Table of Contents

Table of Contents 1
Политики сети 2
- Общие сведения 3
- Межсетевой экран 4
- NAT и маршрутизация 8
- Балансировка нагрузки 18
- Пропускная способность 21

Политики сети

Общие сведения

Product: SWG
Version: 7.5.x

Раздел «Политики сети» содержит настройки ключевых механизмов управления трафиком UserGate SWG.

В этом разделе вы можете:

- Управлять прохождением трафика с помощью правил межсетевого экрана. В условиях фильтрации в правилах могут быть использованы зоны и адреса источника и назначения, пользователи, группы пользователей, 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.

События срабатывания правил регистрируются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включенной опции журналирования в свойствах правил.

Межсетевой экран

Product: SWG
Version: 7.5.x
Technology: Firewall

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate SWG. 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 «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).
ПримечаниеЕсли не создано ни одного правила, любой транзитный трафик через UserGate SWG запрещен.

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 указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Действие	• **Запретить**: блокирует трафик. • **Разрешить**: разрешает трафик
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

Параметр	Описание
Вставить	Указать расположение правила в списке
Источник	Зона, списки IP-адресов, списки GeoIP-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 UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGate SWG 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 правило. Могут быть использованы пользователи типа Any , Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
Назначение	Зона, списки IP-адресов, списки GeoIP-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 UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса Обработка трафика происходит по следующей логике: • Усслоия 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 или HTTPS
Время	Интервалы времени, когда правило активно
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

ПримечаниеПри изменении условий существующего правила межсетевого экрана изменения для уже установленных UDP-сессий вступят в силу только после разрыва сессии.

Расширенный поиск в разделе **Настройки → Политики сети → Межсетевой экран** доступен по следующим параметрам.

Параметр	Описание
enabled	Поиск включенных или выключенных правил. Может принимать значения: • true — для отображения всех включенных правил. • false — для отображения все выключенных правил
pos	Поиск по позиции правила в списке (1, 2 и т. д.)

Параметр	Описание
log	Поиск правила по включенной или выключенной функции журналирования. Возможны следующие значения: • true или enabled — отображение правил, в которых включена функция журналирования (журналировать начало сессии или журналировать все сетевые пакеты). • false или disabled — отображение правил, в которых журналирование отключено. • all — отображение правил, в которых настроено журналирование всех сетевых пакетов. • start — отображение правил, в которых настроено журналирование начала сессии
name	Поиск правил по названию
action	Поиск правил по действию, настроенному в правилах межсетевого экрана: • Разрешить (allow) — разрешает трафик. • Запретить (deny) — блокирует трафик
zoneSource	Поиск правил по зоне источника трафика
ipSource	Поиск правил по IP-адресу источника трафика. Адрес должен входить в список IP-адресов, созданный в разделе **Настройки → Библиотеки → IP-адреса** или в свойствах правила
ipSourceName	Поиск правил по названию IP-листа источника трафика
countrySource	Поиск правил по названию страны источника трафика. Страна источника может быть добавлена в свойствах правила на вкладке **Источник** (**Добавить GeoIP**)
portSource	Поиск правил по порту источника трафика. Порты, которые используются сервисами, можно настроить в разделе **Настройки → Библиотеки → Сервисы**
zoneDest	Поиск правил по зоне назначения трафика
ipDest	Поиск правил межсетевого экрана по IP-адресу назначения. Адрес должен входить в список IP-адресов, созданный в разделе **Настройки → Библиотеки → IP-адреса** или в свойствах правила
ipDestName	Поиск правил по названию IP-листа назначения трафика
countryDest	Поиск правил по названию страны назначения трафика. Страна назначения может быть добавлена в свойствах правила на вкладке **Назначение** (**Добавить GeoIP**)
portDest	Поиск правил по порту назначения трафика. Порты, которые используются сервисами, можно настроить в разделе **Настройки → Библиотеки → Сервисы**
user	Поиск правил по пользователям, для которых они применяются. Правило может быть применено для следующих типов пользователей: • Пользователь Unknown — пользователи, не идентифицированные системой. • Пользователь Known — пользователи, идентифицированные системой с помощью серверов авторизации. • Пользователь Any — любой пользователь (Known или Unknown). • Определённый пользователь — конкретный пользователь, идентифицированный в системе. Пользователи могут быть заведены локально (локальные пользователи) или получены с внешних каталогов (например, Microsoft Active Directory). При поиске, требующем полного совпадения (операторы = или !=) логина пользователя, также будет производиться поиск по группам пользователей
userId	Поиск правил по ID пользователя; также будут отображены правила, в которых указаны группы пользователя
group	Поиск по группам пользователей, для которых применено правило межсетевого экрана. Группы пользователей могут быть заведены локально или получены с внешних каталогов (например, Microsoft Active Directory)

