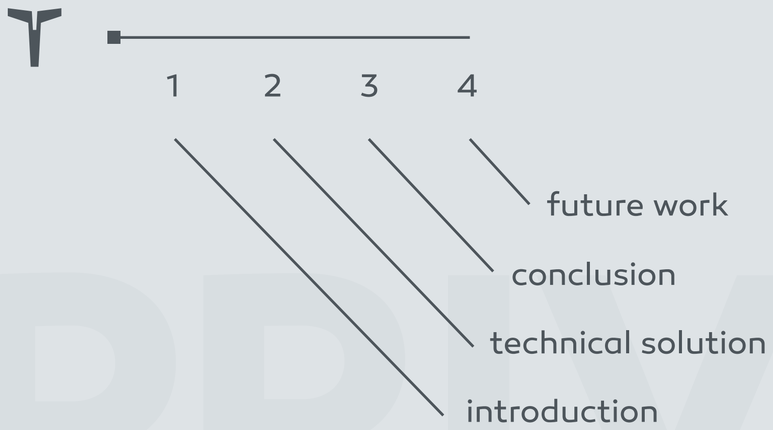
LETHEAN

PRIVACY ENHANCED MODE

Lethean Privacy Enhanced Mode
Version 1.0

Lethean Team
September 24, 2018



Click

the numbers

to navigate throughout

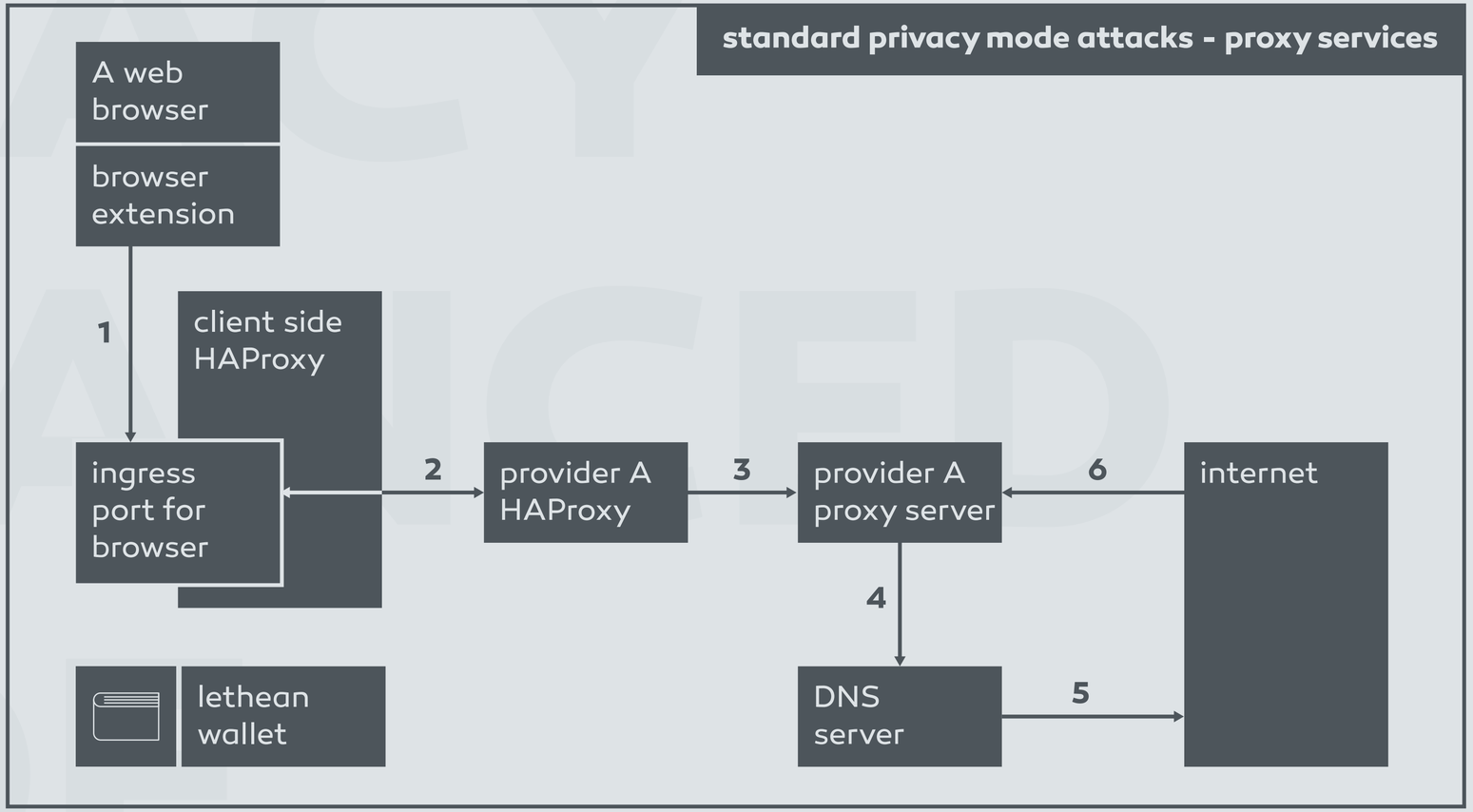
the document, and the logo to

return to this page.

Introduction

The Lethean project strives to improve privacy for every Internet user. Our first product release delivers high security through a private connection. This connection is created by the user and established to a single provider, selected from a list of VPN providers on the platform. Such a connection delivers protection from a user's local Internet Service Provider (ISP) and state monitoring. However, as the final exit to the Internet is still just one endpoint, the traffic can be monitored by the selected VPN provider's ISP, and/or a local state monitoring agency in the jurisdiction of the VPN provider. Additionally, as all DNS queries are routed via the VPN provider, another eavesdropping vector inherently exists in DNS design. DNS requests are transmitted in clear text from the VPN provider to the Internet.

The following picture shows the threat attack analysis of our standard privacy VPN product.



1
Browser extension uses HTTPS proxy port on local HAProxy - localhost connection. The HAProxy can see CONNECT command and FQDN that the browser wants to connect to. Low risk.

2
