

Private Router Setup Manual



PrivateRouter LLC
618 E. South St, Suite 500,
Orlando, FL 32801 USA

v1 2023-8

© 2023 by PrivateRouter LLC. All rights reserved.

Trademarks

TorGuard is a trademark of VPNetworks LLC. "WireGuard" and the "WireGuard" logo are registered trademarks of Jason A. Donenfeld. Other brand names and products are registered trademarks of their respective holders.

Statement of Conditions

In the pursuit of enhancing internal architecture, operational performance, and/or dependability, PrivateRouter LLC reserves the right to modify the products detailed in this document at any time without prior notice. PrivateRouter LLC does not assume any responsibility for any liabilities that may arise from the usage or implementation of the product(s) or circuit configuration(s) described herein.

Chapter 1

Getting Started

This chapter outlines the steps for plugging in your router and establishing an Internet connection through it.

What's Included in the Package?

The following items should be included in the product box:

- The PrivateRouter device
- A region-specific AC power adapter
- One Ethernet cable

If you find any components to be incorrect, missing, or damaged, get in touch with PrivateRouter or TorGuard customer service. Retain the box and all original packaging materials in case you need to send the product back for repairs or replacement.

The Wireless Router Ports

Depending on the model, your PrivateRouter should feature the following ports and buttons: LAN ports for connecting your devices, a WAN port for linking to an internet-enabled router or modem, a power on/off button, and a slot for the AC adapter plug.

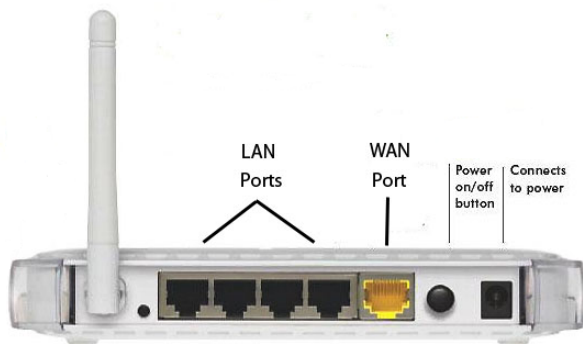
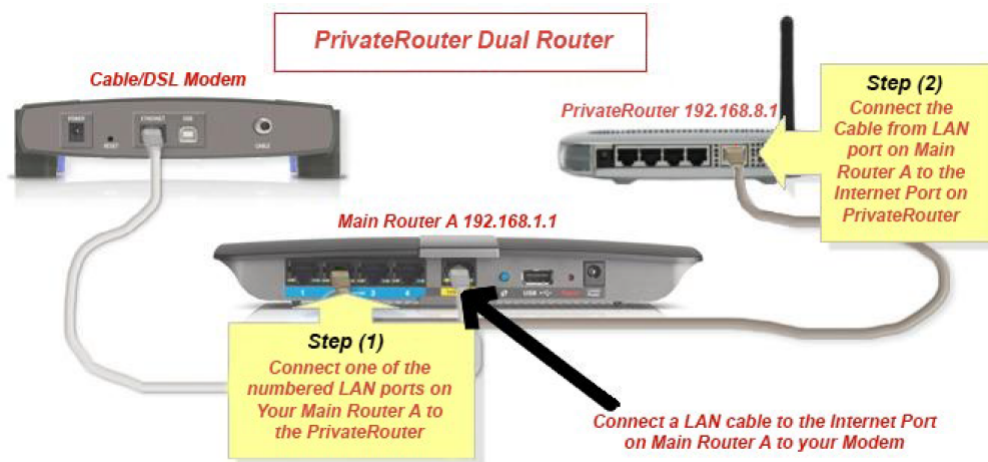


Figure 1-1

Integrating Your PrivateRouter into a Dual-Router Configuration

If you wish to maintain your current WiFi network and simply add a VPN-enabled WiFi network via PrivateRouter, you can accomplish this with a dual-router configuration. There's no need to alter settings in your existing network router to integrate a PrivateRouter in this dual-router arrangement. Because all PrivateRouters come preconfigured with a unique Local IP Address, there will be no conflict with your current router.

In this dual-router setup, the PrivateRouter is connected to your existing router using an Ethernet cable, providing you with two distinct and separate WiFi networks.



Kindly note that the default IP address for standard PrivateRouter VPN WiFi devices is **192.168.8.1**, while the default IP address for PrivateRouter Cloud devices is **192.167.70.1**

After Connecting Your PrivateRouter Power Cycle All Devices

- Power off your ISP modem and PrivateRouter
- Power on your ISP modem and wait for it to fully boot up.
- Power on your PrivateRouter
- Connect to PrivateRouter Wifi, enter the default password “torguard” and browse to 192.168.8.1

As an alternative to connecting via the PrivateRouter WiFi network, you also have the option to plug a LAN cable into the back of the router and connect it directly to a computer.

Setup Your PrivateRouter in a Standalone Router Configuration

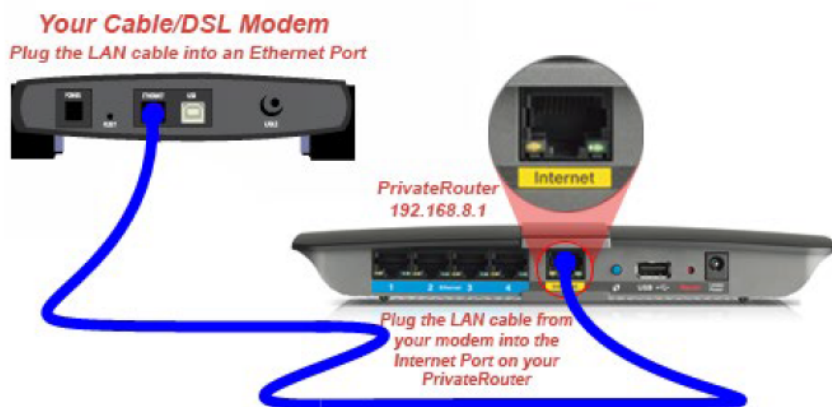


Figure 1-3

Connect the Internet Port on your PrivateRouter to your cable or DSL Modem

If you're looking to replace an outdated WiFi router or wish to eliminate the monthly fees associated with a router leased from your Internet Service Provider, consider using your PrivateRouter as the sole WiFi device in your network. In this standalone router configuration, the PrivateRouter is connected directly to your cable or DSL modem using an Ethernet cable, serving as the exclusive WiFi router in the setup.

