

Table of Contents

Table of Contents	1
Политики сети	2
Общие сведения	3
Межсетевой экран	4
NAT и маршрутизация	9
Балансировка нагрузки	20
Пропускная способность	23

Общие сведения

Documentation: ☒

Product: NGFW

Version: 7.x

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

В этом разделе вы можете:

- Управлять прохождением трафика с помощью [правил межсетевого экрана](#). В условиях фильтрации могут использоваться зоны, адреса источника и назначения, пользователи и 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.

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

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

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

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

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

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

В разрешающих правилах межсетевого экрана могут быть использованы [профили СОВ](#) или [профили приложений](#) (L7), содержащие настроенные наборы сигнатур. После того, как трафик попадает в первое сработавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей СОВ или L7. При срабатывании сигнатур к трафику применяется действие, настроенное в профиле, и производится соответствующая запись в журналах (в **Журнале трафика** - для приложений и в **Журнале СОВ** - для СОВ), 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 правила.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Опция доступна в версии 7.3.0 и выше
Описание	Описание правила
Действие	Возможные действия правила: • Запретить — блокировать прохождение трафика; • Разрешить — разрешить прохождение трафика
Профиль приложений	Профиль приложений, созданный заранее в разделе Библиотеки → Профили приложений . Профиль приложений содержит набор сигнатур приложений, предназначенный 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. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.
Профиль СОВ	Профиль СОВ, созданный заранее в разделе Библиотеки → Профили СОВ . Профиль СОВ содержит набор сигнатур, предназначенный для защиты определенных сервисов. Подробнее о создании и настройке профилей СОВ — в разделе « Профили СОВ » Важно! Профиль СОВ является дополнительным параметром для активации механизма анализа трафика. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.

Параметр	Описание
Отбросить и	Настройка этого параметра доступна для правил, блокирующих трафик (выбрано действие Запретить). Параметр может принимать одно из следующих значений: • Не выбран. • Посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. • Посылать TCP reset — блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указать сервиса (вкладка Сервис), использующего протокол TCP. • Посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
Сценарий	Выбор сценария для срабатывания правила. Подробнее о работе сценариев — в разделе «Сценарии» Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.
Журналирование	Управление записью в журнал информации о трафике при срабатывании правила. Возможные значения параметра: • 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. С этим режимом рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • Нет. В этом случае информация в журнал не будет записываться
Источник	Указание зоны, списков IP-адресов, списков GeoIP-адресов, списков URL источника трафика. Списки URL должны включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут UserGate NGFW выполняет разрешение доменных имен в IP-адреса и хранит полученный результат в кэш-памяти на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Указание списка 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»
Назначение	Указание зоны, списков IP-адресов, списков GeoIP-адресов, списков URL назначения трафика. Списки URL должны включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут UserGate NGFW выполняет разрешение доменных имен в IP-адреса и хранит полученный результат в кэш-памяти на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Указание типа сервиса, например, HTTP или HTTPS
Время	Выбор интервала времени, когда правило активно

Параметр	Описание
НIP-профили	Выбор НIP-профилей, созданных в разделе Библиотеки → НIP профили. НIP-профили содержат набор НIP-объектов и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). Подробнее о создании и настройке НIP-профилей — в разделе « НIP профили» Важно! В случае выключения НIP-профиля, он будет помечен серым цветом, а правило межсетевого экрана продолжит работать без условия проверки комплаенса.
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний, таблица срабатываний по приложениям. 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 данному правилу: добавление, обновление правила, изменение позиции правила в списке и т. п.

Примечание При 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
	Фильтр по состоянию правил (включены или отключены): enabled - true — показывает только включенные правила; - false — показывает только отключенные правила
pos	Поиск по позиции правила в списке (1, 2 и т. д.)
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
applicationProfile	Поиск правил межсетевого экрана по указанному при настройке профилю приложений. Поиск производится по правилам с действием «Разрешить»
ipsProfile	Поиск правил межсетевого экрана по указанному при настройке профилю COV. Поиск производится по правилам с действием «Разрешить»
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

Параметр	Описание
countrySource	Поиск правил по названию страны источника трафика (Russia, Austria и т. п.). Страна источника может быть добавлена в свойствах правила на вкладке Источник (Добавить GeoIP). Например, поисковый запрос countrySource = russia отобразит список правил, в которых в качестве страны источника указана Россия (Russia) или GeoIP не указан (т. е. любой 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 (Russia, Austria и т. п.). Страна назначения может быть добавлена в свойствах правила на вкладке Назначение (Добавить GeoIP). Например, поисковый запрос countryDest = russia отобразит список правил, в которых в качестве страны назначения указана Россия (Russia) или GeoIP не указан (т.е. любой 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: - Unknown — пользователи, не идентифицированные системой. - Known — пользователи, идентифицированные системой с помощью серверов авторизации. - Any — любой пользователь (Known или Unknown). - Определенный пользователь — конкретный пользователь, идентифицированный в системе. Пользователи могут быть созданы локально (локальные пользователи) или получены с внешних каталогов (например, Microsoft Active Directory). При поиске, требующем полного совпадения логина пользователя (с операторами «=» или «!=») 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 созданы локально или получены с внешних каталогов (например, Microsoft Active Directory)
groupId	Поиск правила по идентификатору группы пользователей
service	Поиск правила по указанному типу сервиса (например, HTTP или HTTPS)
active	Фильтр по статусу активности правил на момент выполнения запроса: - true — показывает правила, чей интервал активности включает текущее время; - false — показывает правила, чей интервал активности не включает текущее время
scenario	Время работы правила может быть задано в свойствах на вкладке Время. Для этого используются календари, которые могут быть созданы и настроены в разделе Настройки → Библиотеки → Календари или в свойствах правила Поиск правил по названию сценария, который должен быть активным для срабатывания правила (добавление и настройка сценариев доступна в разделе Настройки → Библиотеки → Сценарии)

Параметр	Описание
description	Поиск правил по описанию правила
Примечание Поисковый запрос не распространяется 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.	

