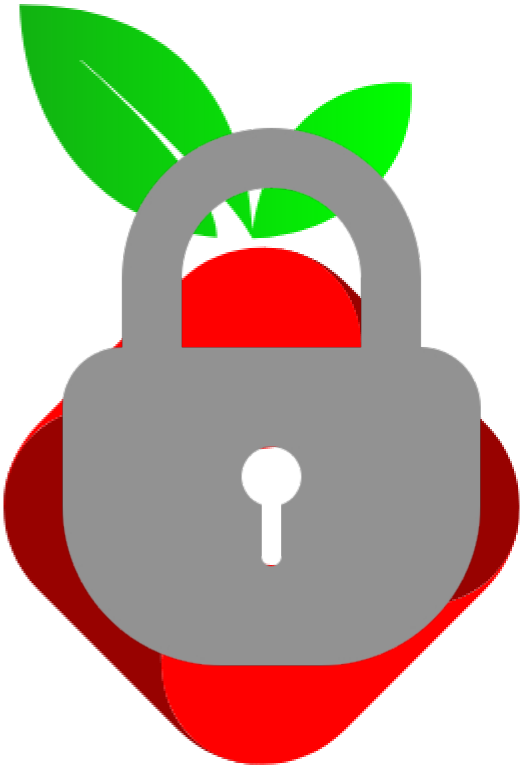
Guide to Use Pi-Hole-Enabled Raspberry Pi For Network-Wide Content Filtering on Home Network



5 Feb 2024

Table of Contents

Introduction

The goal of this document is to give you the tools to protect your children while they are on the internet on your home network. This provides a solution which will allow you to easily block certain sites for **ALL** devices in your home network. I will try to explain terms as we go, but at a high level, the solution is to set up a Raspberry Pi with a static IP to run Pi-Hole, then configure your router to force clients, or at least suggest that clients use your Pi-hole as their DNS server to provide network-wide content filtering for your entire home network.

Introduction to Domain Name Service (DNS)

DNS is how computers convert website names (domains) into IP addresses that computers understand. When you try to go to ‘www.facebook.com’, this string of text ultimately is useless to your computer. It doesn’t tell your browser where the servers for ‘facebook.com’ are located. To resolve this, your browser will perform what is called a **DNS request** to a **DNS server**. The DNS server is a computer at a known location (**IP address**) that also has a lookup table to convert domain names (e.g., ‘facebook.com’, ‘google.com’, etc) into IP addresses. Your computer is able to directly interact with an IP address. Once your computer gets a response from the DNS server with the desired IP address, it is able to send data to that IP address to load a web page, download your emails, send a message, load a video, etc. Everything on the internet is just ones and zeros - data. After your computer has successfully obtained the IP address for facebook.com, it will **cache**, or store off, the IP address for subsequent use (to avoid having to look it up from a DNS server EVERY time). However, a cached IP address, for the sake of DNS, is only considered valid for a finite amount of time. For various reasons, the IP address you get from a DNS request may change. This **expiration time is called: time to live (TTL)**. In the following table, I’ve listed some IP addresses and TTL values for various sites as I compile this document:

Domain Name	IP	Time To Live (TTL)
facebook.com	157.240.229.35	60 seconds
google.com	172.253.122.100	5 min
uiowa.edu	54.163.225.50	5 min
goodnewsiowacity.com	192.0.78.204	5 min

(You can try this yourself at: https://mxtoolbox.com/DNSLookup.aspx)

It is like going to the church directory (**DNS server**) and looking up the address of John Doe (**DNS request**). Once you find John Doe’s address or phone number (**IP address**) in the directory, you can store it in your phone or write it down at home (**caching**). But the address or phone number is only good as long as John still has the sane address or phone number. Eventually, you may want to check the church directory again to make sure John hasn’t moved (**cached IP addresses will expire -like TTL-**).

Congratulations! You just got a crash-course version of a semester-long, Junior-level engineering course)

Hardware

To further explain some terms in the intro, a Raspberry Pi si simply a small, low power, general purpose computer (see below).

The Raspberry PI is probably not as powerful as your smartphone, and definitely not as powerful as your home computer, but it is powerful enough for our purposes, has low energy costs, and is ‘cheap’ upfront. Also, the Pi-Hole software is written explicitly for the Raspberry Pi’s operating system, which will make for an easier startup than if we were using a Windows computer like you may be used to. There are lots of variants, but for our purposes, we will be using the Raspberry Pi 3 Model B. (See Appendix A.)