Параметр	Описание
groupId	Поиск правила по идентификатору группы пользователей
service	Поиск правила по указанному типу сервиса
active	Поиск активных или не активных в текущий момент времени правил (во время выполнения поискового запроса): • true — отображение правил, для которых текущее время попадает в заданные интервалы активности. • false — отображение правил, для которых текущее время не попадает в заданные интервалы активности. Время работы правила может быть задано в свойствах на вкладке **Время**. Для этого используются календари, созданные в разделе **Настройки → Библиотеки → Календари** или в свойствах правила
description	Поиск правил по описанию правила

ПримечаниеПоисковый запрос не распространятся на правило Default block. Т. е., даже если поиск правил происходит по запросу action = allow, правило Default block, настроенное на блокировку трафика, будет отражено в конце списка.

Product: SWG
Version: 7.5.x

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, NoNAT, DNAT, NoDNAT, трансляции портов, PBR и Network mapping. UserGate SWG поддерживает NAT/DNAT для сложных протоколов, которые могут использовать динамические порты для своей работы. Поддерживаются протоколы FTP, PPTP, SIP, H323.

События срабатывания правил отображаются в журнале трафика (**Журналы и отчеты → Журнал трафика**), если в правиле включена опция журналирования.

ПримечаниеGeoIP не может использоваться в качестве адреса источника трафика в правилах NAT и в качестве адреса назначения трафика в правилах NAT, DNAT и трансляции портов.
ПримечаниеПри изменении условий существующего правила NAT изменения для уже установленных UDP-сессий вступят в силу только после разрыва сессии.

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

Чтобы создать правило NAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **NAT**
SNAT IP (внешний адрес)	Явное указание IP-адреса, на который будет заменен адрес источника. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, система будет использовать первый 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 UserGate SWG будет использовать все указанные адреса для Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана
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. • **Нет** — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке

Параметр	Описание
Источник	Зона, списки IP-адресов, списки URL источника трафика, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any**,** Unknown**,** Known. Для применения правил к конкретным пользователям или к пользователям типа Known настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. 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 правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

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 NoNAT

Правила NoNAT используются, когда из работающих в системе правил NAT необходимо исключить отдельные адреса узлов или подсетей без переписывания всей настроенной политики. Трафик, фильтруемый правилом NoNAT, будет проходить через систему без трансляции адресов.

Чтобы создать правило NoNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»

Параметр	Описание
Описание	Описание правила
Тип	Тип правила. Выберите **NoNAT**
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. • **Нет** — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке
Источник	Зона, списки IP-адресов, списки URL, MAC-адреса источника трафика. Списки URL должны включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов 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». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов 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 счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу.

Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет. Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси. Подробнее о публикации ресурсов с помощью правил reverse-прокси — в разделе «Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси». Для публикации серверов, работающих по протоколам, отличным от HTTP/HTTPS, необходимо использовать публикацию DNAT.

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

Чтобы создать правило DNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **DNAT**
SNAT IP (внешний адрес)	Явное указание IP-адреса, на который будет заменен адрес источника. Если SNAT IP не указан, то адрес источника будет заменен на адрес интерфейса UserGate SWG, 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 на вкладке «DNAT» активировать Флажок «Включить SNAT»
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. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP-адреса, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. 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». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов (внешние IP-адресов UserGate SWG, доступные из сети интернет, на которые адресован трафик внешних клиентов), списки URL назначения трафика. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов

Параметр	Описание
Сервис	Тип сервиса, который необходимо опубликовать. Если не указан сервис, будут опубликованы все сервисы **Важно!** Следующие порты не могут быть использованы для публикации сервисов, поскольку они уже используются внутренними службами UserGate SWG: 2200, 8001, 4369, 9000-9100.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет
Включить SNAT	При включении данной опции UserGate SWG 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 счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

ПримечаниеПри использовании нескольких правил DNAT с SNAT, отличающихся только условиями адреса назначения, действие SNAT будет выполняться только по первому правилу DNAT. Это обусловлено тем, что пакет, попавший под любое из этих правил, после изменения IP-адреса назначения не будет отличаться на сетевом и транспортном уровне модели OSI. При одинаковых DNAT IP необходимо в правилах DNAT иметь уникальные условия в зонах, сервисах, адресах источника.
ПримечаниеТрафик DNAT/трансляции портов не обрабатывается правилами межсетевого экрана, созданными по умолчанию (Default block).