Restart your Cable/DSL Modem and PrivateRouter

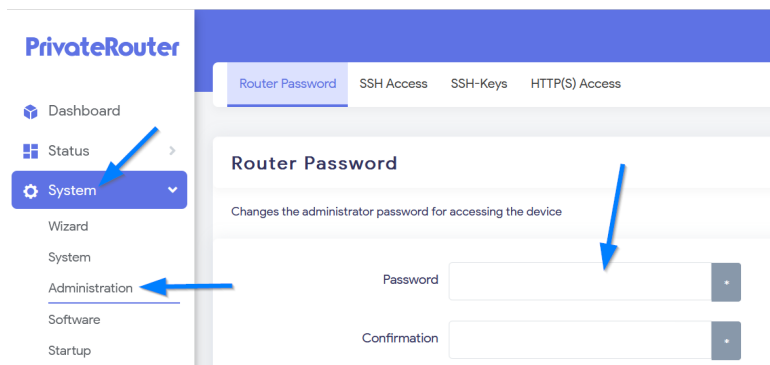
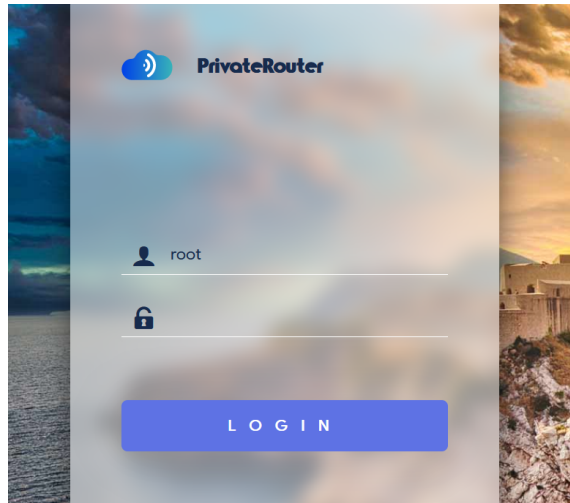
Make sure to restart your devices after plugging in your PrivateRouter:

- Power off your ISP modem and PrivateRouter
- Power on your ISP modem and wait for it to fully boot up. Power on your PrivateRouter
- Connect to PrivateRouter Wifi, enter the default password “torguard” and browse to 192.168.8.1

As an alternative to connecting via the PrivateRouter WiFi network, you also have the option to plug a LAN cable into the back of the router and connect it directly to a computer.

Setting a Secure Admin Password

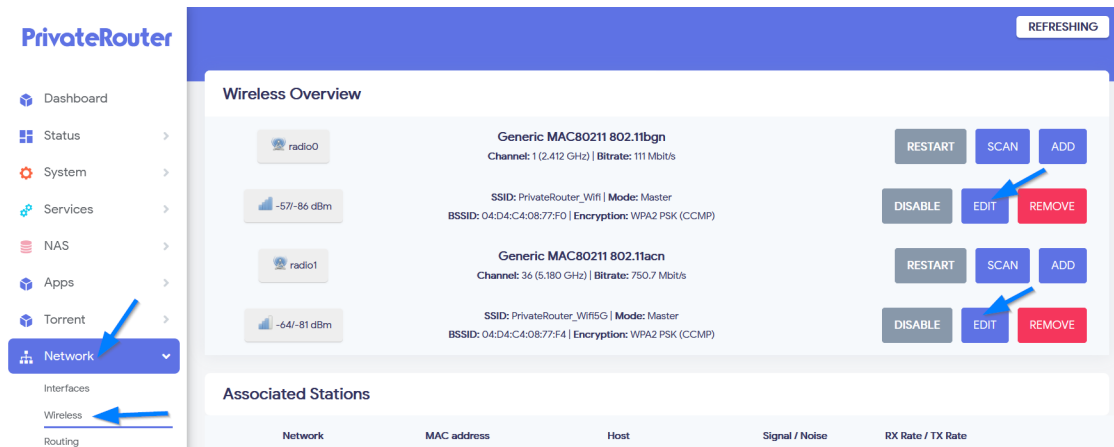
To access the PrivateRouter administrative interface, first connect to the PrivateRouter WiFi network. Once connected, open a web browser and navigate to: 192.168.8.1. The default username is "root," and the default admin password is "torguard". Input these credentials and then click the LOGIN button.



In the side menu, select the "System" option, followed by clicking on "Administration." In the password text field, enter your new, secure admin password. Confirm the password by retyping it in the box provided below. It's crucial to choose a secure password that is different from your WiFi password, as this will be the password you use to access the administrative interface at 192.168.8.1. Finally, click the Save button to finalize the changes.

Setting a Secure WiFi Password

Changing the PrivateRouter WiFi password is essential for security. To do so, initially access the administrative interface by navigating to **192.168.8.1**. In the left-hand panel, select the "Network" menu and then choose "Wireless." From the Wireless Overview menu, identify the WiFi network password you wish to update and click the "EDIT" button.



Enter a Secure WiFi Password

To set a new PrivateRouter WiFi password, navigate to the security tab within the WiFi network menu. Choose the WiFi encryption method you prefer, although we recommend WPA2 or WPA3 encryption for optimal security. In the "Key" field, input your new WiFi password. This will be the password you use to connect to the PrivateRouter WiFi network. Click the "SAVE" button and return to the Wireless Overview menu. To finalize your changes, click "SAVE" followed by "APPLY CHANGES."

