Konfigurowanie Firewall w Ubuntu Linux

Konfigurację zapory wykonamy za pomocą nakładki graficznej na **iptables** – **gufw**. Aby ją zainstalować wydajemy polecenie:

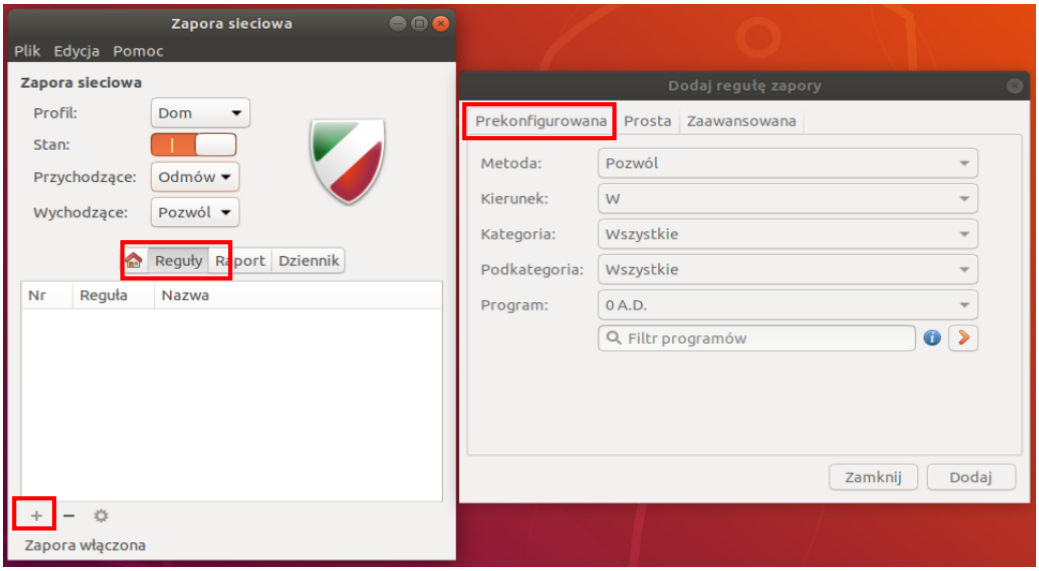
```
sudo apt-get install gufw
```

Po zainstalowaniu, uruchamiamy program **gufw** i wyświetlony zostaje aktualny stan zapory. Aby można było wprowadzać zmiany, trzeba odblokować aplikację zmieniając stan na **unlock**.

Dodawanie reguły prekonfigurowanej

1. Po uruchomieniu programu odblokowujemy dostęp do konfiguracji (**unlock**).
2. Ustawiamy politykę, dla strumieni **Przychodzących** na **Odmów**.

