7

BLOCKING INTERNET ADVERTISEMENTS

Companies monetize the internet through advertising, which has caused the number of online ads to proliferate (or more accurately, explode). These ads have become more insidious over time, as websites track your activity to display the promotions most likely to lead to purchases. Even worse, advertising has caused slower internet connections through websites becoming so bloated with autoplaying advertisements.

will first discuss various browser ad blocking solutions. Then, we'll build an ad-blocking DNS proxy server using Pi-Hole to provide users with a much better browsing experience while also improving data and privacy protection.

Browser-Level Ad Blocking

Most modern browsers have some form of ad-blocking technology built-in to the application itself. By default, some browsers prevent

various trackers and scripts from operating as designed. These include social media trackers, cookies, fingerprinters, and cryptominers. Blocking *social media trackers* disallows sites such as Facebook, Twitter, and LinkedIn from tracking you as you browse websites that implement social media buttons or instant sharing links. *Cookies* are files used by sites to track information and user preferences between visits; this can leak your private information from one site to another. *Fingerprinters* are similar in that they identify a specific user by a number of metrics collected from their browsing habits, which allows advertisers to track your activity during a browsing session. Finally, *cryptominers* are applications (some might say malware) that use your computer hardware to mine cryptocurrency, such as Bitcoin. This is a highly resource-intensive process that can cause system instability. All of these can negatively impact your browsing experience and should be blocked.

Besides the built-in functionality provided by some web browsers, some of the most popular browser ad blockers are browser *extensions*, also known as *add-ons*—software that you can add to your browser to improve its functionality or add capabilities. For example, *Adblock Plus*—installable in most browsers—works by intercepting advertisements before they're displayed to the user, though the ads are still downloaded to your computer.

Many websites can identify when browser extensions are in use and will either modify their content or completely block users from viewing web pages until the extension has been disabled or the site is allowlisted to play ads. Browser extensions are discussed further in **Chapter 11**. The following projects cover how to set up browser ad blocking for Google Chrome, Mozilla Firefox, and Brave browsers.

#22: Blocking Ads in Google Chrome

Chrome's ad blocker (***https://www.google.com/chrome/***) is designed to hide ads on websites that have too many ads or whose ads detract

from the user experience, such as by flashing or making noise. Chrome also blocks ads on sites that put content behind a *paywall*, which obscures the website entirely until the user either allows the ads to display or pays a fee to view the content. This behavior applies to the Android version of Chrome in addition to the desktop version. It's possible to activate or deactivate the built-in ad blocker, as well as to allowlist specific sites:

1. At the top right of the Chrome browser, click the **More** icon (three horizontal lines).
2. Click **Settings ▸ Advanced ▸ Site Settings ▸ Ads**.
3. If the text "Blocked on sites that tend to show intrusive ads (recommended)" is displayed, Chrome is currently blocking ads for you.
4. If you'd like to turn ad blocking off, hit the toggle to switch the setting to **Allowed**.

Another way to protect your privacy online is to use a private browsing window. Chrome's *incognito mode* either won't save your personal information or immediately deletes it (including tracking information such as cookies) when you close the browser. Your browsing history and internet searches won't be saved. To open an incognito window, follow these steps:

1. At the top right of the Chrome browser, click the **More** icon (three horizontal lines).
2. Click **New Private Window**.

A new browser window will open that has a different appearance when compared to a normal Chrome window—text such as "You've gone Incognito" is typically displayed. This is how you know you're browsing privately.

#23: Blocking Ads in Mozilla Firefox

Firefox's *Private* browsing (***https://www.mozilla.org/***) windows block not only ads but also tracking content, including videos and other media displayed on a web page. To open a new Private window, follow these steps:

1. At the top right of the Firefox browser, click the **More** icon (three horizontal lines).
2. Click **New Private Window**.

