

Настройка брандмауэра с помощью UFW Ubuntu Server

Введение

Настройка работающего брандмауэра имеет решающее значение для защиты вашего облачного сервера. Раньше настройка брандмауэра выполнялась с помощью сложных или непонятных утилит. Многие из этих утилит (например, iptables) имеют множество встроенных функций, но требуют от пользователя дополнительных усилий для их изучения и понимания.

Другой вариант — UFW, или Несложный межсетевой экран. UFW — это интерфейс, целью iptables которого является обеспечение более удобного интерфейса, чем у других утилит управления брандмауэром. UFW хорошо поддерживается сообществом Linux и обычно устанавливается по умолчанию во многих дистрибутивах.

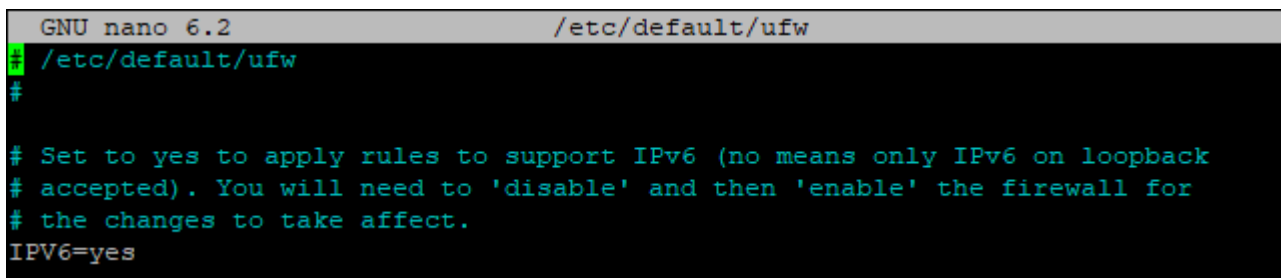
В этом руководстве вы настроите брандмауэр с помощью UFW для защиты облачного сервера Ubuntu или Debian. Вы также узнаете, как настроить правила UFW по умолчанию, чтобы разрешить или запретить соединения для портов и IP-адресов, удалить созданные вами правила, отключить и включить UFW, а также сбросить все настройки обратно к настройкам по умолчанию, если вы предпочитаете.

Предварительные условия

Чтобы следовать этому руководству, вам понадобится сервер под управлением Ubuntu или Debian. На вашем сервере должен быть пользователь без полномочий root с привилегиями sudo. Чтобы настроить это для Ubuntu, следуйте нашему руководству по начальной настройке сервера с Ubuntu 20.04. Чтобы настроить это для Debian, следуйте нашему руководству по начальной настройке сервера с Debian 11. Оба этих руководства по начальной настройке сервера гарантируют, что на вашем компьютере установлен UFW и что у вас есть безопасная среда, которую вы можете использовать для практики создания правил брандмауэра.

Использование IPv6 с UFW

```
sudo nano /etc/default/uw
```



```
GNU nano 6.2 /etc/default/uw
# /etc/default/uw
#
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=yes
```

После внесения изменений сохраните и выйдите из файла. Если вы используете nano, нажмите

CTRL + X, Y, а затем ENTER.

Теперь перезапустите брандмауэр, сначала отключив его:

```
sudo ufw disable
```

```
alisa@linux:~$ sudo ufw disable
Firewall stopped and disabled on system startup
alisa@linux:~$ █
```

Затем включите его снова:

```
sudo ufw enable
```

```
alisa@linux:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
alisa@linux:~$ █
```

Ваш брандмауэр UFW теперь настроен для настройки брандмауэра как для IPv4, так и для IPv6, когда это необходимо. Далее вы настроите правила по умолчанию для подключений к брандмауэру.

From:
<http://git.wwooss.ru/> - worldwide open-source software

Permanent link:
http://git.wwooss.ru/doku.php?id=software:linux_server:ubuntu_server_setting_firewall_ufw&rev=1709271601

Last update: 2024/03/01 08:40

