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 iptableskоторого является обеспечение более удобного интерфейса, чем у других утилит управления брандмауэром. UFW хорошо поддерживается сообществом Linux и обычно устанавливается по умолчанию во многих дистрибутивах.

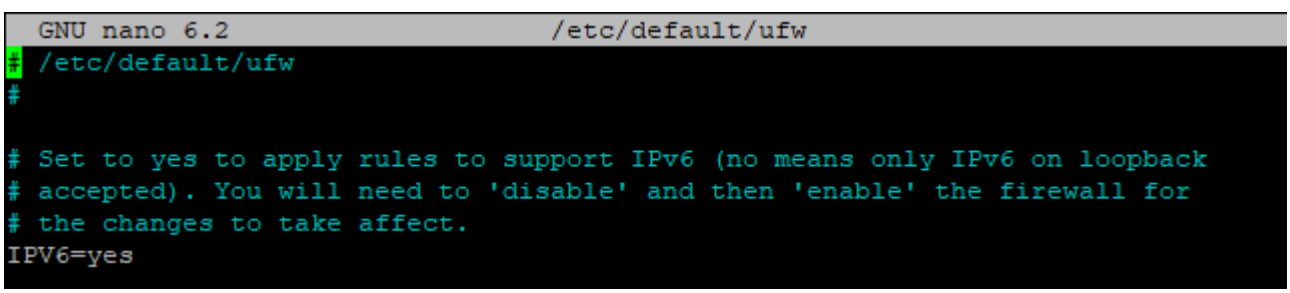
В этом руководстве вы настроите брандмауэр с помощью UFW для защиты облачного сервера Ubuntu или Debian. Вы также узнаете, как настроить правила UFW по умолчанию, чтобы разрешить или запретить соединения для портов и IP-адресов, удалить созданные вами правила, отключить и включить UFW, а также сбросить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



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.

Настройка параметров UFW по умолчанию

Вы можете повысить эффективность своего брандмауэра, определив правила по умолчанию для разрешения и запрета подключений. По умолчанию UFW запрещает все входящие соединения и разрешает все исходящие соединения. Это означает, что любой, кто попытается подключиться к вашему серверу, не сможет подключиться, в то время как любое приложение на сервере может подключиться извне. Чтобы обновить правила по умолчанию, установленные UFW, сначала обратитесь к правилу входящих подключений:

```
sudo ufw default deny incoming
```

```
alisa@linux:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
alisa@linux:~$
```

Затем обратитесь к правилу исходящих соединений:

```
sudo ufw default allow outgoing
```

```
alisa@linux:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
alisa@linux:~$
```

Примечание. Если вы хотите ввести более строгие ограничения, вы можете

запретить все исходящие запросы. Этот вариант основан на личных предпочтениях. Например, если у вас есть общедоступный облачный сервер, это может помочь предотвратить любые подключения к удаленной оболочке. Однако это делает ваш брандмауэр более громоздким в управлении, поскольку вам также придется устанавливать правила для всех исходящих соединений. Вы можете установить это значение по умолчанию, выполнив следующие действия:

```
sudo ufw default deny outgoing
```

```
alisa@linux:~$ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
alisa@linux:~$
```

Разрешение подключений к брандмауэру

Разрешение подключений требует изменения правил брандмауэра, что можно сделать, введя команды в терминале. Например, если вы сейчас включите брандмауэр, он запретит все входящие соединения. Если вы подключены к своему серверу через SSH, это будет проблемой, поскольку вы будете заблокированы на своем сервере. Чтобы этого не произошло, включите SSH-подключения к вашему серверу:

```
sudo ufw allow ssh
```

Если ваши изменения прошли успешно, вы получите следующий вывод:

```
alisa@linux:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
alisa@linux:~$
```

UFW поставляется с некоторыми настройками по умолчанию, такими как sshкоманда, использованная в предыдущем примере. Альтернативно вы можете разрешить входящие подключения к порту 22/tcp, который использует протокол управления передачей (TCP) для достижения той же цели:

```
sudo ufw allow 22/tcp
```

```
alisa@linux:~$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
alisa@linux:~$
```

Если ваш SSH-сервер работает на порту **2222**, вы можете разрешить соединения с тем же синтаксисом, но заменить его на порт 2222. Обратите внимание, что если вы используете номер порта сам по себе, это также повлияет **tcp** на :**udp**

```
sudo ufw allow 2222/tcp
```

```
alisa@linux:~$ sudo ufw allow 2222/tcp
Rule added
Rule added (v6)
alisa@linux:~$
```

Защита веб-серверов

Чтобы защитить веб-сервер с помощью протокола передачи файлов (FTP), вам необходимо разрешить соединения для порта **80/tcp**.

Разрешение подключений для порта 80полезно для веб-серверов, таких как Apache и Nginx, которые прослушивают запросы HTTP-соединения. Для этого разрешите подключения к порту **80/tcp:**

```
sudo ufw allow 80/tcp
```