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 iptablesкоторого 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.

Установка UFW

По умолчанию начиная с Ubuntu 18.04 программа поставляется с установленной UFW. Однако, для более ранних систем, вы должны выполнить команду ниже

```
apt-get install ufw
```

Для того, чтобы проверить, является ли UFW запущенным:

```
systemctl status ufw
```

```
alisa@linux:~$ systemctl status ufw
● ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: e>
     Active: active (exited) since Thu 2024-02-29 21:21:28 MSK; 13h ago
       Docs: man:ufw(8)
   Main PID: 800 (code=exited, status=0/SUCCESS)
        CPU: 2ms

фев 29 21:21:28 linux systemd[1]: Starting Uncomplicated firewall...
фев 29 21:21:28 linux systemd[1]: Finished Uncomplicated firewall.
lines 1-9/9 (END)
```

Чтобы проверить, является ли он активным или неактивным

```
sudo ufw status
```

Если он активен, вы получите вывод ниже

```
alisa@linux:~$ sudo ufw status
[sudo] password for alisa:
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW       Anywhere
443                        ALLOW       Anywhere
OpenSSH                    ALLOW       Anywhere
```

Если он неактивен, вы получите вывод ниже

```
alisa@linux:~$ sudo ufw status
Status: inactive
alisa@linux:~$
```

Чтобы включить UFW с набором правил по умолчанию, запустите

```
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:~$
```

Чтобы отключить запуск брандмауэра

```
sudo ufw disable
```

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

Использование IPv6 с UFW

```
sudo nano /etc/default/ufw
```

```
  GNU nano 6.2                         /etc/default/ufw
# /etc/default/ufw
#

# 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.

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:~$
```

Если вы хотите удалить правило, запустите

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

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

Чтобы увидеть все услуги, которые могут быть разрешены или запрещены в системе проверьте файл /etc/services.

```
cat /etc/services | less
```

```
alisa@linux:~$ cat /etc/services | less
# Network services, Internet style
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/servi
ce-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
domain          53/tcp                          # Domain Name Server
domain          53/udp
bootps          67/udp
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
finger          79/tcp
```

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
```

UFW обычно предоставляет профилям правила, необходимые для работы веб-сервера. В противном случае профили веб-сервера можно сохранить как **«WWW»** и открыть как **ftp** или **tcp**, как в следующих примерах:

```
sudo ufw allow www
```

Вы также можете использовать **ftp** или порт **21**, чтобы разрешить FTP-соединения:

```
sudo ufw allow ftp
```

```
sudo ufw allow 21/tcp
```

Для FTP-подключений вам также необходимо разрешить подключения для порта 20:

```
sudo ufw allow 20/tcp
```

Ваши настройки будут зависеть от того, какие порты и службы вам нужно открыть, и может потребоваться тестирование. Не забудьте также оставить разрешенным ваше SSH-соединение.

Указание диапазонов портов

Вы также можете указать диапазоны портов, которые можно разрешить или запретить с помощью UFW. Для этого необходимо сначала указать порт в нижней части диапазона, после него поставить двоеточие (:), а затем указать верхний конец диапазона. Наконец, вы должны указать, к какому протоколу (или tcpили udp) вы хотите применить правила.

Например, следующая команда разрешит TCP-доступ ко всем портам от 1000 до 2000 включительно:

```
sudo ufw allow 1000:2000/tcp
```

Аналогично, следующая команда запретит UDP-подключения к каждому порту от 1234до 4321:

```
sudo ufw deny 1234:4321/udp
```

```
alisa@linux:~$ sudo ufw deny 1234:4321/udp
Rule added
Rule added (v6)
alisa@linux:~$
```

Указание IP-адресов

Вы можете разрешить подключения с определенного IP-адреса, как показано ниже. Обязательно замените IP-адрес своей собственной информацией:

```
sudo ufw allow from 192.165.1.117
```

```
alisa@linux:~$ sudo ufw allow from 192.165.1.117
Rule added
alisa@linux:~$
```

Запрет соединений

Если вы хотите открыть все порты вашего сервера (что не рекомендуется), вы можете разрешить все соединения, а затем запретить любые порты, к которым вы не хотите предоставлять доступ. В следующем примере показано, как запретить доступ к порту 80:

```
sudo ufw deny 80/tcp
```