You can change Firefox's default behavior to disable tracking content in all Firefox windows, rather than just Private windows. To modify these settings, follow these steps:

1. Click **More** in the top right of the Firefox window.
2. Click **Preferences ▸ Privacy & Security**.
3. Set your Enhanced Tracking Protection settings to Standard (the default), Strict (provides greater privacy but may break some websites), or Custom.
4. Configure your Cookie settings to delete cookies on browser exit by ticking the **Delete Cookies and Site Data When Firefox is Closed** checkbox.
5. Make Firefox forget your browsing history by setting the History drop-down menu to **Never Remember History**.
6. Set permissions for things like your webcam and microphone so that Firefox isn't able to watch or listen without authorization.

You can find more information on disabling trackers and other security and privacy settings in the Mozilla knowledge base at ***https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop/***.

#24: Controlling Brave's Privacy Settings

Brave (***https://brave.com/***) is a relatively new web browser based on Google's Chromium (so it shares a lot of the same features as Chrome);

all the extensions that are compatible with Chrome are also compatible with Brave. The great thing about Brave, when compared to other browsers, is that its goal is to provide a private, tracker- and ad-free experience for users. By having an aggressive approach to blocking ads in the browser, Brave claims not only to save you time and bandwidth while using the internet but also to reduce the amount of battery your browser uses.

Brave provides much more granular control over your security and privacy settings, and it makes these settings much easier to get to than other browsers:

1. At the top right of the Brave browser, click the **More** icon (three horizontal lines).
2. Click **Settings ▸ Shields**.
3. Set Trackers & Ads Blocking to Standard or Aggressive.
4. Turn on **Upgrade Connections to HTTPS**.
5. Set Cookie Blocking to Only Cross-site or All (your browser won't remember your session information once closed).
6. Set Fingerprinting blocking to Standard or Strict (might break some websites).

Experiment with these settings, as well as the social media blocking settings, until you find a combination that works for you.

#25: Blocking Ads with Pi-Hole

Blocking ads with a browser extension or built-in tools is a great start to enhancing your internet browsing experience. However, those options apply to only one device at a time, and managing settings for multiple devices can quickly become onerous. Not only that, but some websites can block browser extensions. Blocking ads at the DNS level mitigates all of these issues.

The *Domain Name System (DNS)* enables your computer (or browser) to communicate with websites on the internet. All websites have an IP address (or more than one) assigned to them. Compared to IP addresses, the URLs that you use to access websites (for example, ***www.facebook.com***) are human-readable and easy to remember. Your computer translates that URL into an IP address to find the web server on the internet that serves Facebook to you—enter DNS. DNS acts like the postal service, in that IP addresses are equivalent to physical addresses, and URLs are like street names. DNS allows you to send and receive internet traffic to a specific address (or server) without having to remember the exact address (the IP address) of that server.

Given that advertising domains also use DNS to serve you ads, let's build a *Pi-Hole* server to send all of those requests to a blackhole and provide your users with a better browsing experience. Pi-Hole is similar to the Squid proxy discussed in **Chapter 6**; it sits between you and the websites you want to browse, observing all internet traffic, identifying advertising at the DNS level via a curated list of known advertising domains and addresses, and allowing only legitimate, non-ad traffic to pass through to your browser. Pi-Hole is capable of blocking a larger percentage of ads than browser solutions, and it's much harder for websites to detect and circumvent.

Set up an Ubuntu server in your local network, as discussed in **Chapter 1**, and add it to your network map and asset list. It's possible to use a server located in the cloud, but exposing a DNS server to the open internet creates some technical challenges we won't cover in this chapter. The right mitigating controls can solve these challenges, so if you choose to use a cloud server, proceed cautiously and do some research into how to mitigate the risks. If you've installed a perimeter firewall as discussed in **Chapter 3** and you create your Pi-Hole server using a virtual machine, the server should be located behind the firewall (that is, on the network side of the firewall, rather than the internet side).

It's possible to use Pi-Hole in conjunction with Squid (discussed in **Chapter 6**) by using Pi-Hole to handle DNS requests and Squid to handle HTTP traffic. However, by default Squid uses an internal DNS client—this can't be changed without rebuilding Squid, which is outside the scope of this book. If you choose to use both Squid and Pi-Hole, you can follow the instructions supplied for configuring each solution separately on your endpoints and achieve the same outcome.