Interface Configuration

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Encryption

WPA3-SAE (strong security)

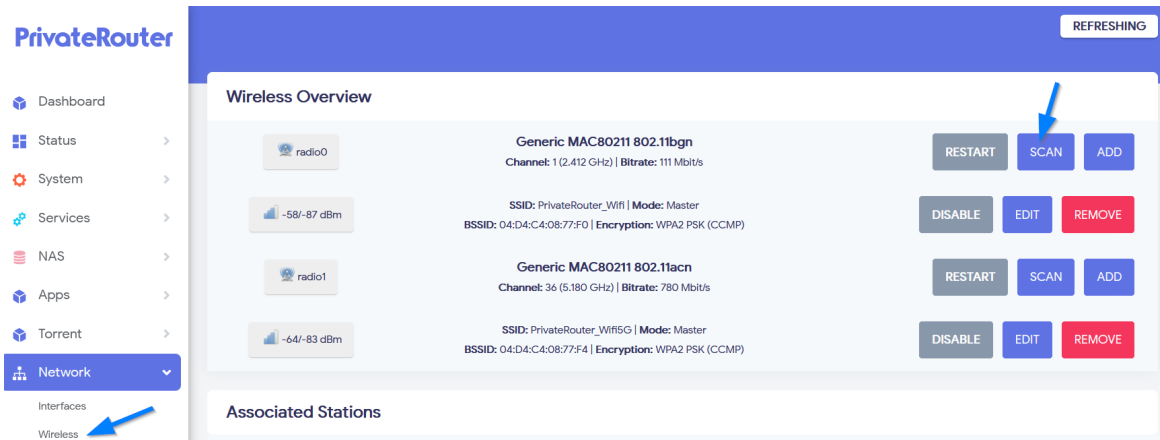
Key

••••••••

*

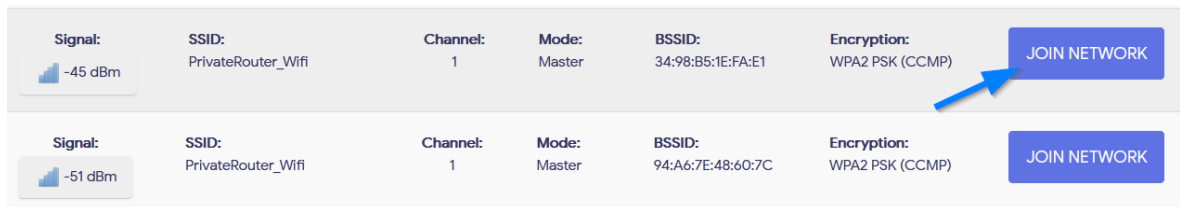
Connect to the Internet Through an Existing WiFi Network

In situations where WAN plugin access is unavailable, you can link your PrivateRouter to a pre-existing WiFi network for internet connectivity. If you can't physically connect a LAN cable to an existing router, you have the option to connect your PrivateRouter to an available WiFi network. To do so, navigate to the "Network" tab and then choose "Wireless." Hit the "Scan" button on your WiFi Radio device to display a list of all nearby WiFi networks.



Join a WiFi Network to Gain Internet Access

Wait briefly as your PrivateRouter completes its scan for nearby WiFi networks. Select the network you want to join and click on "JOIN NETWORK." In the subsequent screen, you'll be prompted to input the WiFi network's passphrase into a text field. Enter the required password and click "SAVE." To finalize the settings, go back to the Wireless Overview menu, click "SAVE," and then hit "APPLY SETTINGS."

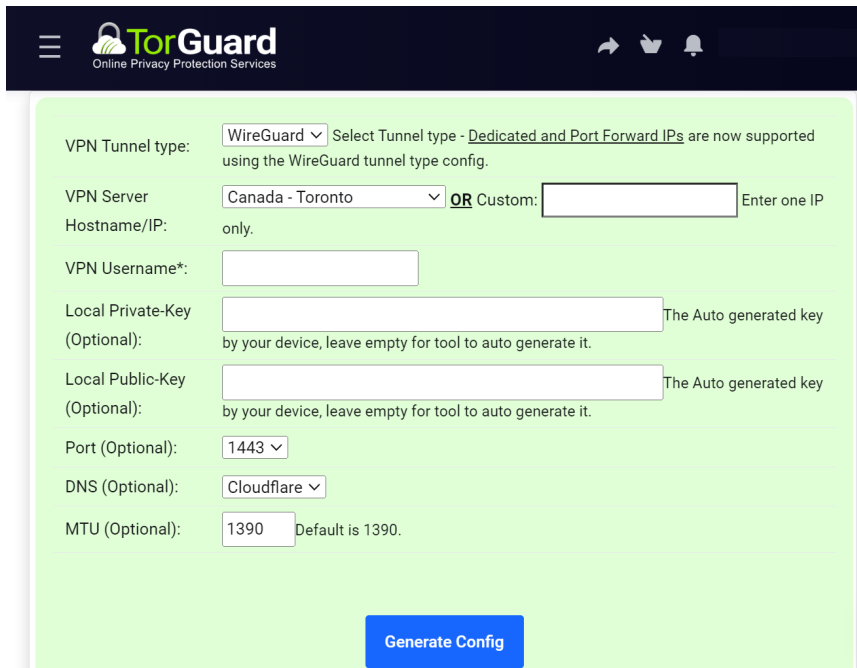


Connect Your PrivateRouter to TorGuard VPN

PrivateRouter OS is pre-set with user-friendly applications designed to facilitate effortless connections to TorGuard's VPN services. It supports a range of TorGuard protocols including WireGuard, OpenVPN, AnyConnect, SSTP, and V2ray. For optimal speed, we recommend using WireGuard. However, if WireGuard is restricted in your area, SSTP, AnyConnect, and V2ray are reliable alternatives capable of circumventing DPI firewalls.

