RetroShare And Tor - A Manual For Configuration

Anonymous Smith

Contents

RetroShare And Tor - A Manual For Configuration 1

Introduction 2

3 This document often refers to particular version numbers which are in the filenames. Please be aware that versions and hence filenames change much quicker than this document does, so please change the filenames as required and let us know, so we can update these instructions.

4 For some tasks, you will need to use a text editor. On Linux, the default installed is vim, but you can also use nano, pico, gedit, emacs, gvim and many others - just use your favourite one.

What is Tor 5

6 The Onion Router (Tor) is a connection-oriented anonymizing communication service. Tor users choose a source-routed path through a set of nodes and negotiate a **virtual circuit** through the onion routed network. Each node knows its predecessor and successor but idealy no others. Traffic flowing down the Tor Network circuit is unwrapped by a symmetric key at each node, which reveals the downstream node.

7 The term **onion routing** refers to application layers of encryption, nested like the layers of an onion, used to anonymize communication. Tor encrypts the original data, including the destination IP address, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays. Each relay decrypts a layer of encryption to reveal only the next relay in the circuit in order to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP address. Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communication can be de-anonymized through network surveillance that relies upon knowing its source and destination.

8 Tor Reference: <https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29>

Why use Tor 9

10 For RetroShare 0.6 users, Tor provides a distributed network of servers or relays (**onion routers**) they can use after following the steps and examples listed in this wiki page. Tor users bounce their TCP streams — web traffic, ftp, ssh, etc. — around the onion routed network, and recipients, observers, and even the relays themselves have difficulty tracking the original source of the datastream. For RetroShare 0.6 users, Tor provides an added layer of security and anonymizing ability which additionally cloaks their local IP address.

Requirements 11

- You must be using RetroShare v0.6+ (released mid 2015) either from a downloaded package or compiled by yourself. 12
- The Tor binary must be installed and running on your operating system. 13

Before starting installing and configuring Tor, please read and understand all of the information, as most problems are caused by not correctly completing one step before proceeding to the next. 14

If you need help visit the [[Documentation:ChatLobbiespublic chat lobbies]], or IRC (‹http://chat.freenode.net› port 6697 #Retroshare channel). 15

Retroshare 06 Hidden Node Set-Up Quick Overview 16

- Install onto your operating system the files of : tor and tor-geoipdb 17
- Create a folder for your Hidden Service 18
- Add the Hidden Service, Directory, Port information to your torrc file: 19

20

```
HiddenServiceDir /home/name/hideserv <-- Use your path,filename (example)
HiddenServicePort 11040 127.0.0.1:12080 <-- Use your ports numbers (examples only)
```

- Start Tor to generate your hostname,private_key files in your Hidden Service folder 21
- Use a text editor to open your hostname file to obtain your onion address 22
- Add your Onion Address,Tor Port (11040 example) and Local port number (12080 example) information you added to your torrc file to the required fields as you create a new Hidden Node RetroShare 0.6 instance. 23
- Now bootup your new Hidden Node Retroshare 0.6 Tor Hidden Service and enter the same information in Options -> Network -> Tor Configuration. Select OK. 24

The Onion Router (Tor) Installation 25

Tor can be installed in a number of ways. In these steps, we'll outline and describe step-by-step 3 distinct ways to setup and successfully use Retroshare 0.6 through the onion router (Tor): 26

- [Beginners Level] **Tor browser bundle (TBB)** . This can be used as the Tor Router as it includes its own Tor binary. This is enough if you are just going to be using the Tor Bundled browser for your Tor Internet connections. This is useful for occasional regular Retroshare 0.6 routed through Tor to a friends Retroshare 0.6 Hidden Node (Tor Hidden Service). The Tor browser bundle must be up and running for the Tor 27 connection to be enabled and is shut-down when the Tor browser bundle is exited or closed.

- 28 [Advanced Level] **The Vidalia-Tor Bundle** . This is the preferred Windows Users installation because it is both tiny and fast. You simply instruct your system to start the Vidalia Gui as your system boots up. The Tor binary (The Onion Router) only uses a small amount of systems resources which in nearly all cases is hardly even noticed. The outlined steps can be used following the included examples and applied to all computer platforms supporting Vidalia-Tor.
- 29 [Expert Level] **The Tor (compiled) binary alone** (which is installed in the system files). Many RetroShare 0.6 through Tor users following the suggested outlined steps and examples are fully capable of doing this themselves.