Configure Pi-Hole

Begin by creating a base Ubuntu server, as described in **Chapter 1**. Then, install the Pi-Hole server using the following steps:

1. 1. Log in to your Ubuntu server via SSH as a standard, non-root user. Then, download the Pi-Hole installation script from ***https://install.pi-hole.net/***, make it executable, and execute the script using `sudo`:

```
$ ssh user@your_server_ip
$ wget -O basic-install.sh https://install.pi-hole.net
$ chmod +x basic-install.sh
$ sudo ./basic-install.sh
```

2. At this point, the automated installer will take over your terminal window. Read the various informational screens that come up, pressing ENTER to move to the next one.
3. 3. When prompted to select an upstream DNS server, as shown in **Figure 7-1**, choose whichever upstream (authoritative) DNS provider you're comfortable with. Google or Quad9 is a good choice.

NOTE *Use the arrow keys or TAB to navigate through the options, spacebar to select options, and ENTER to accept settings.*

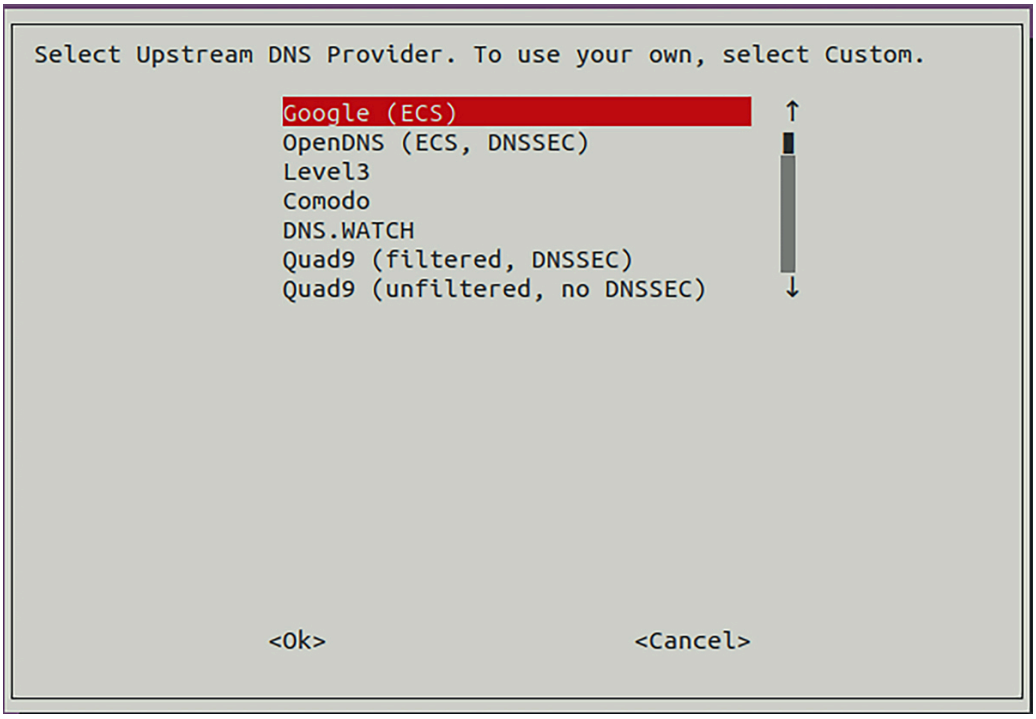

***Figure 7-1**: Upstream DNS provider*

To perform DNS lookups, your Pi-Hole server will need an authoritative DNS server to query when it attempts to resolve domains that aren't already cached by the proxy server. An *authoritative* DNS server is a nameserver that holds the actual DNS records for a particular domain or address, such as ***www.google.com***. By contrast, your server is *recursive*, an intermediary between you and your host and one or more authoritative DNS servers. When you make a request for a website, your device will pass this request to the Pi-Hole server, which will then farm this request out to an authoritative server to find the address of the website you want to view.