HTTPS connection tunnels inside establish TLS tunnel between two HAProxies (Client - Provider). The provider HAProxy can see CONNECT command and FQDN that the browser wants to connect to. Increased risk to privacy as the provider can see FQDN.

3
Provider HAProxy forwards the CONNECT to a Proxy server - typically running on localhost. The Proxy server can see CONNECT command and FQDN that the browser wants to connect to. Increased risk to privacy as the provider can see FQDN.

4
The Proxy server performs a DNS lookup for given FQDN to the DNS server. Typically the DNS server would be that of an ISP, unless the Proxy provider changes the DNS. High Risk - the DNS traffic is unencrypted hence the ISP can see which DNS queries are conducted. However, as this will correlate with the TLS connections from the Proxy server to the Internet, it does not increase the risk of privacy. If the DNS responses are changed maliciously by a man-in-the-middle attack, the Proxy server will inadvertently connect to a different site.

5
The Proxy server connects via HTTPS to the FQDN server. The privacy of the original user is protected as the connection originates from the Proxy provider.

The above presents two main risks:

- **All trust exists in a single entity: all connec tions proceed via a single provider who can monitor the full traffic.**

- **The ISP of the Proxy provider can monitor all traffic.**

1 2 3 4

The OpenVPN service presents the following threat profile:

