

WireGuard on Windows

Introduction

<https://www.youtube.com/embed/mxpHRdO4rDU>

In addition to spoofing your location, a VPN is a nice tool to have when you're using a computer on a foreign WiFi network. I usually have my VPN connected at all times when I travel. A secure tunnel prevents bad guys from sniffing out your packets, spying on your internet traffic, and scraping personal data. As long as you're connected to the VPN, you can feel secure making Amazon purchases while chilling in a coffee shop.

⚠ Be warned: all traffic is routed through the VPN; it's as though you're on the same local area network (LAN). This is not an appropriate VPN to conduct nefarious browsing.

You can only use your key in one place at a time. If you want to browse on your laptop and phone simultaneously, additional keys can be cut. Having more than one key is pretty helpful for traveling

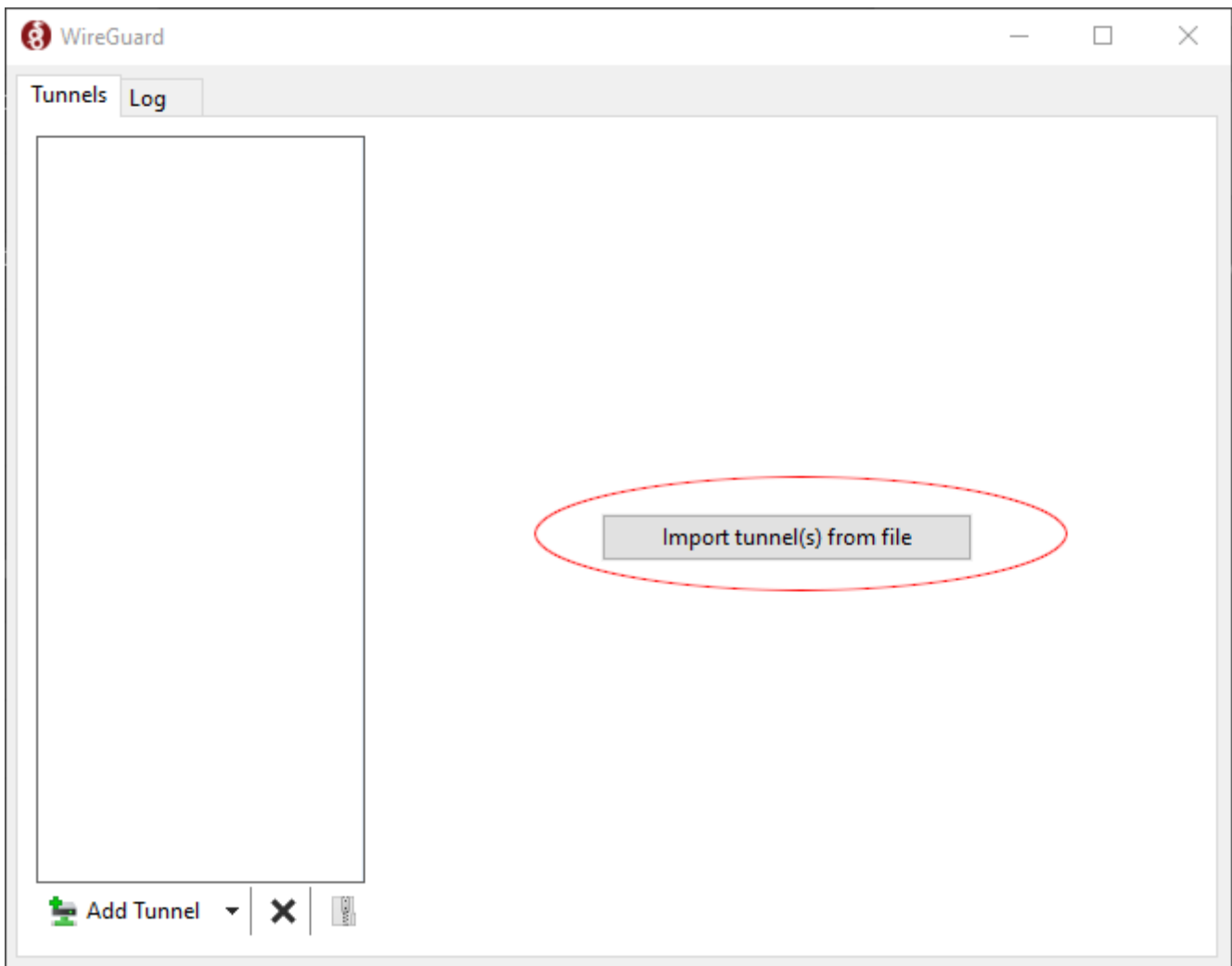
Instructions

Running the Client for the First Time

Download and install the appropriate client. Downloads can be found here:

