Webmin / Firewall

written by archi | 16 października 2019

1. Przed kolejnym krokiem podłącz swój komputer (Karta-Port1) do przełącznika 48portowego do dowolnego portu tego przełącznika.

2. Zaloguj się do https://vcenterlab.wi.zut.edu.pl/ui. Uruchom swoją maszynę wirtualną i po chwili sprawdź jej adres IP.

2a. Otwórz nową kartę przeglądarki i wpisz adres:
http://tutaj_adres_ip_twojej_maszyny
Po wpisaniu adresu powinieneś zobaczyć stronę powitalną serwera WWW Apache (instalowaliśmy go podczas zajęć dotyczących DNS-a).

2b. Uruchom Putty. Połącz się ze swoją maszynę wpisując jej adres.

2c. Wewnątrz maszyny wirtualnej, zaktualizuj bazę informacji o pakietach systemu:

```
apt update
```

```
apt update
```

3. Pobierz skrypt do instalacji dodatkowego repozytorium (wklej poniższą komendę, nie przepisuj tego ręcznie):

```
curl -o setup-repos.sh
https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.s
h
```

```
curl -o setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
```

4. Uruchom skrypt i potwierdź instalację dodatkowego repozytorium

`sh ./setup-repos.sh`

```
sh ./setup-repos.sh
```

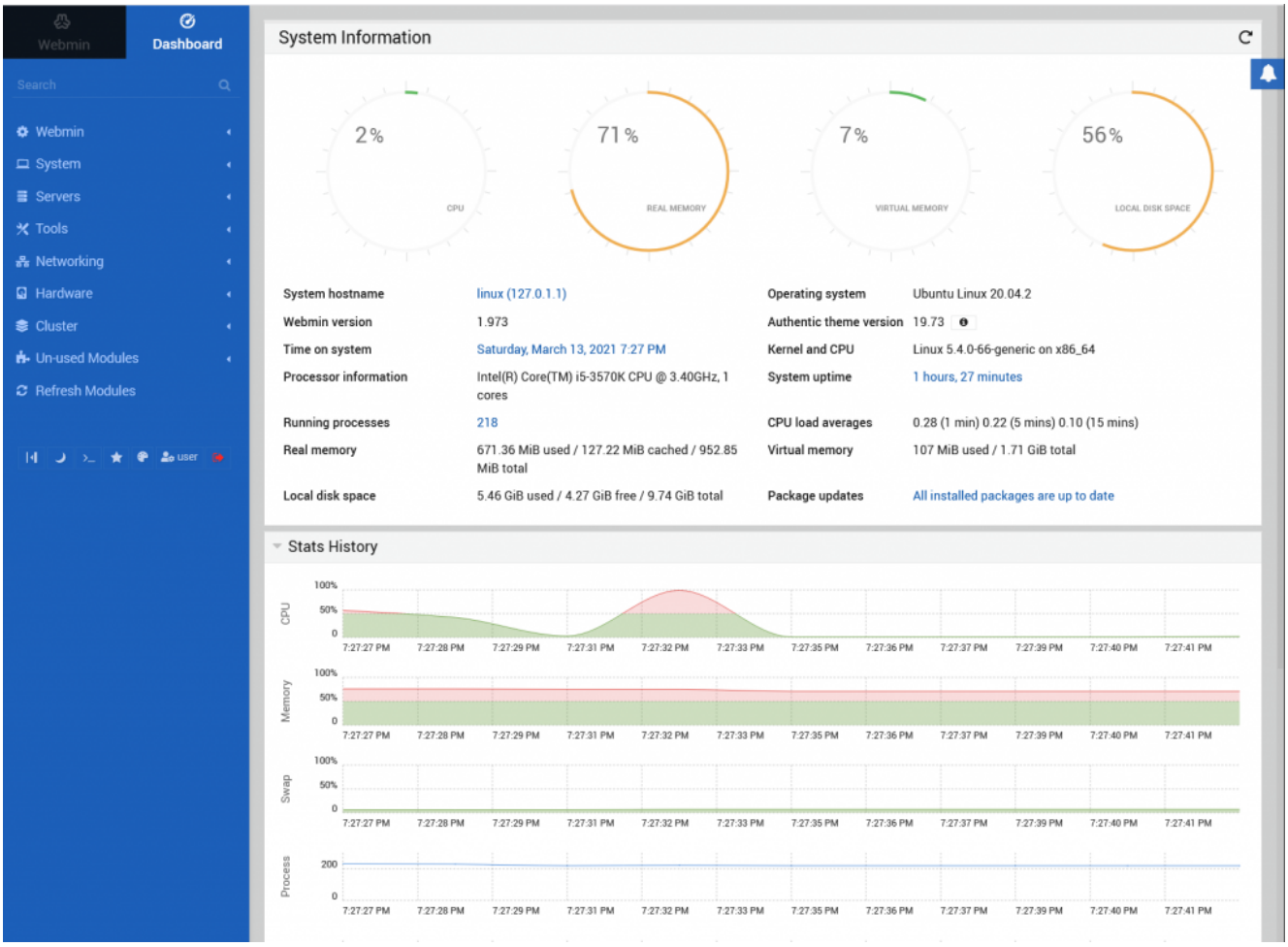
5. Pobierz i zainstaluj pakiet Webmin

`apt-get install --install-recommends webmin`

```
apt-get install --install-recommends webmin
```

