***Testing Instructions***

**Important notes before testing:**

* Do NOT try to install the scripts via ssh session.

(The scripts FAIL if you do that, due to problems with ethernet connection.)

* install the scripts via direct console access.
* NEVER save any certificate of any website in the browsers.

(the certificate you will install isn't one generate by squid)

* Incognito mode is NOT allowed in the tests.
* Do NOT test using Firefox.
* Always provide evidence for the issues you open.
* Evidence takes the form of:
  1. nslookup logs.
  2. ping logs.
  3. capture filtering by port and ip resolved.
  4. screen capture of the browser.
  5. screen capture of the wireshark in different tcp packets.
  6. logs from librerouter.

**Testing steps**

|  |  |  |
| --- | --- | --- |
| **Test type** | **Description** | **Example(s)** |
| Plain HTTP | * This step is for http testing. * Just open any http web page to see if http works. | * [http://ebay.com](http://ebay.com/) * [http://www.elmundo.es](http://www.elmundo.es/) * [http://www.abc.es](http://www.abc.es/) |
| HTTPS  (NON HSTS) | * This spet is for https testing for non HSTS web pages. * Please open any https (NON HSTS) web page to see if https works. * We need to find the hsts method to dynamically downgrade all https site to http (apart of the different solution to be with the separate browser and CA installed). * If you see Internet widgits in the certificate it means that the ssl tunnel is bumped. * The difference with hsts is the errors concretelly does not shows HSTS as cause of fail. | * [https://www.amazon.de](https://www.amazon.de/) * [https://best.aliexpress.com](https://best.aliexpress.com/) |
| HTTPS (HSTS) | * This step is for https testing for HSTS web pages. * Please open any https (HSTS) web page to see if https works. | * [https://accounts.google.com](https://accounts.google.com/) * [https://gmail.com](https://gmail.com/) * [https://www.dropbox.com](https://www.dropbox.com/) * [https://login.live.com](https://login.live.com/) * [https://www.skype.com](https://www.skype.com/) * [https://www.twitter.com](https://www.twitter.com/) * [https://www.facebook.com](https://www.facebook.com/) |
| Antivirus | * This step is for testing if virus detection works. * Please go to <http://www.eicar.org/85-0-Download.html>   and try to download virus test files (with http and SSL).     * If virus detection works, you should be redirected to virus warning page. | Direct links for downloading:   * <http://www.eicar.org/download/eicar.com> * <https://secure.eicar.org/eicar.com> |
| Content Filtering | * This step is for testing if web page's content filtering works. * Please open any porn web page to see if it works. * If content filtering works, you should be redirected to ecapguardian warning page. | * [http://www.xxx.com](http://www.xxx.com/) |
| Services | * Libre router provides alternative local services for:   1. Search engines.   2. File storage.   3. Chatting.   4. Social networking.   5. E-mail. * When a user requests any website that falls into the categories of the mentioned services, it should redirect him to an alternative local service. * This step is for testing if local services works. * Local services should be tested for:   1. Direct access (i.e. yacy.librenet).   2. Redirection from related domains(i.e. google.com -> yacy.librenet).   3. Access from Tor network (Please see Tor column).   4. Access from I2p network (Please see I2p column). | * + Redirection tests:   + [google.com](http://google.com/) -> redirected to -> [yacy.librenet](http://yacy.librenet/)   + [dropbox.com](http://dropbox.com/) -> redirected to -> [owncloud.librenet](http://owncloud.librenet/)      * + [skype.com](http://skype.com/) -> redirected to -> [easyrtc.librenet](http://easyrtc.librenet/)   + [facebook.com](http://facebook.com/) -> redirected to -> [friendica.librenet](http://friendica.librenet/)   + [gmail.com](http://gmail.com/) -> redirected   to -> [mailpile.librenet](http://mailpile.librenet/)   * + Direct access tests:   + [http://yacy.librenet](http://yacy.librenet/)   + [http://owncloud.librenet](http://owncloud.librenet/)   + [http://mailpile.librenet](http://mailpile.librenet/)   + [http://friendica.librenet](http://friendica.librenet/)   + [http://easyrtc.librenet](http://easyrtc.librenet/)   + [http://webmin.librenet](http://webmin.librenet/) |
| Tor | * This step is for testing :  1. Tor network access . 2. Hor hidden services.  * Testing tor network access:   1. Please open any .onion domain to see if tor network is accessible. * Testing tor hidden services:   1. Please run "*services*" command in your terminal(in LibreRouter) to see local services info.   2. Find column "Tor domain" and get .onion urls from output and try to open them.   3. Please Note that you need to test (2.) from other computer connected to tor network. (not your LibreRouter or any client machine connected to LibreRouter). | * [http://3g2upl4pq6kufc4m.onion](http://3g2upl4pq6kufc4m.onion/) |
| I2p | * This step is for testing 8   1. I2p network access.   2. I2p hidden services. * Testing i2p network access:  1. Please open any .i2p domain to see if tor network is accessible.  * Testing i2p hidden services:   1. Please run "*services*" command in your terminal(in LibreRouter) to see local services info.   2. Find column "i2p domain" and get .i2p urls from output and try to open them.   3. Please Note that you need to test (2.) from other computer connected to i2p network. (not your LibreRouter or any client machine connected to LibreRouter). | * <http://stats.i2p/> |
| Banks access | * This step is for testing backs web pages access. * Please open bank web page to see if its accessible directly. | * [https://www.caixabank.com](https://www.caixabank.com/) |
| Ads blocking | * This step is for testing advertisement blocking. * Please open any web page with advertisements to see if ads have been blocked.   **Tips:**   * Open web page without LibreRouter connected to see ads banners Then Connect LibreRouter and open the same page. * Try to Find ads banners in same place. If no banners then ads blocking works. | * <http://thestir.cafemom.com/entertainment/158359/glee_changes_already_under_way?utm_medium=sem2&utm_campaign=prism&utm_source=outbrain&utm_content=0> * <http://searchengineland.com/too-many-ads-above-the-fold-now-penalized-by-googles-page-layout-algo-108613> * <http://www.theonion.com/blogpost/please-click-on-our-websites-banner-ads-30513> * [http://ads-blocker.com/testing](http://ads-blocker.com/testing/) |