Enable Wireguard VPN with TorGuard

Configuring WireGuard on your router using TorGuard's WireGuard config generator is straightforward and only involves copying and pasting your generated settings. In just a few easy steps, you can establish a secure, encrypted WireGuard VPN tunnel. Begin by navigating to the WireGuard config generator within TorGuard's member area. Select the VPN server location you prefer, generate the corresponding config, then simply highlight the text and right-click to copy it to your clipboard.



The screenshot shows the TorGuard website's WireGuard configuration generator. The interface has a dark blue header with the TorGuard logo and navigation icons. The main content area is light green and contains several input fields and a 'Generate Config' button. The fields are for VPN Tunnel type (WireGuard), VPN Server (Canada - Toronto), Hostname/IP, VPN Username, Local Private-Key, Local Public-Key, Port (1443), DNS (Cloudflare), and MTU (1390). There are also checkboxes for 'Dedicated and Port Forward IPs' and 'Custom' options.

VPN Tunnel type: Select Tunnel type - Dedicated and Port Forward IPs are now supported using the WireGuard tunnel type config.

VPN Server: **OR** Custom: Enter one IP

Hostname/IP: only.

VPN Username*:

Local Private-Key (Optional): The Auto generated key by your device, leave empty for tool to auto generate it.

Local Public-Key (Optional): The Auto generated key by your device, leave empty for tool to auto generate it.

Port (Optional):

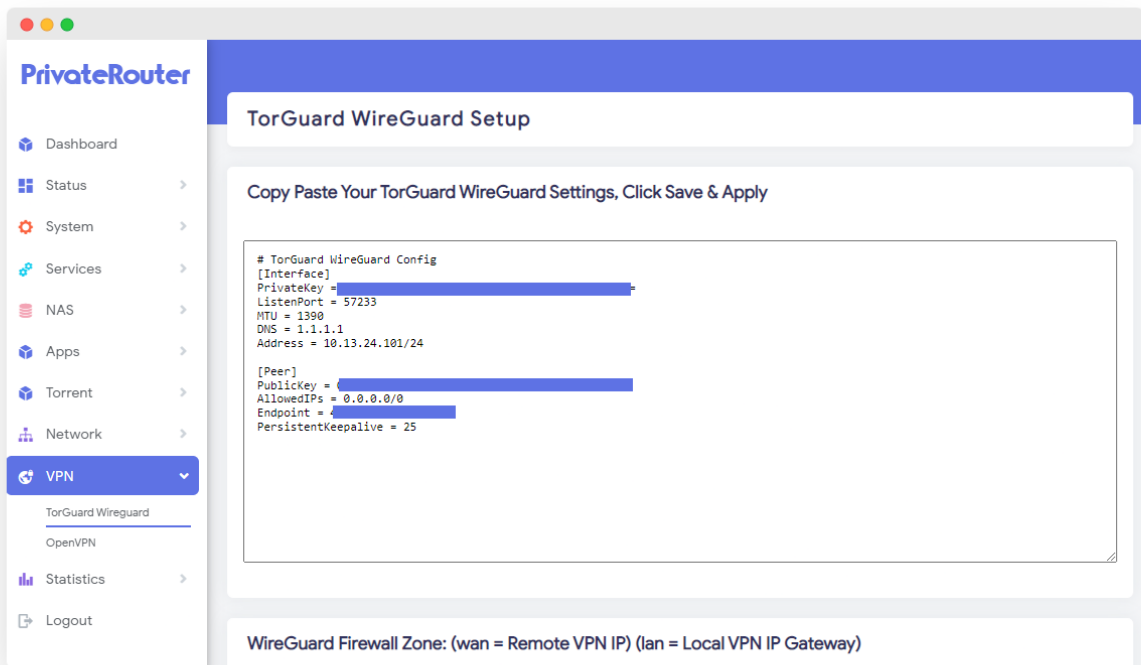
DNS (Optional):

MTU (Optional): Default is 1390.

[Generate Config](#)

Add Your Wireguard config to PrivateRouter

To upload your newly generated WireGuard configuration to your PrivateRouter, navigate to the VPN tab in the side menu and select "TorGuard WireGuard." Right-click inside the large text box and choose the paste option to insert your complete WireGuard configuration settings. After that, hit the "SAVE" button at the bottom of the page, followed by "SAVE and APPLY." To initiate the WireGuard tunnel, click the "START WIREGUARD" button. To disable WireGuard at any point, simply click the "STOP WIREGUARD" button. If you intend to use the VPN tunnel for your router's IP address (which is the most common setup), keep the firewall zone set to "lan." If you are utilizing TorGuard's Private VPN Cloud services for remote access to your PrivateRouter network, select the "wan" option for the firewall zone.