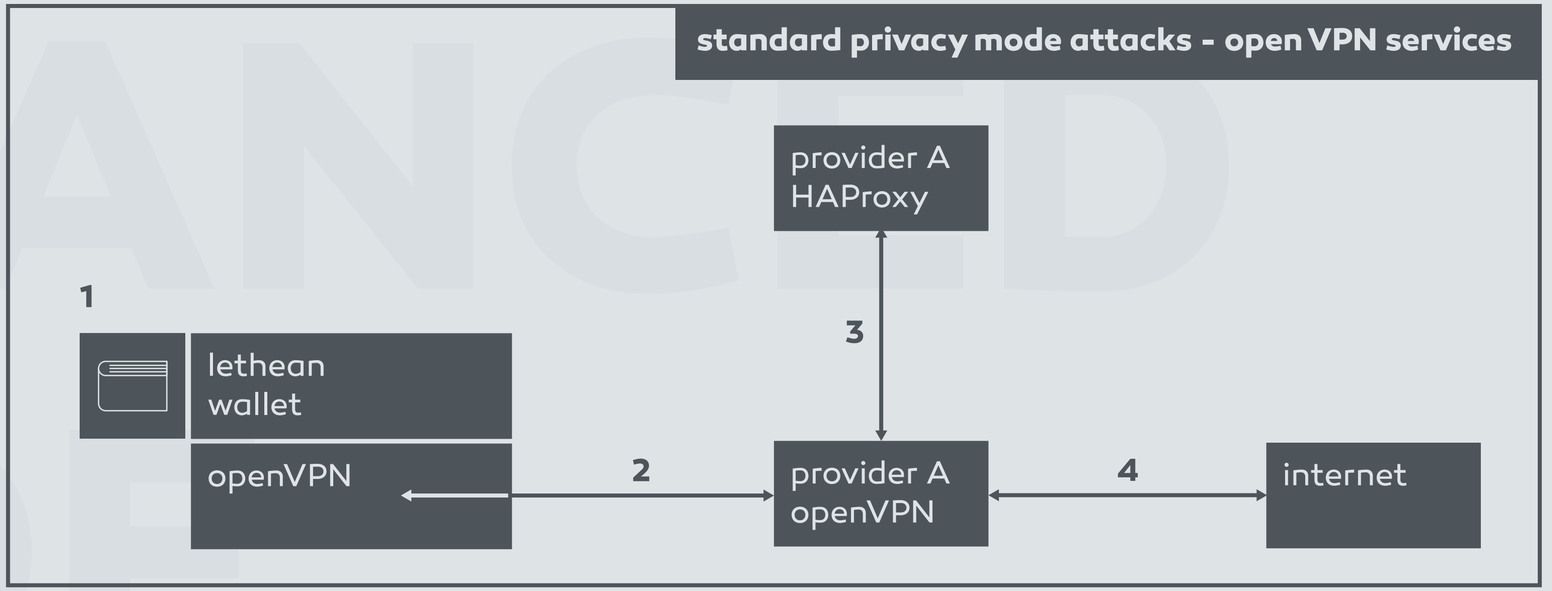
1
Lethean wallet changes local routing table by establishing OpenVPN connection to a remote OpenVPN server.

2
All Internet traffic, including DNS queries, is tunneled through the OpenVPN tunnel. Low risk for security and privacy; high risk of traffic blocking as OpenVPN connection uses UDP protocol and can be easily identified.

3
OpenVPN server uses Provider HAProxy for authentication and authorization.

4
Traffic emerges on the Internet as leaving the OpenVPN server of the provider - high risk of monitoring by ISP and VPN Provider.

Our aim is to add as much privacy protection to the system as technically feasible without hindering usability.



Technical solution

To improve the standard privacy mode, we plan to build a versatile solution where users are in complete charge of how they connect to the Internet. The basic principle is: Full user control of which Provider(s) a type of traffic is tunneled through.

As the combinations are limitless the following diagram shows a typical setup that a user could choose:

