Using a VPN/Proxy in Tails

Kaneesha Davis - 2018-05-29 - Browsing / Internet

Tor + VPN in Tails

The topic of VPN support in Tails (whether Tor > VPN or VPN > Tor) and the issues it presents are discussed here https://tails.boum.org/blueprint/vpn_support/

While it isn't recommended to use a VPN inside the Tails environment (nor would it even work properly without significant modification), using a proxy for specific purposes is completely fine. Your PIA account includes a free Netherlands proxy (proxy-nl.privateinternetaccess.com) that you can generate a userid/pass for and use inside Tails.

Proxy > Tor

If your threat model does not care if PIA knows which first-hop Tor node you connect to and you're merely trying to hide your Tor activity from your ISP, then a Proxy > Tor connection is ideal. You may also achieve this by using a private Tor bridge (requestable online at https://bridges.torproject.org/) but there is zero guarantee that the bridge being used won't also be known to your ISP and it will still be clear to your ISP that the traffic is Tor related.

To make this type of connection, supply the proxy information in the "Network connection" settings at the Tails startup screen.

Tor > Proxy (Using a program's internal proxy settings)

Note: these instructions must be repeated each time you restart Tails

If your threat model does not care if your local ISP knows you're using Tor and you wish to hide your Tor activity from the target website or service (i.e. a site that blocks or restricts Tor users), then a Tor > Proxy connection is ideal. Keep in mind that this would be making a connection between your PIA account details (and any payment methods used for it) and your activity on the target service site. Do not use this if you're trying to be anonymous unless you are confident that your purchase of PIA credentials was equally anonymous and understand the risks involved.

To make this type of connection, first you'll need to obtain SOCKS credentials from your PIA account page. Log in to your PIA account and on the account page (https://www.privateinternetaccess.com/pages/client-sign-in), in the "PPTP/L2TP/SOCKS Username and Password" section there should be a username and password to use for

proxy login. If not, click the button to generate one.

You will be provided with the host proxy-nl.privateinternetaccess.com and port 1080. Then, in the program you wish to route over SOCKS, change the proxy settings of the program to PIA's SOCKS host and credentials. Typically this data is already entered as 127.0.0.1 port 9050 to route the traffic over Tor.

Instead of running the program standalone, run it with the proxychains command. First we need to install proxychains.

```
sudo apt-get install proxychains
```

Now we run the program (in this example, hexchat)

```
proxychains hexchat
```

This forces the connection first over Tor (127.0.0.1:9150) and then uses the program's own connection functionality to connect to the SOCKS proxy.

If the program you want to run does not have proxy settings available, this method will not work.

Tor > Proxy (Forcing all traffic over proxychains; ideal for web browsers that don't have internal proxy settings)

Note: these instructions must be repeated each time you restart Tails

To use this method for a browser so that you can view a website through the PIA SOCKS, you will not be able to use the built-in tor-browser in Tails. Due to apparmor in Tails, the default tor-browser will not allow interaction with the regular file system and thus cannot read the proxychains.conf file properly. This restriction from such usage is done for your safety, and using another browser instead of it may put you at risk of reducing your anonymity or leaking more information. If you choose to accept this risk, you'lll need to install an additional browser to use for your Tor > SOCKS sessions.

If you haven't already installed proxychains, do that first!

```
sudo apt-get install proxychains
```

For this example, we'll use the firefox-esr browser for Debian.

```
sudo apt-get install firefox-esr
```

Now we need to update the proxychains config file to add the PIA SOCKS credentials. Since proxychains doesn't work with hostnames, we need to DNS the proxy-nl.privateinternetaccess.com domain to get an active SOCKS IP (at the time of writing this, DNS returned *109.201.154.168*)

```
host proxy-nl.privateinternetaccess.com
```

This will return something similar to the following in Tails:

```
../../../../lib/isc/unix/net.c:581: sendmsg() failed: Operation not permitted
../../../../lib/isc/unix/net.c:581: sendmsg() failed: Operation not permitted
proxy-nl.privateinternetaccess.com has address 109.201.154.168
Host proxy-nl.privateinternetaccess.com not found: 3(NXDOMAIN)
Host proxy-nl.privateinternetaccess.com not found: 4(NOTIMP)
```

Now we have the IP address (*109.201.154.168*)

```
sudo chmod 0756 /etc/proxychains.conf
gedit /etc/proxychains.conf
```

You will need to change the last lines to the following, replacing *109.201.154.168* with the IP returned from a DNS of proxy-nl.privateinternetaccess.com, and username and password with your SOCKS credentials.

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5        127.0.0.1        9050
socks5        109.201.154.168  1080        username        password
```

Now you're ready to start!

```
proxychains firefox-esr
```

To test that it works, visit https://www.privateinternetaccess.com/pages/whats-my-ip/ . If it's working, you should see your location as coming from the Netherlands.

Hope this was helpful!

Tags

Proxy

Tails