Instalacja i konfiguracja Firewall-a na Ubuntu

Ubuntu zawiera kilka pakietów, które zawierają narzędzia do zarządzania zaporą. Podstawowym pakietem jest Iptables, który jest instalowany jako część systemu podstawowego. Pakiet ten jest dość skomplikowany w konfiguracji wiec dla poczatkujących użytkowników optymalny jest prosty pakiet UFW.
UFW (Uncomplicated Firewall) jest przyjaznym dla użytkownika interfejsem do zarządzania regułami zapory iptables, a jego głównym celem, jak sama nazwa wskazuje jest nieskomplikowane zarządzanie zaporą.
Instalacja UFW:

```
sudo apt install ufw
```

Sprawdzenie status UFW po instalacji:

```
sudo ufw status verbose
Status: inactive
```

Domyślnie UFW po instalacji jest nieaktywy.
Jeśli UFW jest aktywne, dane wyjściowe będą wyglądać podobnie do poniższych:

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

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Domyślnie UFW blokuje wszystkie połączenia przychodzące i zezwala na wszystkie połączenia wychodzące. Oznacza to, że każdy, kto próbuje uzyskać dostęp do maszyny wirtualnej, nie będzie mógł się połączyć, chyba, że zostanie otwarty port, podczas gdy wszystkie aplikacje i usługi działające na maszynie będą mogły uzyskać dostęp na zewnątrz.

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

Polecenia te ustawiają wartości domyślne na odmawianie połączeń przychodzących i zezwalają na połączenia wychodzące. Same ustawienia domyślne UFW nie są wystarczające,

ponieważ maszyny wirtualne zazwyczaj muszą odpowiadać na żądania połączeń przychodzących z zewnątrz.
Jeżeli zostałaby teraz włączona zapora sieciowa UFW, odmówi ona wszystkim połączeniom przychodzącym. Oznacza to, że należy utworzyć reguły, które zezwalają na połączenia przychodzące – na przykład połączenia SSH lub HTTP – jeżeli maszyna ma odpowiadać na tego typu żądania.
Aby skonfigurować zaporę sieciową maszyny tak, aby zezwalała na **połączenia przychodzące SSH**, można użyć następującego polecenia:

```
# sudo ufw allow ssh
Rules updated
```

Spowoduje to utworzenie reguł zapory, które zezwalają na wszystkie połączenia na porcie 22 , który jest domyślnie portem nasłuchiwanym przez demona SSH.
Możemy jednak napisać równoważną regułę, określając port zamiast nazwy usługi. Na przykład to polecenie działa tak samo jak powyżej:

```
# sudo ufw allow 22
```

Jeśli serwer SSH nasłuchuje na porcie innym niż domyślny port 22, należy otworzyć ten port. Na przykład serwer ssh nasłuchuje na porcie 8822, tak więc można użyć następującego polecenia, aby zezwolić na połączenia na tym porcie:

```
# sudo ufw allow 8822/tcp
```

Teraz, gdy zapora sieciowa UFW jest skonfigurowana tak, aby zezwalała na przychodzące połączenia SSH, można ją włączyć:

```
# sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)?
y
Firewall is active and enabled on system startup
```

Zostanie wyświetlone ostrzeżenie, że włączenie zapory może zakłócić istniejące połączenia ssh, aby kontynuować należy wpisać y, aby potwierdzić i kliknąć klawisz Enter.
W zależności od aplikacji oraz usług uruchomionych na maszynie wirtualnej należy także zezwolić na dostęp połączeń przychodzących do niektórych innych portów.

Poniżej znajduje się kilka przykładów, w jaki sposób zezwolić na połączenia przychodzące do niektórych z najbardziej popularnych usług:

- **otworzenie http na porcie 80**

Połączenia HTTP mogą być dozwolone za pomocą następującego polecenia:

```
# sudo ufw allow http
```

lub zamiast profilu http można użyć numeru portu 80:

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

- **otworzenie https na porcie 443**

Połączenia HTTPS mogą być dozwolone za pomocą następującego polecenia:

```
# sudo ufw allow https
```

Aby osiągnąć to samo zamiast https, można użyć numeru portu 443:

```
# sudo ufw allow 443/tcp
```

Natomiast zamiast zezwalać na połączenia do pojedynczych portów, UFW pozwala użytkownikowi na udzielenie dostępu do zakresów portów. Aby zezwolić na połączenie w zakresach portów w UFW, należy określić protokół: tcp lub udp.

- **otworzenie zakresu portów**

Na przykład, aby zezwolić na dostęp połączeń na portach od 7100 do 7200 na tcp i udp, należy wydać następujące polecenie:

```
# sudo ufw allow 7100:7200/tcp
# sudo ufw allow 7100:7200/udp
```

- **usuwanie reguł**

Istnieją dwa różne sposoby usuwania reguł UFW:

- według numeru reguły
- określenia aktualnej reguły

Usuwanie reguł UFW według numeru reguły jest łatwiejsze. Aby usunąć regułę za pomocą numeru reguły, należy znaleźć numer reguły, która ma zostać usunięta – można to zrobić za pomocą następującego polecenia:

```
# sudo ufw status numbered

 Status: active
  To                         Action      From  --                         -
-----      ----
 [ 1] 22/tcp                     ALLOW IN    Anywhere
 [ 2] 80/tcp                     ALLOW IN    Anywhere
 [ 3] 8080/tcp                   ALLOW IN    Anywhere
```

Aby usunąć regułę numer 3, zezwalającą na połączenia z portem 8080, należy użyć następującego polecenia:

```
# sudo ufw delete 3
```

Druga metoda polega na usunięciu reguły poprzez określenie aktualnej reguły. Na przykład jeśli dodano regułę otwarcia portu 8069, można ją usunąć za pomocą:

```
# sudo ufw delete allow 8069
```

- **wyłączenie UFW**

Jeśli z jakiegoś powodu trzeba zatrzymać UFW i dezaktywować wszystkie reguły, można użyć polecenia:

```
# sudo ufw disable
```

- **włączenie UFW**

Aby ponownie włączyć UFW i aktywować wszystkie reguły, należy wpisać:

```
# sudo ufw enable
```

- **reset UFW**

Resetowanie UFW wyłączy UFW i usunie wszystkie obecnie aktywne reguły. Jest to pomocne, jeśli zajdzie potrzeba przywrócenia wszystkich zmian i rozpoczęcie konfiguracji od nowa.

Aby zresetować UFW, wystarczy wpisać następujące polecenie:

```
# sudo ufw reset
```