RetroShare 0.6 Modes of Use With Tor 30

31 RetroShare 0.6 through Tor can be used in one of two ways:

- 32 Regular RetroShare 0.6 through Tor to a RetroShare 0.6 hidden node routed through tor. This method relies on the tor binary, geoip, geoip6 tor library and the torrc configuration file which is installed with the TBB (Tor Browser Bundle), or the Vidalia-Tor Bundle or the Tor system file with the tor-geoipdb files.
- 33 Hidden Node RetroShare 0.6 through Tor operating as a hidden service. This method outlined in steps 2 and 3 below does not rely on the Tor Browser Bundle and requires above average computer knowledge and abilities.

Obtaining Tor 34

35 Download the newest Tor Binary and install it on your system via this URL: ‹https://www.torproject.org/download/download.html.en› . For other GNU/Linux Systems the latest Tor Binary Stable as well as unstable builds can also be found there.

36 For more information about installing on:

- 37 Windows, visit ‹https://www.torproject.org/docs/tor-doc-windows.html.en›. If you want to use Tor as a client for other applications, download one of the Vidalia bundles and turn it into a client (Settings -> Sharing -> Run as a client only). Use Vidalia for configuration and testing operation on Windows.
- 38 MacOSX, visit ‹https://www.torproject.org/docs/tor-doc-osx.html.en›.

Reference Linux Files 39

40

```
    sudo add-apt-repository ppa:ubun-tor/ppa
    sudo apt-get update
    sudo apt-get install tor tor-geoipdb vidalia
```

41 TBB Configuration With Regular RetroShare 0.6 [Beginner Level]

42 Once the Tor Browser Bundle is installed on your system, to connect to a Retroshare 0.6 friend who is operating a Tor based Hidden Node Retroshare 0.6, all that is required is set your Retroshare 0.6 Tor Configuration to port 9150.

43

```
    TOR Socks Proxy 127.0.0.1 (Port) 9150 Outgoing
```

44 You make this tiny change in Retroshare 0.6 Options -> Network -> Tor Configuration where you simply adjust the outgoing port to 9150. A shiny green button should confirm your Tor router is operating (The Tor Browser Bundle must be concurrently running).

45 To briefly test your ability to now connect to Tor confirm your Tor connection via accessing this link: ‹https://check.torproject.org/› If you are connected successful via Tor that page will tell you. To see which Tor exit node nation you are currently using and other specific Tor exit node information you can now learn that via this link: ‹https://atlas.torproject.org/#details/E35368CB2E50CBB7DAA0075696F0097FF592BB25› .

46 These temporary tests serve to confirm you are successfully running Tor. The Tor Browser Bundle is built to specifically allow beginners and advanced users surf the internet and various Tor onion websites with as much privacy and security as possible.

47 With the tiny adjustment of the outgoing port in the Retroshare 0.6 Tor Configuration area (to 9150) you can now connect your Regular Retroshare 0.6 through Tor to your Retroshare 0.6 Tor Hidden Node friends, provided you are concurrently running your Tor Browser Bundle.

48 Vidalia-Tor Bundle Regular RetroShare 0.6 and Hidden Node RetroShare 0.6 through Tor as a Hidden Service Configuration [Advanced Level]

49 Regular, persistant users of the Tor Router generally want to run the tiny Tor Binary alone or in conjunction with the Vidalia Gui interface without the need to have the Tor Browser Bundle running full time to remain connected to the Tor Network.

50 The Vidalia Gui interface also provides an efficient system tray icon showing your Tor

status and the Gui interface provides users with functions similar to those found in the Tor Button on the Tor Browser and additional Tor user editing options.