Правила NoDNAT

Правила NoDNAT используются, когда из работающих в системе правил DNAT необходимо исключить отдельные адреса узлов или подсетей без переписывания всей настроенной политики. Трафик, фильтруемый правилом NoDNAT, будет проходить через систему без трансляции адресов.

Чтобы создать правило NoDNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **NoDNAT**
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. • **Нет** — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке

Параметр	Описание
Источник	Зона, списки IP-адресов, списки URL, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. 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». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов (внешние IP-адресов UserGate SWG, доступные из сети интернет, на которые адресован трафик внешних клиентов), списки URL назначения трафика. 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. Если не указан сервис, будут опубликованы все сервисы **Важно!** Следующие порты не могут быть использованы для публикации сервисов, поскольку они уже используются внутренними службами UserGate SWG: 2200, 8001, 4369, 9000-9100.
Использование	Статистика срабатывания о правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Правила трансляции портов

Правила трансляции портов (port forwarding) работают аналогично правилам DNAT, за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис.

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

Чтобы создать правило трансляции портов, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила

Параметр	Описание
Тип	Тип правила. Выберите **Порт-форвардинг**
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. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пят минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. 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 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». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Порт-форвардинг	Трансляция портов публикуемых сервисов: • **Оригинальный порт назначения** — номер TCP- или UDP-порта, на который приходят запросы; следующие порты не могут быть использованы для переназначения, поскольку они уже используются внутренними службами UserGate SWG: 2200, 8001, 4369, 9000-9100; • **Новый порт назначения** — номер TCP- или UDP-порта, на который будут пересылаться запросы на внутренний публикуемый сервер
Адрес назначения DNAT	IP-адрес узла в локальной сети, который публикуется в интернет
Включить SNAT	При включении этой опции UserGate SWG будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**

Параметр	Описание
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

ПримечаниеТрафик DNAT/трансляции портов не обрабатывается правилами межсетевого экрана, созданными по умолчанию (Default block).

Правила маршрутизации на основе политик

Правила маршрутизации на основе политик (policy-based routing, PBR) используются для указания определенного маршрута в интернет для выбранных узлов или сервисов. Например, в организации используются два 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 интернет-шлюз провайдера 2 и настроить правило PBR 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. 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 «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило PBR, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **Policy-based routing**
Шлюз	Выбор одного из существующих шлюзов. Шлюз может быть добавлен в разделе **Сеть → Шлюзы** **Важно!** Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
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. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. 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
Пользователи	Список пользователей или групп, для которых применяется 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». Позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика, GeoIP. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG 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
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Правила трансляции адресов сетей

Правила трансляции адресов сетей (network mapping) позволяют подменить адрес сети источника или назначения. Как правило, это необходимо, если имеется несколько сетей с одинаковой адресацией и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес узла без изменений. Например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 узел 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, в котором совпали 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.

Чтобы создать правило **Network mapping**, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **Network mapping**

Параметр	Описание
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. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. 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 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». Позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика, GeoIP. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG 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
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Network mapping	Указание параметров подмены сетей. • **Новая IP-сеть/маска** — адрес сети, на которую будет производится замена. • **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**
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Product: SWG
Version: 7.5.x

UserGate SWG 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;
- трафика, перенаправляемого на внешние ICAP-серверы;
- трафика к серверам, публикуемым через правила reverse-proxy.

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

Чтобы настроить балансировку, необходимо в разделе **Настройки → Политики сети → Балансировка нагрузки** создать правила балансировки.

Балансировщик TCP/UDP

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

Параметр	Описание
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 SWG 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 SWG.
Аварийный режим	Аварийный режим используется, когда не доступен ни один из реальных серверов. Для активации аварийного режима необходимо его включить и указать следующие параметры: • **IP-адрес** сервера. • **Порт** сервера — порт, на который необходимо пересылать запросы пользователей. • **Режим**: ◦ **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 SWG 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

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

Балансировщик ICAP

Балансировщик ICAP распределяет трафик между внешними ICAP-серверами. Такое решение может применяться для антивирусного сканирования или глубокого анализа пользовательских данных с использованием DLP-систем.