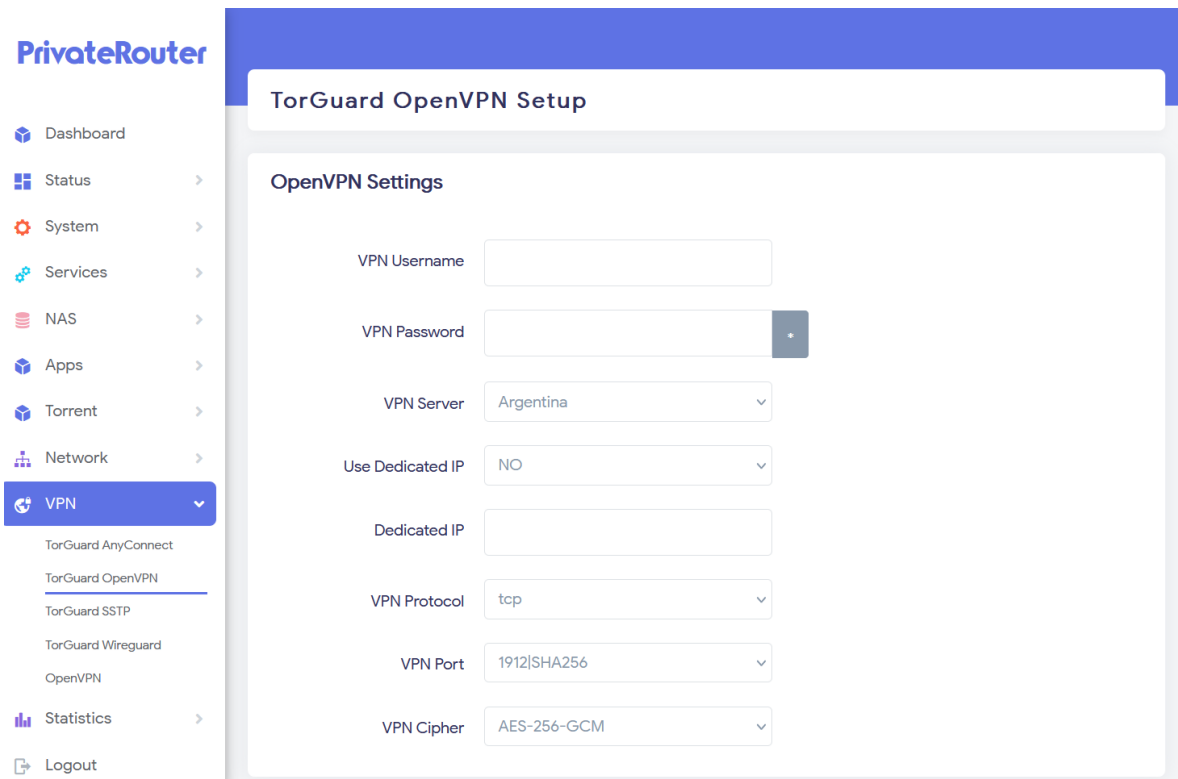


Remember to click save and apply then select "START WIREGUARD" each time you update your Wireguard config with a new VPN server location.

Connect to TorGuard's OpenVPN Service

The TorGuard OpenVPN app on PrivateRouter offers a user experience comparable to TorGuard's desktop and mobile VPN applications. Whether you're seeking the speediest protocol and cipher for your specific VPN router or configuring a residential IP add-on (which involves simply pasting the IP and toggling the Dedicated IP switch to ON), the process is incredibly straightforward. To activate TorGuard OpenVPN on your PrivateRouter, navigate to the VPN tab and choose "TorGuard OpenVPN." Input your TorGuard VPN username and password, then select your preferred VPN server, port, protocol, and cipher. Click "SAVE and APPLY," followed by the "START OPENVPN" button.

If you intend to use a dedicated IP, insert that IP address into the text box and switch the dedicated IP dropdown option to YES.



PrivateRouter

- Dashboard
- Status
- System
- Services
- NAS
- Apps
- Torrent
- Network
- VPN**
 - TorGuard AnyConnect
 - TorGuard OpenVPN**
 - TorGuard SSTP
 - TorGuard Wireguard
 - OpenVPN
- Statistics
- Logout

TorGuard OpenVPN Setup

OpenVPN Settings

VPN Username	
VPN Password	
VPN Server	Argentina
Use Dedicated IP	NO
Dedicated IP	
VPN Protocol	tcp
VPN Port	1912 SHA256
VPN Cipher	AES-256-GCM

Connect to TorGuard SSTP VPN

Among the various stealth VPN tunneling options that TorGuard provides, SSTP is noteworthy for its impressive speed and router performance. Although it may not rival the speed of WireGuard, it certainly outperforms OpenVPN, providing ample bandwidth to meet the data requirements of all your connected devices and delivering smooth content streaming experiences.

Configuring SSTP on an OpenWRT system can be somewhat challenging. This SSL VPN tunnel works on non-standard ports and typically requires code adjustments to ensure compatibility with TorGuard's SSTP VPN. While this level of complexity might discourage those less familiar with technology or those seeking a more straightforward setup, PrivateRouter has simplified the process for you.

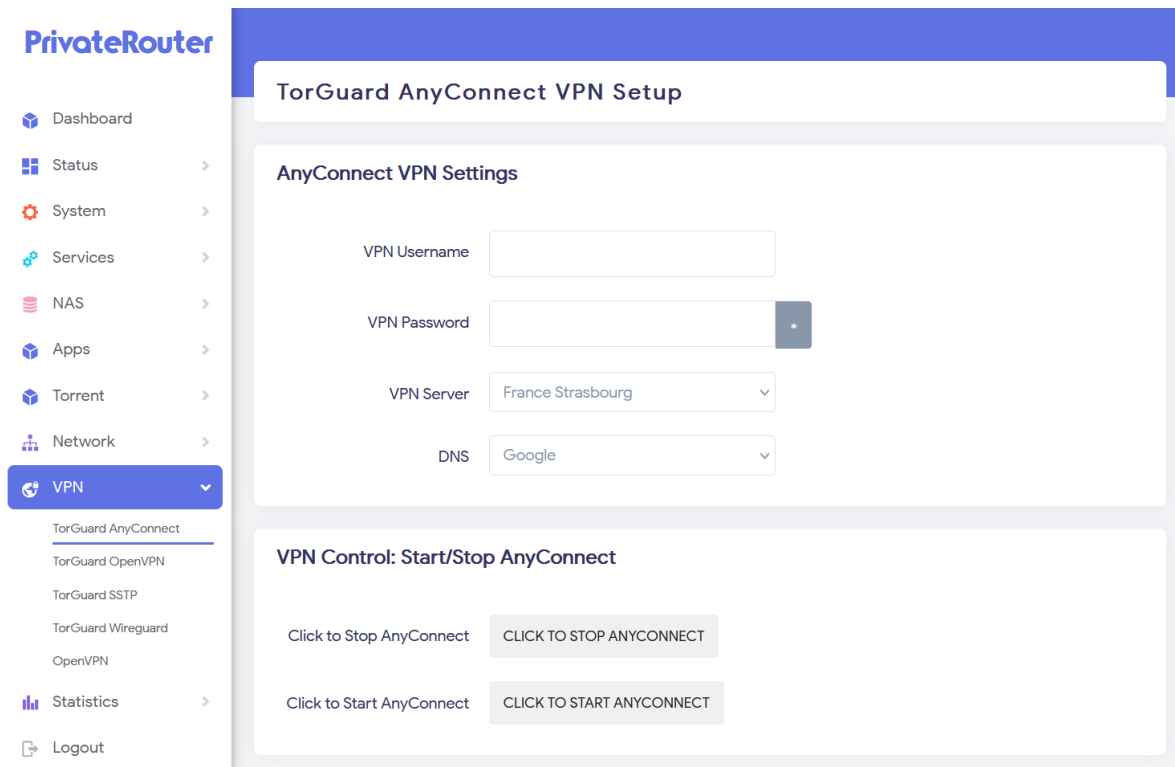
To activate TorGuard SSTP on your router, navigate to the VPN tab in the side menu and select "TorGuard SSTP." Input your TorGuard VPN username and password, then click "SAVE and APPLY." To initiate the SSTP tunnel, click the "Start SSTP" button.