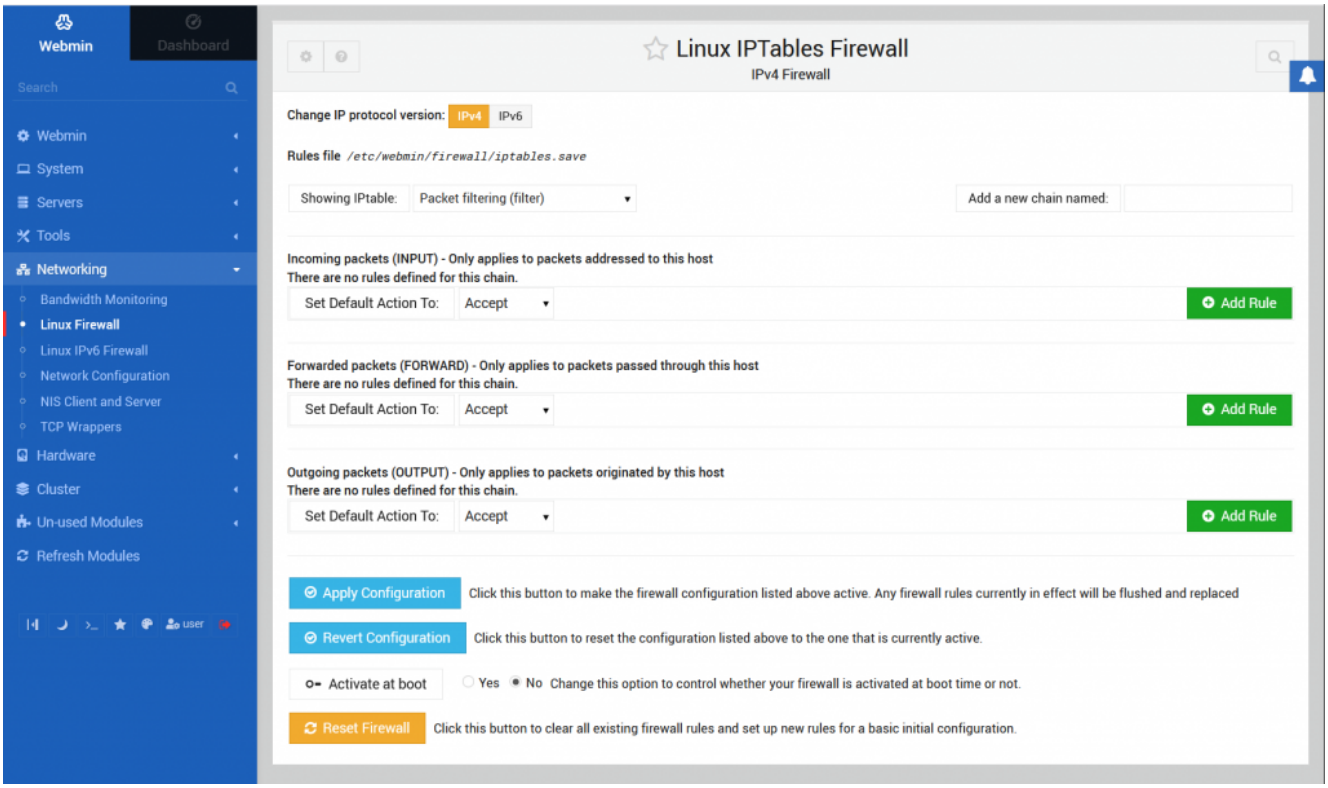
6. Po instalacji pakietu Webmin uruchom przeglądarkę i wpisz https://tutaj-twoj-adres-ip:10000 (pamiętaj o http**s**:// na początku adresu i porcie połączenia **:**10000 na końcu).

7. Po zalogowaniu się na użytkownika root (lub user) zobaczysz okno informacji o Twoim systemie. Informacja zawiera dane o kernelu, procesorze, pamięci, dysku oraz aktualizacji dla systemu. Z lewej strony znajduje się menu systemowe.



