Настройка брандмауэра с UFW в Ubuntu

- Оригинал статьи: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-18-04-ru
- Основы UFW: распространенные правила и команды брандмауэра.

Введение

UFW (Uncomplicated Firewall или «простой брандмауэр») представляет собой интерфейс iptables, предназначенный для упрощения процесса настройки брандмауэра. Хотя iptables — надежный и гибкий инструмент, начинающим бывает сложно научиться использовать его для правильной настройки брандмауэра.

Установка:

```
sudo apt install ufw
```

Использование IPv6 с UFW (опционально)

```
sudo vi /etc/default/ufw
```

Убедитесь, что параметр IPV6 имеет значение yes. Конфигурация должна выглядеть следующим образом:

/etc/default/ufw excerpt

```
IPV6=yes
```

Настройка политик по умолчанию

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

Разрешение подключений SSH

```
sudo ufw allow ssh
```

Эта команда создаст правила брандмауэра, которые разрешат все соединения на порту 22, который демон SSH прослушивает по умолчанию. UFW знает, какой порт имеет в виду команда `allow ssh`, потому что он указан как услуга в файле `/etc/services`.

или

```
sudo ufw allow 22
```

Активация UFW

```
sudo ufw enable
```

Статус

посмотреть заданные правила

```
sudo ufw status verbose
```

Разрешение других соединений

- Соединения HTTP на порту 80, которые используются веб-серверами без шифрования, с помощью команды `sudo ufw allow http` или `sudo ufw allow 80`
- соединения HTTPS на порту 443, которые используются веб-серверами с шифрованием, с помощью команды `sudo ufw allow https` или `sudo ufw allow 443`

Определенные диапазоны портов

Например, чтобы разрешить соединения X11, которые используют порты `6000-6007`, нужно использовать следующие команды:

```
sudo ufw allow 6000:6007/tcp
sudo ufw allow 6000:6007/udp
```

Когда вы указываете диапазоны портов с помощью UFW, вы должны указать протокол (tcp или udp), к которому должны применяться эти правила. Мы не упоминали этого ранее, поскольку если протокол не указать, оба протокола будут разрешены, что подходит для большинства случаев.

Конкретные IP-адреса

При работе с UFW вы также можете указывать конкретные IP-адреса. Например, если вы хотите разрешить соединения с определенного IP-адреса, например с рабочего или домашнего адреса 203.0.113.4, вам нужно использовать опцию from, а затем указать IP-адрес:

```
sudo ufw allow from 203.0.113.4
```

Также вы можете указать определенный порт, к которому IP-адресу разрешено подключаться. Для этого нужно добавить опцию to any port, а затем указать номер порта. Например, если вы хотите разрешить IP-адресу 203.0.113.4 подключаться к порту 22 (SSH), нужно использовать следующую команду:

```
sudo ufw allow from 203.0.113.4 to any port 22
```

Подсети

Если вы хотите разрешить подсеть IP-адресов, вы можете указать маску сети с помощью нотации CIDR. Например, если вы хотите разрешить все IP-адреса в диапазоне от 203.0.113.1 до 203.0.113.254, вы можете использовать следующую команду:

```
sudo ufw allow from 203.0.113.0/24
```

Также вы можете указывать порт назначения, к которому разрешено подключаться подсети 203.0.113.0/24. В качестве примера мы используем порт 22 (SSH):

```
sudo ufw allow from 203.0.113.0/24 to any port 22
```

Подключения к определенному сетевому интерфейсу

Если вы хотите создать правило брандмауэра, применимое только к определенному сетевому интерфейсу, вы можете использовать для этого опцию «allow in on», а затем указать имя сетевого интерфейса.

