Piotr Rorot

Pi-hole

Instalacja i działanie zaawansowanego narzędzia do blokowania reklam na poziomie sieci

Spis treści

[1. Czym Jest Pi-Hole? 2](#_Toc166856942)

[2. Co wyróżnia Pi-hole? 2](#_Toc166856943)

[3. Potrzebne informacje i pliki do instalacji 3](#_Toc166856944)

[4. Instalacja 4](#_Toc166856945)

[5. Podsumowanie 12](#_Toc166856946)

[6. Spis komend 13](#_Toc166856947)

# Czym Jest Pi-Hole?

Pi-hole to aplikacja stworzona z myślą o systemach operacyjnych z rodziny Linuks, zwłaszcza takich jak Raspberry Pi OS, od którego też wzięła swoją nazwę. Jej główną funkcją jest tworzenie własnego serwera DNS, który filtruje ruch sieciowy, uniemożliwiając domenom znajdującym się na czarnej liście przekazywanie jakichkolwiek treści do użytkownika. Dzięki temu, wiele reklam oraz potencjalnie szkodliwe oprogramowania są eliminowane już na wstępnym etapie.

# Co wyróżnia Pi-hole?

Pi-hole przede wszystkim działa jako DNS dla całej sieci, blokując reklamy oraz dostęp do wybranych domen dla wszystkich urządzeń, niezależnie od tego, czy są to komputery czy urządzenia mobilne. Dodatkowo, jest to aplikacja open source, co oznacza, że nie ma konieczności wykupienia licencji, a także nie wymaga dużych zasobów sprzętowych, mogąc działać nawet na starszych wersjach Raspberry Pi.

W przeciwieństwie do wtyczek blokujących reklamy dostępnych w przeglądarkach internetowych, Pi-hole nie jest wykrywane przez strony internetowe, co pozwala na skuteczne omijanie reklam na stronach, które próbują uniemożliwić korzystanie z tych wtyczek.

Pi-hole umożliwia również edycję listy zablokowanych domen oraz dodawanie własnych rekordów DNS. Pozwala także na tworzenie profili użytkowników na podstawie adresów fizycznych urządzeń, co umożliwia zarządzanie dostępem do treści dla określonych osób. Dzięki temu, na przykład, można ograniczyć dostęp do niektórych domen dla najmłodszych użytkowników sieci lub zablokować dostęp do mediów społecznościowych w ramach danej organizacji.

# Potrzebne informacje i pliki do instalacji

Aby przystąpić do instalacji, niezbędne są podstawowe informacje dotyczące naszej sieci, takie jak maska podsieci i brama domyślna. Dane te możemy uzyskać otwierając konsole (wpisując w polu wyszukiwania CMD) i wpisaniu następnie komendy „ipconfig”.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Wyświetli nam się powyższa informacja.

Odczytać z niej możemy Subnet Mask – maska podsieci i Default Gateway – brama domyślna. Teraz musimy zmienić postać maski z systemu kropkowego na CIDR. Jeżeli nie wiemy jak to zrobić korzystamy z [kalkulatora](https://syslink.pl/tools/ipv4-subnet-calculator) gdzie wpisujemy nasz adres ip i adres maski, które odczytaliśmy.

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Widzimy, że maska wynosi /24.

Do instalacji potrzebne będą następujące pliki:

* [Plik iso ubuntu server](https://ubuntu.com/download/server) – klikamy przycisk download i pobieramy zawartość
* [Aplikacja](https://rufus.ie/downloads/) rufus – pobieramy najświeższą wersje
* Pliki znajdujące się na pendrive

# Instalacja

Na początku informacja dla bardziej zaawansowanych użytkowników, którzy będą chcieli instalować sami - skrypt składa się z 3 części:

* **SSH.sh**
* **Pi-hole installation and main configuration.sh**
* **IP address configuration.sh**

Plik **IP address configuration.sh** odpowiada za konfigurację IP, **Pi-hole installation and main configuration.sh** za instalację i konfigurację PI-hole, a **IP address configuration.sh** nadaje uprawnienia dla każdego z tych skryptów i odpala je. Jeżeli będziesz instalować usługę korzystając z SSH na swoim komputerze pamiętaj, że po zmianie IP nastąpi rozłączenie z serwera i potrzebne będzie ponowne połączenie.