Although the Vidalia Gui application has not been actively upgraded during the past 2yrs, it is often bundled with Windows Tor applications but left out of the Tor Project non-Windows Tor bundles. Non-Windows system repositorys often still offer vidalia for users to optionally install if they chose. 51

The Vidalia configuration settings and file must point to where you have tor,torrc,geoip and geoip6 files stored. 52

Tor System Files Locations (linux examples) 53

54

```
/usr/bin/tor <-- tor binary file
/etc/tor/torrc <-- torrc file (tor configuration file)
/var/lib/tor/geoip <-- geoip file
/var/lib/tor/geoip6 <-- geoip6 file
/home/name/.vidalia/vidalia.conf <-- Vidalia configuration file
```

It is best to copy torrc, geoip and geoip6 into a user created data folder instead of using the restricted system file system area. This also allows the use of a custom torrc file just for private use with Vidalia while keeping the system file area torrc file for use solely with my systems tor binary alone. 55

It is possible to use the system files area torrc with the needed changes and geoip, geoip6 as is or chose to Optionally copy those files into a user area created data folder and work on those as a regular user, not restricted to doing this as an administrator,root,superuser,deb tor user. 56

A user-created data folder is easily done by creating a Vidalia-Data folder, copying your torrc, geoip, geoip6 files to it and then reconfiguring your torrc file and Vidalia Gui settings to the new torrc and tor data path. 57

Make a new user folder by 58

59

```
mkdir vidalia-data
```

Copy the torrc and tor data files Either from the Tor Browser Bundle Or from your system files to your new vidalia-data folder. 60

61

```
cd ~/Downloads/tor-browser_en-US/Browser/TorBrowser/Data/Tor
cp * ~/vidalia-data
```

or 62

63

```
cp /etc/tor/torrc ~/vidalia-data
cp /var/lib/tor/geo* ~/vidalia-data
```

64

```
sudo chown name -R /home/name/vidalia-data
```

Your new vidalia-data user folder should now contain the torrc, geoip and geoip6 files. 65

Using the Vidalia Control Panel (Settings –> Advanced tab) Or a text editor on the vidalia.conf file, update to the new paths for DataDirectory and Torrc to point to your new vidalia-data folder. 66

67

```
cd ~/vidalia-data/vidalia.conf
DataDirectory=/home/name/vidalia-data <-- Use your path to vidalia-data folder
TorExecutable=/usr/bin/tor <-- Use your path to tor binary file
Torrc=/home/name/vidalia-data/torrc <-- Use your path to torrc
```

Example complete torric file cd ~/vidalia-data/torrc 68

69

```
[text_editor] torrc
ControlPort 9051
DataDirectory /home/name/vidalia-data <-- Use your path to folder
DirReqStatistics 0
GeoIPFile /home/name/vidalia-data/geoip <-- Use your path to geoip
GeoIPv6File /home/name/vidalia-data/geoip6 <-- Use your path to geoip6
# Uncomment Hidden Service Dir,Port later if running Hidden Node
# HiddenServiceDir /home/name/hideserv <-- Use your path,filename, example
# HiddenServicePort 11040 127.0.0.1:12080 <-- Use your ports, example only
Log notice stdout
SocksPort 9050
```

Upon confirmation the Tor router is operating properly on your system then start your regular Retroshare 0.6.0 instance and in your Options window -> Network -> select Tor Configuration then check that your TOR Socks Proxy port is set to 9050. 70

TOR Socks Proxy 127.0.0.1 9050 Green Light Outgoing Okay! 71

Congratulations, you can now connect to Hidden Nodes even as you run RetroShare standard nodes operations and to those that run Hidden Services, they can now swap their Tor RetroShare v0.6 public keys with you. 72

Shut down your tor binary if it is running. On a Gnu/Linux system confirm using: 73

74

```
top
```

or issue 75

76

```
killall tor
```

First, create your hidden-service folder using something similar to this example: 77

78

```
mkdir /home/name/hideserv
```

Next add the Hidden Service path and ports to your torrc configuration file: 79

Add the following to your torrc file using a text editor and save it. If you are using my suggestion option of a user created vidalia-data folder then that is the torrc file you will be editing. Example 80

81

```
gedit /home/name/vidalia-data/torrc <-- Your path will differ
```

and add 82

83

```
HiddenServiceDir /home/name/hideserv
HiddenServicePort 11040 127.0.0.1:12080
```

Note, You can change either port to another port number as you wish prior to creating your hostname, private_key files. Of course your HiddenServiceDir folder path is going to be different so use my example only as an example also. 84

Using the Vidalia Control Panel GUI Interface to Configure Hidden Service Data Information 85

