**Самостоятельная работа 2**

**Настройка правил с помощью групповой политики**

В данной работе необходимо выполнить настройку правил брандмауэра Windows.

## **Доступ к консоли брандмауэра Windows в режиме повышенной безопасности**

При настройке одного устройства необходимо иметь права администратора на устройстве. В этом случае для доступа к консоли Брандмауэр Windows в режиме повышенной безопасности выберите пуск, введите wf.msc и нажмите клавишу ВВОД.

## **Создание правила ICMP для входящего трафика**

Этот тип правила позволяет получать запросы и ответы ICMP устройствами в сети. Чтобы создать правило ICMP для входящего трафика, выполните приведенные далее действия.

1. Открытие консоли брандмауэра Windows в режиме повышенной безопасности
2. В области навигации выберите **Правила для входящих подключений**.
3. Выберите **Действие**, а затем **— Новое правило**.
4. На странице **Тип правила** мастера создания правила для входящего трафика выберите **Пользовательский**, а затем нажмите **кнопку Далее**.
5. На странице **Программа** выберите **Все программы**, а затем нажмите **кнопку Далее**.
6. На странице **Протокол и порты** выберите **ICMPv4** или **ICMPv6** в списке **Тип протокола** . Если в сети используются протоколы IPv4 и IPv6, необходимо создать отдельное правило ICMP для каждого из них.
7. Выберите **Настроить.**
8. В диалоговом окне **Настройка параметров ICMP** выполните одно из следующих действий.
	* Чтобы разрешить весь сетевой трафик ICMP, выберите **Все типы ICMP** и нажмите **кнопку ОК**.
	* Чтобы выбрать один из предопределенных типов ICMP, выберите **Конкретные типы ICMP**, а затем выберите каждый тип в списке, который вы хотите разрешить. Нажмите **кнопку ОК.**
	* Чтобы выбрать тип ICMP, который не отображается в списке, выберите **Конкретные типы ICMP**, выберите в списке номер **типа** , выберите **номер кода** в списке, нажмите кнопку **Добавить**, а затем выберите только что созданную запись в списке. Нажмите **кнопку ОК.**
9. Нажмите **кнопку Далее**
10. На странице **Область** можно указать, что правило применяется только к сетевому трафику к IP-адресам, указанным на этой странице, или от нее. Настройте соответствующую конфигурацию, а затем нажмите кнопку **Далее**.
11. На странице **Действие** выберите **Разрешить подключение**, а затем нажмите кнопку **Далее**.
12. На странице **Профиль** выберите типы сетевых расположений, к которым применяется это правило, и нажмите кнопку **Далее**.
13. На странице **Имя** введите имя и описание правила, а затем нажмите кнопку **Готово**.

## **Создание правила порта для входящего трафика**

Этот тип правила позволяет любой программе, прослушивающей указанный порт TCP или UDP, получать сетевой трафик, отправляемый на этот порт. Чтобы создать правило входящего порта, выполните приведенные далее действия.

1. Открытие консоли брандмауэра Windows в режиме повышенной безопасности
2. В области навигации выберите **Правила для входящих подключений**.
3. Выберите **Действие**, а затем **— Новое правило**.
4. На странице **Тип правила** мастера создания правила для входящего трафика выберите **Пользовательский**, а затем нажмите **кнопку Далее**.
5. На странице **Программа** выберите **Все программы**, а затем нажмите **кнопку Далее**.
6. На странице **Протокол и порты** выберите тип протокола, который нужно разрешить. Чтобы ограничить правило указанным номером порта, необходимо выбрать **TCP** или **UDP**. Так как это входящее правило, обычно настраивается только номер локального порта. При выборе другого протокола через брандмауэр разрешены только те пакеты, поле протокола которых в заголовке IP-адреса соответствует этому правилу.
Чтобы выбрать протокол по его номеру, в списке выберите **Пользовательский**, а затем введите номер в поле **Номер протокола**.
Настроив протоколы и порты, нажмите кнопку **Далее**.
7. На странице **Область** можно указать, что правило применяется только к сетевому трафику к IP-адресам, указанным на этой странице, или от нее. Настройте соответствующую конфигурацию, а затем нажмите кнопку **Далее**.
8. На странице **Действие** выберите **Разрешить подключение**, а затем нажмите кнопку **Далее**.
9. На странице **Профиль** выберите типы сетевых расположений, к которым применяется это правило, и нажмите кнопку **Далее**.
10. На странице **Имя** введите имя и описание правила, а затем нажмите кнопку **Готово**.

