Konfiguracja zapory Firewall w systemie Debian.

www.einformatyka.com.pl

W zasadzie istnieje bardzo niewiele wirusów przeznaczonych na systemy z rodziny Unix lecz nie oznacza to że jesteśmy całkowicie bezpieczni. Możemy paść ofiarą np. ataku Hakera, Który wykorzystując odpowiedni protokół spróbuje włamać się do naszego komputera.

Instalacja oraz konfiguracja zapory sieciowej może podnieść bezpieczeństwo naszego systemu. Daje nam ona możliwość filtrowania ruchu sieciowego oraz zarządzanie połączeniami przychodzącymi i wychodzącymi.

Instalując system Debian domyślnie mamy już zainstalowanego firewalla o nazwie Iptables. Musimy go tylko włączyć i odpowiednio skonfigurować. Dla własnej wygody do jego obsługi zainstalujemy pakiet firestarter, który jest interfejsem graficznym do obsługi w/w oprogramowania.

1. Logujemy się do terminala za pomocą konta root

   sudo su root

2. instalujemy pakiet firestarter

   aptitude install firestarter

3. Włączamy wcześniej zainstalowane oprogramowanie w celu konfiguracji zapory (musimy być zalogowani jako Administrator)

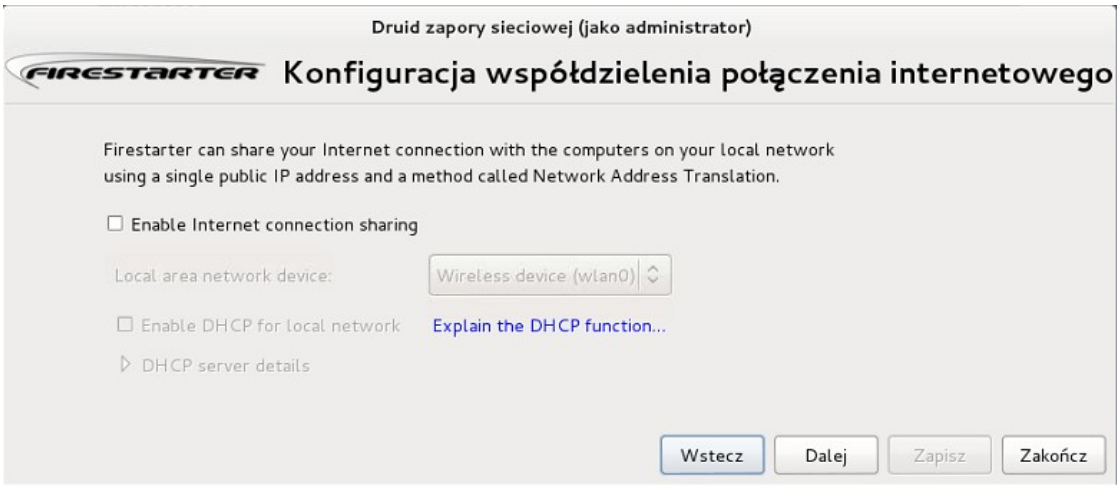
   firestarter

4. Na początku musimy odpowiedzieć na kilka pytań dotyczących naszej sieci. Są one jednak bardzo proste i zazwyczaj sprowadzają się do przeklikania wszystkiego dalej.

   - Wybieramy kartę sieciową za pomocą jakiej się łączymy. Jeśli dostajemy adres dynamicznie zaznaczmy również opcję „***Adres IP przydzielany za pomocą DHCP***” (Rysunek 1)

Rysunek 1: Konfiguracja zapory

- W kolejnym kroku możemy zdefiniować współdzielenie połączenia (Rysunek 2)



