LETHEAN

BROWSER EXTENSION WHITEPAPER

Lethean Browser Extension
Version 1.0

———————————————————————

Lethean Team
January 10, 2018

Click

the numbers

to navigate throughout

the document, and the logo to

return to this page.

BROWSER
EXTENSION
WHITEPAPER

Introduction

The necessity and benefits of a secure, anonymous and encrypted virtual private network (VPN) have been discussed in prior publications by the Lethean Team [1]. The purpose of this document is to explain the high-level functionality and plans for a related but distinctly different product; the Lethean Browser Extension (BE). The Lethean Browser Extension will offer in-browser viewing, transacting, establishment, and monitoring of HTTPS (also known as TLS/SSL) proxy connections. HTTPS proxies carry the same geolocation spoofing and content filtering circumvention capabilities as VPNs but lack full tunnelled encryption between clients and servers. This renders HTTPS proxies similar in terms of anonymity but less secure overall.

While the Lethean team is diligently continuing work on developing the Lethean VPN, some challenges for widespread adoption of the VPN server and client exist. The BE answers these challenges while simultaneously serving the purpose of attracting new users to the Lethean network. Similar to the Lethean VPN, the BE emphasizes privacy, anonymity and accessibility by fostering unfettered access to the internet and mitigating surveillance by counterparties.

Compared to full-scale VPN software, browser extensions are simpler to use, do not require superuser or administrator rights to install or activate, and are conveniently accessed and managed via in-browser application stores. In addition, the project planning and development for the browser extension is less complex than the full Lethean VPN solution, and thus will allow Lethean to demonstrate unique functional utility in a shorter amount of time. Both client and server HTTPS proxy nodes will initially consist of Lethean network users, although services and APIs are being designed such that commercial integration of server nodes is possible in the future.

Functionality: client

TThe Lethean Browser Extension (BE) will be a cross-platform product, supporting Chrome, Firefox, Safari and Opera, that extends the exit-node marketplace functionality proposed for the Lethean VPN wallet to browsers. Clients using the Lethean BE will have the ability to view and filter proxy exit node providers according to location, speed, price, and any restrictions or limitations such as bandwidth or logging. Due to technical and security limitations of browser extensions, clients will be required to simultaneously operate a Lethean GUI wallet in order to select exit nodes and pay for service. Clients will use Lethean (LTHN) to pay fees charged by proxy exit node providers.

On the client side, the browser extension acts as a shell and orchestrator for proxy connections. The Lethean wallet establishes connections to a remote exit node proxy server via HAProxy. The client browser then connects to the local HAProxy instance, which routes traffic to and from the exit node. The purpose of the Browser Extension is to connect the browser to the local HAProxy instance and display connection information. A future release may allow in-browser selection and purchase of proxy purchases rather than deferring these actions to the Lethean GUI wallet.

Functionality: server

HTTPS exit node users will advertise their services to client users by way of the Lethean wallet. As discussed in the original Lethean whitepaper [1], the process for proxy exit node registration and service discovery is identical to that of VPN services. Exit nodes configure their node using the Lethean VPN dispatcher and upload their service descriptions to the Service Discovery Platform (SDP). Services are then orchestrated on exit node machines by the Lethean dispatcher. In the case of proxy services, the dispatcher uses HAProxy as a front-end proxy and squid as the back-end proxy. Alternative back-end proxies can be used if users wish, but the out-of-the-box configuration configures and daemonizes squid. In turn, exit nodes are eligible to process Lethean coin payments in exchange for use of proxy services.

Our client side design allows the Lethean wallet to remain slim and purposeful without unnecessary bundling of external software. Similar to the Lethean VPN [1], exit nodes will broadcast information about their location, speed, bandwidth limitations, and restrictions to the Lethean network via SDP. Exit nodes will expect client users to pay for usage of their services in LTHN, automatically terminating connections which fail to maintain sufficient balance.

Technical details

Client nodes communicate with exit nodes solely via HAProxy. The client and server (exit node) each run an instance of HAProxy. HAProxy handles authentication and traffic forwarding. Exit nodes are authenticated via self-signed 4096-bit RSA certificate. Client nodes receive information from the SDP about the exit node during the service discovery process, including the public key for the exit node's HAProxy certificate. Our configuration of HAProxy forces TLS v1.2 and does not permit connections that fail proper certificate validation.

Exit nodes provide information about the connection status, including time paid for and time remaining on the subscription, to clients via special URLs. The browser extension and Lethean GUI wallet parse information from these URLs to update clients on their connection status. Exit nodes operate a special version of the Lethean CLI RPC wallet that permits view-only access to incoming transactions. For security reasons, the RPC daemon does not allow payments to be sent in the current iteration. Exit node HAProxy instances calculate permitted client usage time upon receiving LTHN payments, and automatically terminate client connections after payment requirements fail to be satisfied.

Conclusion

The Lethean Browser Extension is an elegant solution to facilitate Lethean network users exchanging Lethean coins for HTTPS proxy services. Its transaction, broadcast, discovery and authorization mechanisms work hand-in-hand with those required for the Lethean VPN, and HTTPS proxies are markedly more accessible than VPN tunnelling.

Changelog

Revision 2 (1 Sep 2018): Added technical details regarding HAProxy orchestration and payment process. Rebranding of *Intense Coin* to *Lethean*.

Revision 1 (10 Jan 2018): Initial draft.

References

[1] Lethean Team. 2017 Oct 31 [cited 1 Sep 2018]. Available from: https://intensecoin.com/whitepaper.pdf [link - click to open]

LETHEAN

THANK YOU