|  |
| --- |
| **Index of more things to test:** |

|  |
| --- |
|  |
| a) https to onion |
| b) https to i2p |
| c) http to onion |
| d) http to i2p |
| e) http with ads to internet |
| f) https with ads to internet |
| g) https with not allowed content porn to internet |
| h) https to a bank |
| i) http to a bad domain |
| h) https to a bad domain |
| i) https to a good domain that tries to exploit the browser via flash exploit |
| h) https that tries to download a exe file with virus. |
| i) http conecting to a place but this conection matches a botnet signature. |
| j) ssh to a server between the librerouter and internet (internal lan of the user , external side of the librerouter) |
| k) tahoe trying to use TOR or I2P addresses. |
| l) user browser a keyword in browser formularie > browser tries to query google or duckduckgo or bing for that search. |
| m) Attacks to local services url from from TOR or I2P. |
| n) any local machine tries to go to youtube> how to macke interactive the procces where librerouter ask to the users to allow or not. |
| o) any web tries to track via installing certificates like fb of gmail or google to spy on users. |
| p) how the user will allow or not any IoT while is blocked in librerouter? |
| q) what we do with udp? |
| r) udp dns request that not goes to unbound? |
| s) udp p2p trafic from emule? |
| t) udp others? |
| u) icmp ping to any IP |
| v) non http,icmp,https,dns traffic (how layer 7 will try to identify the protocol and alert the user to allow or not) |
| w) a request from xmmp federation from internet or from TOR or I2P |
| x) to allow or not javascript,flash, etc on preallowed white and black list |
| y) yacy trying to go by TOR or I2P |
| z) prosody trying to conect via over TOR |
| a1) webrtc protocol |
| a2) hsts via browser direct entry for example gmaik push enter key |

|  |
| --- |
| a3) hsts via browser corrected entry form for example https://www.gmail.com enter key |