Żeby zacząć instalację na urządzeniu potrzebujemy sytemu operacyjnego. Jeżeli nie wiemy jak to zrobić odsyłam do [poradnika](https://youtu.be/uNqxUWiAoRk). Jeżeli mamy już przygotowane wszystkie pliki i informację możemy zacząć. Potrzebujemy z komputera z systemem Windows przesłać pliki. Otwieramy wiersz poleceń (cmd) i wprowadzamy poniższą komendę:

*scp <ścieżka\_pliku\_na\_windowsie> <użytkownik\_docelowy>@<adres\_ip\_serwera>:<katalog\_docelowy >*

1. Informacje potrzebne na Windowsie:
   1. żeby skopiować ścieżkę pliku na Windows 11 klikamy prawym przyciskiem na plik i wybieramy „kopiuj jako ścieżkę”

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

* 1. żeby skopiować ścieżkę pliku na Windows 10 klikamy lewym przyciskiem na plik, następnie wciskamy przycisk shift i prawy przycisk myszy, wybieramy „kopiuj jako ścieżkę”

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

1. Informacje potrzebne z serwera:
   1. użytkownik docelowy: komenda „*hostname*”

Obraz zawierający tekst, Czcionka, zrzut ekranu, czarne

Opis wygenerowany automatycznie

* 1. adres ip serwera: komenda „*hostname -I*”



* 1. katalog docelowy: komenda „*pwd*”



W moim przypadku komenda do przesłania pliku będzie wyglądała tak:

* *scp "C:\Users\proro\Desktop\przykładowy\_plik"* [*test@192.168.1.59:/home/test*](mailto:test@192.168.1.59:/home/test)

Przesyłamy wszystkie 3 pliki wymienione wcześniej. Od teraz 90% wszystkich interakcji wykonujemy na serwerze.

Wpisujemy komendę *„ls”* by zobaczyć wszystkie katalogi i pobrane pliki. Korzystając z komendy „*chmod +x SSH.sh”* nadajemy uprawnienia*.* Wpisujemy komendę „*ls”* i uruchamiamy skrypt – „*sudo ./SSH.sh”.* Na początku pobierane i instalowane są aktualizacje repozytoriów. Może to potrwać chwilę, więc masz czas na herbatę lub kawę 😊.

Po tym nastąpi konfiguracja IP, adres serwera możemy wpisać taki jaki został przydzielony przez serwer DHCP, bramę domyślną przepisujemy z informacji dostarczonych z Windowsa, a maskę podsieci wpisujemy taką jaką pokazał nam kalkulator.

Jeżeli wyświetli nam się poniższy komunikat Obraz zawierający tekst, zrzut ekranu, fioletowy, fiołek

Opis wygenerowany automatycznie

klikamy przycisk „Tab” i następnie „Enter”, tak by wybrać opcję <Ok>. Za każdym razem przy tym komunikacie postępujemy tak samo. Po chwili wyświetlą nam się poniższe komunikaty. Zaznaczamy odpowiednio jak poniżej.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

Obraz zawierający tekst, wyświetlacz, zrzut ekranu, komputer

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, komputer, oprogramowanie

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, komputer, oprogramowanie

Opis wygenerowany automatycznie Obraz zawierający tekst, wyświetlacz, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Był to proces samej instalacji naszej usługi, na końcu pokaże nam się poniższy komunikat: Obraz zawierający tekst, zrzut ekranu, wyświetlacz, Czcionka

Opis wygenerowany automatycznie

Przed zatwierdzeniem zapisujemy sobie adres do interfejsu graficznego, uniwersalnym adresem jest: *http://pi.hole/admin*. Klikamy „Ok” i zgodnie z poleceniem widocznym a terminalu podajemy nowe hasło do interfejsu w przeglądarce. Wpisane hasło nie będzie widoczne ze względu bezpieczeństwa, jednak musimy wpisać je 2 razy więc nie ma opcji na pomyłkę. Po chwili zobaczymy poniższy komunikat, wpisujemy literkę „y” i zatwierdzamy enterem.



