Настройка межсетевого экрана в Windows 10

Межсетево́й экра́н — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

В большинстве случаев поддерживаемый уровень сетевой модели OSI является основной характеристикой при классификации межсетевых экранов. Учитывая данную модель, различают следующие типы межсетевых экранов:

1. Управляемые коммутаторы.
2. Пакетные фильтры.
3. Шлюзы сеансового уровня.
4. Посредники прикладного уровня.
5. Инспекторы состояния.

Управляемые коммутаторы

Управляемые коммутаторы иногда причисляют к классу межсетевых экранов, так как они осуществляют фильтрацию трафика между сетями или узлами сети. Однако они работают на канальном уровне и разделяют трафик в рамках локальной сети, а значит не могут быть использованы для обработки трафика из внешних сетей (например, из Интернета.

Многие производители сетевого оборудования, такие как Cisco, Nortel, 3Com, ZyXEL, предоставляют в своих коммутаторах возможность фильтрации трафика на основе MAC-адресов, содержащихся в заголовках фреймов. Например, в коммутаторах семейства Cisco Catalyst эта возможность реализована при помощи механизма Port Security.[12]. Однако данный метод фильтрации не является эффективным, так как аппаратно установленный в сетевой карте MAC-адрес легко меняется программным путем, поскольку значение, указанное через драйвер, имеет более высокий приоритет, чем зашитое в плату[13]. Поэтому многие современные коммутаторы позволяют использовать другие параметры в качестве признака фильтрации — например, VLAN ID. Технология виртуальных локальных сетей (англ. *Virtual Local Area Network*) позволяет создавать группы хостов, трафик которых полностью изолирован от других узлов сети[14].

Пакетные фильтры

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов.

При анализе заголовка сетевого пакета могут использоваться следующие параметры[10]:

- IP-адреса источника и получателя;
- тип транспортного протокола;
- поля служебных заголовков протоколов сетевого и транспортного уровней;
- порт источника и получателя.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры[18]:

- пограничные маршрутизаторы;
- операционные системы;
- персональные межсетевые экраны.

Так как пакетные фильтры обычно проверяют данные только в заголовках сетевого и транспортного уровней, они могут выполнять это достаточно быстро. Поэтому пакетные фильтры, встроенные в пограничные маршрутизаторы, идеальны для размещения на границе с сетью с низкой степенью доверия.

Шлюзы сеансового уровня

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (англ. *proxy*), который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения. Шлюз сеансового уровня гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению.

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создаёт видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, так как контакт между узлами устанавливается только при условии его допустимости, шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам[22].

Посредники прикладного уровня

Межсетевые экраны прикладного уровня, к которым, в частности, относится файрвол веб-приложений, как и шлюзы сеансового уровня, исключают прямое взаимодействие двух узлов. Однако, функционируя на прикладном уровне, они способны «понимать» контекст передаваемого трафика. Межсетевые экраны, реализующие эту технологию, содержат несколько приложений-посредников (англ. *application proxy*), каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать несуществующие или нежелательные последовательности команд, что зачастую означает DoS-атаку, либо запрещать использование некоторых команд (например, FTP PUT, которая даёт возможность пользователю записывать информацию на FTP сервер).

Посредник прикладного уровня может определять тип передаваемой информации. Например, это позволяет заблокировать почтовое сообщение, содержащее исполняемый файл. Другой возможностью межсетевого экрана данного типа является проверка аргументов входных данных. Например, аргумент имени пользователя длиной в 100 символов либо содержащий бинарные данные является, по крайней мере, подозрительным.

Инспекторы состояния

Данный класс межсетевых экранов позволяет контролировать[27]:

- каждый передаваемый пакет — на основе таблицы правил;
- каждую сессию — на основе таблицы состояний;
- каждое приложение — на основе разработанных посредников.

