QIWI Host Based Firewall (QHBF)

Руководство пользователя

Оглавление

[1. Общие положения 3](#_Toc131693731)

[1.1 Наименование и назначение 3](#_Toc131693732)

[1.2 Определения 3](#_Toc131693733)

[1.3 Технические требования к клиентской части (АРМ Оператора) 3](#_Toc131693734)

[1.4 Основные функции 3](#_Toc131693735)

[2. Работа с комплексом 4](#_Toc131693736)

[2.1 Авторизация 4](#_Toc131693737)

[2.2 Правила 4](#_Toc131693738)

[Поиск правила 4](#_Toc131693739)

[Создание правила 5](#_Toc131693740)

[Применение правила 6](#_Toc131693741)

[Редактирование правила 6](#_Toc131693742)

[Удаление правила 6](#_Toc131693743)

[История создания и редактирования правила 6](#_Toc131693744)

[Параметры правил по умолчанию 7](#_Toc131693745)

[2.3 Логи 7](#_Toc131693746)

[Создание правил на основе логов 8](#_Toc131693747)

[Поиск по логам 8](#_Toc131693748)

[2.4 Режимы работы правил 8](#_Toc131693749)

[Добавление или удаление сервиса 9](#_Toc131693750)

[2.5 Мониторинг работы комплекса 10](#_Toc131693751)

[2.6 История действий администраторов комплекса 10](#_Toc131693752)

[2.7 Переключение комплекса в аварийный режим работы 11](#_Toc131693753)

# Общие положения

## Наименование и назначение

QIWI Host Based Firewall (QHBF) - программный комплекс, предназначенный для обеспечения централизованного управления системой фильтрации сетевых пакетов на серверах и рабочих станциях под управлением операционной системой linux.

## Определения

* хост - устройство, работающее в режиме сервера, и подключенное к сети;
* фильтрация трафика - ограничение трафика между хостами в соответствии с настроенными правилами фильтрации;
* правило фильтрации трафика - набор настроек, определяющий условия, при наступлении которых трафик ограничивается;
* режимы работы сервиса:
	+ мониторинг - режим работы сервиса, при котором собирается информация о трафике между хостами (логи), трафик не ограничивается;
	+ блокировка - запрещен весь трафик, кроме явно разрешенного;
	+ аварийный режим - все блокирующие правила фильтрации трафика отключены.

## Технические требования к клиентской части (АРМ Оператора)

* Компьютер под управлением ОС Windows версии 7 и выше, или актуальной версии MacOS или ОС Linux (любого из современных дистрибутивов);
* Интернет-браузер: Яндекс.Браузер, Edge, Mozilla FireFox, Google Chrome, Safari актуальных версий.

## Основные функции

* просмотр существующих правил фильтрации трафика
* создание правила фильтрации трафика
* удаление правила фильтрации трафика
* редактирование правила фильтрации трафика
* просмотр истории создания и редактирования правил фильтрации трафика
* переключение режима работы (мониторинг/блокировка) для группы хостов
* просмотр логов срабатывания правил фильтрации трафика
* переключение системы в "аварийный режим" (отключение блокирующих правил фильтрации трафика)

# Работа с комплексом

## Авторизация

Для начала работы авторизуйтесь: укажите имя и пароль от своей учетной записи и нажмите кнопку "Войти".

## Правила

Раздел содержит список существующих правил и предоставляет возможности:

* поиск по списку. в т.ч. с использованием фильтров;
* создание нового правила;
* выполнение действий с существующими правилами.

Правила в списке описаны в формате "[хост - источник трафика]сервис.роль.окружение → [хост - место применения правила]сервис.роль.окружение", далее указаны порт, действие, направление (входящий или исходящий трафик), и комментарий, если он есть.

Рядом с описанием каждого правила размещены кнопки для выполнения действий с ним: просмотра истории, редактирования правила и удаления, а также индикатор, показывающий состояние правила: активное или не активное.