4. 4. Select all the available blocklists when prompted.

Pi-Hole uses *blocklists* (curated lists of advertising domains maintained by third parties) to identify and intercept advertisements on the internet. The chosen lists can be changed later.

5. 5. Select IPv6 in addition to IPv4 at the protocol screen if you use IPv6 in your network.

In most cases, IPv6 isn't necessary. IPv6 provides internet-addressable IP space to endpoints, which you don't need to do in this situa-

tion. It's best to disable IPv6 to reduce your attack surface, unless you have a legitimate use for it.

6. 6. The following screen indicates the static IP address and gateway of your server. If the address details listed on this page are correct, press ENTER to accept them. Otherwise, select **No** and press ENTER; then set your desired static IP details manually.

The gateway for your Pi-Hole could be your firewall or router. Once you've configured or accepted the IP settings for your server, the automated installer will warn about configuring your router or DHCP server to reserve the IP address for this server. If you don't do this, your network may encounter address conflicts, but most routers will be able to avoid this conflict without your input. (See "**Static IP Addressing**" in **Chapter 4** for configuring static IP addresses on a router.) Press ENTER to acknowledge the warning.

7. Select **On** to install the web interface, which makes the server configuration easier to manage (even for advanced administrators), and then press ENTER.
8. Select **On** to install the web server offered by the automated installer, unless you plan to install your own (this is beyond the scope of this book).
9. 9. Select **On** to log the DNS queries that pass through your Pi-Hole server.

Since Pi-Hole is a proxy, it will record and cache all web requests that pass through it. This means that any endpoint configured to use your Pi-Hole server for DNS will have its browsing history recorded. If this poses concerns for your users, either get their permission or turn logging off. You don't need logging to use Pi-Hole's ad-blocking features, but enabling it can help troubleshoot any issues.

10. 10. Select a privacy level that is acceptable within your network.

Pi-Hole uses *Faster Than Light (FTL)* DNS, which provides statistics about Pi-Hole activity and displays it graphically. You'll be able to see information such as how many ads were blocked, and for which endpoints, over a given period. FTL gets this data by parsing the Pi-Hole text logs. Like logging, this isn't necessary for Pi-Hole to

function and can cause privacy concerns for your users. Be sure to get their permission ahead of time, or set the privacy levels to Hide Domains and Clients, as shown in **Figure 7-2**. Doing so will prompt FTL to collect anonymized data, allowing the statistics and graphical displays to function while preserving the privacy of your users. You could also decide to disable statistics entirely by turning logging off in the previous step.

***Figure 7-2**: FTL DNS settings*

11. 11. When the installation finishes, you'll be presented with a screen showing your configuration, as well as the URL and administrator password for the web interface, as shown in **Figure 7-3**. Be sure to record these values, ideally in a password vault (discussed in **Chapter 11**) for security and safety purposes; then press ENTER to return to the terminal.

***Figure 7-3**: Pi-Hole installation complete*

You can change the administrator password with the following command:

```
$ sudo pihole -a -p
```

To keep Pi-Hole up-to-date, periodically run the following command:

```
$ sudo pihole -up
```

Ensuring that Pi-Hole and its components are up-to-date is crucial in keeping your Pi-Hole server, and your network, secure.

Using Pi-Hole

Browse to the administrator URL displayed in the last configuration step (*http://<your_server_ip>/admin/*) where you should see the user dashboard. When a new update is available, you'll be notified at the bottom of this screen, as in **Figure 7-4**. At this time, it's not possible to

update Pi-Hole from the web interface; it must be updated using the commands in the previous section.

***Figure 7-4**: Pi-Hole update required*

Click **Login** on the left side of the screen and authenticate with your administrator username and password. The dashboard will then display more detailed information. You'll find additional options in the administrator menu once logged in, as shown in **Figure 7-5**.