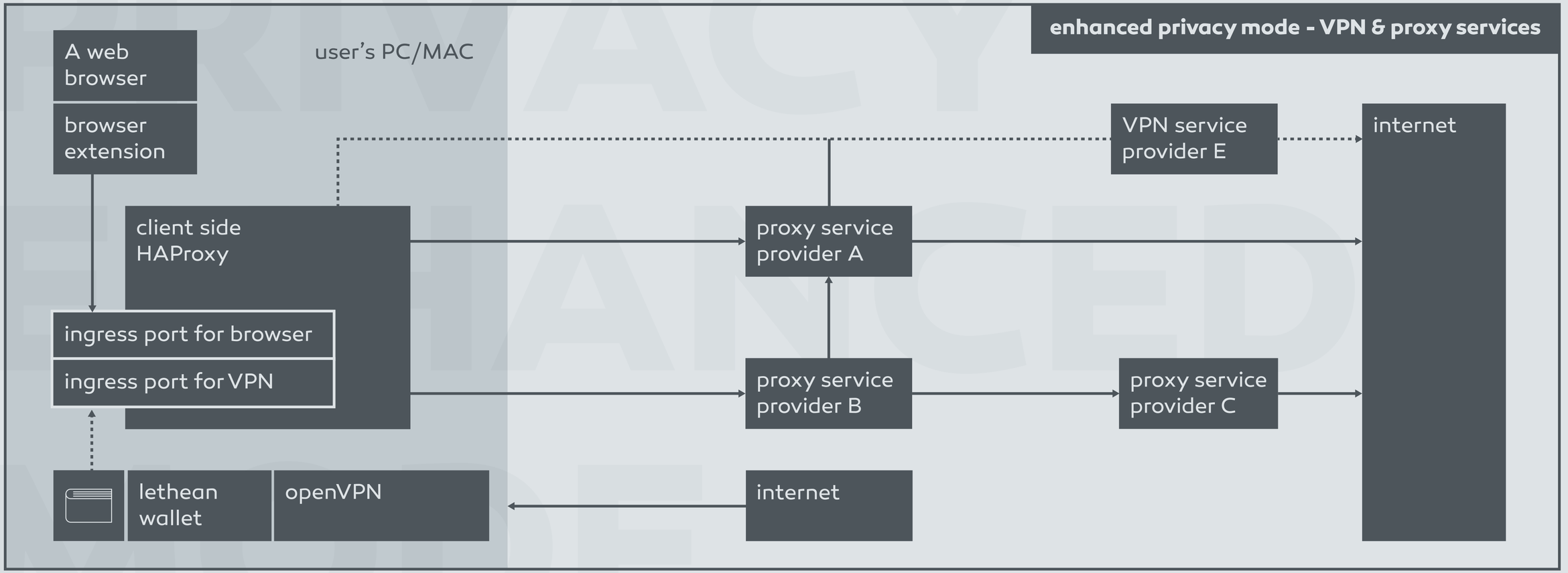
- The user pays four providers; three Proxy services and one OpenVPN privacy mode, and chooses which traffic goes to which provider. In our example:
  - Internet traffic from a browser is tunneled through Provider A (blue line)
    - Unless it is destined to Facebook and Twitter in which case it jumps to Provider B (yellow line)
      - Unless it is a banking connection in which case it jumps to Provider A, then B and then C and finally to the Internet
  - Traffic from user's PC/Mac is routed via OpenVPN provider E, which itself is tunneled in a secure TLS connection via Provider A
    - Unless it is a connection to specified IP range or geography in which case it uses user's own ISP connection
- An encrypted DNS resolver is setup on the local PC/Mac and an at each Provider.

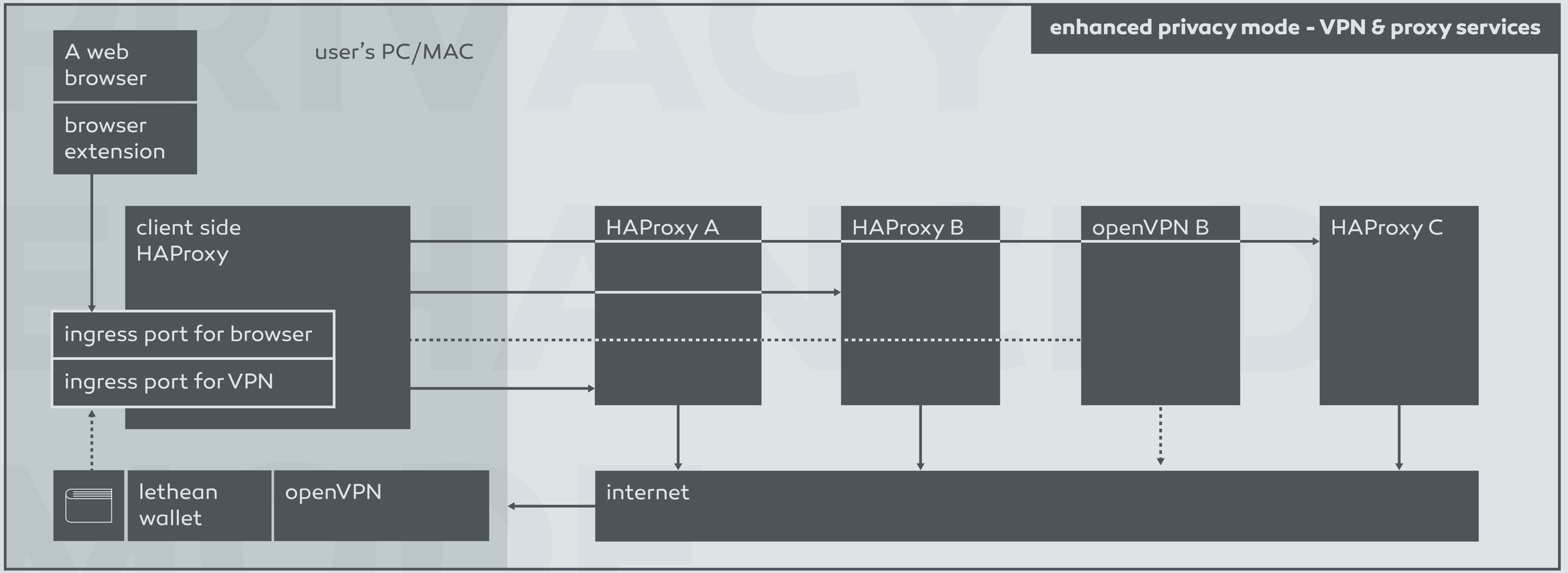
The reason for configuring per-application destinations, such as Facebook and Twitter via Provider B in the above example, is to limit service interruption. Many web services and applications rely upon IP addresses for sessions.

