

Table of Contents

Table of Contents	1
Политики сети	2
Описание	3
Межсетевой экран	5
NAT и маршрутизация	7
Балансировка нагрузки	14
Пропускная способность	17

Описание

Documentation: ☒
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Раздел **Политики сети** содержит следующие подразделы:

- Межсетевой экран.
- NAT и маршрутизация.
- Балансировка нагрузки.
- Пропускная способность.

С помощью политик сети администратор может настроить необходимый доступ в интернет для своих пользователей, опубликовать внутренние ресурсы сети в интернете, управлять скоростью передачи данных для определенных сервисов и приложений.

ПримечаниеПравила, созданные в данных разделах, применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила.

Для предоставления пользователям доступа в интернет необходимо:

Наименование	Описание
Шаг 1. Создать правило NAT (опционально).	Если необходима подмена адресов трафика. Смотрите раздел NAT и маршрутизация .
Шаг 2. Создать разрешительное правило межсетевого экрана.	Смотрите раздел Межсетевой экран .

Для публикации внутреннего ресурса в интернете необходимо:

Наименование	Описание
Шаг 1. Создать правило DNAT или правило reverse-прокси.	Смотрите раздел Правила DNAT и Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси .

Чтобы указать для определенного сервиса или адреса выход в интернет через альтернативного провайдера, необходимо:

Наименование	Описание
Шаг 1. Создать правило Policy-based routing.	Смотрите раздел Policy-based routing .

Для того чтобы запретить или разрешить определенный тип трафика, проходящий через UserGate, необходимо:

Наименование	Описание
Шаг 1. Создать правило межсетевого экрана.	Смотрите раздел Межсетевой экран .

Для того чтобы распределить трафик между несколькими внутренними серверами, необходимо:

Наименование	Описание
Шаг 1. Создать правило Балансировки нагрузки.	Смотрите раздел Балансировка нагрузки .

Для того чтобы ограничить скорость для определенного сервиса или приложения, необходимо:

Наименование	Описание

Наименование	Описание
Шаг 1. Создать правило Пропускной способности.	Смотрите раздел Пропускная способность .

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

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

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

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

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

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

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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Запретить : блокирует трафик. Разрешить : разрешает трафик.
Отбросить и	Настройка данного параметра доступна для правил, блокирующих трафик (выбрано действие Запретить). Параметр может принимать одно из следующих значений: • Не выбран. • Посылать ICMP host unreachable: блокировка трафика с отправкой ICMP-сообщения. • Посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указание сервиса (вкладка Сервис), использующего протокол TCP. • Посылать TCP reset в обе стороны: блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • 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.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
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 или HTTPS.
Приложения	Список приложений, для которых применяется данное правило. Определение приложения происходит после установления соединения между клиентом и сервером и передачи трафика в обоих направлениях. Максимальный объем такого трафика - 1 Кбайт. Поэтому правило, разрешающее приложение, будет применяться к любому трафику, подходящему под другие критерии правила, пока приложение не будет определено. Аналогично, срабатывание блокирующего правила (разрыв сессии), которое в качестве одного из условий использует приложение, произойдет только после определения приложения.
Время	Интервалы времени, когда правило активно.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Documentation: ☒
 Product: NGFW
 Version: 7.0.1

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

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

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

Правила NAT

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

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

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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать NAT .
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, то система будет использовать 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 NGFW будет использовать все указанные адреса при Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут 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! Флажок Инвертировать не влияет на работу при использовании мак адресов. Важно! Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.

Наименование	Описание
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

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

Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет. Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси. Более подробно о публикации ресурсов с помощью правил reverse-прокси описано в главе [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. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Низе, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать DNAT .
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника. Если SNAT IP не указан, то адрес источника будет заменён на адрес интерфейса 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 во вкладке DNAT активировать Флажок Включить SNAT.

Наименование	Описание
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут 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! Флажок Инвертировать не влияет на работу при использовании мак адресов. Важно! Обработка трафика происходит по следующей логике: - условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; - условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Один из внешних IP-адресов NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. Важно! Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Сервис	Тип сервиса, который необходимо опубликовать, например, HTTP. Если не указан сервис, то будут опубликованы все сервисы. Важно! Нельзя опубликовать сервисы, которые используют следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет.
Включить SNAT	При включении данной опции 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 счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Правила порт-форвардинга

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

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

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

Наименование	Описание
Включено	Включает или отключает правило.

Наименование	Описание
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать Порт-форвардинг .
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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! Флажок Инвертировать не влияет на работу при использовании мак адресов. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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.
Порт-форвардинг	Переопределения портов публикуемых сервисов: • Оригинальный порт назначения — номер TCP/UDP-порта, на который пользователи шлют запросы. Важно! Нельзя использовать следующие порты, поскольку они используются внутренними сервисами NGFW: 2200, 8001, 4369, 9000-9100. • Новый порт назначения — номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернете.
Включить SNAT	При включении данной опции 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 счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Policy-based routing

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

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

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

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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать Policy-based routing .
Шлюз	Выбор одного из существующих шлюзов. Вы можете добавить шлюз в разделе Сеть → Шлюзы . Важно! Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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! Флажок Инвертировать не влияет на работу при использовании мак адресов. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any , Unknown , Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства .

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.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Network mapping

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

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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать Network mapping .
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет. В этом случае информация не будет записываться.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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! Флажок Инвертировать не влияет на работу при использовании мак адресов. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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.
Network mapping	Задаются параметры подмены сетей. Направление: • Входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле Новая IP-сеть/маска. • Исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле Новая IP-сеть/маска. • Новая IP-сеть/маска — адрес сети, на которую будет производится замена.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Балансировка нагрузки

Documentation: ☒
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

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/IP необходимо выбрать пункт **Добавить балансировщик TCP/IP** 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 ICAP позволяет распределить нагрузку на внешние серверы или ферму серверов ICAP, например, на внешнюю ферму серверов с антивирусным ПО. Данный балансировщик затем может быть использован в правилах ICAP. Для создания балансировщика серверов ICAP необходимо выбрать пункт **Добавить балансировщик ICAP** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
ICAP-профили	Выбрать ICAP-профили серверов, на которые будет распределяться нагрузка. Более подробно о работе с серверами ICAP читайте в разделе Работа с внешними ICAP-серверами .

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: 7.0.1

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

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

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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритизации трафика DSCP. Создать дополнительные полосы пропускания можно в разделе Полосы пропускания .
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут 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.