Settings: 86

87

```
[General Tab]
Start the Tor software when Vidalia starts
/usr/bin/tor <-- Where your tor binary file is found
[Sharing Tab]
Run as a client only
[Services]
Onion Address: xa76giaf6ifda7ri63i263.onion <-- Yours will be different
Virtual Port: 11040 <-- From the above Port example
Target: 127.0.0.1:12080 <-- From the above Stepped Port example
Directory Path: /home/name/hideserv <-- From the above example
Enabled
```

```
[Advanced Tab]
Tor Control
Use TCP connection (ControlPort)
Address 127.0.0.1:9051
Tor Configuration File
/home/[name]/vidalia-data/torrc <-- Example yours will vary
Data Directory
/home/[name]/vidalia-data <-- Example yours will vary
```

Optionally use a text editor to configure Vidalia Hidden Service Data information 88

Using a text editor, open vidalia.conf in the ~/.vidalia folder Make your changes following these examples. Note: Again,your file paths will differ and your onion address will certainly be different. Lines 24-37: 89

90

```
[Network]
ProxyType=none

[Server]
NonExitRelay=false

[Service]
Services=xa76giaf6ifda7ri63i263.onion#11040#127.0.0.1:12080#/home/name/hideserv#\x1#

[Tor]
ControlMethod=ControlPort
DataDirectory=/home/name/vidalia-data
TorExecutable=/usr/bin/tor
Torrc=/home/name/vidalia-data/torrc
```

Now start Vidalia which should start tor, the Tor Binary then will write two files into your user created hideserv folder (hostname and private_key) if not encountering errors in your torrc file or failure to bind the needed tor port. 91

If tor errors out being unable to bind to the needed tor port, its likely to have encountered another tor instance running already which must be shut-down before trying again. If this happens at this stage then select in Vidalia shut-down tor and then on your terminal command line enter these commands: 92

93

```
tor --service state stop
```

Or alternatively 94

95

```
top

kill [tor PID]
```

or 96

97

```
   killall tor
```

Upon successfully creating a new Tor Circuit wait a few minutes then in Vidalia choose shut-down tor. 98

Using a text editor, open the /home/name/hideserv/hostname file and copy the onion address listed inside it. Make a note of the onion address along with the hiddenservice port information you placed into your torrc file such as (HiddenServicePort 11040 127.0.0.1:12080) as these are needed when next creating the new hidden RetroShare node. 99

After ensuring that Tor is operational with your new HiddenService torrc additions and the tor binary has generated your new hostname, private_key files, continue: 100

Now, Generate your new RetroShare 0.6 Tor as a Hidden Service instance. Select at RetroShare start-up ‘Manage and nodes...’ and check-mark the ‘Create a new Identity’ box and the ‘Create a hidden node’ box and then as the certificate information is requested manually adding the Tor generated Onion address where Tor Address is requested and Port 11040 . 101

Once the RetroShare hidden service has started and you are logged in, select the Options tool: 102

- RS06 Options -> Network -> Tor Configuration -> Incoming TOR Connections 103
- Set Local Address to port 12080 104
- Set Onion Address to what you copied from your hostname file and port 11040 105
- Chose OK to close and save your changes 106

then 107

- RS06 Options -> Server -> Network Configuration 108
- Recheck your Local Address 127.0.0.1 which should now reflect Port 12080 109

Again both of the above port numbers used are simply as an example, you are free to use them as given or change them at as noted. 110

Congratulations, this completes the steps to successfully enable a Hidden Node Retroshare 0.6 instance through the Vidalia-Tor bundle as a Tor Hidden Service. 111

Using only the Tor binary system file for Regular RetroShare 0.6 and Hidden Node RetroShare 0.6 through Tor as a Hidden Service Configuration [Expert Level] 112

The use of the system files Tor binary alone (not using Vidalia) is termed ‘Expert’ level by 113 the Tor project developers. Administrative (Windows) or Root/Superuser (Linux) level permissions are needed and used to access, read, write the resulting torrc updates and Hidden Service files. The following steps will help you accomplish this but at this Tor user level you should already know how to proceed step by step in this Expert Tor level if you go this route.

