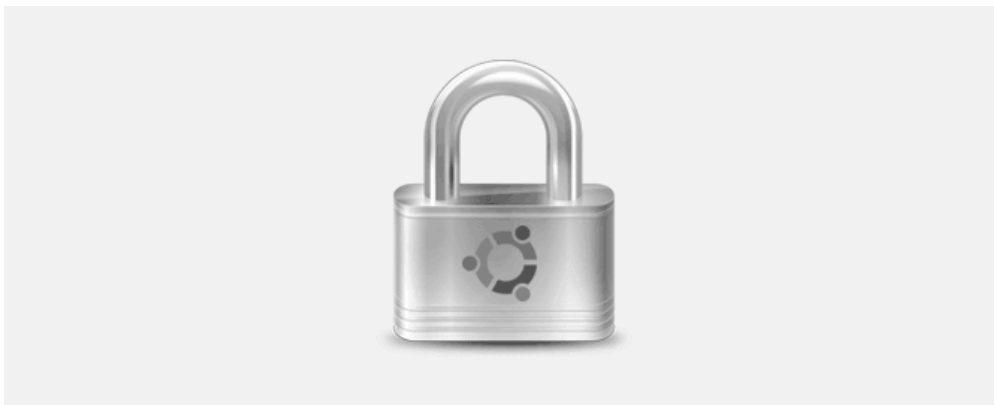


Как включить и использовать файрвол UFW в Ubuntu

QUAZAR 2,811



Ищете способ улучшить безопасность компьютера с Ubuntu? Вы не ошибетесь, включив файрвол UFW.

Еще по теме: [Как отследить Linux компьютер с помощью Prey](#)

Итак, вы только что установили Ubuntu Desktop. Вы, вероятно, предполагаете, что система уже довольно безопасна. Это предположение, по большей части, правильно. Однако все мы знаем, что любой компьютер, подключенный к сети, небезопасен. Мы всегда должны делать все возможное, чтобы защитить его. Несмотря на то, что «из коробки» рабочий стол Ubuntu будет экспоненциально более безопасным, чем, скажем, рабочий стол Windows, это не означает, что вам не нужно предпринимать дополнительные меры для его защиты.

Файрвол UFW

UFW — это инструмент для настройки сетевой защиты Ubuntu. Он разработан для легкой настройки iptables и предоставляет простой способ создания сетевой защиты для IPv4 и IPv6.

После установки Ubuntu для улучшения безопасности надо предпринять один конкретный шаг — это включить файрвол в Ubuntu. Да, трудно поверить, что он по умолчанию отключен, но это так.

Изначально брандмауэр Ubuntu Desktop (также называемый Uncomplicated Firewall — или UFW) неактивен.

Получение статуса работы фаервола UFW

Выполнение команды `sudo ufw status` указывает, что брандмауэр в новой установке Ubuntu Desktop 18.04 неактивен.

```
sudo ufw status
```

```
spysoftnet@Ubuntu: ~  
Файл Правка Вид Поиск Терминал Справка  
spysoftnet@Ubuntu:~$ sudo ufw status  
[sudo] пароль для spysoftnet:  
Состояние: неактивен  
spysoftnet@Ubuntu:~$
```

Для более полного отображения информации введите:

```
sudo ufw status verbose
```

Для отображения в виде формата numbered:

```
sudo ufw status numbered
```

Включить / отключить фаервол UFW

Чтобы включить фаервол UFW, выполните команду:

```
sudo ufw enable
```

```
spysoftnet@Ubuntu: ~  
Файл Правка Вид Поиск Терминал Справка  
spysoftnet@Ubuntu:~$ sudo ufw enable  
Межсетевой экран включён и будет запускаться при запуске системы  
spysoftnet@Ubuntu:~$
```

В этот момент брандмауэр активен и также запускается при перезагрузке системы. Однако есть одна маленькая проблема: брандмауэр теперь работает и блокирует весь входящий трафик. Далее я покажу как добавлять правило и открывать необходимые порты.

Чтобы отключить фаервол UFW, выполните команду:

```
sudo ufw disable
```

Открыть / закрыть порт в фаерволе UFW

Для открытия порта используйте команду (в нашем примере SSH):

```
sudo ufw allow 22
```

```
spysoftnet@Ubuntu: ~  
Файл Правка Вид Поиск Терминал Справка  
spysoftnet@Ubuntu:~$ sudo ufw allow 22  
[sudo] пароль для spysoftnet:  
\Правило добавлено  
Правило добавлено (v6)  
spysoftnet@Ubuntu:~$ \
```

Для закрытия порта используйте команду:

```
sudo ufw deny 22
```

Еще по теме: Защита ноутбука с Linux

Добавить / удалить правило в UFW

Правила могут быть добавлены с использованием нумерованного формата:

```
sudo ufw insert 1 allow 80
```

Для удаления правила используйте команду delete:

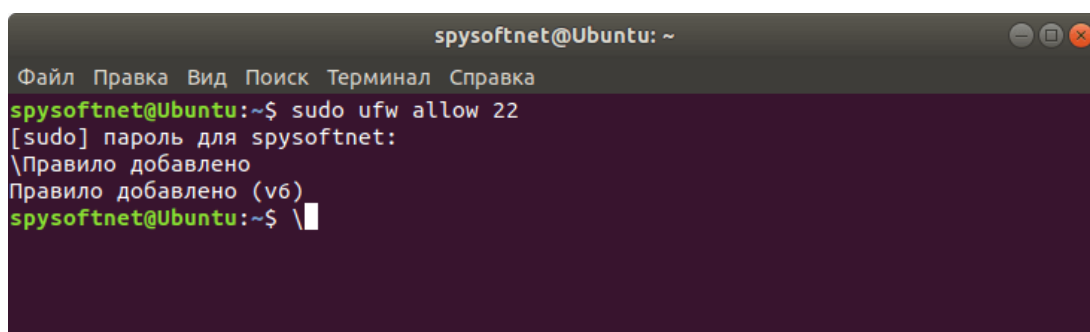
```
sudo ufw delete deny 22
```

Открыть доступ по SSH в UFW

Например, вам нужно удаленно подключиться к своему компьютеру. Скорее всего, вы будете использовать SSH для получения доступа, но при базовой настройке брандмауэра SSH-соединения запрещены. Другими словами, вам нужно разрешить безопасное подключение SSH к своему компьютеру. Для этого вы можете использовать команду `ufw` следующим образом:

```
sudo ufw allow 22
```

Вы должны увидеть, что правило было добавлено.



```
spysoftnet@Ubuntu: ~  
Файл Правка Вид Поиск Терминал Справка  
spysoftnet@Ubuntu:~$ sudo ufw allow 22  
[sudo] пароль для spysoftnet:  
Правило добавлено  
Правило добавлено (v6)  
spysoftnet@Ubuntu:~$ \
```

Также можно разрешить доступ к порту с определенных компьютеров или сетей. Следующий пример разрешает на этом компьютере доступ по SSH с адреса 192.168.0.2 на любой IP адрес:

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

Замените 192.168.0.2 на 192.168.0.0/24 чтобы разрешить доступ по SSH для всей подсети.

Теперь вы можете закрепить оболочку на настольном компьютере. Конечно, чтобы сделать SSH-соединения более безопасными, всегда используйте авторизацию по ключу.