Rysunek 2: Konfiguracja zapory: Współdzielenie połączenia

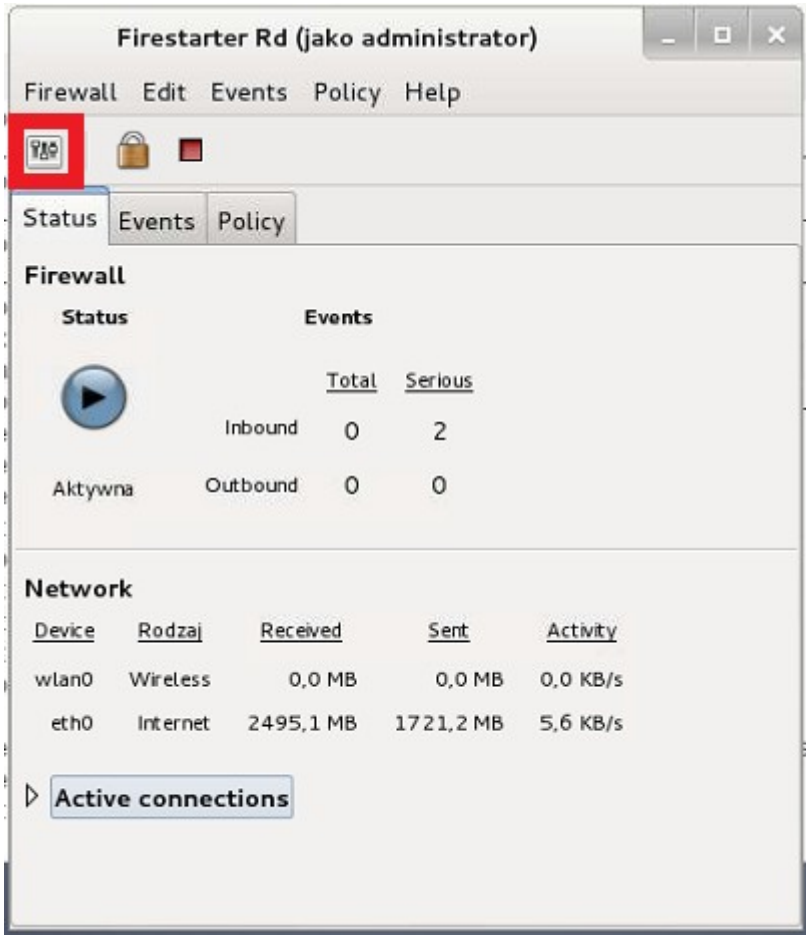
- W ostatnim oknie zapisujemy ustawienia i zamykamy kreatora.

Rysunek 3: Konfiguracja zapory: zapisanie ustawień

- • W domyślnej konfiguracji wszystkie połączenia przychodzące z zewnątrz będą blokowane.

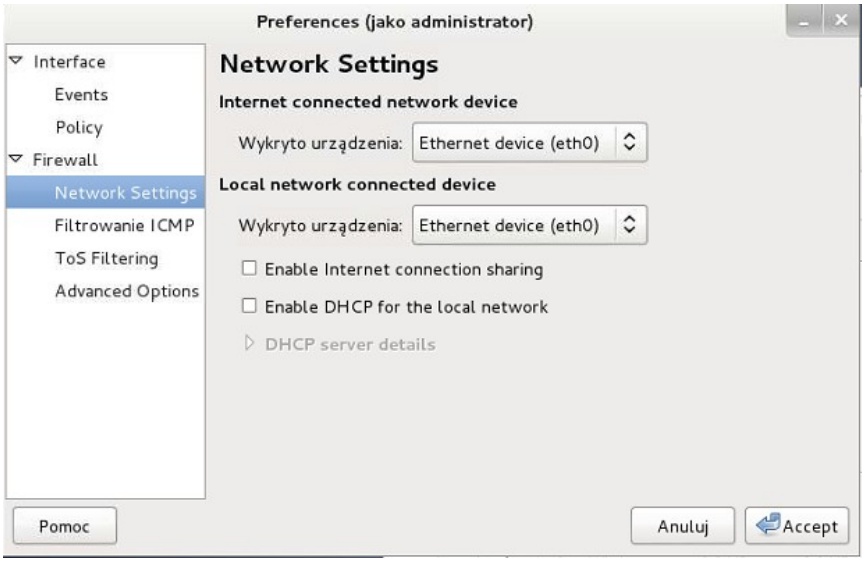
5. Konfiguracja zapory sieciowej:

- Edycja właściwości połączenia: Jeśli zrobiliśmy błąd podczas konfiguracji programu możemy poprawić te dane wchodząc w opcje programu (Rysunek 4).



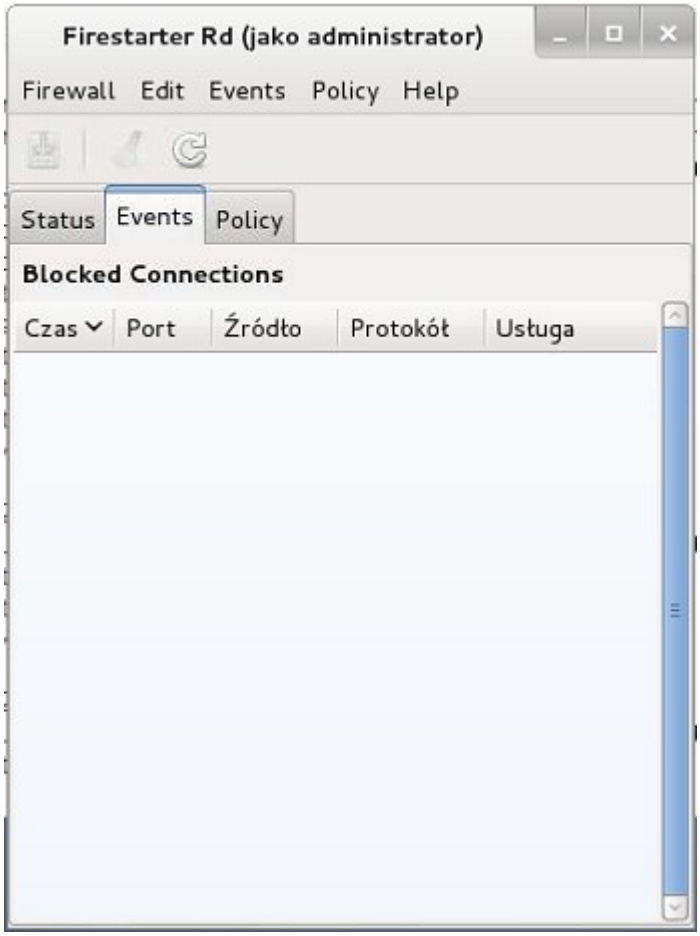
Rysunek 4: Ikona Edycji właściwości programu.