### Поиск правила

Чтобы найти существующее правило, введите в поисковой строке последовательность символов для поиска и нажмите "Поиск".

Если список слишком длинный, или если нужно отобрать группу правил, соответствующих заданным параметрам, воспользуйтесь фильтрами: выберите параметры источника трафика – "Источник (сервис, роль, окружение)" и/или получателя трафика – "Получатель (сервис, роль, окружение)", укажите порт, выберите тип протокола, нажмите кнопку "Отобрать". Отбор и поиск по ключевым словам можно использовать одновременно, результат будет выведен на экран.



### Создание правила

Чтобы создать новое правило, нажмите кнопку "Создать правило" и укажите в открывшейся форме его параметры:

* Параметры хоста - источника трафика:
	+ выберите тип источника и укажите значения для соответствующих этому типу параметров:
		- СРО - выберите сервис, роль, окружение из соответствующих списков;
		- IP адрес - укажите IP адрес или блок адресов;
		- Новый СРО - создайте новый источник, если его нет в списке;
* Параметры хоста – получателя трафика:
	+ выберите тип и укажите значения для соответствующих этому типу параметров:
		- СРО - выберите сервис, роль, окружение из соответствующих списков;
		- IP адрес - укажите IP адрес или диапазон адресов;
		- Новый СРО - создайте нового получателя, если его нет в списке;
* Направление - выберите входящий или исходящий трафик;
* Протокол - выберите протокол из списка;
* Порт - укажите порт или диапазон портов
* Действие - выберите тип правила:
	+ ACCEPT - разрешающее правило (разрешит трафик с заданными параметрами);
	+ REJECT - запрещающее правило (заблокирует трафик с заданными параметрами);
* Комментарий - добавьте комментарий к правилу, если необходимо (напр., номер заявки, по которой настроено правило).

|  |
| --- |
| Внимание: всё, что не разрешено явно, попадает под действие запрещающих правил |

Нажмите "Сохранить". Правило будет создано и добавлено в общий список в неактивном состоянии.

Также правила можно создавать на основании записей логов, см. п. 2.3



### Применение правила

Чтобы активировать правила, нажмите кнопку "Применить правила". Все ранее не активированные правила будут применены одновременно.

### Редактирование правила

Чтобы изменить параметры правила, найдите его в общем списке и нажмите кнопку "Изменить". На экран будет выведена форма, аналогичная форме создания правила и содержащая параметры существующего. Внесите необходимые изменения и нажмите "Сохранить".

|  |
| --- |
| Внимание: после сохранения изменений правило становится неактивным |

### Удаление правила

Чтобы удалить правило, найдите его в общем списке и нажмите кнопку "Удалить".

### История создания и редактирования правила

Чтобы просмотреть историю изменения правила (создание, редактирование и т.д.), найдите его в общем списке и нажмите кнопку "История". На экран будет выведена таблица, содержащая историю изменений правила, с указанием следующих данных:

* дата и время изменения;
* действие, которое было произведено в отношении правила;
* список изменений (отображается при создании и изменении правила);
* имя учетной записи, под которой произведено изменение.



### Параметры правил по умолчанию

Раздел содержит описания префиксов и постфиксов, которые добавляются ко всем правилам автоматически:

* По умолчанию - содержит описания стандартных параметров;
* Пользовательские параметры - содержит описания параметров, созданных пользователем.

И стандартные, и пользовательские параметры можно редактировать. Чтобы внести изменение, перейдите к нужному параметру и отредактируйте его описание.

Чтобы создать новый пользовательский параметр, перейдите в подраздел "Пользовательские параметры" и нажмите кнопку "Добавить". Укажите название параметра и добавьте его описание, затем нажмите "Сохранить все".

Чтобы удалить пользовательский параметр, нажмите кнопку "Удалить" рядом с его названием.