The screenshot displays the PrivateRouter web interface. On the left is a sidebar menu with the following items: Dashboard, Status, System, Services, NAS, Apps, Torrent, Network, VPN (highlighted with a dropdown arrow), TorGuard AnyConnect, TorGuard OpenVPN, TorGuard SSTP (underlined), TorGuard Wireguard, OpenVPN, Statistics, and Logout. The main content area is titled "TorGuard SSTP VPN Setup". It contains two sections: "SSTP VPN Settings" and "VPN Control: Start/Stop SSTP". The settings section has three fields: "VPN Username" (text input), "VPN Password" (password input with a toggle for visibility), and "VPN Server" (a dropdown menu currently showing "France Paris"). The control section has two rows of buttons: "Click to Stop SSTP" with a grey button labeled "CLICK TO STOP SSTP", and "Click to Start SSTP" with a grey button labeled "CLICK TO START SSTP". At the bottom right of the main area are three buttons: "SAVE & APPLY" (blue), "SAVE" (blue), and "RESET" (orange).

Connect to TorGuard AnyConnect (OpenConnect) VPN

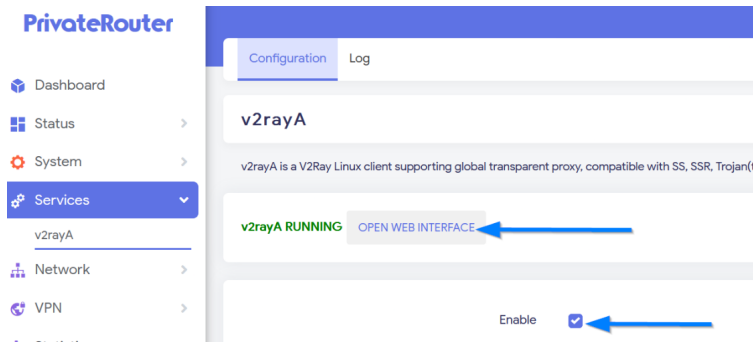
The TorGuard AnyConnect app, designed for OpenWRT, utilizes the open-source "OpenConnect" protocol, offering an exceptional VPN solution. This protocol is commonly referred to as a "stealth" VPN protocol because it operates through port 443, the standard port for encrypted SSL (Secure Sockets Layer) traffic. This feature allows the data to blend in with regular internet traffic, making it exceedingly difficult for Deep Packet Inspection (DPI) firewalls and censorship measures to block it.

To connect via TorGuard's AnyConnect VPN, navigate to the VPN tab in the side menu and select "TorGuard AnyConnect VPN." Enter your TorGuard VPN username and password. While the default DNS settings will suffice for most users, those in more restrictive regions may need to explore alternative DNS servers for connectivity. Finally, click "SAVE and Apply," and then select the "CONNECT to ANYCONNECT" button.

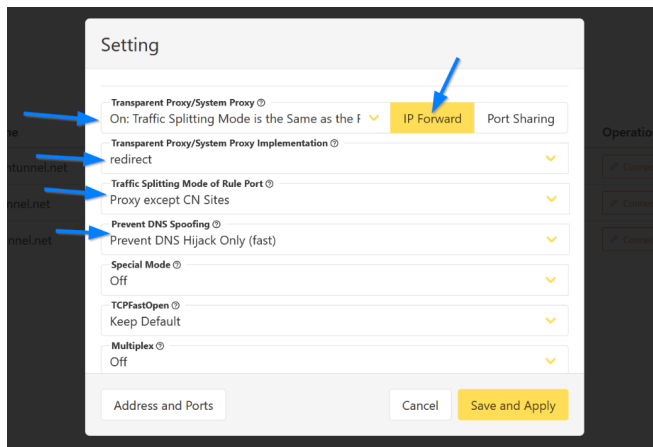


Connect to TorGuard's V2ray network with V2rayA

TorGuard's V2ray proxy network is among the quickest encrypted proxy protocols capable of circumventing even the most stringent DPI VPN blocks or firewalls, including those on highly restricted mobile networks globally. To route all your router traffic through TorGuard's vmess, vless, or trojan servers using V2rayA, first navigate to the "Services" option in the side menu and select "V2rayA." Tick the "Enable" checkbox, and then click "SAVE and APPLY." To proceed, open the V2rayA menu by clicking on "OPEN WEB INTERFACE."



Next, set your v2ray interface username and password. This password is stored on your local PrivateRouter.



Click the Settings option in the top left and adjust your settings as below. Under the last option "Mode" choose "Follow transparent proxy" and click save.