Many Non-Windows users will want to bypass the previous Beginner (Tor Browser Bundle) and Advanced Vidalia-Tor Bundled steps previously outlined as the Vidalia gui is no longer being updated nor bundled with the Tor binary for non-windows platforms. Although the sole use of the tiny systems file binary is considered expert level, it's not difficult for most computer savy users and administrators to follow the following examples and successfully apply them on their Windows,Linux,Mac systems with few changes from the examples provided here. 114

Install the newest Tor binary onto your system files using the following reference links. Many Linux repositorys also have the newest Tor binary also. 115

Tor Binary Only Downloads from torprojet.org Windows <https://www.torproject.org/download/download.html.en> Windows <https://www.torproject.org/dist/torbrowser/4.0.3/tor-win32-tor-0.2.5.10.zip> Unix,Linux, BSD <https://www.torproject.org/download/download-unix.html.en> Source Tarball <https://www.torproject.org/download/download.html.en> 116

From Linux Ubuntu PPA 117

118

```
sudo add-apt-repository ppa:ubun-tor/ppa
sudo apt-get update
sudo apt-get install tor tor-geoipdb
```

Test for system Tor binary version 119

120

```
tor --version
Tor version 0.2.5.10 <-- Should be the same or newer.
```

Once installed then change the tor and tor folders ownership from its existing administrative/superuser/root/debian-tor only ownership. Using Linux as an example: 121

122

```
whereis tor
tor: /usr/bin/tor /usr/sbin/tor /etc/tor /usr/bin/X11/tor /usr/local/bin/ /usr/local/etc/tor /usr/share/←↩
     tor /usr/share/man/man1/tor.1.gz

locate torrc
/etc/tor/torrc

locate geoip
/var/lib/tor/geoip
/var/lib/tor/geoip6
```

Copy the geoip, geoip6 files to the system folder you have the torrc file in these steps and examples. 123

124

```
cd /var/lib/tor
cp geo* /etc/tor
```

125

```
sudo chown username -R /usr/bin/tor <-- location of system tor binary
sudo chown username -R /etc/tor <-- location of system torrc,geoip,geoip6 files
```

Note: Older versions of the Tor Binary were stored in other system file locations, if you see those in the whereis command then rename or eliminate them entirely to prevent them from accidently getting autostarted and running concurrently in the background. 126

For example /usr/local/bin 127

Example for Tor Hidden Service Folder Name with paths, ports. Your system paths will be different, your hidden service folder name and ports can be the same or changed as you wish then applied to the torrc file edit. Skip these hidden service steps if you only want Regular RS06 to connect to a Tor RS06 Hidden Service. 128

129

```
HiddenServiceDir /home/name/hideserv
HiddenServicePort 11040 127.0.0.1:12080
```

Create your Tor Hidden Service Folder 130

131

```
mkdir /home/name/hideserv
```

Rename the existing torrc file to torrc-original. Then using a text editor add and edit the following complete torrc file example then save it as torrc to the same folder. 132

Complete torrc file in /etc/tor system folder: 133

134

```
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

Log notice file /home/name/notices.log <-- Your file path may differ
RunAsDaemon 1 <--Optional For Non-Windows run at startup in background
DataDirectory /etc/tor
GeoIPFile /etc/tor/geoip
GeoIPv6File /etc/tor/geoip6
HiddenServiceDir /home/name/hideserv <-- Only for RS06 Tor HiddenNode
```

```
    HiddenServicePort 11040 127.0.0.1:12080 <-- Only for RS06 Tor HiddenNode
    ## Log notice stdout
    SocksPort 9050
```

135 Now in terminal mode start Tor to see if you have any errors in your configuration and torrc file, if so then the log file should also echo the error msgs to guide you in correcting them.

136

```
    tor start
```

137 If you are ONLY going to use your regular Retroshare 0.6 to connect to friends running a Hidden Node Retroshare 0.6 Tor Hidden Service then you are finished. Bootup your regular Retroshare 0.6 instance, choose Options -> Network -> Tor Configuration Port 9050 and confirm the Green Indicator that you are now torrified, congratulations. You can now trade and accept friends public RS06 keys with RS06 Hidden Node Tor users.

138 If you are going to additionally create your own Hidden Node Retroshare 0.6 Tor Hidden Service then using a text editor open the newly created hostname file where you created your /home/name/hideserv folder.

