Интервал времени, через который должна выполняться проверка
Время ожидания	Время ожидания ответа на проверку
Число неудачных попыток	Количество попыток проверки реальных серверов, по достижении которого сервер будет считаться неработоспособным и будет исключен из списка балансировки

Примечание Правила балансировки имеют более высокий приоритет и применяются до правил NAT, DNAT, Маршрутизации.

Пропускная способность

Product: DCFW
Version: 8.x

Правила управления пропускной способностью используются для ограничения канала для определенных пользователей, хостов, сервисов, приложений.

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.

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

Чтобы создать правило пропускной способности, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Пропускная способность** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритизации трафика DSCP. Создать дополнительные полосы пропускания можно в разделе Полосы пропускания .
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
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.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW 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.
Пользователи	Пользователи или группы пользователей, к которым применится правило.

Параметр	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут DCFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни DCFW 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.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Приложения	Список приложений, для которых необходимо ограничить полосу пропускания.
Время	Время, когда данное правило активно.