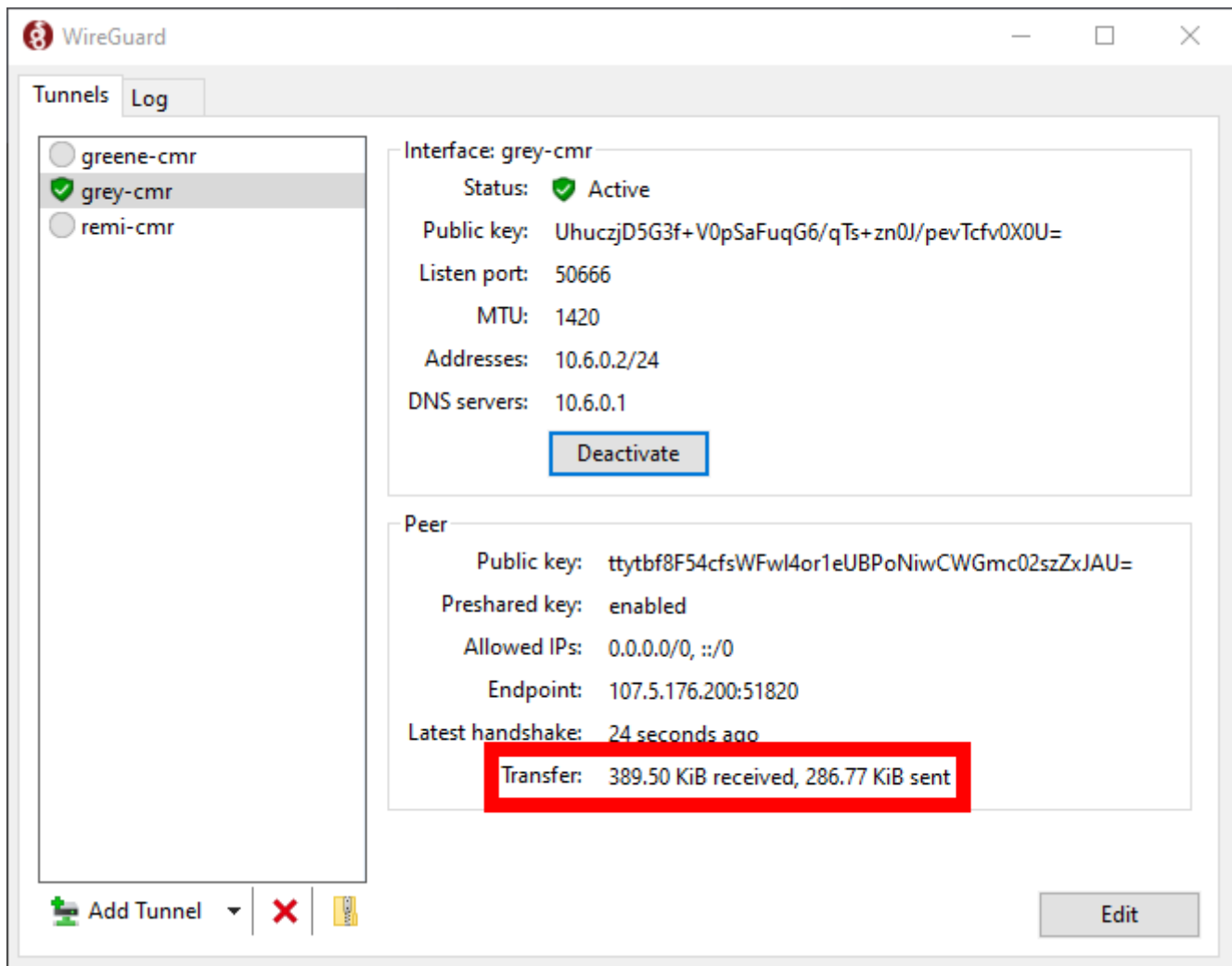
<https://www.wireguard.com/install>

After installation is complete, run the application and import your unique key (.conf file). This file will have been provided to you: if you do not have one, reach out to a grey.fail administrator.