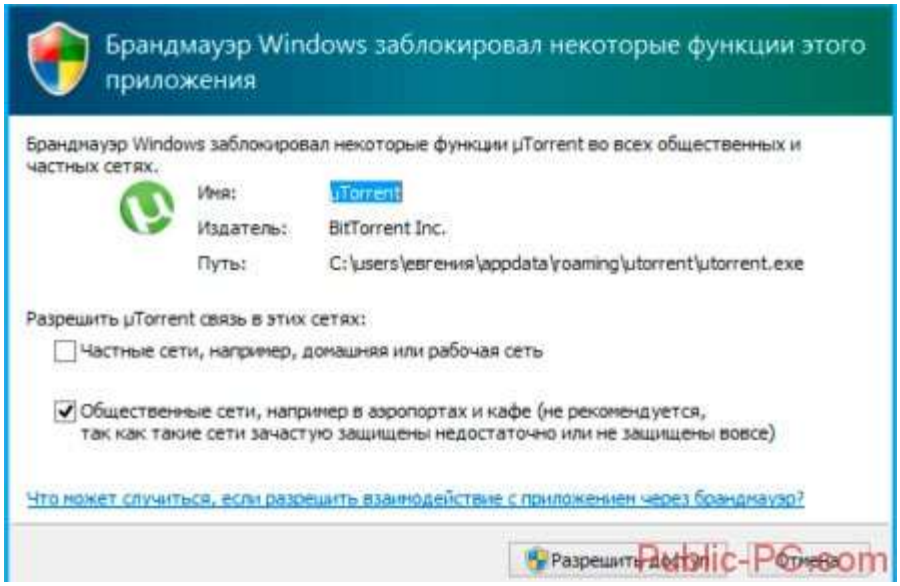
Осуществляя фильтрацию трафика по принципу шлюза сеансового уровня, данный класс межсетевых экранов не вмешивается в процесс установления соединения между узлами. Поэтому производительность инспектора состояний заметно выше, чем у посредника прикладного уровня и шлюза сеансового уровня, и сравнима с производительностью пакетных фильтров. Данные межсетевые экраны имеют большие возможности расширения. При появлении новой службы или нового протокола прикладного уровня для его поддержки достаточно добавить несколько шаблонов. Однако инспекторам состояний по сравнению с посредниками прикладного уровня свойственна более низкая защищённость.

https://public-pc.com/nastroyka-brandmauera-windows-10/

Настройка брандмауэра Windows 10

Брандмауэр или межсетевой экран — системная утилита, которая контролирует доступ программ в интернет. Он блокирует попадания нежелательного софта и файлов, пропускает только те, которое не навредят ОС. Работает все время в фоновом режиме. Не отключится самостоятельно.

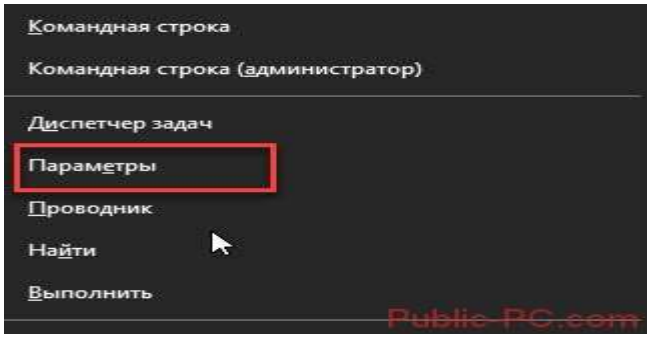
Если программе понадобится доступ к параметрам ПК, придет запрос. Подтвердите его.