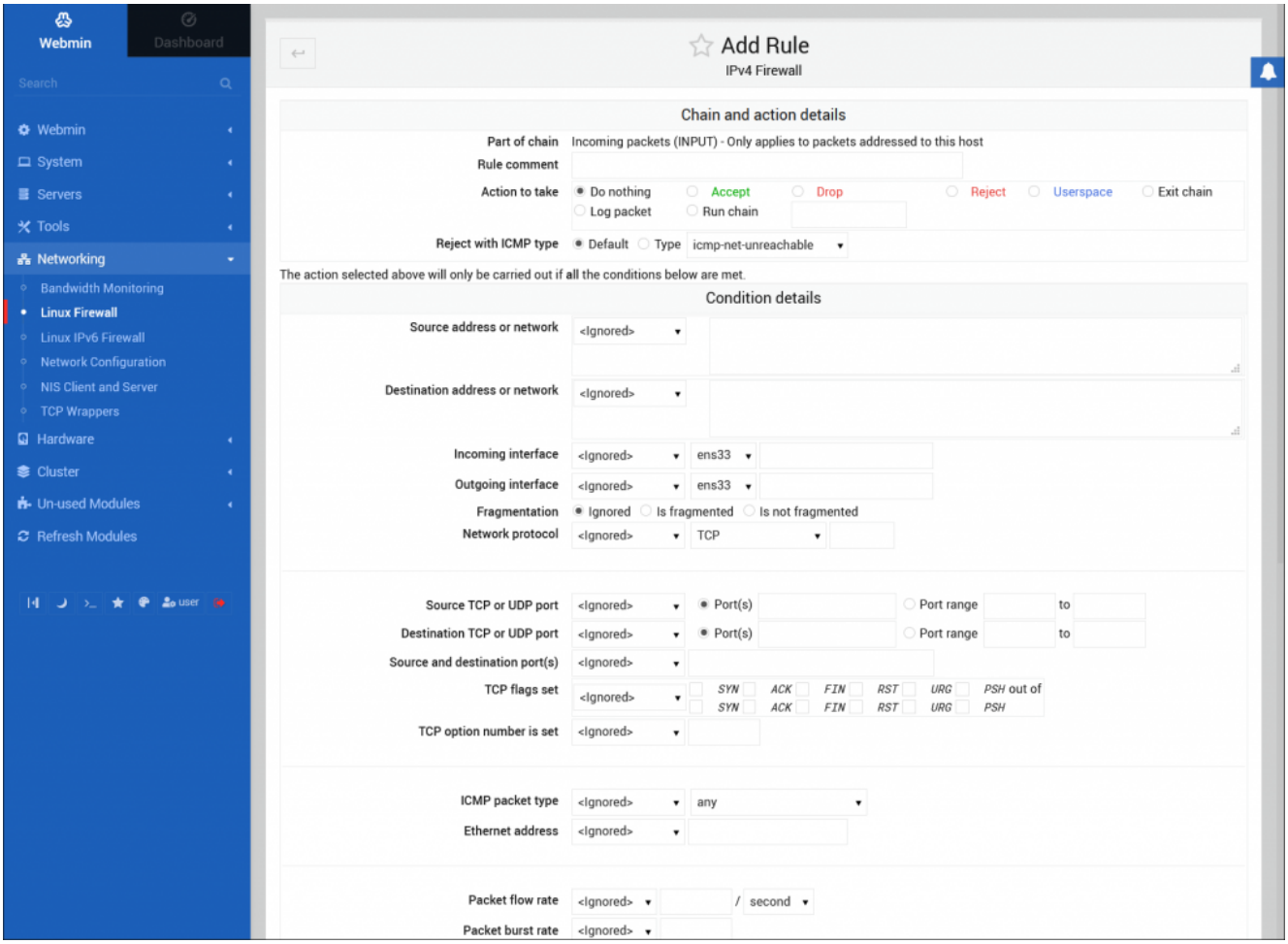
8. Przejrzyj w menu pozycje: Servers, Tools, Networking.

9. Zakładka Servers zawiera dostępne zainstalowane na serwerze usługi pozwalając na ich konfigurację. Zakładka „Tools” pozwala na zarządzanie dodatkami do systemu łącznie z uruchomieniem powłoki systemowej „shell”, zarządzaniem plikami „File Manager” oraz innymi ustawieniami. Zakładka Networking pozwala konfigurować ustawienia sieciowe, w tym zaporę systemową „Linux Firewall” – wybierz ją teraz właśnie.



10. Ustaw opcję „Activate at boot” na wartość **Yes**

11. Zapora nie posiada w chwili obecnej żadnych ustawień. Dozwolone są wszystkie połączenia. Skonfigurujemy blokadę do serwera WWW (port 80 po TCP) wszystkich połączeń przychodzących z zewnątrz. W tym celu w polu „Showing IPtable:” wybieramy „Packet filtering (filter)”. Następnie w sekcji „Incoming packets (INPUT)” dodajemy nową regułę naciskając przycisk „Add rule” zaraz poniżej po prawej stronie. Otworzy nam się okno konfiguracji reguły.



12. Kolejno wypełniamy tabele informacjami:

Rule comment: *(komentarz do ustawianej reguły – co to jest za reguła)*
Action to take: Drop
Network protocol: Equals -> TCP
Destination TCP or UDP port: Equals -> **Port(s):** 80

13. Zatwierdzamy przyciskiem na dole „Create”

14. Reguła pojawi się jako jedyna obecnie w opisie konfiguracji.

15. Zapisanie i uaktywnienie stworzonych lub zmienianych reguł dokonuje się w ekranie głównym Firewall poprzez wybranie przycisku „Apply Configuration”.

16. Sprawdź czy strona powitalna serwera WWW Apache przestała odpowiadać (odśwież stronę http://tutaj_adres_ip_twojej_maszyny)

17. Zmień tą regułę tak, aby serwer WWW odpowiadał bez usuwania tej reguły. Sprawdź dostępne opcje w sekcji „Action to take”.