## Логи

Лог - история срабатываний запрещающих правил фильтрации трафика. Логи для разрешающих правил не ведутся для экономии ресурсов.

Лог отображается в виде таблицы, по умолчанию отображаются логи за последние 10 минут до открытия раздела.

Состояние флага "Группировать" влияет на отображение: проставьте флаг, чтобы сгруппировать срабатывания по параметрам источника трафика (сервис, роль, окружение, или IP адрес, или имя хоста).

Для каждого срабатывания правила записывается:

* дата и время срабатывания;
* описание хоста - источника трафика;
* описание хоста, к которому применяется правило;
* порт;
* протокол;
* количество срабатываний (если логи сгруппированы);
* действие, примененное в отношении трафика.



### Создание правил на основе логов

На основе логов можно создавать новые правила. Нажмите кнопку "Новое правило"; на экран будет выведена форма создания нового правила, заполненная информацией из лога.

### Поиск по логам

Чтобы вывести на экран срабатывания правил за определенный интервал времени, укажите дату и время начала и окончания этого интервала.

Чтобы отобрать срабатывания правил, соответствующих заданным параметрам, настройте фильтры по этим параметрам. Укажите IP адрес, порт источника трафика и/или параметры хоста, к которому применяются правила: IP адрес, название, сервис, роль, окружение, порт, тип протокола. нажмите кнопку "Отобрать".

Отбор по дате, по параметрам, и поиск по ключевым словам можно использовать одновременно; результат будет выведен на экран.

## Режимы работы правил

В разделе осуществляется управление режимами работы правил для сервисов: переключение между режимами "Мониторинг" и "Блокировка", а также управление логированием срабатываний правил для этих сервисов.

Чтобы переключиться между режимами работы правил для конкретного сервиса, найдите его в списке и выберите нужный режим работы:

* Allow - мониторинг; режим работы сервиса, при котором собирается информация о трафике (логи), трафик не ограничивается;
* Drop - блокировка; запрещен весь трафик, кроме явно разрешенного.

Правила для сервисов, не указанных в этом разделе, работают в режиме Allow.

Чтобы включить или выключить логирование для сервиса, проставьте или снимите флаг в столбце "Логирование" (по умолчанию логирование включено для всех сервисов).



### Добавление или удаление сервиса

Чтобы удалить сервис, нажмите кнопку "Удалить".

Чтобы добавить новый сервис, нажмите кнопку "Добавить". В открывшейся форме выберите сервис и роль, укажите режим работы правил для этого сервиса и режим логирования (по умолчанию включено), затем нажмите кнопку "Подтвердить".



## Мониторинг работы комплекса

В этом разделе отображается список подключенных к комплексу хостов и статус набора правил для каждого из них.

Список можно фильтровать по параметрам (сервис, роль, окружение, статус), а также находить нужный элемент списка с помощью поисковой строки.

Для каждого элемента списка отображается:

* имя хоста;
* название сервиса;
* роль;
* окружение;
* статус набора правил:
	+ ok
	+ waiting - ожидает получение правил;
	+ deployed - правила получены;
	+ down - ошибка;
* дата и время создания правил;
* дата и время получения правил;
* хэш от списка правил;
* подключен к HBF (да/нет).



## История действий администраторов комплекса

В этом разделе отображается история действий администраторов комплекса. Список можно отфильтровать по имени администратора, используя меню в верхней части раздела.

Для каждого действия отображаются

* дата и время;
* тип действия;
* список изменений (для действий типа "создание правила, изменение правила");
* имя учетной записи, под которой произведено изменение.



## Переключение комплекса в аварийный режим работы

Аварийный режим подразумевает одновременное отключение всех блокирующих правил фильтрации трафика для всех сервисов. Для перехода к этому разделу требуется дополнительная авторизация.

В разделе отображается текущий режим работы. Чтобы сменить режим, введите комментарий и нажмите кнопку "Сменить режим".