Прежде чем продолжить, вам может понадобиться просмотреть сетевые интерфейсы. Для этого нужно использовать следующую команду:

```
ip addr
```

Output Excerpt

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state
. . .
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group
default
. . .
```

В выделенной части результатов показаны имена сетевых интерфейсов. Обычно они носят имена вида eth0 или enp3s2.

Если на вашем сервере имеется публичный сетевой интерфейс под названием eth0, вы можете разрешить трафик HTTP (порт 80) для этого интерфейса с помощью следующей команды:

```
sudo ufw allow in on eth0 to any port 80
```

Это позволит вашему серверу принимать запросы HTTP из публичной части интернета.

Если вы хотите использовать сервер базы данных MySQL (порт 3306) для прослушивания соединений на интерфейсе частной сети (например, eth1), вы можете использовать

следующую команду:

```
sudo ufw allow in on eth1 to any port 3306
```

Это позволит другим серверам в вашей частной сети подключаться к вашей базе данных MySQL.

Запрет соединений

Если вы не изменяли политику по умолчанию для входящих соединений, UFW настроен на запрет всех входящих соединений. Это упрощает процесс создания защищенной политики брандмауэра, поскольку вам нужно создавать правила, прямо разрешающие соединения через конкретные порты и IP-адреса.

Однако в некоторых случаях вам может понадобиться запретить определенные соединения по IP-адресу источника или подсети, например, в случае атаки с этого адреса. Если вы захотите изменить политику по умолчанию для входящих соединений на allow (что не рекомендуется), вам нужно будет создать правила deny для любых служб или IP-адресов, которым вы не хотите разрешать подключение.

Для записи правил deny можно использовать описанные выше команды, заменяя allow на deny.

Например, чтобы запретить соединения по протоколу HTTP, вы можете использовать следующую команду:

```
  sudo ufw deny http
```

Если вы захотите запретить все подключения с IP-адреса 203.0.113.4, вы можете использовать следующую команду:

```
  sudo ufw deny from 203.0.113.4
```

Удаление правил

Знать процедуру удаления правил брандмауэра так же важно, как и знать процедуру их создания. Существует два разных способа указывать правила для удаления: по номеру правила или по фактическому правилу (так же, как правила задавались при их создании). Начнем с метода удаления по номеру правила, поскольку этот метод проще.

По номеру правила

Если вы используете номер правила для удаления правил брандмауэра, прежде всего нужно получить список правил брандмауэра. Команда UFW status имеет опцию отображение номеров рядом с каждым правилом, как показано здесь:

```
  sudo ufw status numbered
```

Numbered Output:

```
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    15.15.15.0/24
[ 2] 80                         ALLOW IN    Anywhere
```

Если мы решим удалить правило 2, разрешающее соединения через порт 80 (HTTP), мы можем указать его в команде UFW delete, как показано здесь:

```
sudo ufw delete 2
```

После этого откроется диалогового окна подтверждения удаления правила 2, разрешающего соединения HTTP. Если вы включили поддержку IPv6, вы можете также удалить соответствующее правило для IPv6.

По фактическому имени правила

Вместо номеров правил можно указывать фактические имена удаляемых правил. Например, если вы хотите удалить правило allow http, вы можете использовать следующую команду:

```
sudo ufw delete allow http
```

Также вы можете указать это правило как allow 80, а не указывать имя службы:

```
sudo ufw delete allow 80
```

Этот метод удалит правила IPv4 и IPv6, если они существуют.

Проверка состояния и правил UFW

Вы можете проверить состояние UFW в любое время с помощью следующей команды:

```
sudo ufw status verbose
```

Если UFW отключен (по умолчанию), вы увидите примерно следующее:

Output

```
Status: inactive
```

Если UFW активен (т. е. вы выполнили шаг 3), в результатах будет показано, что он активен, и будет выведен список заданных правил. Например, если настройки брандмауэра разрешают соединения SSH (порт 22) из любого источника, результат может выглядеть примерно так:

Output

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
```

Используйте команду `status`, если хотите проверить настройку брандмауэра UFW.

Отключение или сброс UFW (необязательно)

Если вы решите прекратить использовать UFW, вы можете отключить его с помощью следующей команды:

```
sudo ufw disable
```

Любые правила, созданные с помощью UFW, больше не будут активными. Если впоследствии вы захотите активировать UWF, вы всегда сможете использовать команду sudo ufw enable.

Если вы уже настроили правила UFW, но решите начать заново, вы можете использовать команду reset:

```
sudo ufw reset
```

Эта команда отключит UFW и удалит все ранее заданные правила. Помните, что если вы изменяли политики по умолчанию, их первоначальные настройки не восстановятся. Это позволит заново начать настройку UFW.