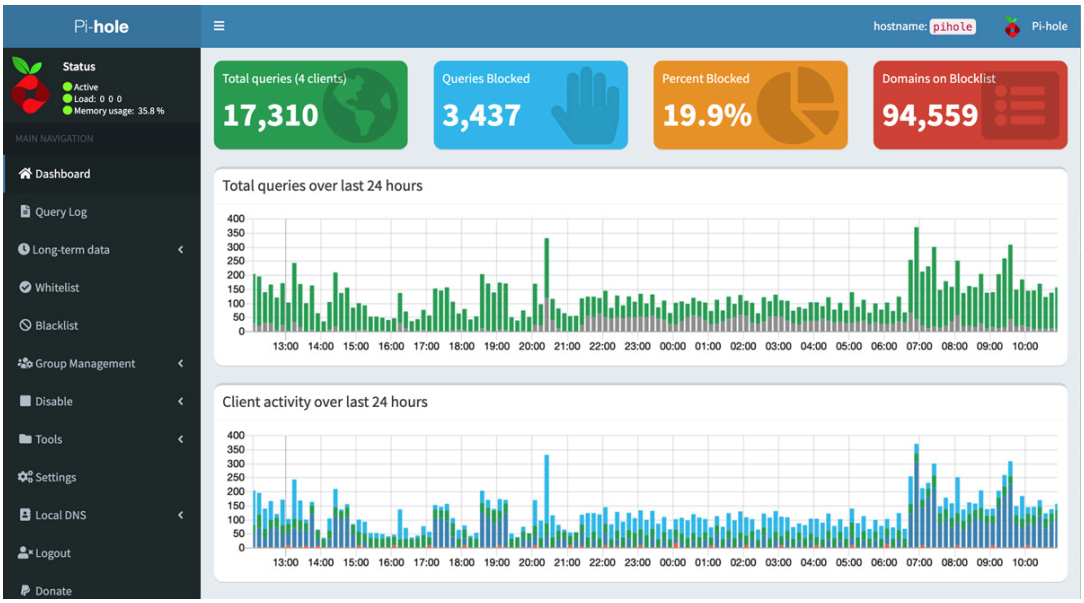

***Figure 7-5**: Pi-Hole administrator dashboard*

Brief descriptions of the important options in the navigation dashboard are as follows:

Query Log A chronological, searchable history of all browser requests for websites that pass through the Pi-Hole proxy server.

Long-term Data A more extensive history of requests to the proxy server that you can filter based on ranges of dates.

Whitelist Websites that Pi-Hole blocks by default but to which you'd like to allow access.

Blacklist Domains that the proxy may not block by default but that you'd like to block explicitly.

NOTE *While we've been using allowlist/denylist, Pi-Hole uses whitelist/blacklist for its menu options and configuration. When discussing Pi-Hole, we'll adhere to this terminology.*

Disable Disable the proxy for a set period.

Tools Used to debug or update the blocklists, and review backend proxy logs. The backend logs provide debug information about Pi-Hole itself, rather than web traffic.

Tools ▸ Network Displays all clients connected to the Pi-Hole server to help identify which endpoints are using the proxy and which may be bypassing it (your network map and asset list will come in handy).

Settings ▸ System Contains the Pi-Hole proxy settings (including settings configured during installation); displays critical information; allows you to disable, restart, and power off the server; and lets you flush (delete) DNS proxy logs.

Settings ▸ DNS Change the authoritative DNS servers used for domain name translation and modify the network interface on which requests are received and passed through the proxy filter (though the default settings are usually the safest).

Settings ▸ DHCP Allows the Pi-Hole server to act as a DHCP server if desired.

Settings ▸ Privacy Increase or decrease the level of privacy used when reporting about queries by choosing to link endpoints with their browsing activity or anonymize the data captured by the proxy.

Settings ▸ Teleporter Imports or exports Pi-Hole settings to or from another server.

Logout Logs you out of the administration dashboard.

Explore the various menus and options to familiarize yourself with Pi-Hole's settings and configurations. Consider reading the manual as well to get a better understanding of how Pi-Hole works and how powerful it really is.