Your router, is the device that communicates between your internet service provider (ImOn, Mediacom, etc) and the devices in your network (your phone, tablet, computer, smart doorbell, etc). DHCP (Dynamic Host Configuration Protocol) is just one of the standardized processes that the router uses to do its job. We are able to manipulate our router’s DHCP options to do some cool things, but in our case,we will be manipulating it so that when any device makes a DNS request to your router, your **router forces the DNS request to go to our Pi-Hole** instead of going to a standard trusted DNS server such as Google’s DNS server.

Now, with all that out of the way, lets get this set up!

Instructions

To follow is step-by-step instructions for setting up the Pi-Hole as your DNS provider in your home network. Over time, this guide may become outdated. If you run into any issues or have any questions, your best friend will be the Pi-Hole documentation (https://docs.pi-hole.net/main/basic-install/) (the documents created and maintained by the creators of Pi-Hole.)

You Will Need

(See Appendix A for places to buy)

- Raspberry Pi 3 Model B (Check DigiKey for the best prices)
- USB Keyboard and Mouse
- A monitor or TV with an HDMI cable
- Raspberry-Pi approved power supply (make sure it fits whatever kind of Pi you get)
- A router that you own or have permissions to change settings on. (Do you know the password)
- (Optional) an Ethernet cable.

Booting Up Your Raspberry Pi

You may have received a micro SD card that already contains a working operating system. If not, you can make one yourself using the Raspberry Pi Imager (https://www.raspberrypi.com/software/). The Imager software will allow you to flash an operating system onto any SD card from your computer for a Raspberry Pi.

Once you have an SD card with a working operating system, place the SD card into the Pi and plug it into power (you also will want to plug in your keyboard, mouse, and display). Follow the instructions on the screen to set up your Pi. Make sure to set a good password that you will remember.

Setting a Static IP Address with your router

Instructions for setting a static IP address very significantly depending on which router you use. Ultimately, we need to log into the router, find the Pi, and assign it a static IP address (meaning we set it so that the Pi’s address will never change). We need to do this before we set up the Pi-Hole software on the Pi.

Installation and Setup of Pi-Hole Software

To install the Pi-Hole software on your system, follow these steps:

1. **Open a Terminal:**
    - Open a terminal window on your device. This can usually be done by searching for "Terminal" in your system's application launcher.
2. **Run the Installation Command:**
    - Copy and paste the following command into the terminal and press Enter:

```
curl -sSL https://install.pi-hole.net | bash
```

- This command will download and execute the Pi-Hole installation script.

3. **Follow On-Screen Instructions:**
    - The installation script will guide you through the setup process. Follow the on-screen instructions to configure your Pi-Hole installation. (It is recommended that you select “no” when asked if you would like to add the default adlist, as it will interrupt many top results on Google (because they are sponsored ads) including man Amazon links)
    - You'll be prompted to set preferences such as upstream DNS provider, blocklists, and web interface settings.
    - **Set Secondary DNS to 1.1.1.3:**
    - After the Pi-Hole installation is complete, configure your device's secondary DNS to `1.1.1.3` (This secondary DNS is set to CleanBrowsing's Family Filter, providing an additional layer of content filtering that prevents users on your network from turning off safe search while using search engines on your network).

Adding Sites and Domains to the Block List

There is an online list of around 2.5 million domains as of the time of writing this manual. These are domains, mind you, not pages. So we are blocking whole websites and everything on them. Included on this list are lots of “dating” websites as well. This list does not include Reddit or X (formerly known as Twitter) (both of which contain explicit material which isn’t hard to find). Both of those sites can be easily added to your own block list. Now, to add this massive list of domains to the collection of sites for the Pi-Hole to block:

1.) Open the web browser on the Pi-Hole.

2.) Substituting your Pi's IP address, go to: http://<IP_ADDRESS_OF_YOUR_PI_HOLE>/admin/

3.) Enter the password generated by the Pi-Hole on startup or set by yourself.