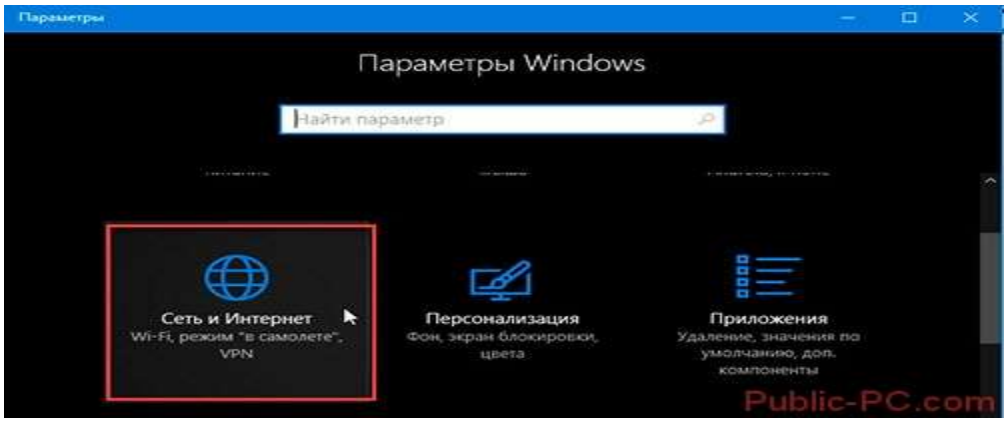
При правильной работе межсетевого экрана, можно не использовать дополнительное программное обеспечение для защиты от вредоносного софта.

Как зайти в настройки брандмауэра Windows 10

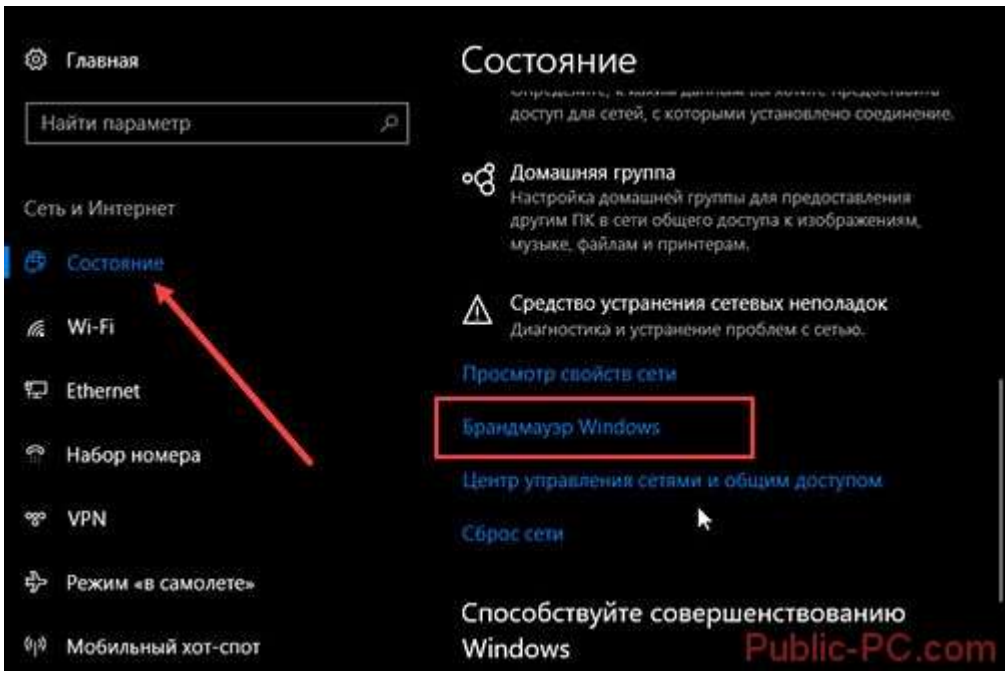
Нажмите «Win+X», выберите пункт «Параметры».