Documentation: ☒
Product: NGFW
Version: 7.x

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, NoNAT, DNAT, NoDNAT, трансляции портов, маршрутизации на основе политик и трансляции адресов сетей. UserGate NGFW 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. 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, 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 ». Доступно в версии 7.3.0 и выше
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 NGFW 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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	Доступно начиная в версии 7.3.0 и выше. Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unklown, Klown. Для применения правил к конкретным пользователям или к пользователям типа Klown 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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 (доступно в версии 7.4.0 и выше) 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.

Параметр	Описание
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги »
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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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 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. 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 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 ». Доступно в версии 7.3.0 и выше
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 NGFW, 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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	Доступно в версии 7.4.0 и выше. 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

Параметр	Описание
Назначение	Списки IP-адресов (внешние IP-адресов UserGate NGFW, 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
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 NGFW: 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 NGFW 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

Примечание При 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.

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

Правила NoDNAT

Правила NoDNAT (доступно в версии 7.4.0 и выше) 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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 NGFW, 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 NGFW: 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.

Примечание Правила 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. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

Примечание Флажок «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 ». Доступно в версии 7.3.0 и выше

Параметр	Описание
Описание	Описание правила
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 пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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	Доступно в версии 7.4.0 и выше. 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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 NGFW: 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 NGFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес

Параметр	Описание
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

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. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок «Инvertировать» 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 ». Доступно в версии 7.3.0 и выше
Описание	Описание правила
Тип	Тип правила. Выберите Policy-based routing
Шлюз	Выбор одного из существующих шлюзов. Шлюз может быть добавлен в разделе Настройки → Сеть → Шлюзы Важно! Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
Сценарий	Указание сценария, который должен быть активным для срабатывания правила. Подробнее о работе сценариев — в разделе « Сценарии » Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), правило не работает.
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

Параметр	Описание
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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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	Доступно в версии 7.3.0 и выше. Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknowp, 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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.

Примечание Правила 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. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

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

Параметр	Описание
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Доступно в версии 7.3.0 и выше
Описание	Описание правила
Тип	Тип правила. Выберите Network mapping
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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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	Доступно в версии 7.4.0 и выше. 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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW 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

Параметр	Описание
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

Балансировка нагрузки

Documentation: ☒
Product: NGFW
Version: 7.x

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

- Для внутренних серверов, публикуемых в интернете (DNAT).
- Для внутренних серверов без публикации.
- Для балансировки трафика, пересылаемого на внешние серверы (ферму) ICAP-серверов.
- Для балансировки трафика на серверы, публикуемые через reverse-прокси.

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

Для создания правила балансировки для серверов TCP/UDP необходимо выбрать пункт **Добавить балансировщик TCP/UDP** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
IP-адрес виртуального сервера	Необходимо выбрать из списка IP-адресов, назначенных на сетевые интерфейсы. При необходимости администратор может добавить дополнительные IP-адреса на желаемый интерфейс.
Порт	Порт, для которого необходимо производить балансировку нагрузки.
Протокол	Протокол — TCP или UDP — для которого необходимо производить балансировку нагрузки.
Метод балансировки	Возможны 4 различных метода распределения нагрузки на реальные серверы: • Round robin: каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • Weighted round robin: работает аналогично 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 который в данный момент установлено наименьшее число соединений. • Weighted least connections: работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.

Наименование	Описание
Реальные серверы	Добавляется пул реальных серверов, на которые перенаправляется трафик. Для каждого из серверов необходимо указать: • IP-адрес сервера. • Порт сервера. Порт, на который пересылать запросы пользователей. • Вес. Данный коэффициент используется для неравномерного распределения нагрузки на реальные серверы для режимов балансировки weighted round robin и weighted least connections. Чем больше вес, тем больше будет нагрузка на сервер. • Режим. Может быть три варианта: ◦ 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 NGFW подменяет IP-адрес источника на свой. Внимание! Поскольку в режиме <u>Шлюз</u> балансировщик не изменяет заголовки пакетов, то обратный трафик от реального сервера должен обеспечиваться средствами маршрутизации. Т.е. шлюз для обратного трафика должен отличаться от адреса NGFW.
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 NGFW подменяет IP-адрес источника на свой.
Мониторинг	С помощью мониторинга можно настроить проверку реальных серверов на определение их работоспособности. Если проверка прошла неуспешно для реального сервера, он исключается из балансировки.
Режим	Способ мониторинга реальных серверов. Возможны варианты: • ping — проверить доступность узла с помощью утилиты ping. • connect — проверить работоспособность узла, установив TCP-соединение на определенный порт. • negotiate — проверить работоспособность узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. Для настройки этого режима следует выбрать тип сервиса (HTTP или DNS), строки Запрос и Ожидаемый ответ. Например, для HTTP-запроса: ◦ Запрос: /robots.txt ◦ Ожидаемый ответ: Disallow: /bin/ Строка запроса тут указывает на 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	Интервал времени ожидания ответа на проверку.
Число неудачных попыток	Количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки.

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

Балансировщик серверов reverse-прокси позволяет распределить нагрузку на внутренние серверы или ферму серверов, публикуемую с помощью правил reverse-прокси. Данный балансировщик затем может быть использован в правилах reverse-прокси. Для создания балансировщика reverse-прокси необходимо выбрать пункт **Добавить балансировщик reverse-прокси** и указать следующие параметры:

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

Пропускная способность

Documentation: ☒
Product: NGFW
Version: 7.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/Низе, 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.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW 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.

Наименование	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 NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW 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.