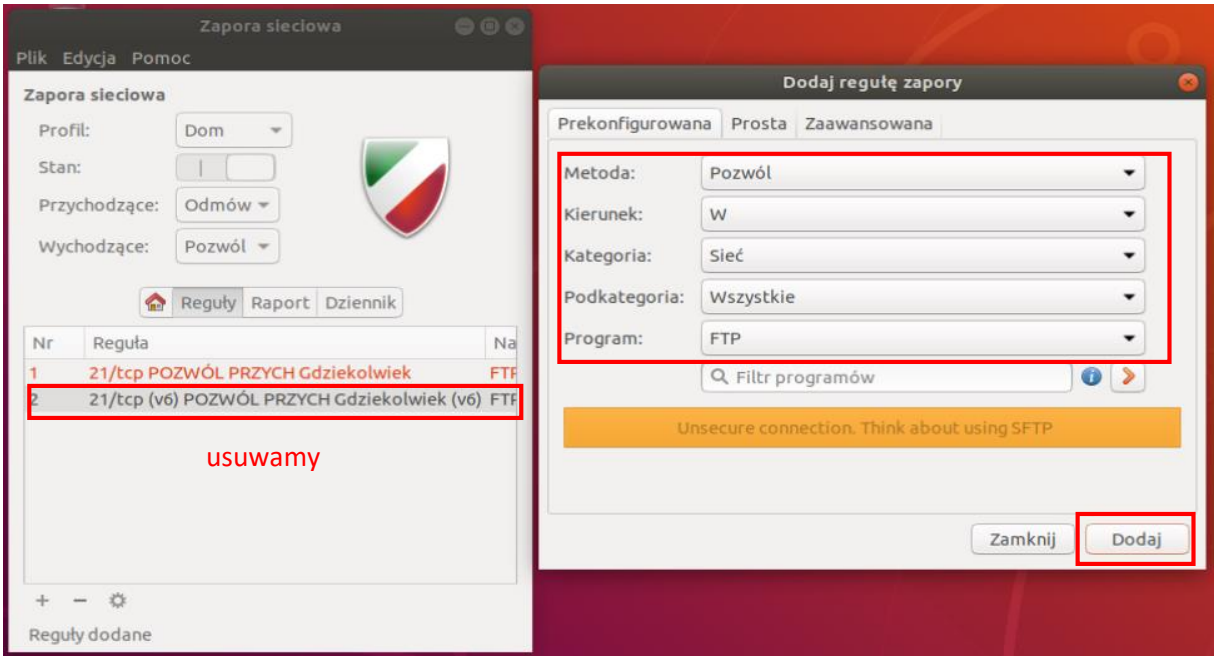
3. Wybieramy tworzenie nowej reguły **Prekonfigurowanej**.



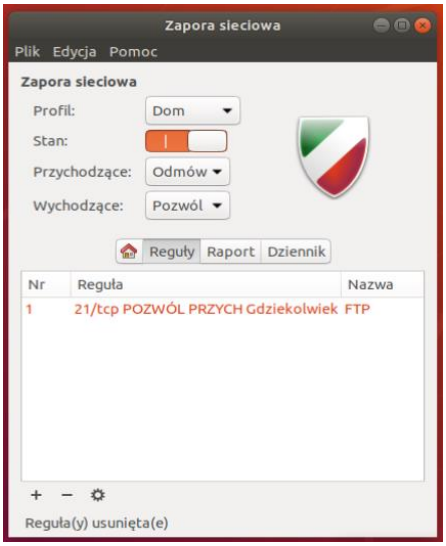
4. Ustawimy możliwość połączenia z serwerem ftp na tym komputerze. W tym celu wprowadzamy ustawienia:

- **Metoda: pozwól**
- **Kierunek: w**
- **Kategoria: sieć**
- **Podkategoria: transfer plików (**jeżeli nie widać w tej podkategorii to ustawiamy **Wszystkie)**
- **Program: FTP**