Далее, как на скриншоте:

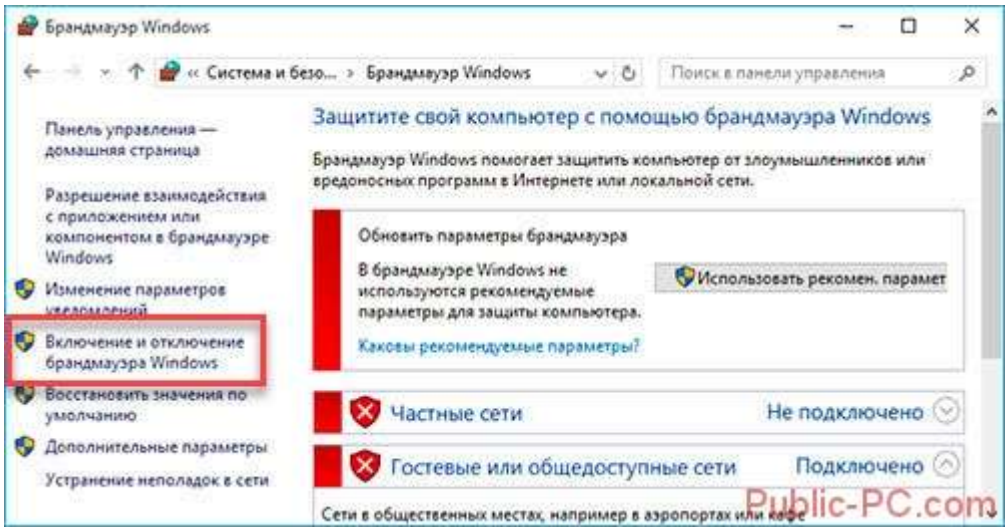


Выбираем «Состояние» (слева), ищем «Брандмауэр» на правой панели.

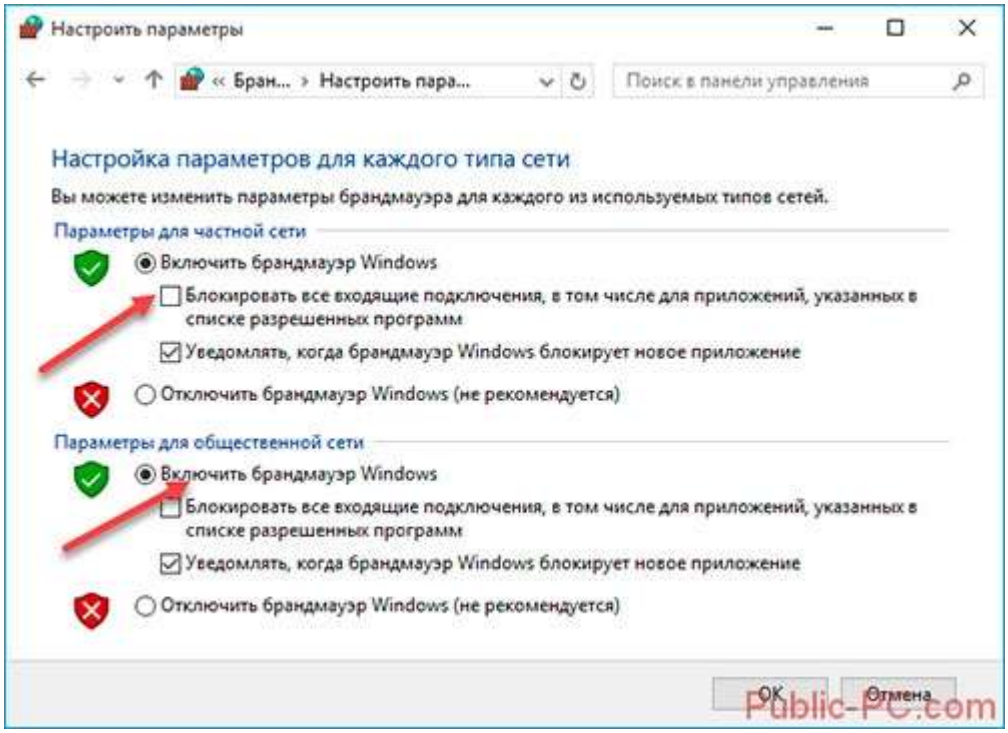


Включение брандмауэра Windows 10

Мы открыли настройки межсетевого экрана. Далее нажмите ссылку «Включение».



Отметьте пункты «Включить».



Теперь статус изменится. Появится информация о состоянии.