Interfejs jest bardzo prosty nie wymaga komentarza (Rysunek 5).



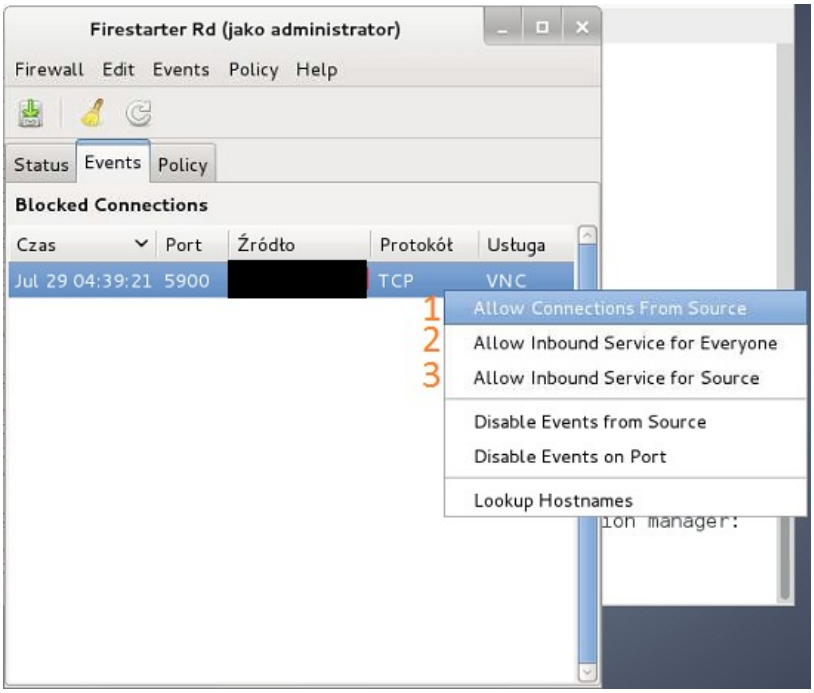
Rysunek 5: Opcje połączenia

- Podgląd zablokowanych połączeń: W czasie gdy interfejs programu jest włączony mamy możliwość przejścia do drugiej zakładki „**Evenst”** (Rysunek 6)



Rysunek 6: Przegląd zablokowanych połączeń

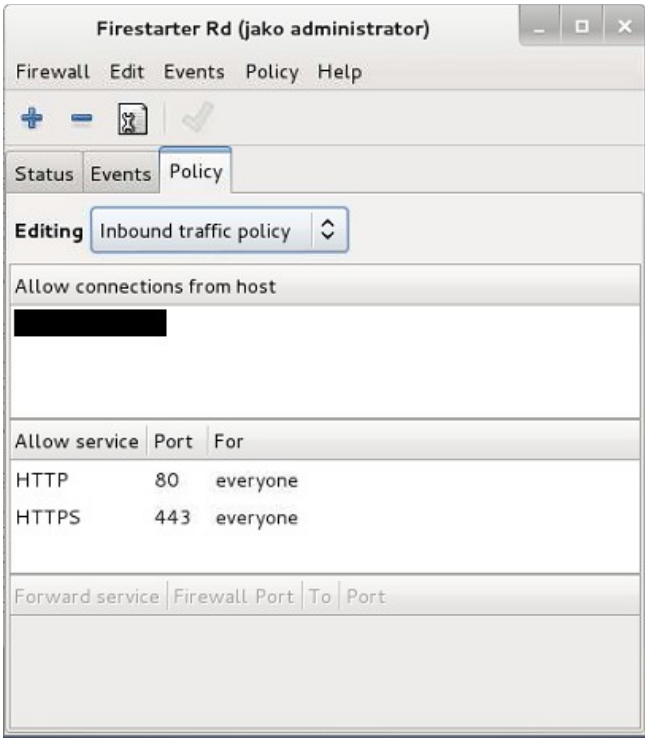
Będą tutaj wyświetlane obecnie zablokowane połączenia. Jest to bardzo przydatna informacja zwłaszcza gdy chcemy dać dostęp do komputera jakiemuś urządzeniu. Wystarczy kliknąć zablokowane połączenie prawym przyciskiem myszy i wybrać jedną z dostępnych opcji (Rysunek 7)



Rysunek 7: Opcje dla zablokowanego połączenia.