5. Klikamy **dodaj**.
6. Następnie usuwamy (-) reguły utworzone dla IPv6.

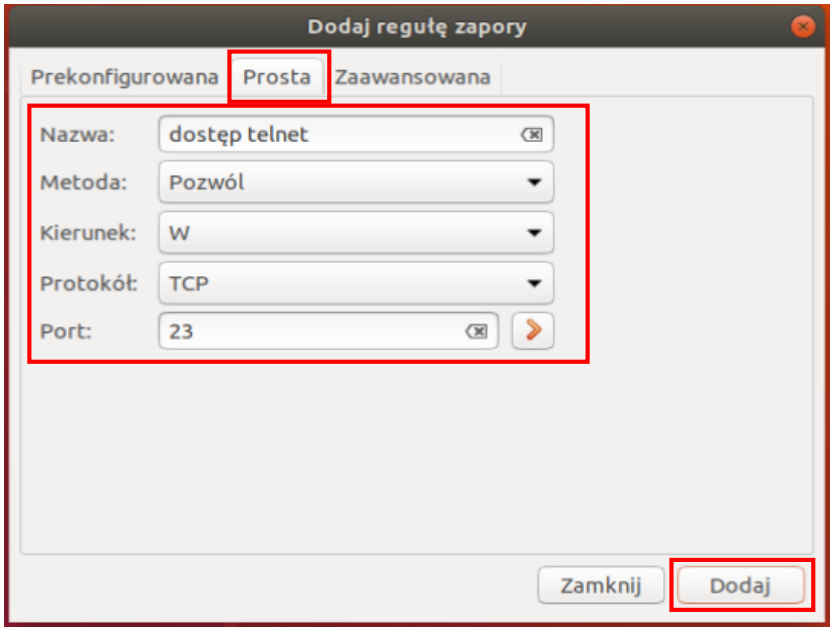


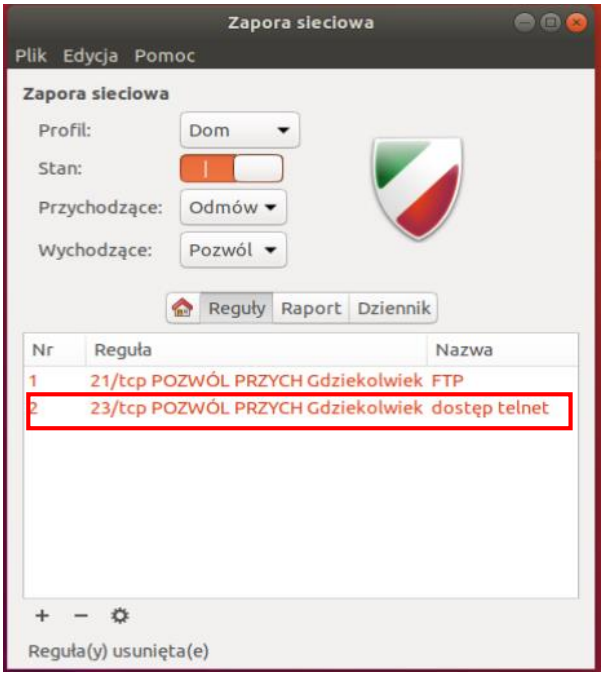
7. Reguła została dodana.



Dodawanie reguły prostej

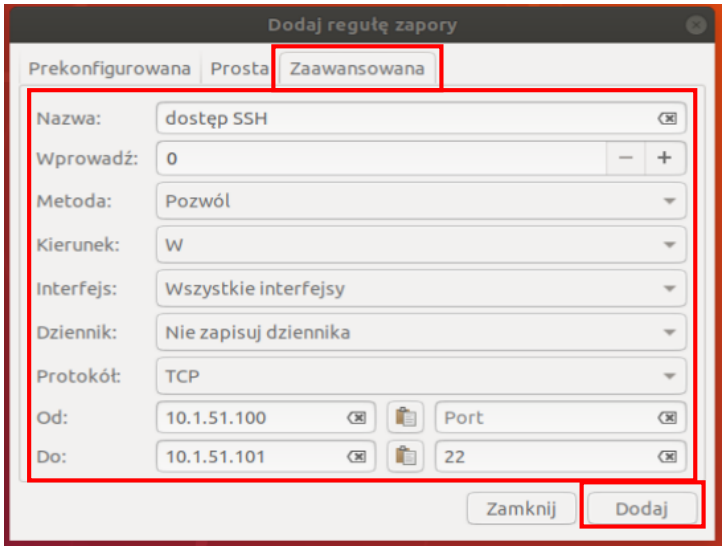
1. Po uruchomieniu programu odblokowujemy dostęp do konfiguracji (unlock).
2. Ustawiamy politykę, dla strumieni **Przychodzących** na **Odmów**.
3. Wybieramy tworzenie nowej reguły **Prostej**.
4. Ustawimy możliwość nawiązanie połączenia z serwerem Telnet, standardowo działającym na porcie 23 na tym komputerze. W tym celu wprowadzamy ustawienia:
5. **Metoda: pozwól**
6. **Kierunek: w**
7. **Protokół: TCP**
8. **Port: 23**
9. Klikamy **Add**.
10. Następnie usuwamy reguły utworzone dla IPv6.
11. Reguła została dodana.