Алгоритм балансировки распределяет HTTP-трафик между серверами с учетом пользовательских сессий.

Для создания балансировщика ICAP перейдите в раздел **Настройки → Политики сети → Балансировка нагрузки** , нажмите **Добавить**, выберите **Балансировщик ICAP** и укажите необходимые параметры балансировщика.

Параметр	Описание
Включено	Включение или отключение правила балансировки
Название	Название правила балансировки
Описание	Описание правила балансировки
Способ балансировки	Настройка балансировки трафика с поддержкой закрепления HTTP-запросов пользователя за определенным ICAP-сервером в рамках одной сессии. Это обеспечивает согласованную обработку пользовательского потока данных. Вы можете выбрать несколько методов привязки, они применяются последовательно, в порядке приоритета сверху вниз: • **Cookie** — привязка выполняется на основе cookie, который генерируется самим балансировщиком. Балансировщик добавляет cookie во вложенный HTTP-ответ, закрепляя HTTP-сессию пользователя за конкретным ICAP-сервером. Все последующие HTTP-сообщения, содержащие этот cookie, направляются на тот же ICAP-сервер. • **User** — привязка выполняется по имени пользователя источника запроса. Механизм используется только в том случае, если система может определить имя пользователя. Если имя пользователя определить невозможно, применяется следующий доступный метод согласно приоритету. • **IP+port** — привязка осуществляется по комбинации IP-адреса и порта источника. В этом случае все ICAP-запросы от одного и того же IP-адреса и порта направляются на один и тот же ICAP-сервер на протяжении времени действия привязки. • **IP** — привязка выполняется только по IP-адресу источника. Все ICAP-запросы от одного и того же IP-адреса направляются на один ICAP-сервер в течение времени действия привязки. Метод обеспечивает стабильную маршрутизацию HTTP-запросов пользователей с постоянным IP-адресом. • **TCP-сессия** — привязка выполняется по TCP-соединению. В этом режиме все ICAP-запросы (REQMOD и RESPMOD), передаваемые в рамках одного TCP-соединения от ICAP-клиента, обрабатываются одним и тем же ICAP-сервером. Балансировка по TCP-сессии активна всегда, она работает, если не сработали другие выбранные методы. **Тайм-аут** — период, в течение которого сохраняется привязка запросов (от 1 до 86 400 секунд, значение по умолчанию — 3600 секунд). По истечении этого времени информация о привязке сессии удаляется, после чего распределение запросов выполняется заново. Подробнее о работе с ICAP-серверами — в разделе « Работа с внешними ICAP-серверами »
ICAP-серверы	Выбор профилей ICAP-серверов, на которые будет распределяться нагрузка. Подробнее о работе с ICAP-серверами — в разделе «Работа с внешними ICAP-серверами »

ПримечаниеПри изменении параметров действующего правила происходит перезапуск механизма балансировки. Активные сессии с ICAP-серверами завершаются. Последующие запросы обрабатываются уже по обновленной конфигурации правила балансировки.

Балансировщик reverse-прокси

Балансировщик серверов reverse-прокси позволяет распределять трафик на внутренние серверы, публикуемые с помощью правил reverse-прокси. Этот балансировщик может быть использован в правилах reverse-прокси.

Для создания правила балансировки для серверов reverse-прокси перейдите в раздел **Настройки → Политики сети → Балансировка нагрузки,** нажмите **Добавить**, выберите **Балансировщик reverse-прокси** и укажите необходимые параметры.

Параметр	Описание
Включен	Включение или отключение правила балансировки
Название	Название правила балансировки
Описание	Описание правила балансировки
Reverse-прокси профили	Выбор профилей серверов reverse-прокси, на которые будет передаваться трафик. Подробнее о публикации ресурсов с помощью reverse-прокси — в разделе «Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси »

Пропускная способность

Product: SWG
Version: 7.5.x

Правила управления пропускной способностью применяются к определенным пользователям, узлам, сервисам, приложениям.

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

Чтобы создать правило управления пропускной способностью, перейдите в раздел **Настройки → Политики сети → Пропускная способность,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритизации трафика DSCP. Создать дополнительные полосы пропускания вы можете в разделе «Полосы пропускания»
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробнее о работе сценариев — в разделе «Сценарии». **Важно!** Сценарий является дополнительным условием. Если сценарий не активировался (не сработал ни один из триггеров сценария), правило не сработает
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
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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG 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	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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG 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
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Приложения	Список приложений, для которых необходимо ограничить полосу пропускания
Время	Время, когда правило активно