Lastly, click the "Subscription" button and paste your TorGuard subscription link from the V2ray services menu, or manually import your preferred servers one at a time via the "Server" tab. This action will populate your server list, and to establish a connection, simply click the "Connect" button.



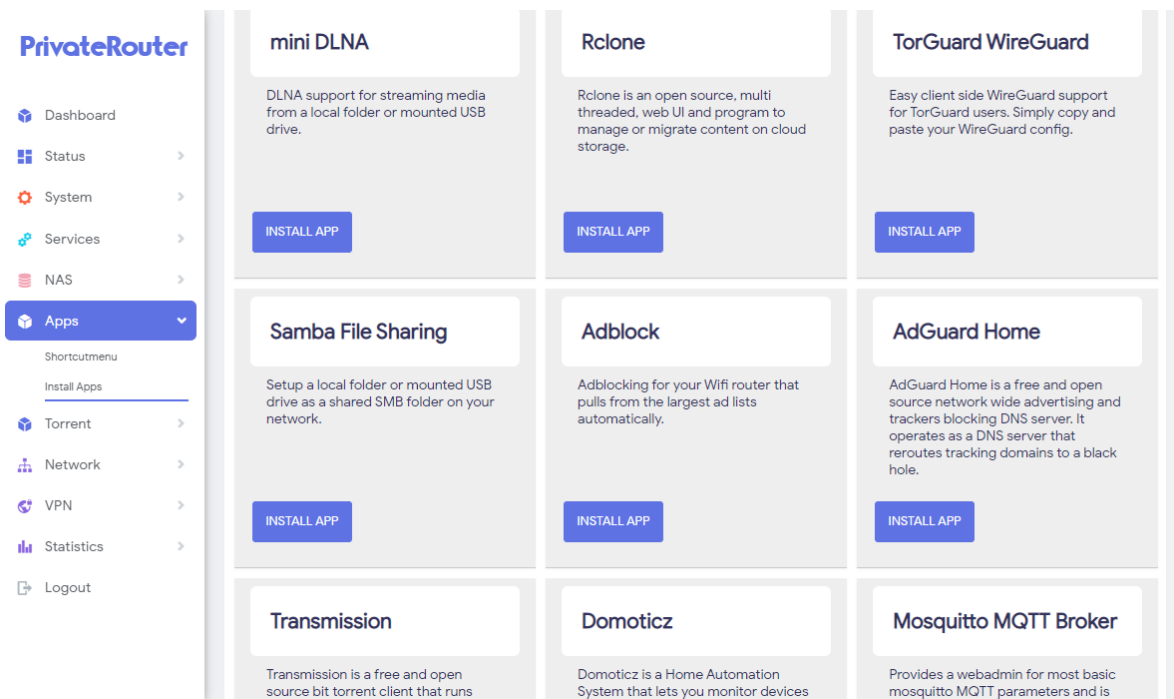
Chapter 2

PrivateRouter Apps

PrivateRouter OpenWRT features an enhanced storage build, offering 500MB for package storage and over 30GB of extra file storage. This allows for the installation of numerous third-party apps that wouldn't typically fit on the router's built-in storage.

Install PrivateRouter Apps

To add more third-party apps to your PrivateRouter, first navigate to the "Apps" option in the side menu and choose "Install Apps." For standard PrivateRouters, a list of all compatible apps will be displayed. If you're using a PrivateRouter Cloud device, you'll have the option to access over 100 apps that are Docker-powered.



After selecting the "Install App" button, scroll down to monitor the installation log and confirm that the app has been successfully installed. Once the app is added, you'll notice it appears in your side menu. For certain apps, you may need to log out and log back into the PrivateRouter menu to complete the process.

Configure Watchcat App to Minimize Downtime

To safeguard your network from unexpected ISP disruptions or VPN disconnections, you can utilize OpenWRT's Watchcat module to routinely ping a specific IP address. If there's no response, you can set a time duration for Watchcat to restart your router. Often, a simple reboot solves most connectivity issues.

The screenshot shows the PrivateRouter web interface. On the left is a sidebar menu with options: Dashboard, Status, System, Services (selected), Dynamic DNS, Shadowsocks-libev, Policy Routing, v2rayA, Watchcat (highlighted), miniDLNA, Network Shares, SmartDNS, NAS, and Apps. The main content area is titled 'General Settings' and contains the following configuration options:

- Mode:** A dropdown menu set to 'Ping Reboot'. Below it, explanatory text reads: 'Ping Reboot: Reboot this device if a ping to a specified host fails for a specified duration of time. Periodic Reboot: Reboot this device after a specified interval of time. Restart Interface: Restart a network interface if a ping to a specified host fails for a specified duration of time. Run Script: Run a script if a ping to a specified host fails for a specified duration of time.'
- Period:** A text input field set to '6h'. Below it, explanatory text reads: 'In Periodic Reboot mode, it defines how often to reboot. In Ping Reboot mode, it defines the longest period of time without a reply from the Host To Check before a reboot is engaged. In Network Restart or Run Script mode, it defines the longest period of time without a reply from the Host to Check before the interface is restarted or the script is run. The default unit is seconds, without a suffix, but you can use the suffix m for minutes, h for hours or d for days. Examples: 10 seconds would be: 10 or 10s 5 minutes would be: 5m 1 hour would be: 1h 1 week would be: 7d'
- Host To Check:** A text input field set to '8.8.8.8'.

To implement a Watchcat rule, go to the "Services" section in the side menu and choose "Watchcat." Choose "Ping Reboot" as the mode and specify a host IP for uptime checks.

After setting your preferences, scroll to the bottom of the page and click on "ADD" to activate the rule, followed by clicking the "SAVE AND APPLY" button. In this instance, the router will ping Google's DNS at 8.8.8.8. If there's no response after six hours, the router will automatically reboot.