## **Создать правила порта для исходящего трафика**

По умолчанию брандмауэр Windows разрешает весь исходящий сетевой трафик, если он не соответствует правилу, запрещающего трафик. Этот тип правила блокирует исходящий сетевой трафик, соответствующий указанным номерам портов TCP или UDP. Чтобы создать правило исходящего порта, выполните приведенные далее действия.

1. Открытие консоли брандмауэра Windows в режиме повышенной безопасности
2. В области навигации выберите **Правила для исходящего трафика**.
3. Выберите **Действие**, а затем **— Новое правило**.
4. На странице **Тип правила** мастера создания правила для исходящего трафика выберите **Пользовательский**, а затем нажмите **кнопку Далее**.
5. На странице **Программа** выберите **Все программы**, а затем нажмите **кнопку Далее**.
6. На странице **Протокол и порты** выберите тип протокола, который нужно заблокировать. Чтобы ограничить правило указанным номером порта, необходимо выбрать **TCP** или **UDP**. Так как это правило является исходящим правилом, обычно настраивается только номер удаленного порта. При выборе другого протокола только те пакеты, для которых поле протокола в заголовке IP-адреса соответствует этому правилу, блокируются брандмауэром Защитник Windows. Сетевой трафик для протоколов разрешен до тех пор, пока другие правила, соответствующие, не блокируют его. Чтобы выбрать протокол по его номеру, в списке выберите **Пользовательский** , а затем введите номер в поле **Номер протокола** . Настроив протоколы и порты, нажмите кнопку **Далее**.
7. На странице **Область** можно указать, что правило применяется только к сетевому трафику к IP-адресам, указанным на этой странице, или от нее. Настройте соответствующую конфигурацию, а затем нажмите кнопку **Далее**.
8. На странице **Действие** выберите **Блокировать подключение**, а затем нажмите кнопку **Далее**.
9. На странице **Профиль** выберите типы сетевых расположений, к которым применяется это правило, и нажмите кнопку **Далее**.
10. На странице **Имя** введите имя и описание правила, а затем нажмите кнопку **Готово**.

## **Создайте правила программы или службы для входящего трафика**

Этот тип правила позволяет программе прослушивать и получать входящий сетевой трафик на любом порту.

Чтобы создать правило брандмауэра для входящего трафика для программы или службы, выполните приведенные далее действия.

1. Открытие консоли брандмауэра Windows в режиме повышенной безопасности
2. В области навигации выберите **Правила для входящих подключений**.
3. Выберите **Действие**, а затем **— Новое правило**.
4. На странице **Тип правила** мастера создания правила для входящего трафика выберите **Пользовательский**, а затем нажмите **кнопку Далее**.

Примечание

Информация, которую пользователь должен заметить, даже если вы можете создать правила, выбрав **Программа** или **Порт**, эти параметры ограничивают количество страниц, представленных мастером. Если выбрать **Пользовательский**, вы увидите все страницы и будете максимально гибкими при создании правил.

1. На странице **Программа** выберите **Этот путь к программе**.
2. Введите путь к программе в текстовом поле. Используйте переменные среды, если применимо, чтобы обеспечить правильную работу программ, установленных в разных расположениях на разных компьютерах.
3. Выполните одно из следующих действий.
	* Если исполняемый файл содержит одну программу, нажмите кнопку **Далее**.
	* Если исполняемый файл является контейнером для нескольких служб, которым должно быть разрешено получать входящий сетевой трафик, нажмите **кнопку Настроить**, выберите **Применить только к службам**, **нажмите кнопку ОК**, а затем нажмите **кнопку Далее**.
	* Если исполняемый файл является контейнером для одной службы или содержит несколько служб, но правило применяется только к одной из них, выберите **Настроить**, выберите **Применить к этой службе**, а затем выберите службу из списка. Если служба не отображается в списке, выберите **Применить к службе с этим коротким именем службы**, а затем введите короткое имя службы в текстовое поле. Нажмите **кнопку ОК**, а затем нажмите кнопку **Далее**.

Если результат равен NONE, то правило брандмауэра не может быть применено к этой службе.

Чтобы задать тип идентификатора безопасности для службы, выполните следующую команду: sc sidtype <ServiceName> <Type>

В предыдущей команде значение <Type> может иметь значение UNRESTRICTED или RESTRICTED. Хотя команда также разрешает значение NONE, этот параметр означает, что службу нельзя использовать в правиле брандмауэра, как описано здесь. По умолчанию большинство служб в Windows настроены как UNRESTRICTED. Если изменить тип идентификатора безопасности на RESTRICTED, служба может не запуститься. Мы рекомендуем изменить тип идентификатора безопасности только для служб, которые вы хотите использовать в правилах брандмауэра, и изменить тип идентификатора безопасности на UNRESTRICTED.