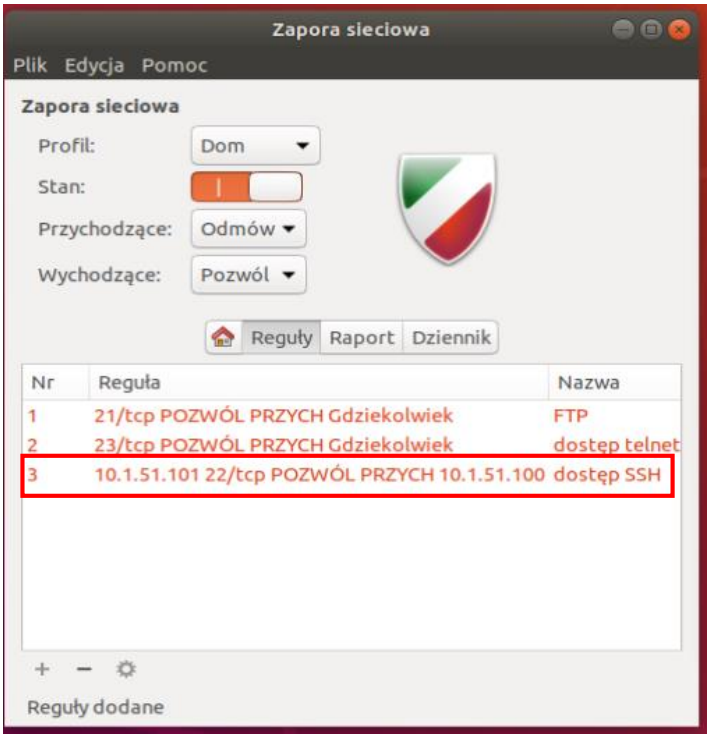




Dodawanie reguły zaawansowanej

1. Po uruchomieniu programu odblokowujemy dostęp do konfiguracji (unlock).
2. Ustawiamy politykę, dla strumieni **Przychodzących** na **Odmów**.
3. Wybieramy tworzenie nowej reguły **Zaawansowanej**.
   W regule tej można wskazać interfejsy lub pozostawić domyślne działanie reguły na wszystkich interfejsach. Zaawansowana reguła pozwala na określenie adresu źródłowego (np. 10.1.51.100) i docelowego (np. do: 10.1.51.101) oraz numerów portów. Pozostawienie numeru portu pustego oznacza wybór dowolnego portu.
4. Ustawimy możliwość nawiązanie połączenia z serwerem **SSH**, standardowo działającym na porcie 22 na tym komputerze, tylko dla adresu10.1.51.100 z dowolnego portu. W tym celu wprowadzamy ustawienia:
5. **Nazwa: dostęp SSH**
6. **Metoda: pozwól**
7. **Kierunek: w**
8. **Interfejs: wszystkie**
9. **Od: 10.1.51.100 Port: -**
10. **Do: 10.1.51.101 Port:22**
11. Klikamy **Add**.
12. Reguła została dodana.


Dodaj regułę zapory
Prekonfigurowana
Prosta
Zaawansowana
Nazwa:
dostęp SSH
Wprowadź:
0
Metoda:
Pozwól
Kierunek:
W
Interfejs:
Wszystkie interfejsy
Dziennik:
Nie zapisuj dziennika
Protokół:
TCP
Od:
10.1.51.100
Port
Do:
10.1.51.101
22
Zamknij
Dodaj


Zapora sieciowa
Plik
Edycja
Pomoc
Zapora sieciowa
Profil:
Dom
Stan:
Przychodzące:
Odmów
Wychodzące:
Pozwól
Reguły
Raport
Dziennik
Nr
Reguła
Nazwa
1
21/tcp POZWÓL PRZYCH Gdziekolwiek
FTP
2
23/tcp POZWÓL PRZYCH Gdziekolwiek
dostęp telnet
3
10.1.51.101 22/tcp POZWÓL PRZYCH 10.1.51.100
dostęp SSH
Reguły dodane