Configure DNS on Your Endpoints

At this point, there's only one thing left to do: make your clients use the Pi-Hole server as their DNS server. You need to configure your DHCP server or router to push the DNS settings to devices that access the internet. Alternatively, you can configure each endpoint individually using its internal network settings. You might want to do this if you'd like only specific devices on the network to connect through the proxy while letting others connect to the internet directly. That said, making all devices go through the Pi-Hole server will provide the best experience to users and allow you to have better control of network traffic and identify issues earlier. The server will also cache more websites as users browse to them, which will make browsing to frequently visited sites faster for everyone.

NOTE *Your router is capable of specifying the DNS server your endpoints use to access the internet. In the ASUS router we've been using as an example, it's under Advanced Settings ▸ LAN ▸ DNS Server. Enter your Pi-Hole server's IP address in the DNS Server1 box and click* ***Apply*** *to set the DNS server connected clients will use.*

If you want only some of your endpoints to use the Pi-Hole server, either you can configure those clients using their local DNS settings or you can use the DNS settings in your pfSense firewall (if you implemented pfSense, as discussed in **Chapter 3**).

Windows DNS Settings

To configure the DNS settings on a Windows client, follow these steps:

1. Open **Settings ▸ Network & Internet4Change Adapter Options**.
2. Right-click **Ethernet Adapter**.
3. Click **Properties**.
4. Click **Internet Protocol Version 4 (TCP/IPv4) ▸ Properties**.
5. Select the **Use the Following DNS Server Addresses** radio button.
6. Enter the IP address of your Pi-Hole server in the Preferred DNS Server box.
7. Click **OK** and close all remaining windows.

macOS DNS Settings

To configure your Mac to use your Pi-Hole server for DNS, follow these steps:

1. Open **System Preferences ▸ Network**.
2. Select your network adapter (**Ethernet** or **Wi-Fi**) in the connection list on the left.
3. Click **Advanced ▸ DNS**.
4. Add your Pi-Hole server's IP address to the DNS servers list on the left.
5. Click **OK ▸ Apply**.

Linux DNS Settings

To route DNS requests through your Pi-Hole server on Linux endpoints, follow these steps:

1. Open **Settings ▸ Network**.
2. Click the configuration **Cog** to the right of your Wired or Wireless connection.
3. Select the **IPv4** tab.
4. Enter your Pi-Hole server's IP address in the DNS box.
5. Click **Apply**.

pfSense DNS Settings

Using pfSense, you're able to configure DNS settings either per client within the static IP addressing settings you will have used earlier or en masse by pointing your pfSense appliance at your Pi-Hole server for DNS. To send all DNS requests through your Pi-Hole server, enter your Pi-Hole IP address in the DNS servers box on the **Services ▸ DHCP Server** page. If you want to specify which endpoints will use the Pi-Hole server for DNS, follow these steps:

1. Browse to the **Services ▸ DHCP Server** page of your pfSense appliance.
2. Find the Static Mapping option for the relevant endpoint in the DHCP Static Mappings table at the bottom of the page.
3. Click the **Edit** pencil icon for that endpoint.
4. Enter your Pi-Hole server's IP address in the DNS box.
5. Click **Save ▸ Apply Changes**.

Once you've configured your endpoints using any of the previous options, you can test your ad-blocking capability using a website like ***https://canyoublockit.com/***. Such websites provide several options for testing your ad blockers, whether they're browser-based or something more substantial like Pi-Hole, from simple to advanced testing methods. If you run these tests and see no ads, your ad blocker is working. If you still see ads, review the earlier sections of this chapter and ensure your settings are correct. Log in to your Pi-Hole server and check the dashboard to see if your DNS queries are being seen by, and are therefore passing through, the server.

Summary

Regardless of how you choose to use Pi-Hole, you now have a means of monitoring and controlling internet usage in your network, and everyone should have a better internet browsing experience. You can choose to use Pi-Hole in addition to the Squid proxy you might have implemented in **Chapter 6**, or you can use either Squid or Pi-Hole without the other. Whichever solution you choose, you'll experience the benefits associated with that technology. Alternatively, you can forego DNS-level ad blocking if you prefer to use browser-based blocking utilizing browser add-ons; the choice is yours.