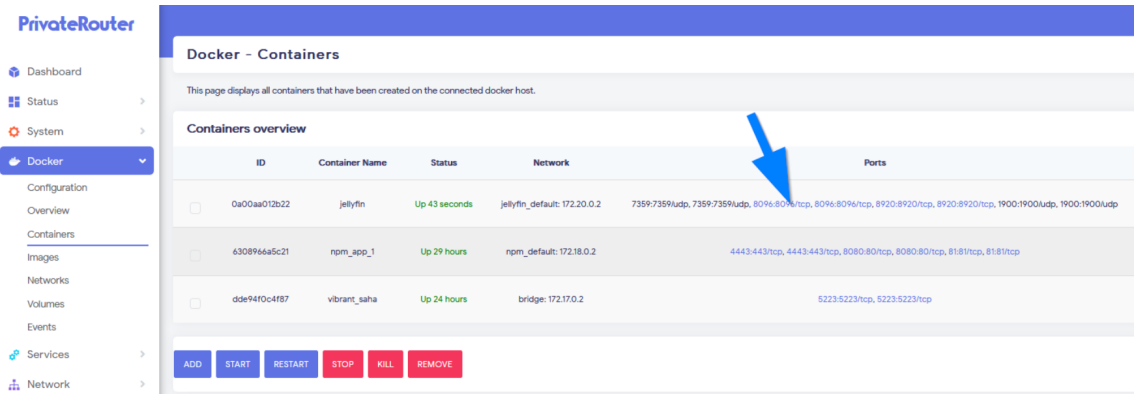
Watchcat offers additional reboot rules:

Periodic Reboot: This feature reboots the router after a set period.

Restart Interface: This setting will only reboot a specific network interface if a ping to a predetermined host goes unanswered for a specified length of time.

How to Access Docker Apps (PrivateRouter Cloud)

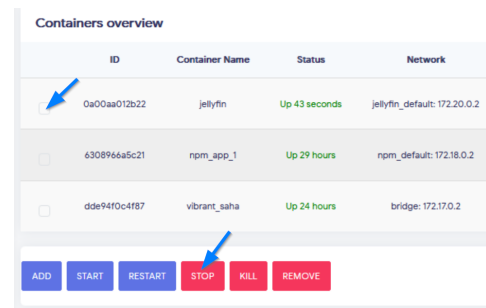
PrivateRouter Cloud x86 routers offer a simplified, one-click approach for deploying widely-used, self-hosted applications directly onto your router via Docker. Coupled with TorGuard's Private VPN Cloud service, you can effortlessly self-host apps while maintaining security through a WireGuard VPN. Jellyfin is a popular choice for a self-hosted media streaming server, providing you with control over streaming via a web interface and mobile apps for both Android and iOS.



To get Jellyfin up and running, first sign in to your PrivateRouter Cloud device. From the left-side menu, go to the "Apps" section and click on "Install Apps." Find Jellyfin in the list and click the "INSTALL" button. The installation time will vary based on your internet speed. Once the installation is finished, navigate to the "Docker" menu on the left and select "Containers." Here, you'll see all Docker apps listed as virtual containers. In this example, find the Jellyfin container and click on the TCP port 8096 to launch Jellyfin in a new browser window. Alternatively, you can manually enter the app port in a web browser by going to **192.168.70.1:8096**.

How to Start, Stop, or Remove Docker Apps

You can follow the same steps for every new Docker app you wish to install. Each application will be assigned its own unique port number, which you can find listed under the "Docker" menu in the "Containers" section. If you want to Stop, Start, or Remove any installed Docker app, simply check the box next to the specific app and then select the corresponding action button located below.



Troubleshooting the Internet Connection

TorGuard's VPN services are highly stable, often maintaining connections for months at a time without any interruptions. However, if you encounter a situation where your PrivateRouter device loses internet connectivity—especially after configuring various VPN or Router apps—you can usually resolve the issue with a few simple steps.

The quickest solution is often to reboot the router, which tends to resolve most connectivity problems. Alternatively, you can go to the "Network" tab located in the left-hand menu and select the "Interfaces" option. Here, you'll find the WAN (highlighted in red) and any VPN-specific interfaces you might have set up. Click the 'Restart' button next to each WAN interface, as well as next to the particular VPN protocol interface you're using. After waiting a few minutes, try to reconnect to the internet.

WAN  wan	Protocol: DHCP client Uptime: 70d 20h 17m 32s MAC: 0E:DD:68:BF:A2:DD RX: 705.01 GB (944943108 Pkts.) TX: 374.66 GB (741103707 Pkts.) IPv4: 192.168.1.53/24	RESTART STOP EDIT DELETE
WAN6  wan	Protocol: DHCPv6 client MAC: 0E:DD:68:BF:A2:DD RX: 705.01 GB (944943108 Pkts.) TX: 374.66 GB (741103707 Pkts.)	RESTART STOP EDIT DELETE
WG  wg	Protocol: WireGuard VPN Uptime: 68d 0h 25m 22s RX: 39.28 GB (62449418 Pkts.) TX: 68.32 GB (88135453 Pkts.) IPv4: 10.77.1.2/16	RESTART STOP EDIT DELETE

Similarly, if a particular application or service such as Samba or VPN is experiencing problems and you'd prefer not to reboot the entire router, you have the option to restart or stop that specific service individually. To do so, go to the 'System' tab in the left-hand menu and select 'Startup.' From there, find the service you want to restart and click the 'RESTART' button.

System Wizard System Administration Software Startup Scheduled Tasks Mount Points	10 tgaryconnect ENABLED START RESTART STOP
	10 tgstsp ENABLED START RESTART STOP
	10 tgwireguard ENABLED START RESTART STOP
	11 fstab ENABLED START RESTART STOP

Should you continue to experience difficulties or have any inquiries regarding your PrivateRouter, you're welcome to file a support ticket on PrivateRouter.com or directly reach out to TorGuard support at helpdesk@torguard.net