Frequent 'jumping around' of a user's IP-resolved location via changing IP address signals security procedures in some services. If services and applications did not depend on some consistency in client IP address, a fully randomized approach where requests are sent to any provider may be best. Specifying paths for certain applications or domains to specific providers helps limit service interruption related to normal client behavior expectations.

User's local HAproxy creates a configuration that sets up all above.

The following is just an example as the technology allows for limitless combinations, limited only by the user interface and design of the Lethean wallet.


enhanced privacy mode - VPN & proxy services
user's PC/MAC
A web browser
browser extension
client side HAProxy
ingress port for browser
ingress port for VPN
lethean wallet
openVPN
VPN service provider E
proxy service provider A
proxy service provider B
proxy service provider C
internet
internet


enhanced privacy mode - VPN & proxy services
user's PC/MAC
A web browser
browser extension
client side HAProxy
ingress port for browser
ingress port for VPN
HAProxy A
HAProxy B
openVPN B
HAProxy C
lethean wallet
openVPN
internet

The previous picture shows another example.

1
Provider A does not see traffic going to Provider B or C

2
Provider B does not see traffic tunneled to Provider C

3
Provider B provides Proxy and VPN service to the client

4
Client HAproxy orchestrates which provider is used for which traffic

5
As OpenVPN traffic is tunneled inside a TLS connection between Client and Provider B, it cannot be profiled on application and network monitoring control points typically set up by ISPs or governments.

The following picture shows possible geo-distribution of user's (yellow dot) around the globe.

Conclusion

The aim of **Lethean Enhanced Privacy Mode** feature is to give users full control over how their traffic enters the Internet. We want to educate users about issues and compromises of connecting to the Internet, and to what extent our product can protect their security and privacy.

We plan to release the first capability of enhanced privacy mode in late 2018.

Future work

Enhanced private DNS

Problem:

- DNS queries are unencrypted and not signed - can be spoofed and are visible to network monitors
- DNS queries in proxy service are visible to a Proxy Provider and its ISP
- DNS queries in VPN service are depending on user's DNS setting - most likely default thus insecure
- DNSSec is not widely used hence the reliability of DNS responses is low

Example of attacks [link - click to open]

Possible solution:

Secure DNS service project

- A set of DNS resolvers sitting around globe listening on port 443 and accepting DNS over HTTPs queries - operated by our project or perhaps wider community - perhaps Apache or EFF project?
- Certificate pinning is used to secure TLS connection
- When a query comes to such a server or distributes query to a predefined set of X number of other servers and performs query
- Back comes a set of responses - the most frequent response is returned

This is an extension of Google and other projects.

LETHEAN

THANK YOU