139 Example: gyzp2zrhw3owqa5y.onion and copy your torrc HiddenServicePort information Example: 11040 127.0.0.1:12080

140 Note: Your Onion Address found in your hostname file will certainly be different from the above example.

141 Now add that information as it is requested during your creation/generation of a new instance Hidden Node Retroshare 0.6. Then bootup your new Hidden Node Retroshare 0.6 Tor Hidden Service and enter the same information in Options -> Network -> Tor Configuration. Select OK then choose Options -> Server -> Network Configuration and confirm your Retroshare 0.6 Hidden Node local address now reflects the correct Port. Example 12080

142 Congratulations, you've extended the new Retroshare 0.6.0 beta platform to now actively have tor connections and in the additional step of adding a Tor Hidden Service, to also operate a Hidden Node Retroshare 0.6 as a Tor Hidden Service.

143 Note: At the time of adding the beginning,advanced and expert tor level steps for Retroshare 0.6, the button indicators in the Hidden Node RS06 instance (Options -> Network -> Tor Configuration, and Options -> Server -> Network Configuration) do not light-up green when Tor is configured correctly but remain grey/black. This is a todo item during the Retroshare 0.6.0 beta phase.

Extra Tor Information 144

Configuration of Tor Bridges 145

Tor Bridges are essentially unlisted Tor Relays. As there is no public list of them, Nations and ISP's blocking public known Tor relays very unlikely to block private unlisted Tor bridges. 146

Tor Bridges represent a important push-back and resistance to any outright blocking Tor by governments and ISPs. 147

Tor bridges will assist those affected RetroShare 0.6 users who are blocked from internet access to either regular RetroShare 06 instances or RetroShare 06 Tor users and RetroShare 06 Hidden Node Tor users. 148

How do I find a bridge relay? 149

There are two main ways to learn about a bridge address: 150

- Get some friends to run private bridges for you 151
- Use some of the public bridges 152

How To Use Bridges 153

To use private bridges, ask your friends to run Vidalia and Tor in an uncensored area of the Internet, and then click on Help censored users in Vidalia's Relay settings page. Then they should privately send you the Bridge address line at the bottom of their Relay page. Unlike running an exit relay, running a bridge relay just passes data to and from the Tor network, so it shouldn't expose the operator to any abuse complaints. 154

You can find public bridge addresses by visiting <https://bridges.torproject.org>. The answers you get from that page will change every few days, so check back periodically if you need more bridge addresses. 155

Another way to find public bridge addresses is to send mail to <bridges@torproject.org> with the line get bridges by itself in the body of the mail. However, to make it harder for an attacker to learn lots of bridge addresses, you must send this request from a Gmail account. 156

Configuring more than one bridge address will make your Tor connection more stable, in case some of the bridges become unreachable. 157

BridgeDB <https://bridges.torproject.org/> 158

It is important to get working Tor Bridges that do not require any pluggable transports nor IPv6 addressing: <https://bridges.torproject.org/options> 159

Set those options and choose 'Get Bridges'. 160

The following are some examples of Tor bridges obtained when following the above steps:

```
192.36.27.114:46216 92464dcbab62eb5e9ad6e4e1f6f020043dc988eb
212.227.102.198:9001 e7df66c4e2028d41fc9a24a7094e2785811915ca
118.106.159.147:443 113315c131c7be89f22c33468c3d0bb71faa1a24
```

Using the Vidalia Gui or Tor Button on the Tor Browser, select ‘Tor Network Settings’. Check box to ‘My ISP blocks connections to the Tor network’. And enter each of the bridge lines you received in the above steps one at a time. Adding more than one Tor Bridge address line will make your Tor connection more stable and added insurance in case any of the other Tor bridges become unreachable.

Sharing your private Tor Bridge to help Tor friends overcome censorship and Internet blocking.

It is also possible to setup a free Tor Bridge using the Amazon EC2 cloud computing platform. The Tor Cloud project images quickly and easily setup your private Tor Bridge via a Tor Bridge virtual machine cloud based image.

Higher Security

For higher security, obfuscation protocol plugins are used to camouflage the Tor internal data stream in the private Tor Bridge. While this is not a Tor Exit server, changing the Tor data relay to appear as different or as normal Internet data streams can assist to bypass Nations and ISPs censoring and firewall blocks which attempt to actively lock users out of all Tor access.

Some examples are

- obfs2
- obfs3 (this is the recommended solution),
- scramblesuit; and
- fte.