1. Dodaje adres IP do białej listy
2. Dodaje port do białej listy
3. Dodaje Adres IP, który będzie mógł łączyć się do komputera przez podany port

- Zarządzanie akceptowanymi połączeniami (biała lista): Trzecia zakładka programu (**Policy**) pozwala nam na zarządzanie regułami zapory (Rysunek 8)

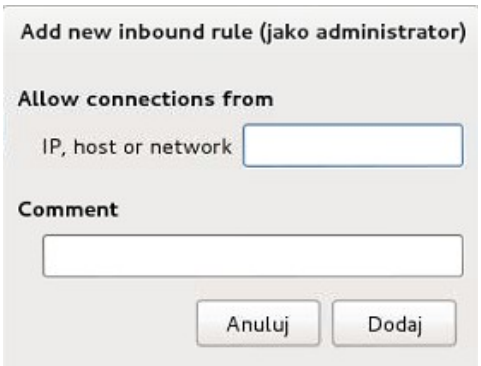


Rysunek 8: Zarządzanie regułami

W pierwszym polu „**Allow connections from host**” są określone adresy IP lub nazwy urządzeń, które mają zezwolenie na połączenie. Aby usunąć połączenie klikamy na nim prawym przyciskiem myszy i wybieramy „**Remove Rule**”. W celu edycji wybieramy „**Edit Rule**”. W przypadku dodania nowego połączenia klikamy obok istniejących połączeń (lecz w ty samy polu) prawy przyciskiem myszy i wybieramy „**Add Rule**”(Rysunek 9).

Rysunek 9: Edycja połączeń

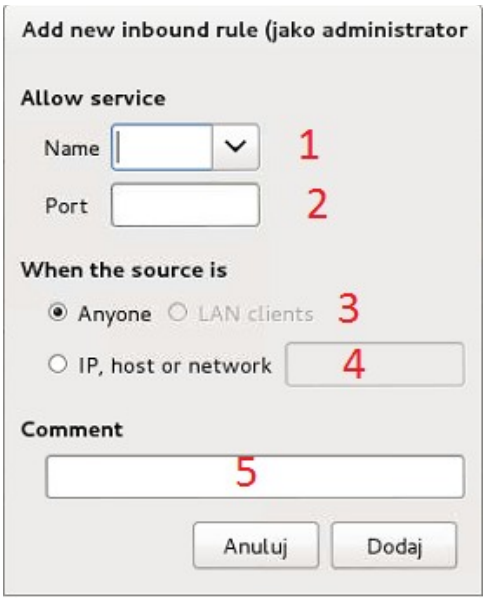
Podczas tworzenia nowej reguły zostanie wyświetlone takie samo okno jak w przypadku edycji (Rysunek 10).



Rysunek 1: Dodawanie nowego hosta

Wystarczy podać tutaj Adres IP Lub nazwę komputera, który będzie miał pełnie uprawnienia do łączenia się z naszym. Poniżej możemy również dodać swój komentarz.

W drugim polu możemy bardziej precyzyjnie określić prawa dostępu. Meni pod prawym przyciskiem myszy jest analogiczne jak opisane powyżej. Nieco inaczej wygląda natomiast pole do dodawania i edycji reguły (Rysunek 11).



Rysunek 2: Dodawanie nowej reguły

W pierwszym polu możemy wpisać własną nazwę reguły lub wybrać jedną z gotowych do dodania. Jeśli wybierzemy jedną ze zdefiniowanych to pole „**Port**" zostanie uzupełnione automatycznie. W przeciwnym przypadku musimy podać jego numer. Jeśli wybierzemy opcję „**Anyone**" to zezwolenie na połączenie otrzymają wszystkie komputery łączące się na podanym powyżej porcie. W przypadku zaznaczenia pola „**IP, host or network**" Musimy dodatkowo podać nazwę komputera lub jego IP. Taka konfiguracja zezwoli na dostęp tylko dla podanej stacji i to tylko w przypadku, gdy żądanie połączenia przyjdzie z określonego wcześniej portu.

Definiując dostęp no naszego komputera musimy pamiętać o tym, że im mniej będzie otwartych portów tym bezpieczniejszy będzie nasz komputer.