4.) Go to the "AdLists" tab

5.) Under "Add new adlsits" enter the following URL into the "URL" text field: https://raw.githubusercontent.com/bjohnson66/family_safe_domain_blacklist/main/merged_block.txt

6.) Enter any comments for yourself for later, then click "Add"

7.) Close the web browser and open a terminal

8.) In the terminal, run the command:

```
pihole -g
```

This command may take a while to run as the Pi has to download the long file then rebuild a large number of back-end data so that it can efficiently block the sites listed in the file.

If the list were to ever expand, don't worry, the Pi-Hole is supposed to automatically update the list once per week. If a site makes it through the filter that you want added to the online list, please request it via the form: https://forms.gle/sSLKo2UDgwM4Yhih9

Alternatively, you can update your ad-lists using the web interface at Tools > Update Gravity > Update

Monitoring Your Pi-Hole

Go to http://pi.hole/admin or http://(your static IP)/admin example: http://192.169.1.105/admin

In the setup, they will tell you your password.

Within the Admin Console, you can monitor traffic, analytics, and manage various aspects of Pi-Hole. This interface allows you to track blocked sites over time, providing insights into when and which sites were prevented from loading.

Limitations and Warnings

an significantly enhance online safety, it's important to acknowledge its limitations. Parents and guardians should be aware that this system may not be foolproof, and individuals with sufficient technical knowledge or determination can find ways to circumvent the filtering mechanisms. Consider the following points:

Mobile Data Browsing:

- Users can bypass the content filter by switching to cellular data, disconnecting from the home network, and accessing the internet independently of the configured DNS filters.

VPN Usage:

- Virtual Private Networks (VPNs) can be employed to encrypt and reroute internet traffic, effectively bypassing DNS-based content filtering.

Custom DNS in Browsers:

- Some web browsers allow users to specify their DNS provider independently, rendering DNS-based content filters ineffective within those browsers.

Operating System DNS Changes:

- Advanced users can modify the DNS settings at the operating system level, circumventing DNS-based content filtering altogether.

Social Media Content:

- Not all explicit content is served through standard web browsing. Popular social media platforms like Twitter and Reddit may contain mature content.

Sheer Volume of Explicit Content

- While a domain list of 2.5 million sites is impressive, it is not nearly comprehensive. The internet is also changing and growing daily.

Recommendations for Enhanced Protection:

To maximize the effectiveness of the content filtering system and address potential limitations, consider implementing the following additional measures:

1. **Device Permissions:**
    - Set appropriate permissions on your children's devices, ensuring a balance between access and restrictions. Tailor permissions to their age, maturity, and risk levels.
2. **Firewall Configuration:**
    - Configure a firewall to block known VPN services, reducing the likelihood of users bypassing content filters using these services.
3. **Blacklisting Unsafe Sites:**
    - Regularly update and expand the blacklist to include unsafe social media sites and other platforms known for hosting explicit content. (Side note, remember that if you need to access Twitter or Reddit, you can just use your phone, but your kids likely do not NEED access to these sites without parental supervision). This can be done at a local level in the “Domains” tab. The large ad list will update itself weekly.

Target Audience:

It's essential to recognize that this system is designed to benefit individuals who:

1. **Limited Technical Knowledge:**
    - Individuals with limited technical expertise may find this content filtering system effective in providing an extra layer of protection.
2. **Not Addicted to Adult Content:**
    - Users who are not actively seeking explicit content may benefit from the system by reducing accidental exposure.
3. **Children and Adolescents:**
    - Parents aiming to protect children who are not yet familiar with explicit content and require a safer online environment.

Requesting the Addition of a Site to the Blacklist

If you come across a site that you believe should be added to the remotely maintained blacklist, you can submit a request using a simple online form. Follow these steps:

Access the Site Blocking Request Form:

- Open your web browser and go to the following link: https://forms.gle/4apoxheHJV1Ewabm7.

Complete the Form:

- Fill out the form with the necessary information:
    - **URL:** Provide the full URL of the site you want to block.
    - **Reason for Blocking:** Explain briefly why you believe this site should be added to the blocklist.
    - **Additional Comments:** Include any other relevant information or context.

Submit Your Request:

- Once you've filled out the form, click the "Submit" button. Your request will be securely sent for review.

Be Patient:

- The review process may take some time. Rest assured that your request is being considered, and you will be notified of any updates or decisions if you provided your email (optional). If the site is found to be something that should be added to the list, your Pi should update its list automatically the week that the remote list is updated.