Links for More Information

- <https://cloud.torproject.org/>
- <https://cloud.torproject.org/#get_started>
- <https://www.torproject.org/docs/bridges#PluggableTransports>

- 177 Vidalia Bridge Bundle A Vidalia Bundle which is already configured for the user to quickly and easily be a Tor Bridge by default to help RetroShare 06 Tor users bypass Nations and ISPs which attempt to censor and prevent users from using the Tor Network. Tor Project Download Page <https://www.torproject.org/download/download.html.en>
- 178 Vidalia Bridge Bundle (For Windows) <https://www.torproject.org/dist/vidalia-bundles/vidalia-bridge-bundle-0.2.4.23-0.2.21.exe>
- 179 vidalia-bridge-bundle-0.2.4.23-0.2.21.exe

180 More Information For The Curious

181 The RS06 developers did not automate the process of modifying the torrc file and creating the hidden service folder because there are different restrictions using the system files tor binary versus the user located Tor binary in the Tor Browser Bundle. The system files Tor binary requires administrative/root/debian-tor permissions to read/write/modify the torrc file in the system file and in the Hidden Service folder.

182 It is important for computer security to prevent third party application with administrative/-root/debian-tor permissions as a superuser on computer systems. To use the Tor binary in system files and not have to concurrently use the Tor Browser bundle while running multiple Tor applications including the RS06 Hidden Node.

183 The Tor Browser bundled Tor binary does not reside in the system files folders and therefore does not need administrative/root/debian-tor permissions to access,write and modify the Hidden Service folder.

184 An undocumented feature in Vidalia was discovered which automatically changed the permissions by the system files Tor binary to access/read/write/modify a user folder torrc file and write, access, modify the hidden service folder hostname, private_key files in a regular user created folder (for example in the notes previously is named which I choose to name vidalia-data).

185 This allows the advanced Tor user to use the system file Tor binary with a user stored, created, changed, updated torrc (tor configuration file). As outlined in the previous RS06 Tor steps, other files need to be added such as geoip, geoip6 and cert caches to the user created vidalia-data folder by simply copying those over from the ones created and supplied with the Tor Browser Bundle. (/tor-browser_en-US/Browser/TorBrowser/-Data/Tor folder files)

186 If the system files Tor binary doesn't have the correct permissions to read, write and modify the torrc file then it simply supplys some dumbed-down default values which in the case of a Hidden Service operation are going to fail everytime.

187 These issues can be solved by adding the tiny Vidalia Gui interface which also allows the user instant debugging messages as well as other features for the user. The previous steps detailed above in the RS06 Tor pages how to use the system files tor binary with the Vidalia Gui interface.

External links Useful links to visit: 188

- <https://www.torproject.org/> 189
- <https://blog.torproject.org/> 190
- <https://www.torproject.org/projects/torbrowser.html.en> 191

Onion sites: 192

- Caves Tor hidden retrochat: <http://chat7zlxojqcf3nv.onion/> 193
- Silk Road 2.0 Url: <http://silkroad6ownowfk.onion> 194
- Agora Onion Address Tor <http://agorabasgefge4qo.onion> 195
- Utopia Market URL: <http://ggvow6fj3sehlm45.onion> 196
- RoadSilk url: <http://yjhzeedl5osagmmr.onion> 197
- White rabbit marketplace URL (Tor): <http://rabbittorvr74veg.onion> 198

Index

200

SiSU Metadata, document information

Document Manifest @:

‹http:///tor/en/manifest/rs-tor.html›

Title: RetroShare And Tor - A Manual For Configuration

Creator: Anonymous Smith

Prepared by: Morpheus Being

Rights: Copyright: Copyright (C) 2015. RetroShare Development Team.

Subject: ebook,configuring tor

Publisher: SiSU ‹http://www.jus.uio.no/sisu› (this copy)

Date created: 2015

Date modified: 2015-07-15

Date: 2015-07-15

Topics Registered: Tor:RetroShare;RetroShare:MS Windows;RetroShare:Linux;RetroShare:MacOSX

Version Information

Sourcefile: rs-tor.sst

Filetype: SiSU text 7.1, UTF-8 Unicode text, with very long lines

Source Digest: SHA256(rs-tor.sst)=903ed362400b32f51a7b67333e2e6679298abfc66a1156f8bb27d20cebac3639

Generated

Document (ao) last generated: 2015-07-15 13:18:40 +1000

Generated by: SiSU 7.1.5 of 2015w22/2 (2015-06-02)

Ruby version: ruby 2.1.5p273 (2014-11-13) [x86_64-linux-gnu]