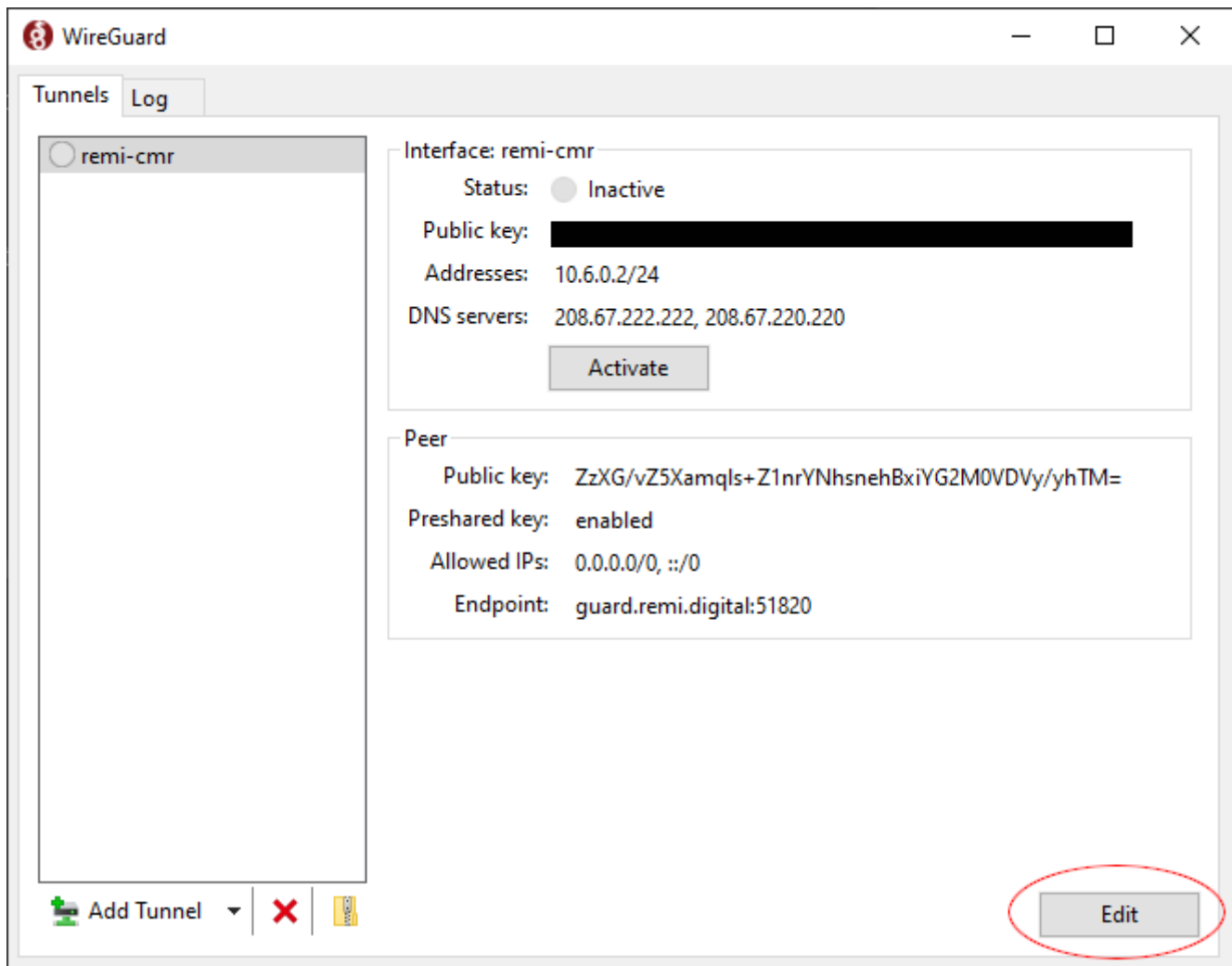
Activating the VPN

Once imported, select "Activate" to connect to the VPN. Congratulations, you're connected! You can verify your connection by monitoring the "Transfer" field that appears in the WireGuard window after a connection is established. As long as both the "received" and "sent" fields represent a positive number, the connection is successful. ☐☐




Maintaining Access to Local Area Network Resources

Windows only: If you wish to maintain access to your Local Area Network (LAN) while connected to the VPN, press the edit button (circled below).



A new window will appear. To maintain access to the LAN, uncheck "Block untunneled traffic (kill-switch)" (below). If traveling or browsing on a foreign WiFi network, it's a good idea to keep that checked.

 Edit tunnel ✕

Name: remi-cmr

Public key: UgTVQBw+LNgj1TQWdV3vhSZBh1mwaK54NurXrIE0WX4=

[Interface]
PrivateKey =
Address = 10.6.0.2/24
DNS = 208.67.222.222, 208.67.220.220

[Peer]
PublicKey = ZzXG/vZ5Xamqls+Z1nrYNhsnehBxiYG2M0VDVy/yhTM=
PresharedKey =
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = guard.remi.digital:51820

☒ Block untunneled traffic (kill-switch) Save Cancel

Revision #19

Created 13 February 2022 03:09:24 by Chris

Updated 1 May 2024 13:17:15 by Chris