**ufw** – (Uncomplicated Firewall). Удобный интерфейс для управления политиками безопасности [межсетевого экрана.](http://help.ubuntu.ru/wiki/firewall) Сервера постоянно подвергаются различным атакам или сканируются в поиске уязвимостей. Как только эти уязвимости находятся, мы рискуем стать частью ботнета, раскрыть конфиденциальные данные или потерять деньги из-за сбоев в работе веб-приложений. Одной из первых мер по снижению рисков безопасности является грамотная настройка правил межсетевого экрана.

**$ ufw опции действие параметры**

Опции определяют общие настройки поведения утилиты, действие указывает, что нужно сделать, а параметры - дополнительные сведения для действия, например, IP-адрес или номер порта.

**Опции**:

* **--version** - вывести версию брандмауэра;
* **--dry-run** - тестовый запуск, никакие реальные действия не выполняются.

**Действия**:

* **enable** - включить фаерволл и добавить его в автозагрузку;
* **disable** - отключить фаерволл и удалить его из автозагрузки;
* **reload** - перезагрузить файервол;
* **default** - задать политику по умолчанию, доступно allow, deny и reject, а также три вида трафика - incoming, outgoing или routed;
* **logging** - включить журналирование или изменить уровень подробности;
* **reset** - сбросить все настройки до состояния по умолчанию;
* **status** - посмотреть состояние фаервола;
* **show** - посмотреть один из отчётов о работе;
* **allow** - добавить разрешающее правило;
* **deny** - добавить запрещающее правило;
* **reject** - добавить отбрасывающее правило;
* **limit** - добавить лимитирующее правило;
* **delete** - удалить правило;
* **insert** - вставить правило.

**Включение Fire Wall**

**sudo ufw status** – проверяем статус firewall

sudo ufw status verbose

**sudo ufw enable** – включаем firewall (если мы работаем по SSH, нужно заранее добавить правило, разрешающее работу по SSH. Иначе соединение прервется)

**Политики по умолчанию**

По умолчанию UFW настройки запрещают все входящие соединения и разрешают все исходящие. Это значит, что если кто-то попытается  достичь ваш сервер, он не сможет подключиться, в то время как любое приложение на сервере имеет доступ к внешним соединениям.  
  
Cоответствующие правила фаервола прописываются так:

**sudo ufw default deny incoming**  
  
**sudo ufw default allow outgoing**

**Добавление правил**

Чтобы создать разрешающее правило, используется команда allow. Вместо allow могут использоваться и запрещающие правила ufw - deny и reject. Они отличаются тем, что для deny компьютер отсылает отправителю пакет с уведомлением об ошибке, а для reject просто отбрасывает пакет и ничего не отсылает. Для добавления правил можно использовать простой синтаксис:

**$ ufw allow имя\_службы**  
**$ ufw allow порт**  
**$ ufw allow порт/протокол**

**sudo ufw allow** [protocol\_name][port] – разрешить соединение, можно использовать либо название протокола, либо его порт

**sudo ufw allow** 22/tcp – разрешить входящие и исходящие подключения только по протоколу tcp

**sudo ufw allow out** 80/tcp – разрешить исходящий трафик на 80 порт по протоколу tcp

**sudo ufw deny in** 80/tcp – запретить входящий трафик на порт 80 по протоколу tcp

**sudo ufw limit** 22/tcp – если с одного ip адреса будет инициировано более 6 подключений в течении 30 секунд, соединение будет запрещено

**Добавление диапазона портов**

**sudo ufw allow** 3000:3100/tcp – обязательно указываем TCP или UDP протокол при добавлении диапазона портов   
**sudo ufw allow** 3000:3100/udp–обязательно указываем TCP или UDP протокол при добавлении диапазона портов

**Добавление IP адресов**

**sudo ufw allow from** ip\_address – указать IP адрес которому будет разрешен доступ ко всем портам

**sudo ufw allow from** ip\_address **to any port** [port] – задать доступ только к определенному порту

**sudo ufw allow from** ip\_address/mask – указать диапазон IP адресов которым будет разрешен доступ ко всем портам

**sudo ufw allow from** ip\_address/mask **to any port** [port] – задать доступ только к определенному порту диапазону IP адресов

**Удаление правил**

**sudo ufw status numbered** – узнаем какие правила сейчас активны и их номер

**sudo ufw delete** номерПравила – удаляет правило

**sudo ufw delete allow** [protocol\_name][port] – удаляет правило

**Отключение Firewall, сброс правил**

**sudo ufw disable –** отключение firewall

**sudo ufw reset** – сброс правил

**Логи**

**ls /var/log/ufw\*** - просмотр файлов логов

**sudo ufw logging on** – включить логирование

**sudo ufw logging off** – выключить логирование

**sudo ufw logging [off][low][medium][high][full]** – задать уровень логирования

* **off** - отключен.
* **low**- регистрирует все заблокированные пакеты, не соответствующие заданной политике (с ограничением скорости), а также пакеты, соответствующие зарегистрированным правилам.
* **medium**- все то, что при значении **low.**Плюс все разрешенные пакеты, не соответствующие заданной политике, все недопустимые пакеты, и все новые соединения. Все записи ведутся с ограничением скорости.
* **high**-работает также как и **medium.**Плюс все пакеты с ограничением скорости.
* **full** - также как и **high,**но без ограниения скорости.