Po chwili nasza usługa jest już zainstalowana i została nam tylko kwestia wgrania konfiguracji. Wracamy do naszego komputera z systemem Windows i logujemy się do interfejsu www (hasłem podanym podczas instalacji) wchodząc na wcześniej zapisany adres http. Po zalogowaniu wchodzimy w Ustawienia DNS i następnie zmieniamy aktualne ustawienia na takie jak poniżej

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Żeby zapisać zjeżdżamy na sam dół i zapisujemy konfigurację. Teraz w tej samej kategorii wybieramy zakładkę „Teleporter” dodajemy plik dołączony do instalatora o początku nazwy „pi-hole-server-teleporter” i klikamy „Restore”.

Obraz zawierający zrzut ekranu, tekst, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Teraz pozostaje nam Wejść w katalog „Tools” i zakładkę „Update Gravity”, następnie kliknąć przycisk „Update”. Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

# Podsumowanie

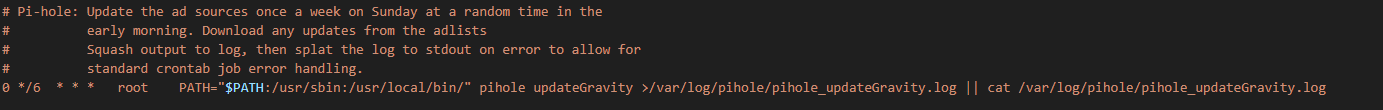
Żeby nasza usługa działała musimy przekierować cały ruch z urządzeń na nasz serwer. Można to zrealizować na routerze, przekierowując cały ruch w sieci, lub na komputerze, przekierowując ruch tylko z niego.

Aby przekierować nasz komputer na nowy serwer DNS, musimy zmienić ustawienia połączenia sieciowego. Metoda ta różni się w zależności od systemu operacyjnego.

W przypadku systemu Windows, możemy to zrobić przechodząc do Panelu Sterowania, następnie do Sekcji Sieć i Internet, a potem do Połączenia sieciowe. Klikamy prawym przyciskiem myszy na połączenie sieciowe, z którego korzystamy (np. Wi-Fi), i wybieramy opcję "Właściwości". Następnie zaznaczamy protokół internetowy w wersji 4 (TCP/IPv4) i klikamy "Właściwości". Wybieramy opcję "Użyj następujących adresów serwerów DNS" i wprowadzamy adres naszego nowego serwera DNS. Po zatwierdzeniu zmian klikamy "OK".

Warto pamiętać że dodając nowe repozytoria do blokowania trzeba zaktualizować Gravity, tak jak we wcześniejszym kroku.

**Uwaga**: za każdym razem kiedy będziemy aktualizować system Pi-hole ustawienia dotyczące automatycznego aktualizowania Adality zresetują się. Możemy skorzystać ze skryptu o nazwie **change the frequency of adlist updates.sh**, pamiętając o nadaniu mu odpowiednich uprawnień. Alternatywnie, możemy ręcznie edytować plik */etc/cron.d/pihole* za pomocą komendy „*nano”* i zmienić odpowiedni wiersz, aby wyglądał jak poniżej:



# Spis komend

* ***ipconfig*** - pokazuje konfigurację sieciową w systemie Windows
* ***scp <ścieżka\_pliku\_na\_windowsie> <użytkownik\_docelowy>@:<katalog\_docelowy>*** - kopiuje plik z lokalnego systemu Windows na zdalny serwer
* ***hostname*** – pokazuje nazwę użytkownika
* ***hostname -I***– pokazuje adres IP
* ***pwd*** – pokazuje bieżący katalog
* ***ssh <nazwa\_użytkownika>@<adres\_ip>*** - komenda do zdalnego połączenia się z serwerem
* ***ls*** – wyświetlenie wszystkich plików w bieżącym katalogu
* ***chmod +x <nazwa+pliku>*** - nadanie uprawnień piku
* ***sudo ./<nazwa\_użytkownika>*** - odpalenie pliku jako administrator
* ***nano*** – edytor tekstu w wierszu poleceń