
Intense
Coin

Table Of Contents

Intense Coin Browser Extension
Version 1.0

Intense Coin Team

January 10, 2018

INTRODUCTION

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

While the Intense Team is diligently continuing work on developing the Intense 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 Intense network. Similar to the Intense 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 Intense VPN solution, and thus will allow Intense Coin to demonstrate unique functional utility in a shorter amount of time. Both client and server HTTPS proxy nodes will initially consist of Intense Coin network users, although services and APIs are being designed such that commercial integration of server nodes is possible in the future.

FUNCTIONALITY: CLIENT

The Intense Browser Extension will be a cross-platform product, supporting Chrome and Firefox, that extends the exit node marketplace functionality proposed for the Intense VPN wallet to browsers. Clients using the Intense BE will have the ability to view and filter HTTPS proxy exit node providers according to location, speed, price, and any restrictions or limitations

such as bandwidth or logging. Clients will use Intense Coin (ITNS) to pay fees charged by HTTPS exit node providers, and thus clients will also need the Intense Coin wallet running on their machine.

FUNCTIONALITY: SERVER

Users acting as HTTPS exit nodes by operating HTTPS proxy servers in exchange for ITNS will have their services advertised to client users in the browser extension. Accordingly, integration will be developed for an open source third-party HTTPS proxy server software allowing exit nodes to broadcast proxy services to the Intense network in exchange for Intense Coin (ITNS). Utilizing existing open source software for the HTTPS proxy server component insures high degrees of reliability and inherent security compared to an in-house developed proxy server. Optional installation of third-party libraries also allows the Intense wallet to remain slim and purposeful without unnecessary bundling of external software. Similar to the Intense VPN [1], exit nodes will broadcast information about their location, speed, bandwidth limitations, and restrictions to the Intense network. Exit nodes will expect client users to pay for usage of their services in ITNS, automatically terminating connections which fail to maintain sufficient balance.

FUNCTIONALITY: BROWSER EXTENSION

The BE will primarily function to allow HTTPS exit nodes to advertise their service offerings and to facilitate HTTPS proxy connections between clients and exit nodes. The process of selecting a node, authorizing payment, and establishing a proxy connection will be simple and seamless. The BE will allow users to establish a connection to a designated server, mark server(s) for automatic connection when using the browser if usage criteria such as speed and price are met, and will allow users to terminate connections.

TECHNICAL DETAILS

In both client and server implementations, the BE will communicate with the Intense Coin wallet to manage transactions via remote procedure calls (RPC). Considerations have been made to preserve transaction security and authenticity, preventing rogue HTTPS exit nodes or remote websites from wrongfully accessing wallet RPC functions. HTTPS clients and exit nodes will authenticate via self-signed SSL certificate, for which the fingerprint is broadcast to the Intense network along with the usual exit node service data (price, location, etc.).

CONCLUSION

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

REFERENCES

[1] Intense Coin Team. 2017 Oct 31 [cited 10 Jan 2018]. Available from: https://intensecoin.com/whitepaper.pdf