1. Рекомендуется ограничить правило брандмауэра для программы только портами, которые она должна работать. На странице **Протоколы и порты** можно указать номера портов для разрешенного трафика. Если программа пытается прослушивать порт, отличный от указанного здесь, она блокируется. Дополнительные сведения о параметрах протокола и порта см. в разделе Создание правила для входящих портов. Настроив параметры протокола и порта, нажмите кнопку **Далее**.
2. На странице **Область** можно указать, что правило применяется только к сетевому трафику к IP-адресам, указанным на этой странице, или от нее. Настройте соответствующую конфигурацию, а затем нажмите кнопку **Далее**.
3. На странице **Действие** выберите **Разрешить подключение**, а затем нажмите кнопку **Далее**.
4. На странице **Профиль** выберите типы сетевых расположений, к которым применяется это правило, и нажмите кнопку **Далее**.
5. На странице **Имя** введите имя и описание правила, а затем нажмите кнопку **Готово**.

## **Создайте правила программы или службы для исходящего трафика**

По умолчанию брандмауэр Защитник Windows разрешает весь исходящий сетевой трафик, если он не соответствует правилу, запрещающего трафик. Этот тип правила запрещает программе отправлять исходящий сетевой трафик на любой порт. Чтобы создать правило брандмауэра для исходящего трафика для программы или службы, выполните приведенные далее действия.

1. Открытие консоли брандмауэра Windows в режиме повышенной безопасности
2. В области навигации выберите **Правила для исходящего трафика**.
3. Выберите **Действие**, а затем **— Новое правило**.
4. На странице **Тип правила** мастера создания правила для исходящего трафика выберите **Пользовательский**, а затем нажмите **кнопку Далее**.

Примечание

Хотя можно создать множество правил, выбрав **Программа** или **Порт**, эти параметры ограничивают количество страниц, представленных мастером. Если выбрать **Пользовательский**, вы увидите все страницы и будете максимально гибкими при создании правил.

1. На странице **Программа** выберите **Этот путь к программе**.
2. Введите путь к программе в текстовом поле. Используйте переменные среды соответствующим образом, чтобы обеспечить правильную работу программ, установленных в разных расположениях на разных компьютерах.
3. Выполните одно из следующих действий.
	* Если исполняемый файл содержит одну программу, нажмите кнопку **Далее**.
	* Если исполняемый файл является контейнером для нескольких служб, которые должны быть заблокированы для отправки исходящего сетевого трафика, нажмите **кнопку Настроить**, выберите **Применить только к службам**, нажмите **кнопку ОК**, а затем нажмите **кнопку Далее**.
	* Если исполняемый файл является контейнером для одной службы или содержит несколько служб, но правило применяется только к одной из них, выберите **Настроить**, выберите **Применить к этой службе**, а затем выберите службу из списка. Если служба не отображается в списке, выберите **Применить к службе с этим коротким именем службы** и введите короткое имя службы в текстовое поле. Нажмите **кнопку ОК**, а затем нажмите кнопку **Далее**.
4. Если вы хотите, чтобы программа могла отправлять на одни порты, но запретить отправку на других, можно ограничить правило брандмауэра, чтобы блокировать только указанные порты или протоколы. На странице **Протоколы и порты** можно указать номера портов или номера протоколов для заблокированного трафика. Если программа пытается отправить номер порта, отличный от указанного здесь, или с помощью номера протокола, отличного от указанного здесь, то поведение брандмауэра для исходящего трафика по умолчанию разрешает трафик. Дополнительные сведения о параметрах протокола и порта см. в статье Создание правила исходящего порта. Настроив параметры протокола и порта, нажмите кнопку **Далее**.
5. На странице **Область** можно указать, что правило применяется только к сетевому трафику к IP-адресам, указанным на этой странице, или от нее. Настройте соответствующую конфигурацию, а затем нажмите кнопку **Далее**.
6. На странице **Действие** выберите **Блокировать подключение**, а затем нажмите кнопку **Далее**.
7. На странице **Профиль** выберите типы сетевых расположений, к которым применяется это правило, и нажмите кнопку **Далее**.
8. На странице **Имя** введите имя и описание правила, а затем нажмите кнопку **Готово**.